D-Link®

Version 1.00 | 08/16/2019

User Manual

Wireless AC1200 4G LTE Multi-WAN Router

DWR-956

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.

Manual Revisions

Revision	Date	Description
1.00	August 16, 2019	• Initial release

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 © 2019 by D-Link Corporation.

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

ErP Power Usage

This device is an Energy Related Product (ErP) that automatically switches to a power-saving Network Standby mode within 1 minute of no packets being transmitted. It can also be turned off through a power switch to save energy when it is not needed.

Network Standby: 3.57 watts

Switched Off: 0.07 watts

Table of Contents

Package Contents

DWR-956 Wireless AC1200 4G LTE Multi-WAN Router

Power Adapter

3G/4G Antennas

RJ-45 Cable

RJ-11 Cable

If any of the above items are missing, please contact your reseller.

System Requirements

- A compatible SIM/UICC card with service.*
- Computer with Windows 10/8/7/Vista/XP, Mac OS 10.3 or above, or Linux-based operating system with a compatible network adapter.
- Java-enabled browser such as Internet Explorer 9, Safari 7, Chrome 28, or Firefox 23 or above (for configuration).

* Subject to services and service terms available from your carrier.

Introduction

D-Link's DWR-956 Wireless AC1200 4G LTE Multi-WAN Router allows you to access mobile broadband networks from anywhere. Once connected, you can check e-mail, surf the web, and stream media. Use your carrier's SIM/UICC card to share your 4G Internet connection through an encrypted wireless network or by using any of the four gigabit Ethernet ports.

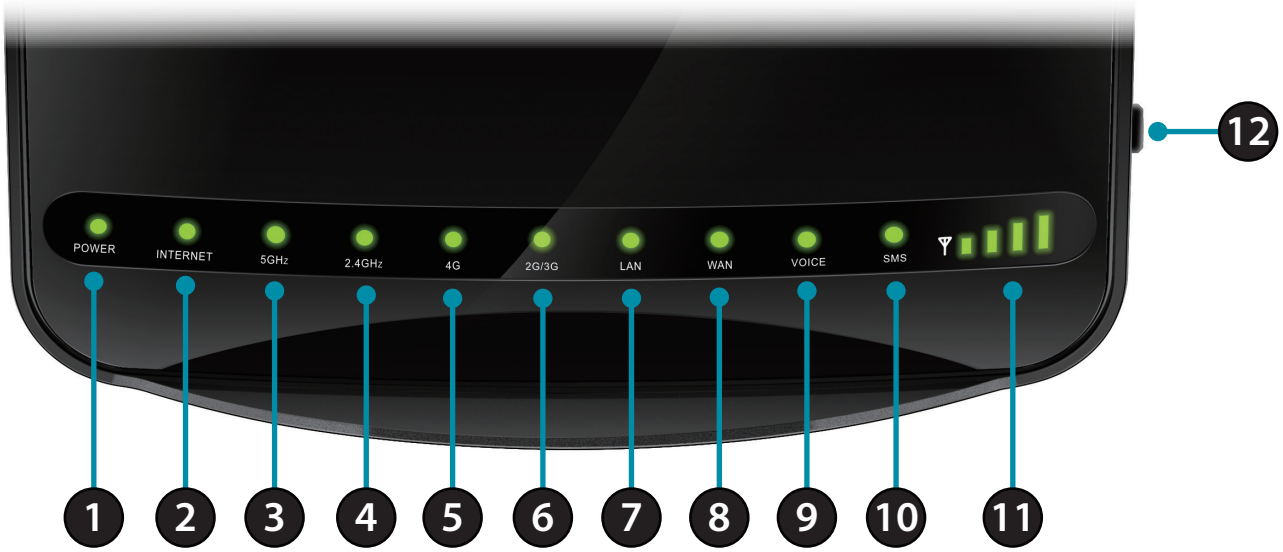
The DWR-956 lets you connect to your 4G mobile connection with fast downlink speeds of up to 150 Mbps and uplink speeds up to 50 Mbps, giving you the speed to ensure fast, responsive Internet access. Surf the web with ease and stream music and video over the Internet to your PCs and mobile devices.

The DWR-956 utilizes dual-active firewalls (SPI and NAT) to help resist potential attacks across the Internet. Industry standard WPA/WPA2 wireless encryption standards help protect your wireless network and traffic from unwanted access while sharing your 4G connection.

The DWR-956 can be installed quickly and easily almost anywhere. It can be configured through almost any web browser without the need for special software. This router makes it possible to stay connected, even when conventional broadband services are unavailable.

Hardware Overview

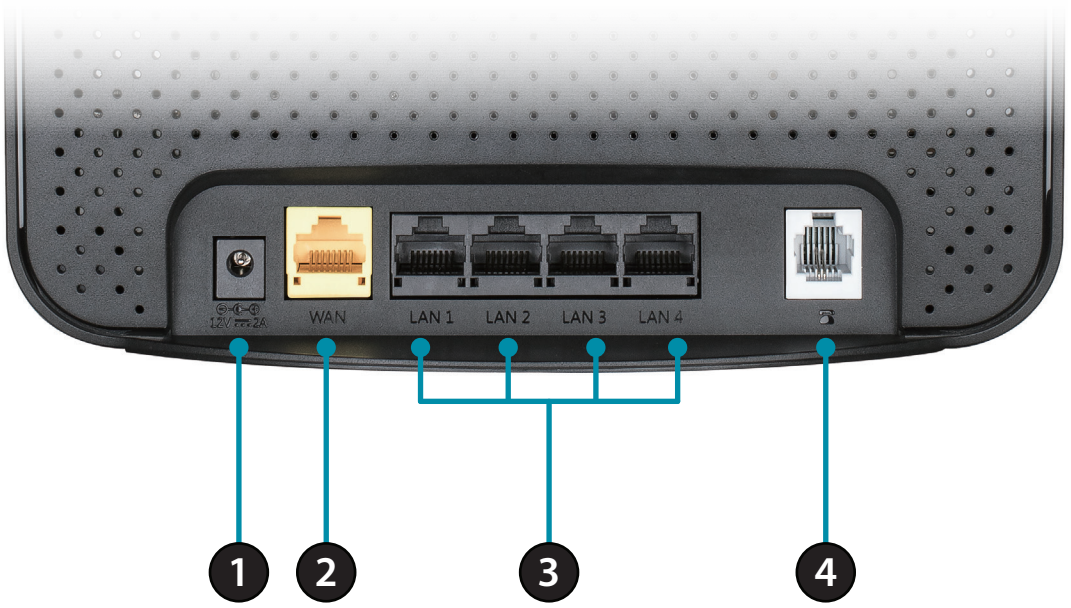
Front View



1	**Power LED**	Will be lit green if the device is powered on and working. Will turn red if there is an error.
2	**Internet**	Will be lit if an Internet connection is established, and will blink when data is being transferred.
3	**5 GHz Wi-Fi/WPS**	Will be lit if the 5 GHz wireless function is enabled, blinks when data is transferred or during WPS pairing.
4	**2.4 GHz Wi-Fi/WPS**	Will be lit if the 2.4 GHz wireless function is enabled, blinks when data is transferred or during WPS pairing.
5	**4G**	Will be lit if a 4G LTE connection is established.
6	**2G/3G**	Will be lit if a 2G or 3G connection is established.
7	**LAN**	Will be lit if an Ethernet LAN connection is established, and will blink when data is being transferred.
8	**WAN**	Will be lit if an Ethernet WAN connection is established, and will blink when data is being transferred.

9	**Voice**	Will be lit green if there is an incoming call or a call is in progress.
10	**SMS**	Will be solid green if the SMS inbox is full, or blinking if there is an unread new SMS message.
11	**Signal Strength LED**	Indicates 4G signal strength with bars. More bars indicates a stronger signal.
12	**Power Button**	Powers the device on or off.

Back View



1	**Power Connector**	Connects to the included power adapter.
2	**Ethernet WAN Port**	For connection to a DSL/cable modem or router.
3	**Ethernet LAN Ports**	For connection to a network-enabled desktop or notebook computer.
4	**Phone Port**	Connect a phone here that uses a regular phone line.

Side View

1	**Reset Button**	Press this button with an unfolded paperclip and hold for ten seconds to reset the device.
2	**WPS Button**	Press this button to initiate a new WPS connection. See **WPS Button** on page **119** for details.
3	**WLAN**	Press this button to toggle wireless LAN on or off.
4	**SIM Card Slot**	Accepts a standard mini-SIM/UICC card for 4G LTE connectivity.
5	**Power Button**	Turns the device on or off.

Installation

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

Before You Begin

Ensure that your DWR-956 Wireless AC1200 4G LTE Multi-WAN Router is disconnected and powered off before performing the steps below..

1. Verify that your SIM/UICC card is installed and has been activated by your carrier.

Caution: Always unplug/power down the router before installing or removing the SIM/UICC card. Never insert or remove the SIM/UICC card while the router is in use.

2. Attach the included antennas to the back of the router, screwing them in clockwise. Arrange them so that they point upward.

3. Connect the power adapter to the socket on the back panel of your DWR-956. Plug the other end of the power adapter into a wall outlet or power strip. Make sure the power button is in the "On" position.
   a. The Power LED will light up to indicate that power is being supplied to the router and the router is turned on.
   b. The LEDs on the front panel will flash on and off as the DWR-956 Mobile Router performs initialization and Internet connection processes.
   c. After a few moments, if a connection has been established, the following LEDs will turn solid green: Power, Network, Wi-Fi (if enabled), LAN (if connected), WAN (if connected), and Signal Strength.

Note: By default, the DWR-956 uses the mobile network as the sole Internet connection. If you wish to use your mobile connection as a backup to a wired connection, or you wish to use a wired connection exclusively, you must use the Optional Advanced Setup procedure.

4. Connect to the device via Wi-Fi using the SSID and password printed on the bottom of the router, or through Ethernet via one of the LAN ports on the back of your DWR-956.

Wireless Installation Considerations

The DWR-956 can be accessed using a wireless connection from anywhere within the operating range of your wireless network. Keep in mind that the quantity, thickness, and location of walls, ceilings, or other objects that the wireless signals must pass through may limit the range of the wireless signal. 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. Minimize the number of walls and ceilings between the D-Link router and other network devices. Each wall or ceiling can reduce your adapter's range from 3 to 90 feet (1 to 30 meters).

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.

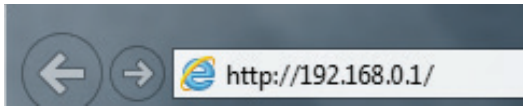
3. Try to position access points, wireless routers, and computers so that the signal passes through open doorways and drywall. Materials such as glass, metal, brick, insulation, concrete, and water can affect wireless performance. Large objects such as fish tanks, mirrors, file cabinets, metal doors,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

4. 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 is 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.

Configuration

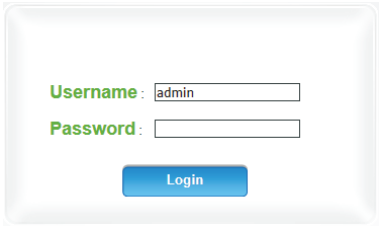
Getting Started

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



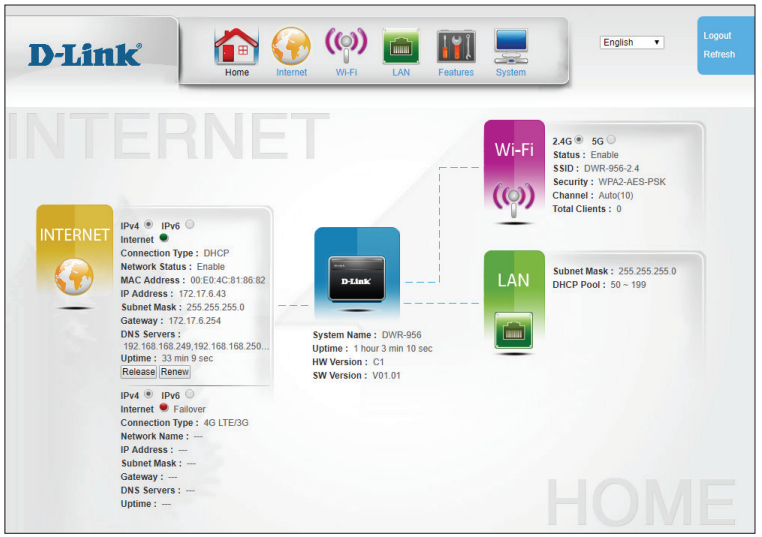
To log in to the configuration utility, **admin** is the default username and the default password is **admin**.

Note: *If you get a* ***Page Cannot be Displayed*** *error, please refer to the* ***Troubleshooting*** *section for assistance.*



Once you have successfully logged in, you will see the **Home** page. On this page you can view information about your Internet connection, the wireless/LAN status, and system information.

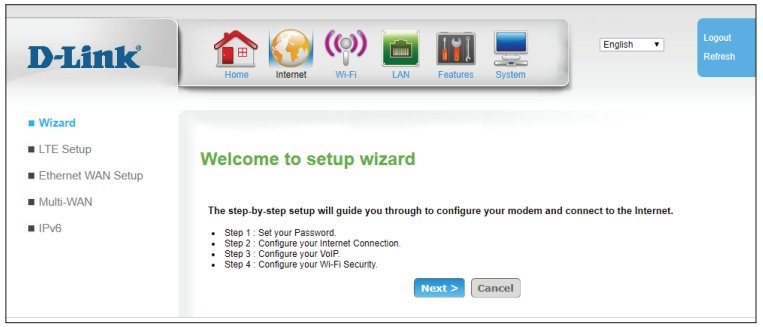
At the top of the page is a menu. Clicking on one of these icons will take you to the appropriate configuration section.



Internet

Wizard

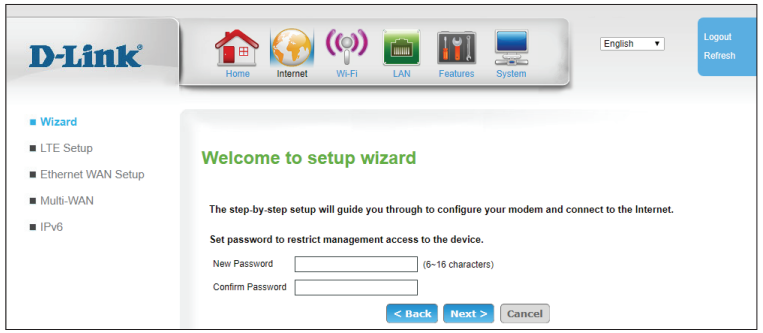
When you access the web configuration utility for the first time, the wizard will automatically start. This wizard will guide you through a step-by-step process to configure your router to connect to the Internet over Ethernet.



Click **Next** to continue.

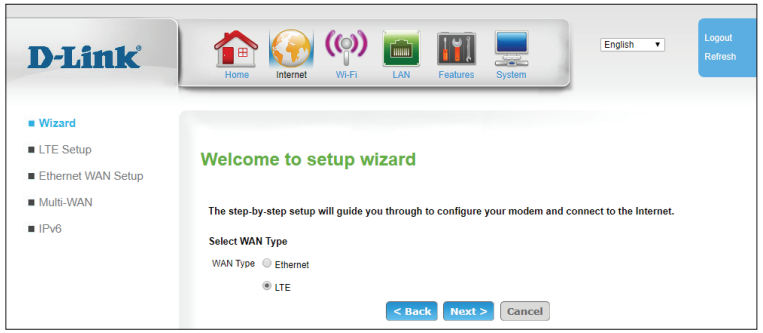
Note: While using the wizard, you can click **Back** to go back to the previous step, or you can click **Cancel** to close the wizard.

In order to secure the router's configuration access, please enter a password. You will be prompted for this password every time you want to use the router's web configuration utility.



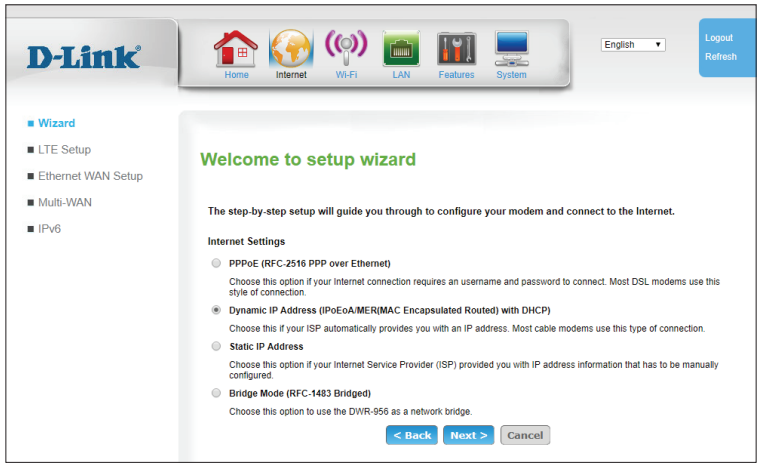
Click **Next** to continue.

Select the Internet connection type you use. The connection types are explained on the following page. If you are unsure which connection type you should use, contact your Internet Service Provider (ISP).



Click **Next** to continue.

The subsequent configuration pages will differ depending on the selection you make on this page.



Internet Settings

PPPoE (RFC-2516 PPP over Ethernet): Choose this option if your Internet connection requires a username and password to connect. Most DSL modems use this style of connection. See **PPPoE (Username / Password)** on page **19** for information about how to configure this type of connection.

Dynamic IP Address (IPoEoA/ MER(MAC Encapsulated Routed) with DHCP): Choose this if your ISP automatically provides you with an IP address. Most cable modems use this type of connection. See **Dynamic IP (DHCP)** on page **22** for information about how to configure this type of connection.

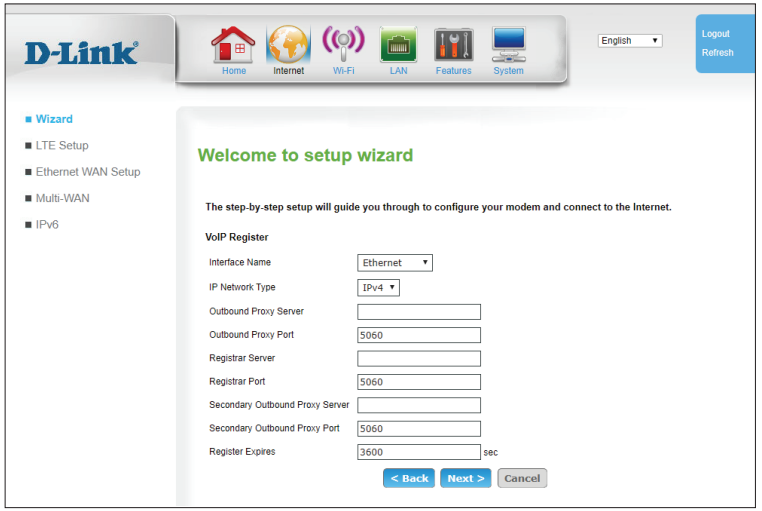
Static IP Address: Choose this option if your Internet Service Provider (ISP) provided you with IP address information that has to be manually configured. See **Static IP** on page **23** for information about how to configure this type of connection.

Bridge Mode (RFC-1483 Bridged): Choose this option to use the DWR-956 as a network bridge. For details see **Bridge Mode (RFC-1483 Bridged)** on page **24**.

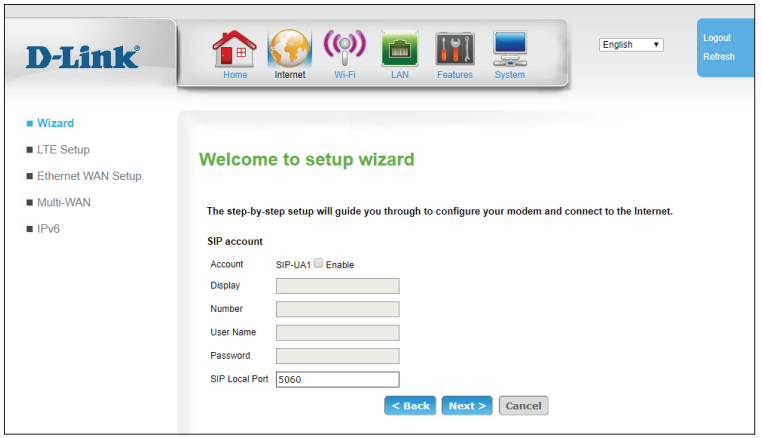
After entering the requested information, click **Next** to continue.

Note: If you are not sure what connection type to use or what settings to enter, check with your Internet Service Provider (ISP).

Enter the information of the primary VoIP registration servers in these sections. This information should be provided by your VoIP provider. Click **Next** to continue.

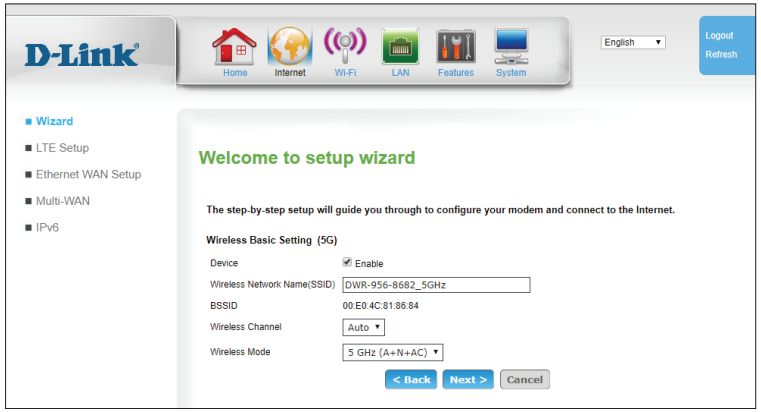


SIP is a VoIP protocol, a networking language which allows your VoIP devices and servers to communicate with one another. Enter your SIP account information here. Click **Next** to continue.

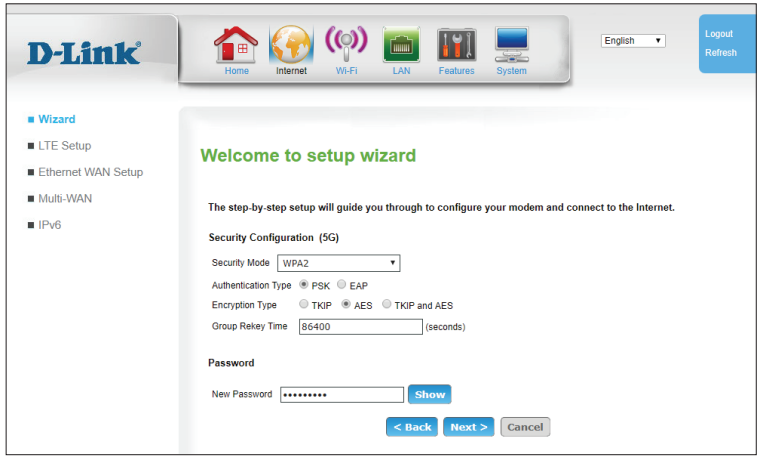


Once your network connection has been configured, you will be directed to configure your wireless connection.

Enter a Wireless Network Name (SSID) for your 5G connection, then click **Next** to continue.

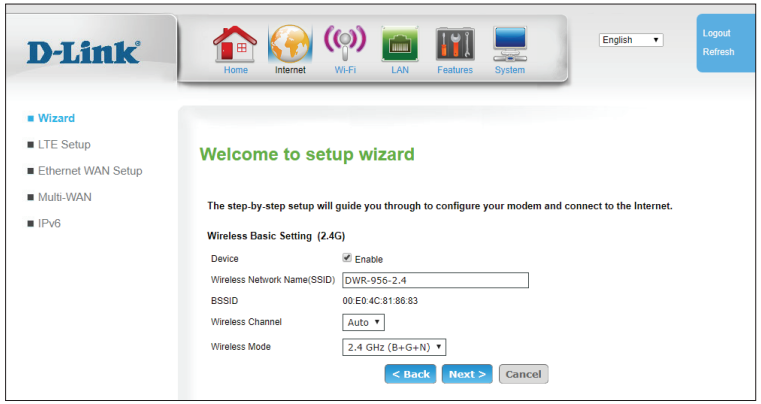


Choose the best security level supported by your wireless client. Enter a security password. Clients must enter this password to connect to your wireless network. Click **Next** to continue.

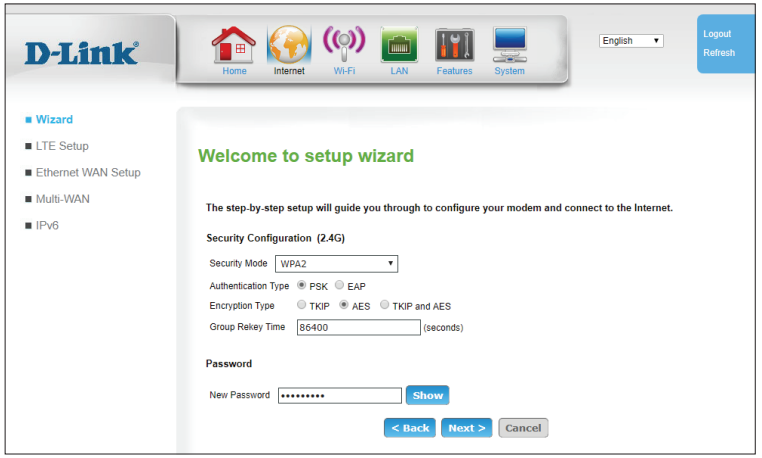


Once your network connection has been configured, you will be directed to configure your wireless connection.

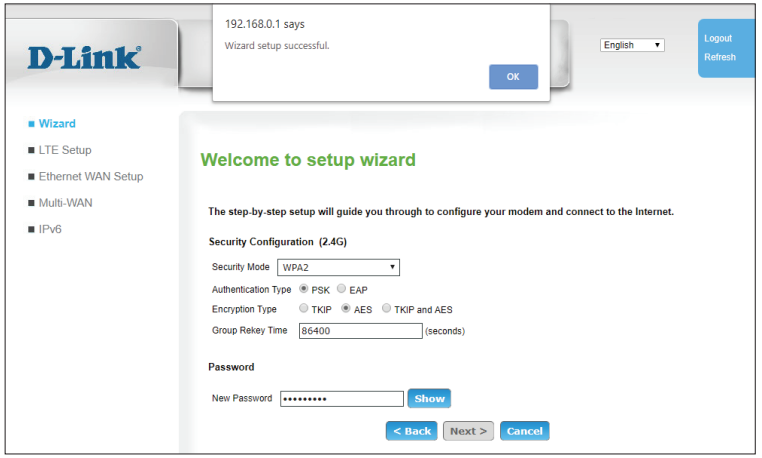
Enter a Wireless Network Name (SSID) for your 2.4G connection, then click **Next** to continue.



Choose the best security level supported by your wireless client. Enter a security password. Clients must enter this password to connect to your wireless network. Click **Next** to continue.

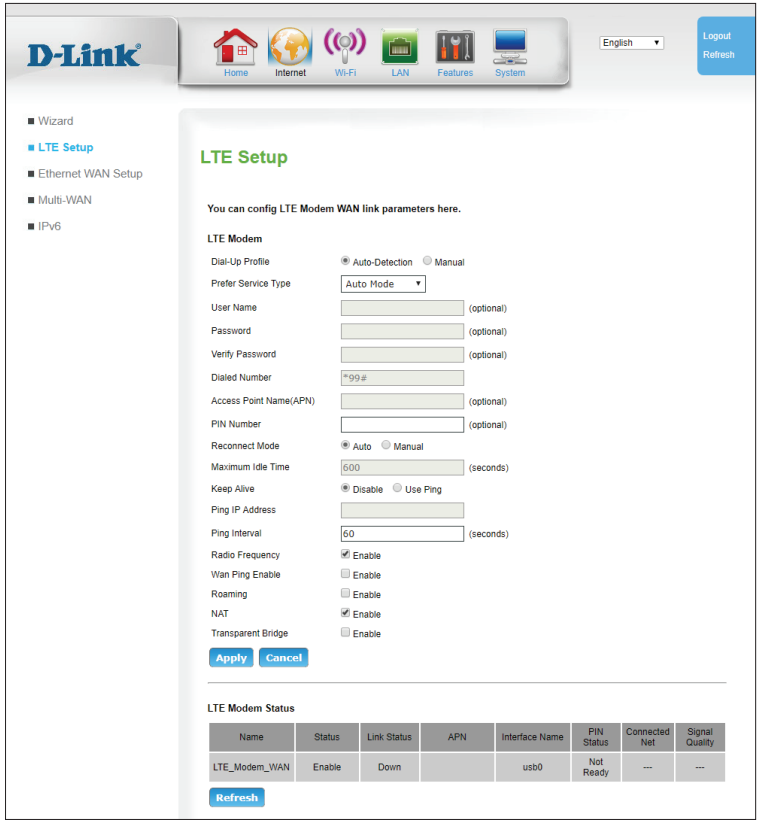


Click **OK** to complete the setup wizard for the device.



LTE Setup

This page allows you to configure your 3G/4G LTE Internet connection. Note that by default, the router uses this connection as the primary Internet connection.



LTE Modem

Dial-Up Profile: Select **Auto-Detection** to have the router automatically detect the settings for your connection. Select **Manual** to enter the details of your connection manually.

Prefer Service Type: Choose whether the DWR-956 should only use 4G networks, 3G networks, 2G networks, or use **Auto Mode** to automatically select a network.

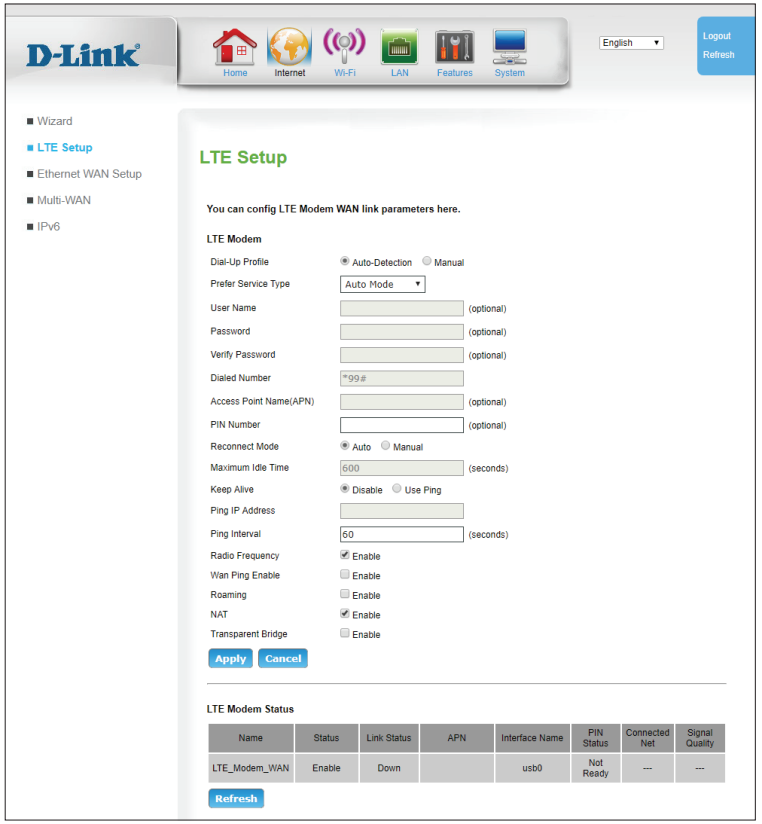
User Name (Optional): Fill in only if requested by ISP.

Password (Optional): Fill in only if requested by ISP.

Verify Password (Optional): Re-type your password in this field.

Dialed number: Some ISPs require a special access number to be dialed for Internet access. The default value for most GSM-based networks is *99#.

Access point Name (APN) (Optional): Enter the access point name provided by your carrier.



PIN Number (Optional): If your SIM/USIM card is protected with a PIN number, enter it here. Note that repeatedly entering the wrong PIN may cause the SIM card to become locked.

Reconnect Mode: Select **Auto** or **Manual** to determine whether the router should reconnect to your 3G/4G network automatically or manually.

Maximum Idle Time: Set the maximum time your connection can be idle before disconnecting. Set it to 0 or choose **Auto** in Reconnect Mode to disable this feature.

Keep Alive: Select **Use Ping** to have the router periodically ping an IP address in an attempt to maintain a connection. Some ISPs will close your connection if no activity is detected.

Ping IP Address: If **Keep Alive** has been set to **Use Ping**, enter an IP address to be pinged.

Ping Interval: If **Keep Alive** has been set to **Use Ping**, specify an interval between the pings in seconds. The default setting is 60 seconds.

Radio Frequency: Check this box to enable cellular radios. If this box is unchecked, the 3G/4G radios will be disabled.

WAN Ping Enable: Check this box to enable response when the router is pinged.

Roaming: Check this box to enable roaming.

NAT: Check this box to enable network address translation.

Transparent Bridge: Check this box to enable transparent bridging.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

LTE Modem Status

Name: Indicates the name of the LTE modem.

Status: Indicates whether the modem is **Enabled** or **Disabled**.

Link Status: Indicates the LTE link status.

APN: Indicates the APN to which the router is connected.

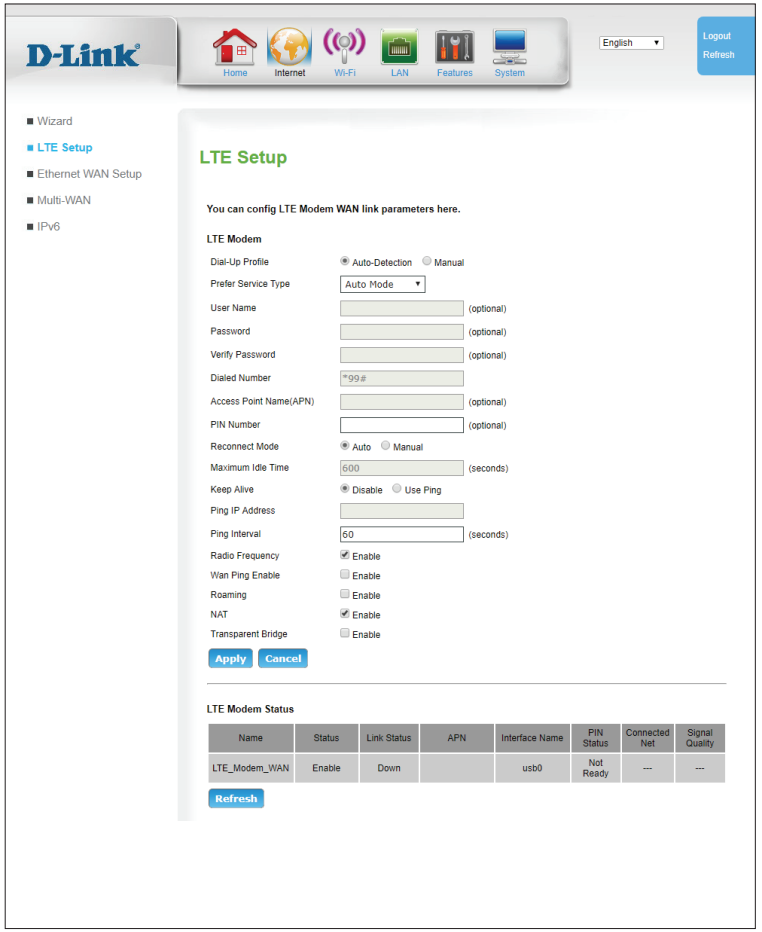
Interface Name: Indicates the physical interface to which the LTE modem is connected. This information is provided for debugging purposes.

PIN Status: Indicates the current status of the PIN security feature.

Connected Net: Indicates the cellular network to which the modem is connected.

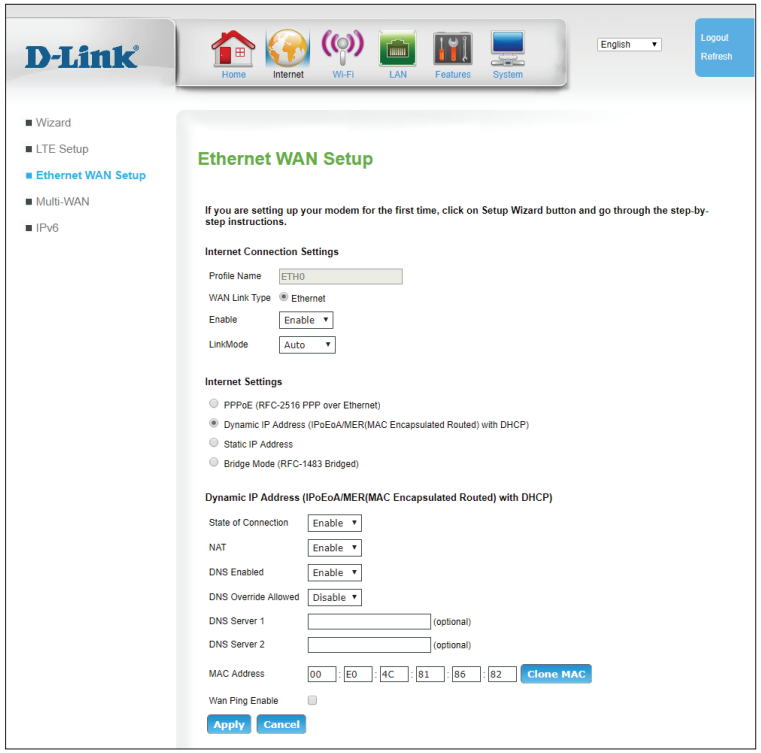
Signal Quality: Indicates the signal quality in dBi. The value is negative. A higher value is a stronger signal. For example -78 is a stronger signal than -90.

Click **Refresh** to update the table.



Ethernet WAN Setup

On this page you can configure your Ethernet WAN connection. This would be used if you have an Internet connection from a DSL, Cable, or other external source. Note that, by default, the 4G connection is used as your primary connection. If you are not sure which settings to use, please contact your Internet Service Provider (ISP).



Internet Connection Settings

Profile Name: Displays the name of the current profile.

WAN Link Type: Indicates the interface used by the WAN connection. As of this writing, only Ethernet is available.

Enable: Enable or Disable the interface.

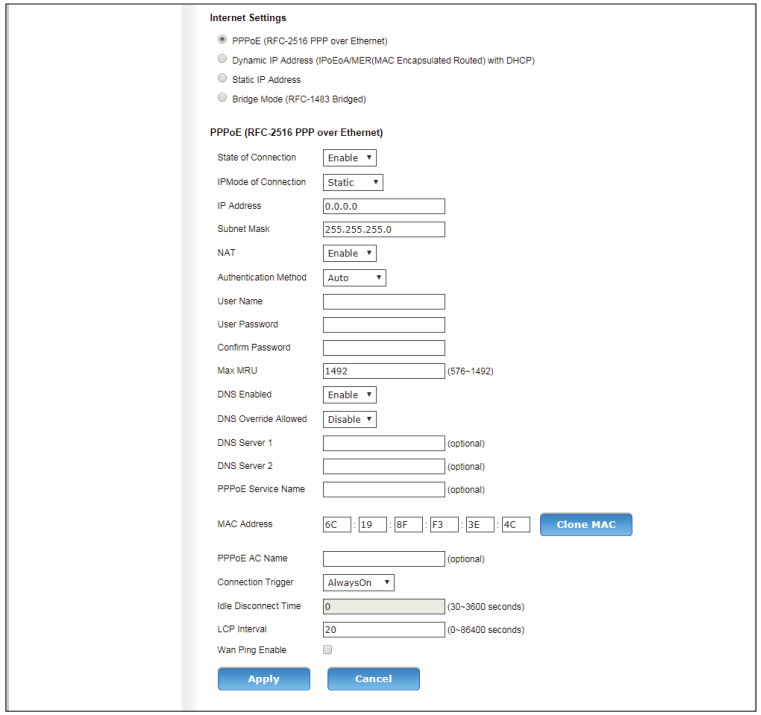
LinkMode: Choose a link speed for the Ethernet interface. The default and recommended setting is **Auto**.

Internet Settings

Select an Internet connection type for your Ethernet WAN. This information should be provided by your ISP.
If you have chosen **PPPoE**, see **PPPoE (Username / Password) on page 19.**
If you have chosen Dynamic IP, see **Dynamic IP (DHCP) on page 22**.
If you have chosen Static IP, see **Static IP on page 23**.
If you have chosen Bridge Mode, see **Bridge Mode (RFC-1483 Bridged) on page 24**.

PPPoE (Username / Password)

PPPoE (RFC-2516 PPP over Ethernet)



State of Connection: Select **Enable** to enable the connection or **Disable** to disable the connection.

IPMode of Connection: Specify a **Static** or **Dynamic** IP address.

IP Address: If you have selected **Static** IP, enter the IP Address provided by your ISP or network administrator.

Subnet Mask: If you have selected **Static** IP, enter the subnet mask provided by your ISP or network administrator.

NAT: Disabling this option will disable the NAT firewall function of the DWR-956, exposing all connected devices directly to the Internet. This is an advanced feature and not recommended for normal use.

Authentication Method: Specify if the connection is authenticated with **PAP** (Password Authentication Protocol), **CHAP** (Challenge-Handshake Authentication Protocol), **MS-CHAP** (Microsoft Challenge Handshake Authentication Protocol), or **Auto**. This setting is determined by your ISP or network administrator.

User Name: The username provided by your ISP for your PPPoE account.

User Password: Password provided by your ISP for your PPPoE account.

Confirm Password: Re-type your password in this field.

Max MRU: You may need to change the Maximum Receive Unit (MRU) for optimal performance. The default value is 1492.

DNS Enabled: Enables DNS lookup.

DNS Override Allowed: Check this box to override the DNS provided by the DHCP lease. Normally, connections using Dynamic IP/DHCP should not need this.

DNS Server 1/2: Fill in if provided by your ISP. If not, keep the default value (optional).

PPPoE Service Name: Fill in if provided by your ISP. (Optional)

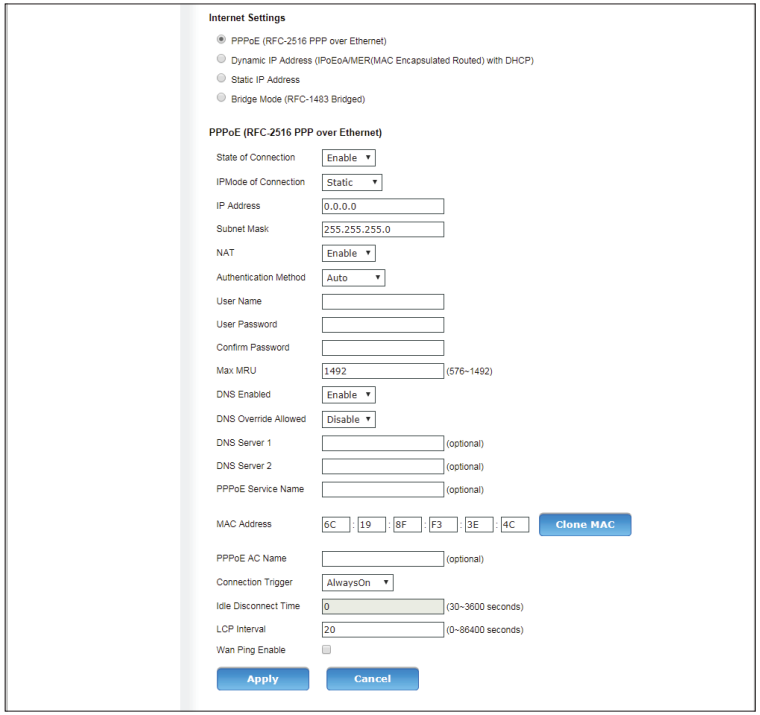
MAC Address: The default MAC address is set to the WAN port's physical interface MAC address on the router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone** button to replace the WAN port's MAC address with the MAC address of your PC.

PPPoE AC Name: If your network uses an Access Concentrator (AC), enter the name here.

Connection Trigger: Specify whether the connection should be **Always On**, **On Demand**, or **Manual**. This determines under what circumstances the connection is dialed.

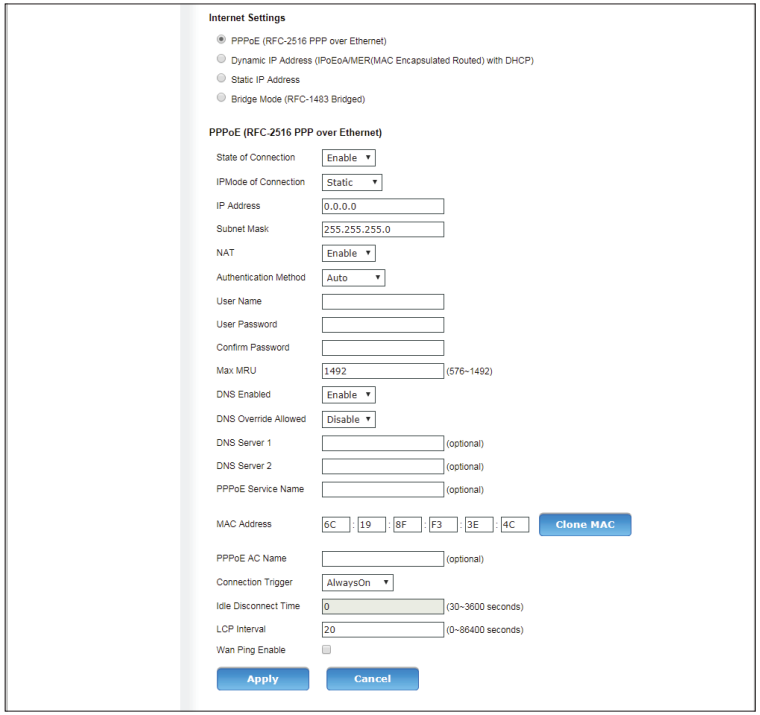
Idle Disconnect Time: The amount of time of inactivity before disconnecting an established PPPoE session. Set it to zero or enable auto-reconnect to disable this feature.

LCP Interval: Specifies the Link Control Protocol (LCP) interval in seconds.



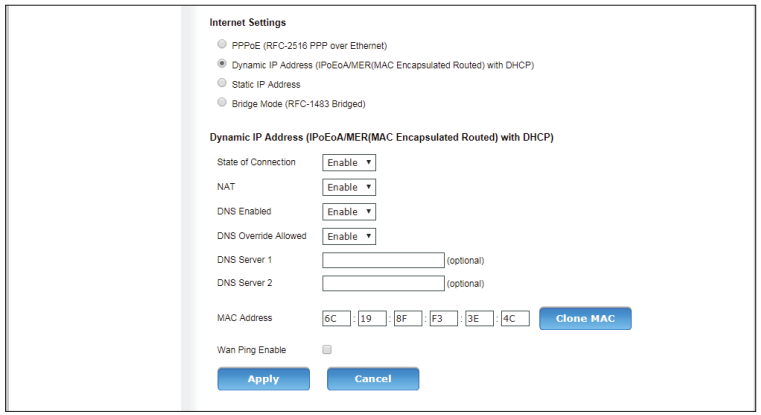
Wan Ping Enable: Check this box to have the router respond to WAN pings. This is not recommended.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.



Dynamic IP (DHCP)

Dynamic IP Address (IPoEoA/MER(MAC Encapsulated Routed) with DHCP)



State of Connection: Select **Enable** to enable the connection or **Disable** to disable the connection.

NAT: Disabling this option will disable the NAT firewall function of the DWR-956, exposing all connected devices directly to the Internet. This is an advanced feature and not recommended for normal use.

DNS Enabled: Enables DNS lookup.

DNS Override Allowed: Check this box override the DNS provided by the DHCP lease. Normally, connections using Dynamic IP/DHCP should not need this.

DNS Server 1/2: Fill in if provided by your ISP. If not, keep the default value (optional).

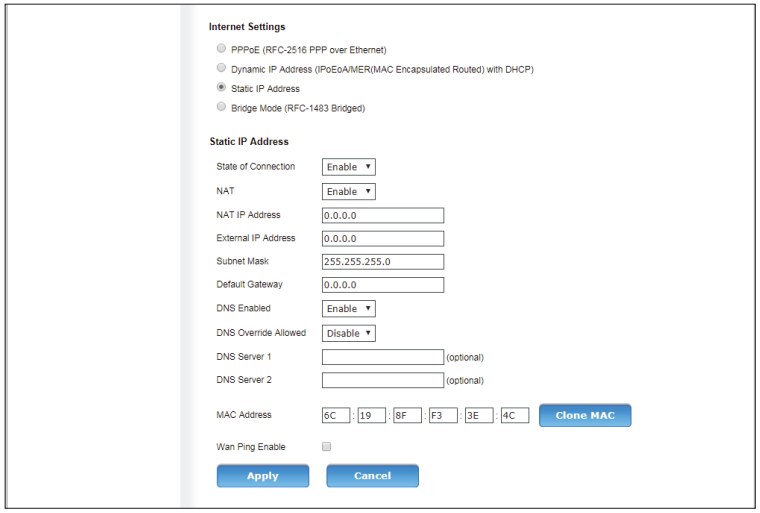
MAC Address: The default MAC address is set to the WAN port's physical interface MAC address on the router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone** button to replace the WAN port's MAC address with the MAC address of your PC.

Wan Ping Enable: Check this box to have the router respond to WAN pings. This is not recommended.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Static IP

Static IP Address



State of Connection: Select **Enable** to enable the connection or **Disable** to disable the connection.

NAT: Disabling this option will disable the NAT firewall function of the DWR-956, exposing all connected devices directly to the Internet. This is an advanced feature and not recommended for normal use.

DNS Enabled: Enables DNS lookup.

DNS Override Allowed: Check this box override the DNS provided by the DHCP lease. Normally, connections using Dynamic IP/DHCP should not need this.

DNS Server 1/2: Fill in if provided by your ISP. If not, keep the default value (optional).

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

Wan Ping Enable: Check this box to have the router respond to WAN pings. This is not recommended.

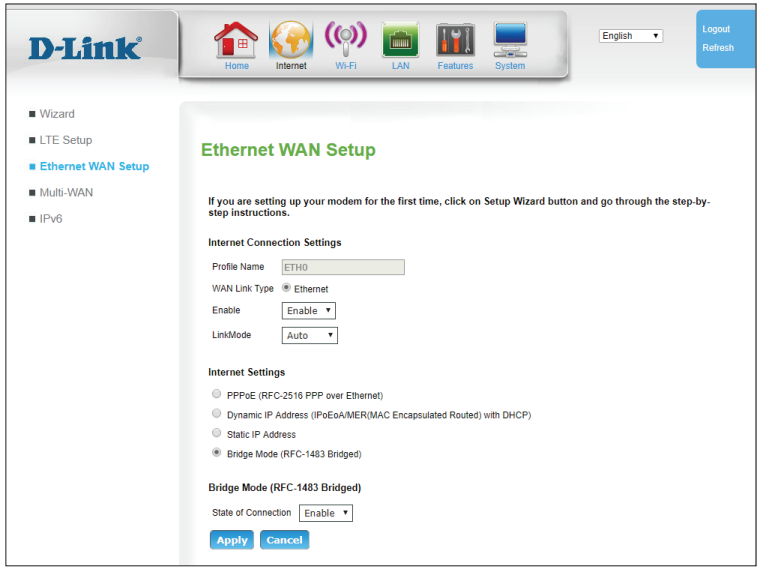
Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Bridge Mode (RFC-1483 Bridged)

Bridge Mode (RFC-1483 Bridged)

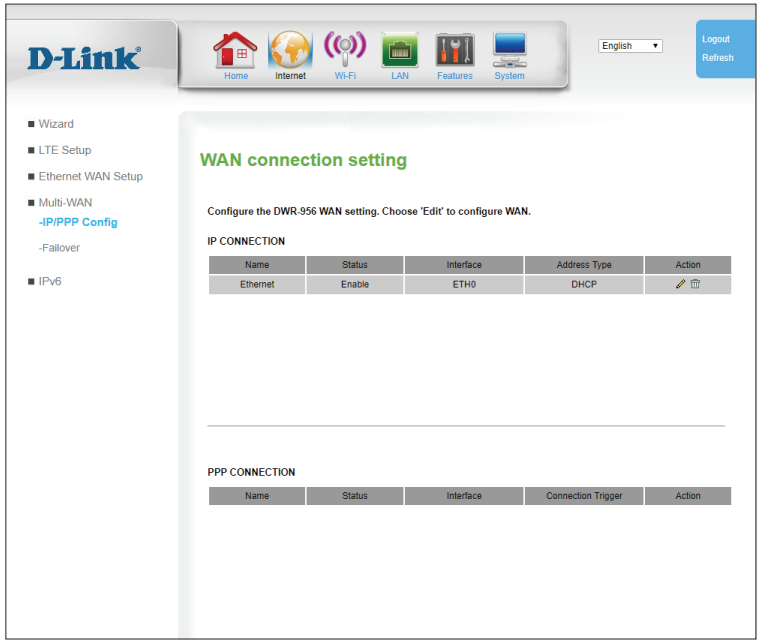
State of Connection: Select **Enable** to enable the connection or **Disable** to disable the connection.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.



Multi-WAN
IP/PPP Config

The DWR-956's multi-WAN feature allows you to set your router to automatically switch to a secondary Internet connection if your primary Internet connection is lost. Note that you must first setup your Ethernet connection before you can configure failover. By default, the primary connection is 3G/4G.



IP Connection

Name: Indicates the name of the connection.

Status: Indicates whether the connection is **Enabled** or **Disabled**.

Interface: Indicates the physical interface of the connection.

Address Type: Indicates how the IP address is assigned (DHCP, Static etc...).

Action: Click the pencil (✎) icon to edit the connection, click the trash can icon (🗑) to delete the connection.

PPP Connection

Name: Indicates the name of the connection.

Status: Indicates whether the connection is **Enabled** or **Disabled**.

Interface: Indicates the physical interface of the connection.

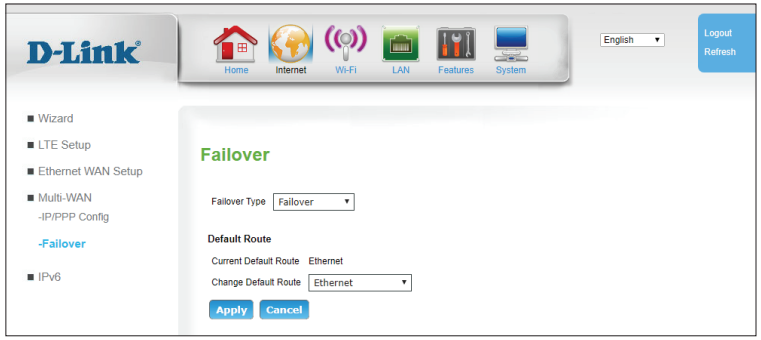
Connection Trigger: Specifies the circumstances when the connection will be established (**Always On**, **Manual**, or **On Demand**).

Action: Click the pencil (✎) icon to edit the connection, click the trash can icon (🗑) to delete the connection. Note that the 3G_Modem_PPP connection cannot be modified or deleted.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Default Route

Default Route



Current Default Route: Displays the current default route.

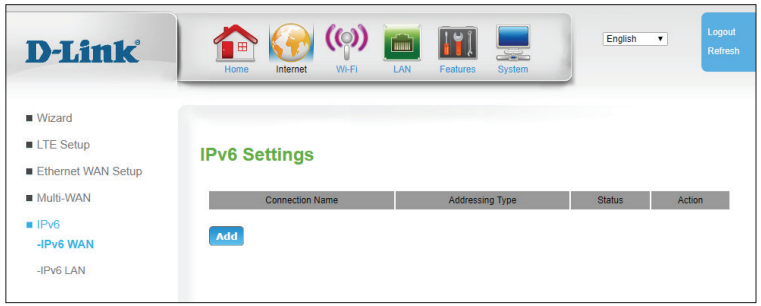
Change Default Route: If you wish to change the default route, select **ETH0_WAN** (if your Ethernet is configured for Static IP, DHCP, or Bridge mode),**ETH0_PPPoE** (if your Ethernet WAN is configured for PPPoE), or **LTE_Modem_PPP** for cellular Internet access.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

IPv6

IPv6 WAN

WAN IPv6 Address Settings



Connection Name: Indicates the name of the interface being used by the IPv6 WAN connection.

Addressing Type: Indicates which addressing type is used by the connection.

Status: Indicates whether the connection is Enabled or Disabled.

Action: Click the pencil (✎) icon to edit the connection, click the trash can icon (🗑) to delete the connection.

Click **Add** to add a new connection, described on the following page.

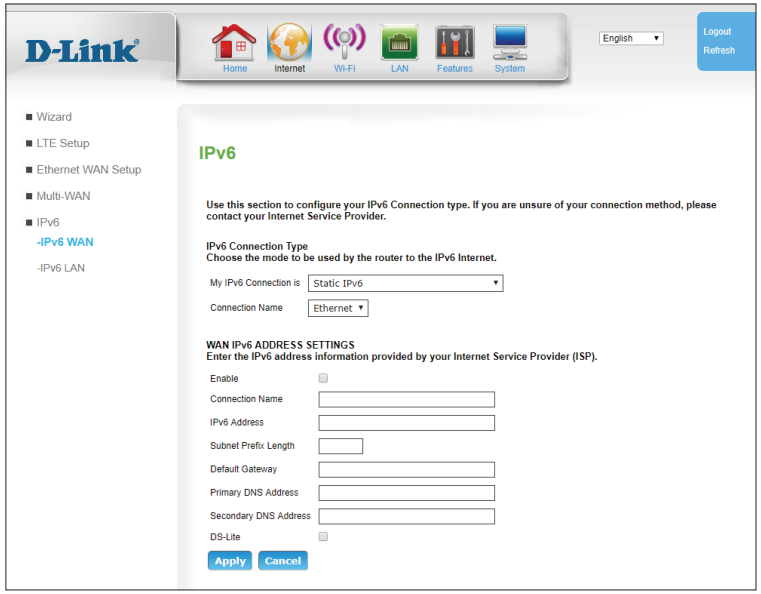
Add IPv6 Connection

IPv6 Connection Type

My IPv6 Connection is: Specify the type of IPv6 connection your ISP uses. Choose from **Static IPv6**, **Autoconfiguration (Stateless/DHCPv6)**, **PPPoE**.

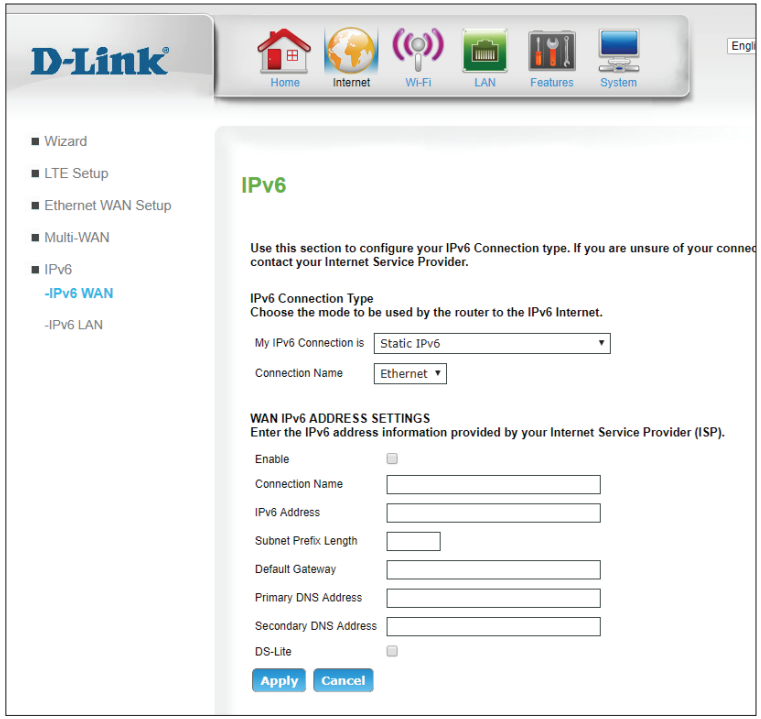
Connection Name: Select a LAN interface from the list to apply the IPv6 connection settings.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.



Static IPv6

WAN IPv6 Address Settings



Enable: Check this box to enable WAN connection over IPv6

Connection Name: Enter a name for this connection

IPv6 Address: Enter the static IPv6 address of the router.

Subnet Prefix Length: Enter the subnet prefix length.

Default Gateway: Enter the LAN (local) IPv6 address for the router.

DNS Addresses: Enter the primary and secondary DNS server addresses.

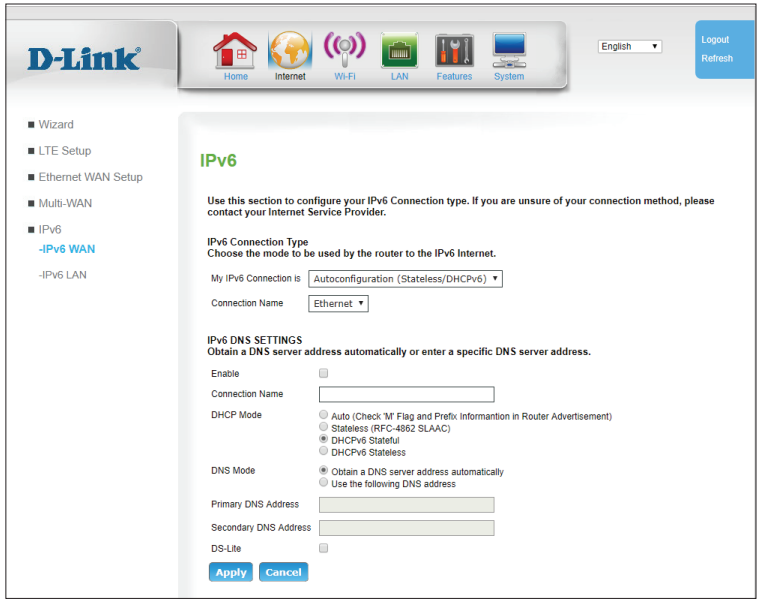
DS-Lite: Dual Stack Lite (DS-Lite) is used by some ISPs to manage IPv4-IPv6 transitions. Check this box if your connection uses DS-Lite.

AFTR IPv6 Address: If **DS-Lite** is enabled, enter the AFTR IPv6 address provided by your ISP.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Autoconfiguration (SLAAC/DHCPv6)

IPv6 DNS settings



Enable: Check this box to enable WAN connection over IPv6

Connection Name: Enter a name for this connection

DHCP Mode: Specify how your IPv6 WAN connection will get an IP address. Choose from **Auto**, **Stateless**, **DHCPv6 Stateful**, or **DHCPv6 Stateless**.

DNS Mode: Specify if DNS address are obtained automatically or enter them manually.

DNS Addresses: If you selected manual DNS, enter the primary and secondary DNS server addresses.

DS-Lite: Dual Stack Lite (DS-Lite) is used by some ISPs to manage IPv4-IPv6 transitions. Check this box if your connection uses DS-Lite.

AFTR IPv6 Address: If **DS-Lite** is enabled, enter the AFTR IPv6 address provided by your ISP.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

IPv6 LAN Setting

LAN IPv6 Gateway Interface Address Setting

WAN interface: If you wish to connect an IPv6 WAN connection to an IPv6 LAN and have already created the IPv6 connection, select it from the list. If you wish to add a new connection, see **IPv6 WAN** on page **27**. If you do not need IPv6 on your LAN connection, select **Disable**. Additional settings are only displayed if an IPv6 WAN connection is selected.

Enable DHCP-PD: Enables IPv6 Prefix Delegation (PD) over DHCPv6. This will disable the LAN Global Address.

LAN Global Address: If DHCP-PD is disabled, specify a global address.

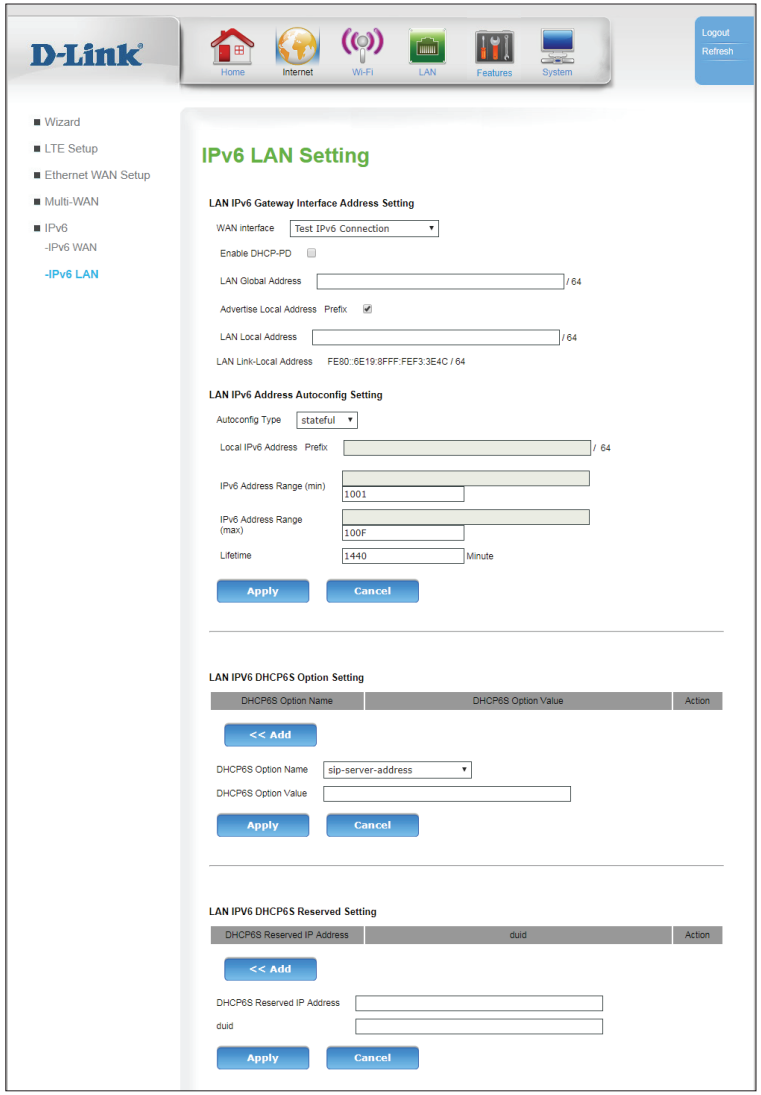
Advertise Local Address Prefix: If you have selected an **Autoconfig Type** below, you can enable local prefix advertising here.

LAN Local Address: If applicable, enter the LAN Local Address here.

LAN Link-Local Address: Displays the link-local address.

LAN IPv6 Gateway Interface Address Setting

Autoconfig Type: Specify **none**, **stateless**, or **stateful**.



Local IPv6 Address Prefix: If **Advertise Local Address Prefix** is checked, the prefix will be displayed here.

IPv6 Address Range (min): If **stateful** has been selected, enter the start of the IPv6 address range here.

IPv6 Address Range (max): If **stateful** has been selected, enter the end of the IPv6 range.

Lifetime: If **stateful** or **stateless** have been selected, specify a lifetime in minutes for IPv6 addresses to expire.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

LAN IPv6 DHCP6 S Option Setting

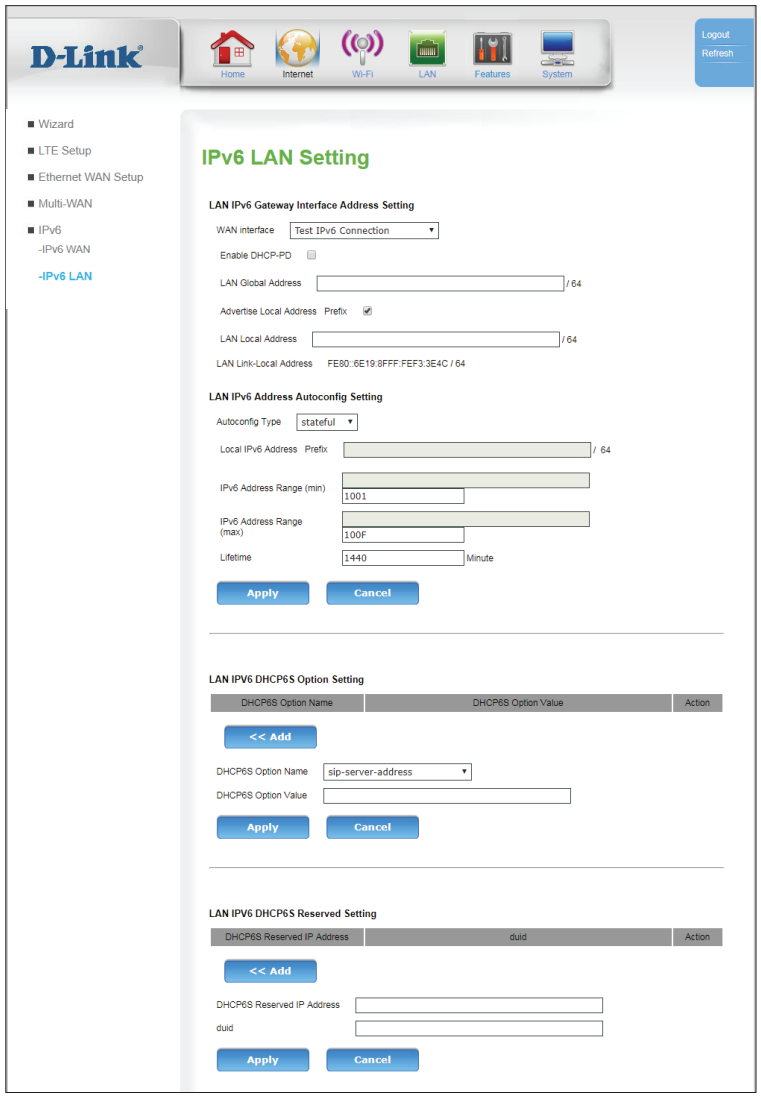
Add: Click **Add** to display the following options

DHCP6S Option Name: Select a DHCP6S option from the list. If you need multiple options, add them separately.

DHCP6S Option Value: Enter the option value.

Action: Click the trash can icon (🗑) to delete options already stored in the table.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.



LAN IPv6 DHCP S Reserved Setting

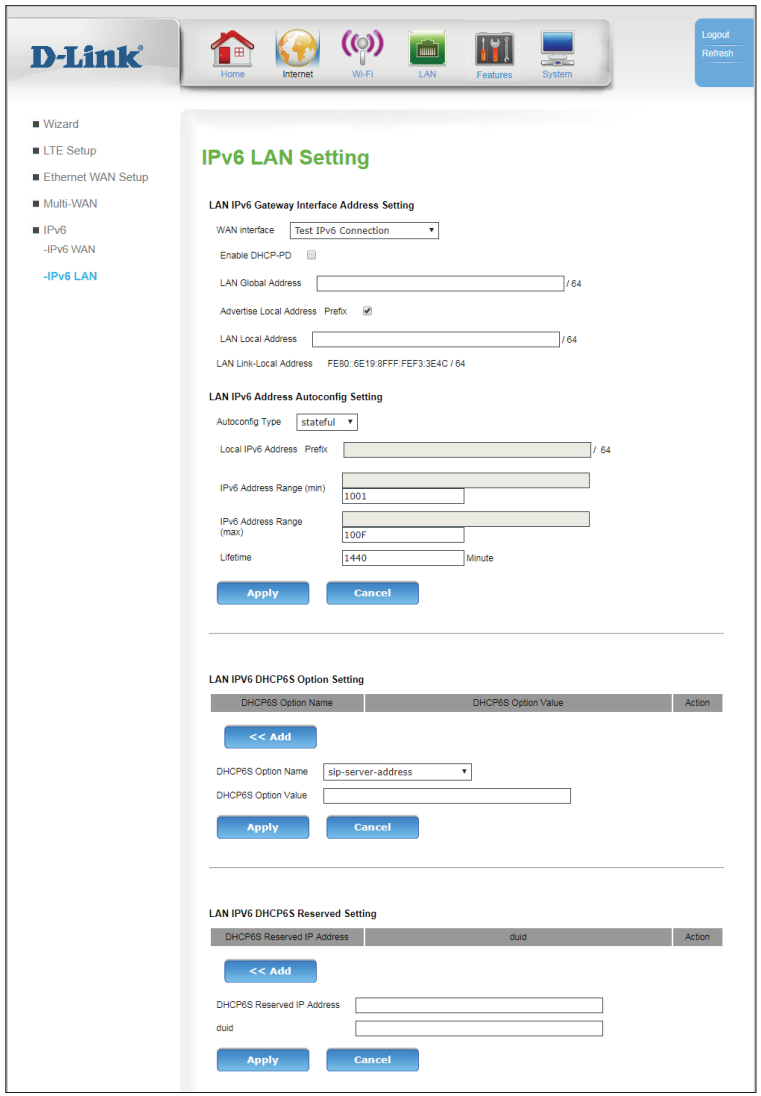
Add: Click **Add** to display the following options

DHCP6S Reserved IP Address: Enter the address to reserve.

duid: Enter the DHCP Unique Identifier (DUID) to which the address will be assigned

Action: Click the trash can icon (🗑) to delete options already stored in the table.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.



Wi-Fi

Wireless 5G/2.4G

This page lets you set up your wireless network and configure security details. The settings for 5 GHz and 2.4 GHz networks are almost identical, but must be configured separately. Note that Wireless AC operates on the 5 GHz band only. Be certain to configure encryption for all enabled networks for maximum protection.

Basic Setting

Enable: Check this box to enable wireless access. When you enable this option, the following parameters take effect.

SSID: The Service Set Identifier is the name of your Wireless Local Area Network (WLAN). Enter a name using up to 32 alphanumeric characters. The SSID is case-sensitive.

BSSID: Displays the MAC address of the above SSID.

Wireless Channel: If Auto Channel Scan is disabled, select the desired channel here.

Wireless Mode: Select the IEEE 802.11 standard used by your wireless clients.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Security Setting

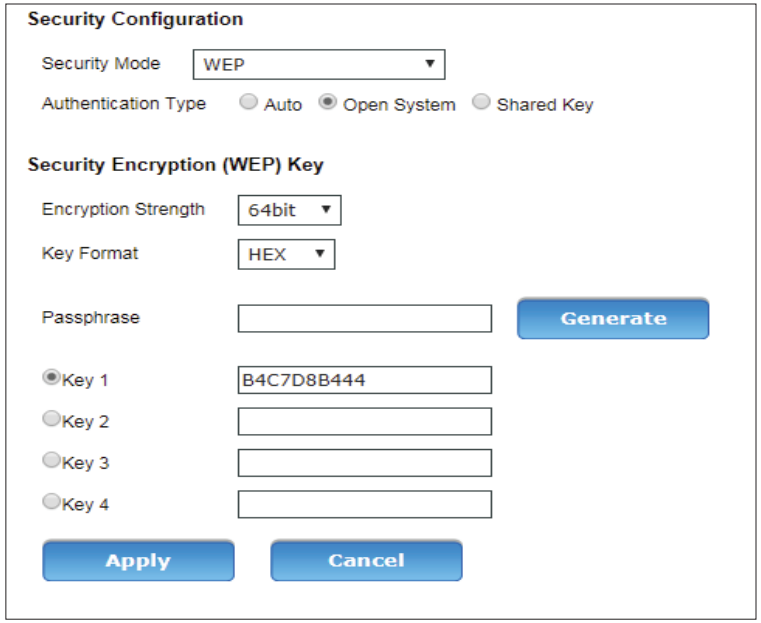
Wireless Network

Name(SSID): If you have multiple SSIDs, select the SSID you wish to apply security settings to.

Security Configuration

Security Mode: Choose **WEP**, **WPA**, **WPA2**, or **WPA/WPA2+TKIP/AES**. This setting will alter the following options. The default and recommended setting for home users is **WPA2.**

If you have selected **WEP**:



Security Configuration

Authentication Type: Choose from **Auto**, **Open System**, or **Shared Key**.

Security Encryption (WEP) Key

Encryption Strength: Set the WEP key/password for your wireless network. Based on whether you are using 64 or 128-bit encryption, and whether you are using a HEX or ASCII key, you will need to enter different numbers of characters for your key, as indicated below the WEP Key text box. ASCII keys may use letters and numbers only, and HEX keys may use numbers 0-9 and letters A-F only.

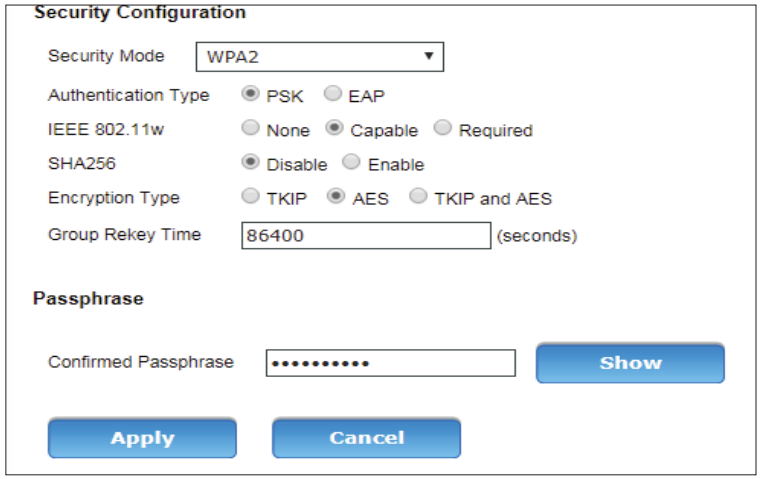
Key Format: Choose **HEX** or **ASCII**.

Passphrase: Enter a passphrase. Click **Generate** to generate a new, random passphrase.

Key 1-4: Select an WEP key index.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

If you have selected **WPA ,WPA2, or WPA/WPA2+TKIP/AES**:



Security Configuration

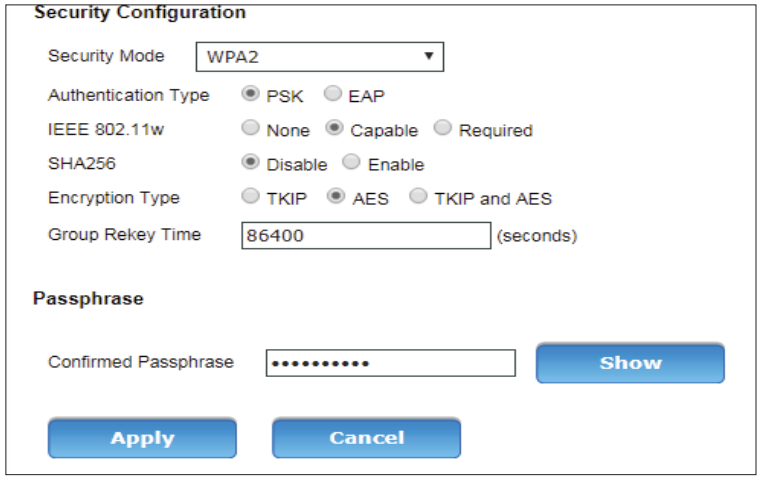
Authentication Type: Choose from **PSK** (Pre-shared key) or **EAP** (Extensible Authentication Protocol).

IEEE 802.11w: Only if you have selected WPA2:
802.11w increases security of management frames. Select **None**, **Capable**, or **Required**.

SHA256: If you have selected **Capable** for IEEE 802.11w, specify if SHA256 will be enabled.

Encryption Type: Select **TKIP**, **AES**, or **TKIP and AES**. Note that for WPA+WPA2, only **TKIP and AES** will be available.

Group Rekey Time: Enter the time in seconds between group key updates.



If you have selected **PSK** under **Authentication Type**:

Passphrase

Confirmed Passphrase: This is the password that will be required to connect to your network. Enter the key/password you want to use for your wireless network. The key must be between 8 and 63 characters long, and may only contain letters and numbers.

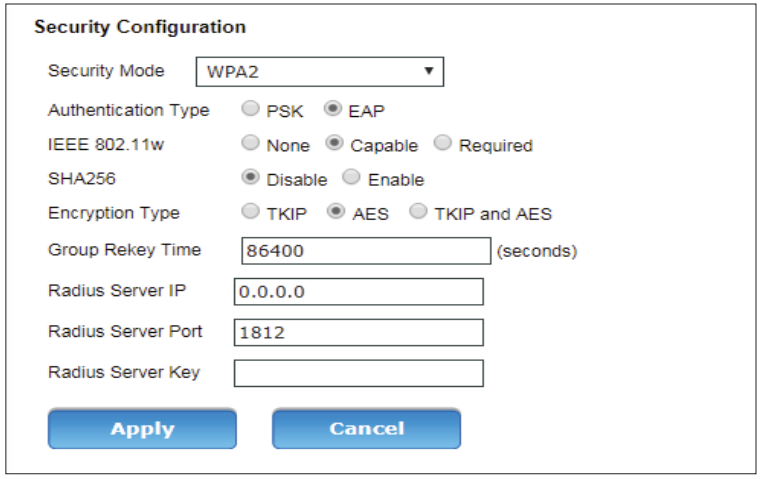
If you have selected **EAP** under **Authentication Type**:

Radius Server IP: 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 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.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.



Advanced Wireless

Wireless router settings:

SSID Advertise: The default setting is **Enable**. Select **Disable** if you do not want to broadcast the SSID of your wireless network.

Transmit Power: Set the transmit power of the Wi-Fi radios.

Fragment Threshold: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

RTS Threshold: This value should remain at its default setting of 2347. If inconsistent data flow is a problem, only a minor modification should be made.

Beacon Interval: Specify a value for the beacon interval. Beacons are packets sent by an access point to synchronize a wireless network. 100 is the default setting and is recommended.

Settings for 11n mode only

Channel Width: Specify a channel width of **20**, **40** , or **80 MHz** (5 GHz only). The wider the channel, the faster the maximum data rate. However, wider channels both cause more interference and are themselves more vulnerable to interference. Therefore, in crowded network environments, smaller channel sizes may be more appropriate. The default and recommended setting is **40 MHz**.

20/40MHz Coexist: Enable this option to reduce interference from other wireless networks in your area. If the channel width is operating at 80 or 40 MHz and there is another wireless network's channel overlapping and causing interference, the router will automatically change to 20 MHz. This option is only available over 2.4 GHz.

Legacy Protection: Enables backward compatibility with legacy protocols. This option is only available over 2.4 GHz.

Control Sideband: Choose the channel selection mode as **Upper** or **Lower**. The default setting is **Upper**.

Aggregation: Check this box to enable frame aggregation. Frame aggregation is a feature of 802.11n and 802.11ac that allows overhead to be reduced by transmitting multiple frames simultaneous under the same header. Disabling this feature will reduce throughput, but may increase compatibility with legacy equipment or allow links in poor network conditions. The default and recommended setting is **Enable.**

Short GI: Check this box to reduce the guard interval to 400 ns. This can increase the throughput rate provided that the delay spread of the connection is also low. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Wireless MAC Filter

The **Wireless MAC (Media Access Controller) Filter** option is used to control wireless 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.

Wireless Network

Name (SSID): Select an SSID to which the rule will apply.

MAC Restrict Mode: Select **Disable** to disable the filter. Clicking **Deny** will deny connectivity to all MAC addresses on the list, creating a black list. Clicking **Allow** will only allow connectivity to MAC addresses on the list, effectively creating a whitelist.

MAC Address: Enter a MAC address to be filtered. MAC addresses must be HEX numbers 0-9 and A-F. To find the MAC address of connected clients, see **Wireless 5G/2.4G Clients** on page **114**. Once you have entered a MAC address, click **<< Add** to add it to the filter.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

MAC Address list

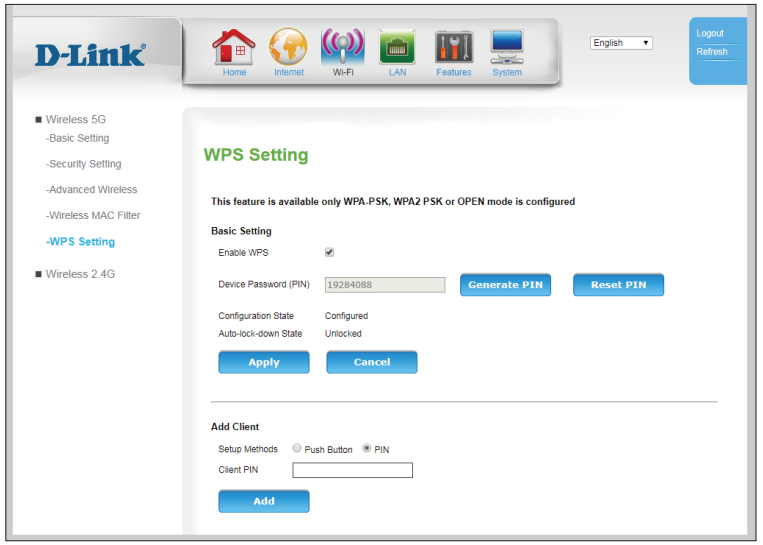
MAC Address: Indicates the MAC address being filtered.

Action: Click the trash can icon (🗑) to delete the rule.

WPS

The Wi-Fi Protected Setup page allows you to create a wireless connection between your router and a device automatically by simply pushing a button or entering a PIN code.

Basic Setting



Enable WPS: Check this box to enable pairing via WPS

Device Password (PIN): If you use Windows 7's **Connect to a network** wizard to do initial configuration of the router, you will have the option to enter the WPS PIN/AP PIN into the wizard when prompted. The factory default WPS PIN/AP PIN is printed on a label located on the bottom of the router. You can click the **Generate New PIN** button to change it to a randomly generated PIN. Note that the PIN is provided for compatibility purposes only, and has minimal functionality for your protection.

Configuration State: If this is set to **CONFIGURED**, the router will be marked as "already configured" to computers that try to use WPS-PIN configuration, such as Windows 7's **Connect to a network** wizard. For your protection, the **CONFIGURED** flag is permanently set in order to close vulnerabilities in the WPS-PIN configuration.

Auto-lock-down State: Auto-lock-down is activated when a device attempts too many unsuccessful PIN-based WPS pairing attempts.

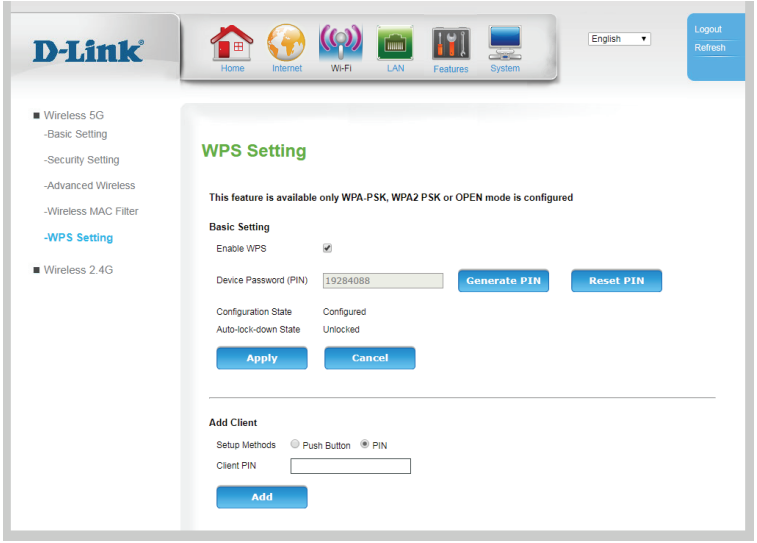
Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Add Client

Setup Methods: Choose **Push Button** or **PIN**.

Client PIN: If the client device has a PIN, you may enter it here.

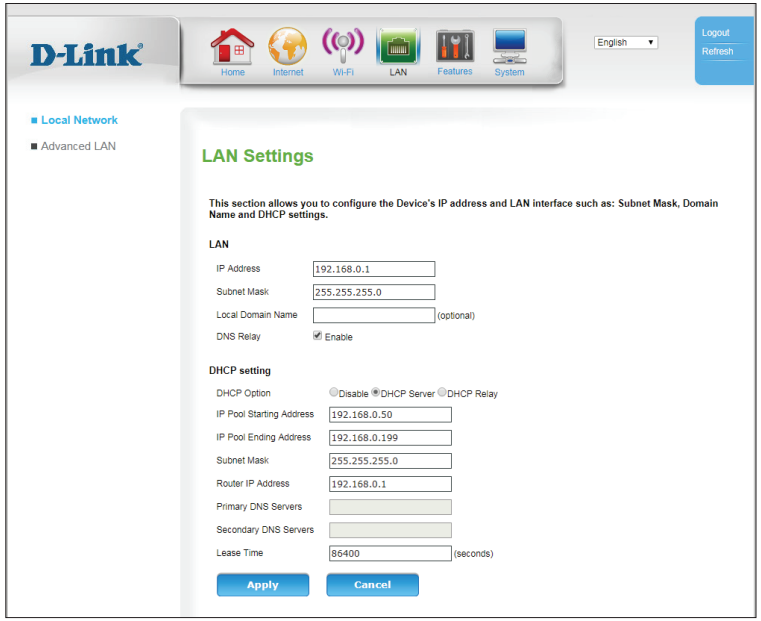
Add: If you have selected **Push Button**, clicking **Add** will trigger the pairing process. If you have selected **PIN**, clicking **Add** will pair using the PIN entered in the **Client Pin** field.



LAN

This section will help you to change the local network settings of your router and to configure the DHCP Server settings.

LAN Settings



LAN

IP Address: Enter the IP address you want to use for the router. The default IP address is **192.168.0.1**. If you change the IP address, you will need to enter the new IP address in your browser to get into the configuration utility.

Subnet Mask: Enter the subnet mask of the router. The default subnet mask is **255.255.255.0**.

Local Domain Name: Enter the local domain name for your network. (Optional)

DNS Relay: Disable to transfer the DNS server information from your ISP to your computers. If enabled, your computers will use the router for a DNS server.

DHCP Setting

DHCP Option: Select **Disable**, **DHCP Server**, or **DHCP Relay**. **DHCP Server is the default and recommended setting, where your router will serve as the DHCP server for your LAN.**

IP Pool Starting Address: Enter first address in the range of IPs the DHCP server will use to assign IP addresses to devices on your network.

IP Pool Ending Address: Enter last address in the range of IPs the DHCP server will use to assign IP addresses to devices on your network.

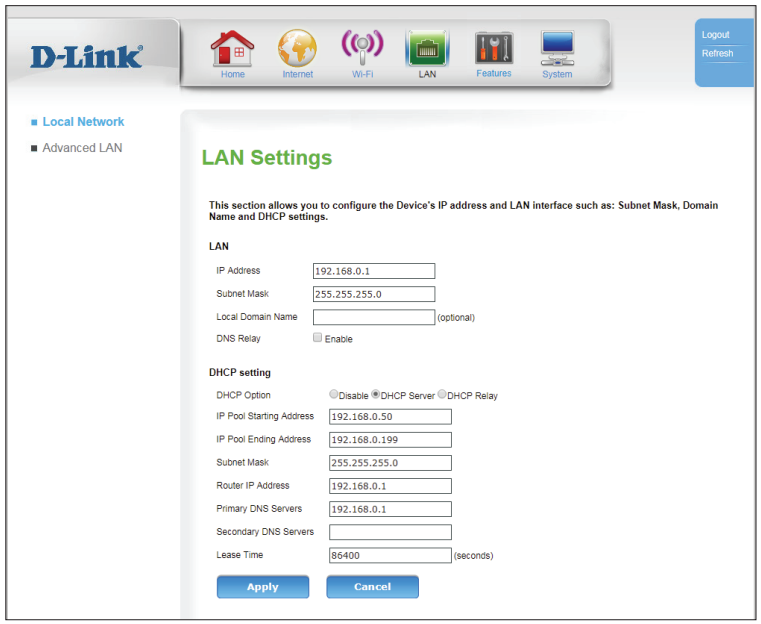
Subnet Mask: Enter the subnet mask for the LAN. The default subnet mask is **255.255.255.0** Using the router's Subnet Mask is recommended for most configurations.

Router IP Address: Enter the default gateway the router's DHCP server should assign to your devices. Using the router's IP address is recommended for most configurations.

Primary DNS Servers: Enter the primary DNS IP address that will be assigned to DHCP clients. Disabled if **DNS Relay** is checked.

Secondary DNS Servers: Enter the secondary DNS IP address that will be assigned to DHCP clients. Disabled if **DNS Relay** is checked.

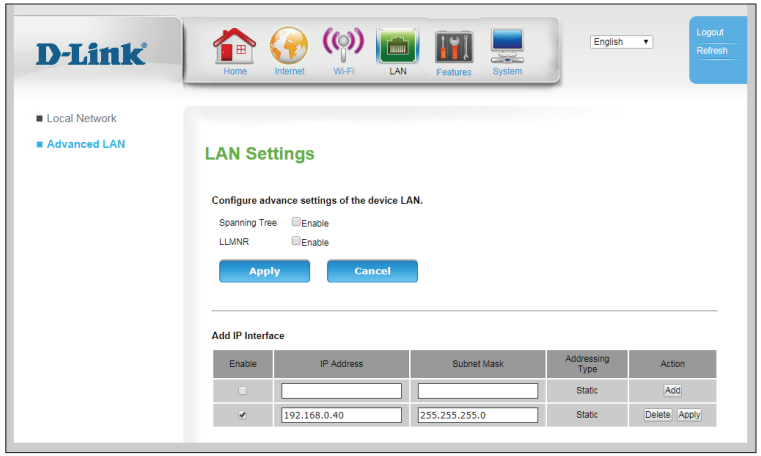
Lease Time: The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.



Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Advanced LAN

Configure advance settings of the device on LAN



Spanning Tree: Check this box to enable spanning tree over Ethernet. This is disabled by default.

LLMNR: Check this box to enable Link-Local Multicast Name Resolution.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Add IP Interface

Enable: Check this box to enable access to the GUI over an alternative static IP address. This is particularly useful for VLANs or bridges.

IP Address: Enter the static IP that will be used to access the GUI management interface.

Subnet Mask: Enter the subnet mask over which this IP address will function.

Addressing Type: Displays the type of address

Action: Click **Delete** to delete an interface, or click **Apply** to apply any changes made in the previous fields.

Features

RIP Settings

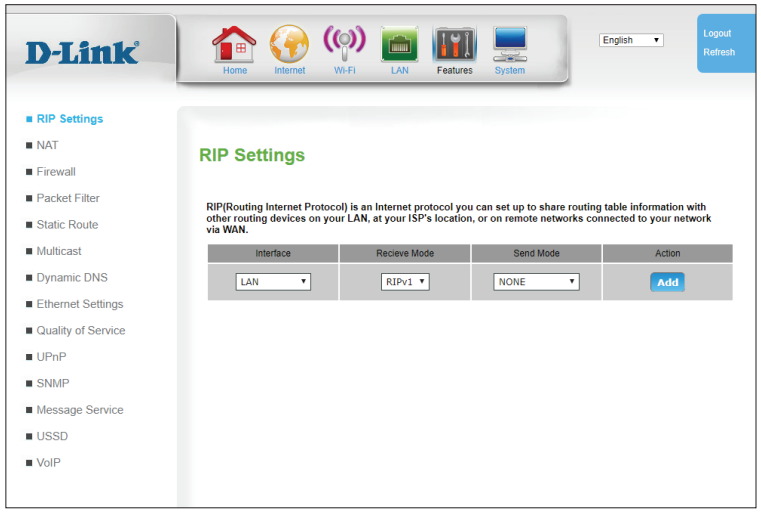
From this page advanced users can configure the router to use the Routing Internet Protocol (RIP). RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via WAN.

Interface: Select the interface to apply the RIP rule to.

Receive Mode: Select the version of RIP protocol to use when receiving RIP updates.

Send Mode: The options are RIP1, RIP2, or Both.

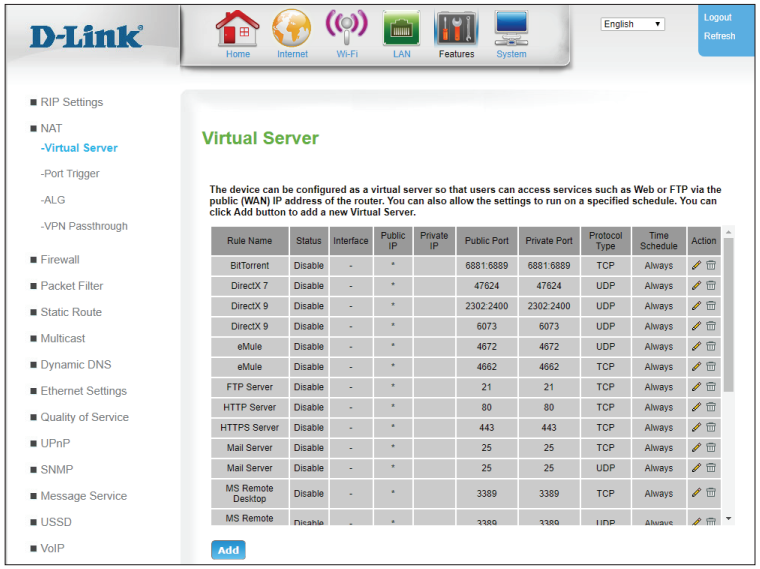
Action: Click **Add** to add your current settings to the table. Click the trash can icon (🗑) to delete rules already stored in the table.



NAT

Virtual Server

The device can be configured as a virtual server so that users can access services such as Web or FTP via the public (WAN) IP address of the router. You can also allow the settings to run on a specified schedule.



Virtual Server

Rule Name: Displays the name of the rule.

Status: Indicates whether the rule is enabled or disabled.

Interface: Show which interface the rule is bound to.

Public IP: Indicates the public IP of a service to which the filter rule will apply.

Private IP: Enter an IP address of the client hosting the server on your LAN.

Public Port: Indicates the public port(s) that will trigger the rule.

Private Port: Indicates the port of the client hosting the server on your LAN.

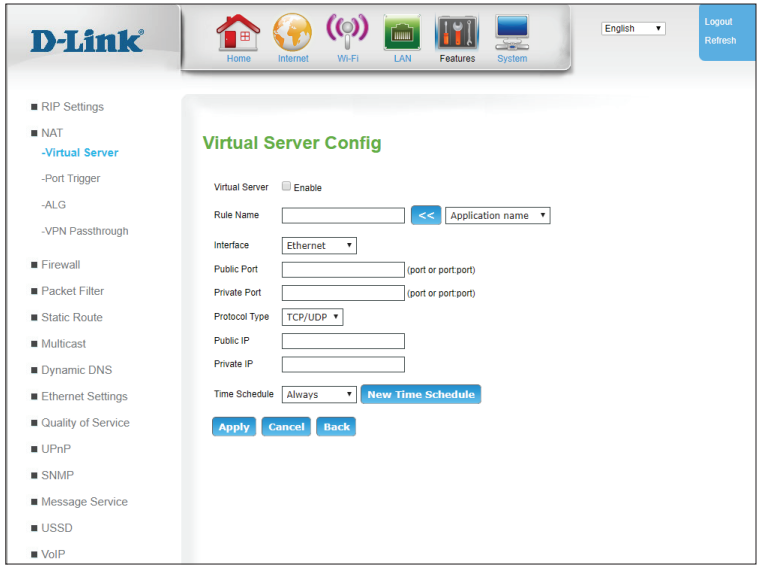
Protocol Type: Indicates the protocol type that triggers the virtual server rule.

Time Schedule: Indicates the time schedule during which the virtual server rule is active.

Action: Click the pencil (✎) icon to edit the filter, click the trash can icon (🗑) to delete the virtual server rule.

Click **Add** to add a new Virtual Server, described on the following page.

Virtual Server Config



Virtual Server: Check this box to enable the virtual server.

Rule Name: Specify the name of the rule for reference. Alternatively, select known service from the box on the right and click << to automatically populate all fields.

Interface: Specify which interface the rule is bound to.

Public Port: Specify the public port(s) that will trigger the rule.

Private Port: Specify the port of the client hosting the server on your LAN.

Protocol Type: Specify the protocol type that triggers the virtual server rule.

Public IP: Specify the public IP of a service to which the filter rule will apply.

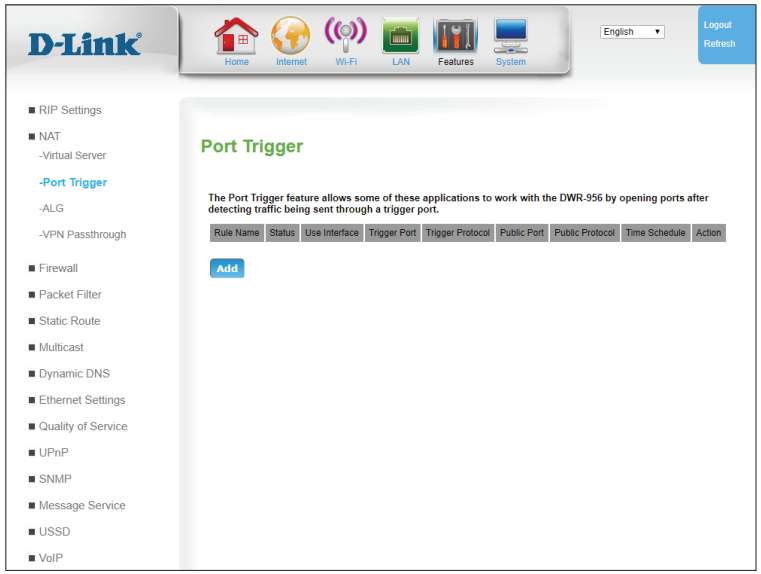
Private IP: Enter an IP address of the client hosting the server on your LAN.

Time Schedule: Select the time schedule during which the virtual server rule is active. To create a new time schedule, click **New Time Schedule.**

Click **Apply** to save your settings, **Cancel** to revert to your previous settings, or **Back** to return to the previous screen.

Port Trigger

Some legacy applications require multiple connections, such as Internet gaming, video conferences, and Internet telephony. These applications may have difficulty working through NAT (Network Address Translation). The **Port Trigger** feature allows some of these applications to work with the DWR-956 by opening ports after detecting traffic being sent through a trigger port.



Rule Name: Indicates the name of the rule for reference.

Status: Indicates the current status of the trigger.

Use Interface: Indicates which interface the rule is bound to.

Trigger Port: Indicates the port(s) on LAN that will trigger the rule.

Trigger Protocol: Indicates the protocol that will trigger the rule.

Public Port: Indicates the public port(s) that the trigger will forward to.

Public Protocol: Indicates the protocol type that triggers the rule.

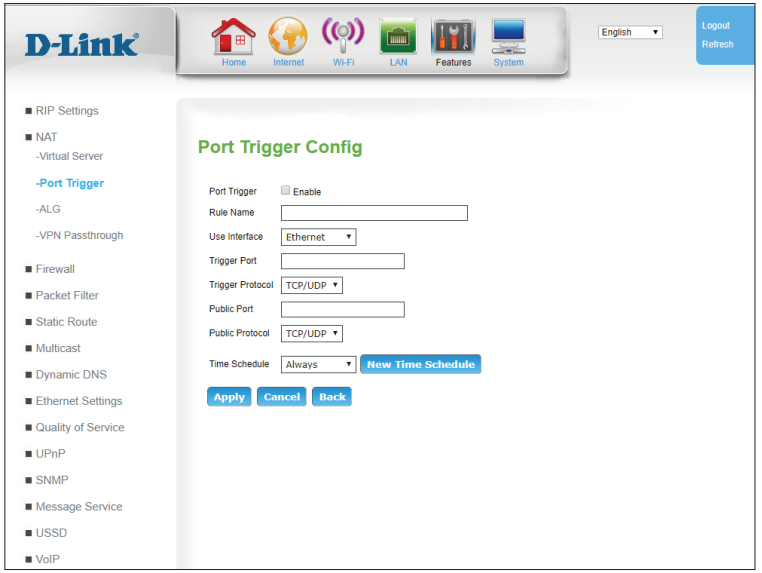
Time Schedule: Select the time schedule during which the port trigger rule is active. To create a new time schedule, click **New Time Schedule.**

Action: Click the pencil (✎) icon to edit the filter, click the trash can icon (🗑) to delete the port trigger.

Click **Add** to add a new port trigger, described on the next page.

Port Trigger Config

Port Trigger Config



Port Trigger Check this box to enable the port trigger.

Rule Name: Specify the name of the rule for reference.

Use Interface: Specify which interface the rule is bound to.

Trigger Port: Specify the internal port that will initiate the port trigger.

Trigger Protocol: Specify the protocol that will initiate the port trigger.

Public Port: Specify the public port(s) that to which the trigger will forward.

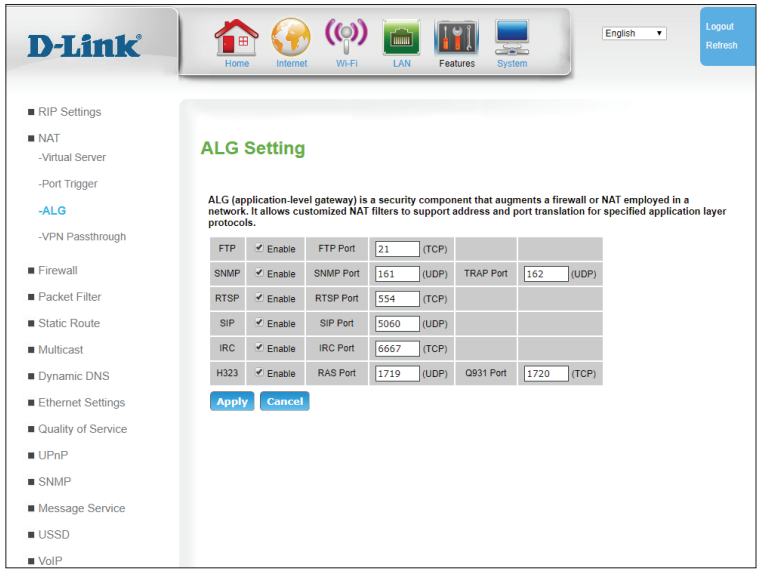
Public Protocol: Select a public protocol

Time Schedule: Select the time schedule during which the port trigger rule is active. To create a new time schedule, click **New Time Schedule.**

Click **Apply** to save your settings, **Cancel** to revert to your previous settings, or **Back** to return to the previous screen.

ALG

An application-level gateway (ALG) is a security component that augments a firewall or NAT employed in a network. It allows customized NAT filters to support address and port translation for specified application layer protocols. For each protocol type, check **Enable** to activate the ALG, and specify a port. Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.



VPN Passthrough

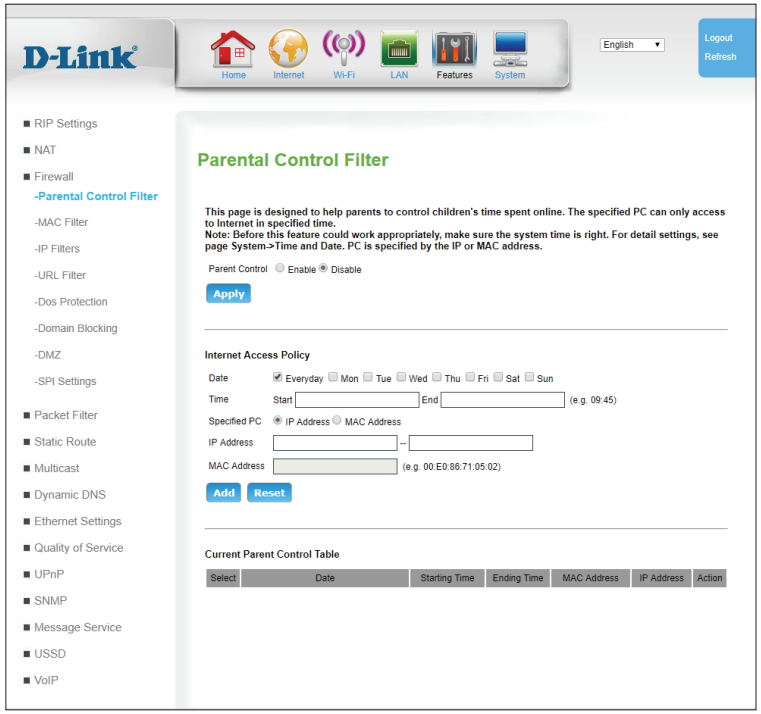
The device supports VPN (Virtual Private Network) passthrough for PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and IPSec (IP security). Once VPN passthrough is enabled, there is no need to create any Virtual Server or Port Forwarding entries in order for outbound VPN sessions to establish properly. Multiple VPN connections can be made through the device. This is useful when you have many VPN clients on the Local Area Network. For each VPN type, check **Enable** to activate the passthrough, and specify a port. Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Firewall

Parent Control Filter

The **Parent Control Filter** allows you to enable Internet connectivity for some devices on a fixed schedule. Note that for the dates to be effect, the date, time, and time zone must be set correctly in **Time Settings** on page **104**. Devices can be listed multiple times, and will be granted internet connectivity during all dates and times listed.

Parent Control: When Parent Control is set to **Enable**, devices listed in the **Current Parent Control Table** will only be able to access the Internet on the specified days during the specified times.



Click **Apply** to save your settings.

Internet Access Policy

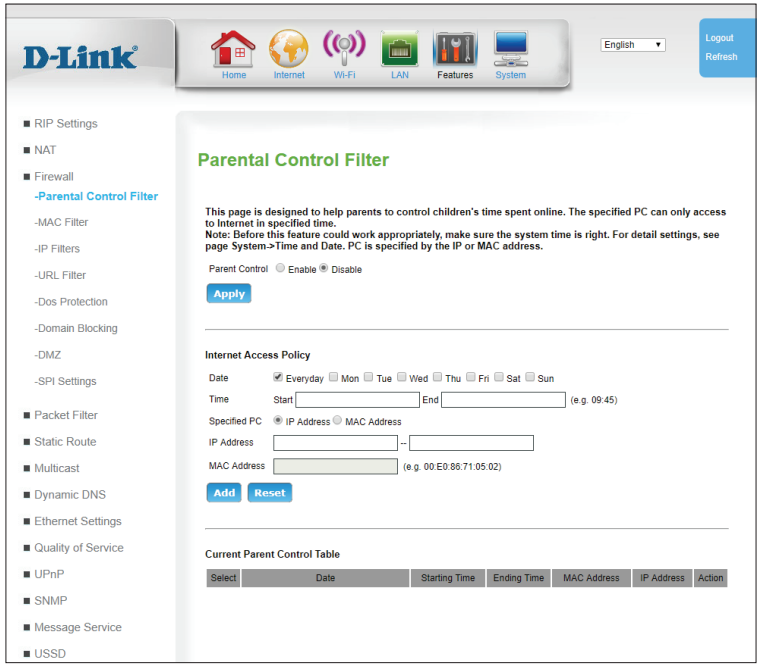
Date: Select a day(s) of the week when Internet access will be permitted.

Time: Specify a time during the specified days when Internet access will be permitted. The time must be specified in 24 hour HH:MM format, where 10 AM would be 10:00 and 10 PM would be 22:00.

Specified PC: You can specify whether the filters will be applied to devices by **MAC Address** or by **IP Address**. Note that by default, LAN IPs are dynamic.

IP Address: If you have specified **IP Address** above, enter an IP address range to which this filter will apply. You can check addresses of currently connected devices using the Clients sections under **Status** on page **114**.

MAC address: If you have specified **MAC Address** above, enter a single MAC address to which this filter will apply. You can check addresses of currently connected devices using the Clients sections under **Status** on page **114**.



Click **Add** to add a new rule to the Parent Control list. Click **Reset** to clear all fields.

Current Parent Control Table

Select: Indicates the ID of each rule.

Date: Indicates the days where Internet access is granted.

Starting Time: Indicates the starting time of Internet access on the specified days.

Ending Time: Indicates the ending time of Internet access on the specified days.

MAC Address: Indicates the MAC Address (if selected) to which Internet access is granted during the specified times.

IP Address: Indicates the IP Address range (if selected) to which Internet access is granted during the specified times.

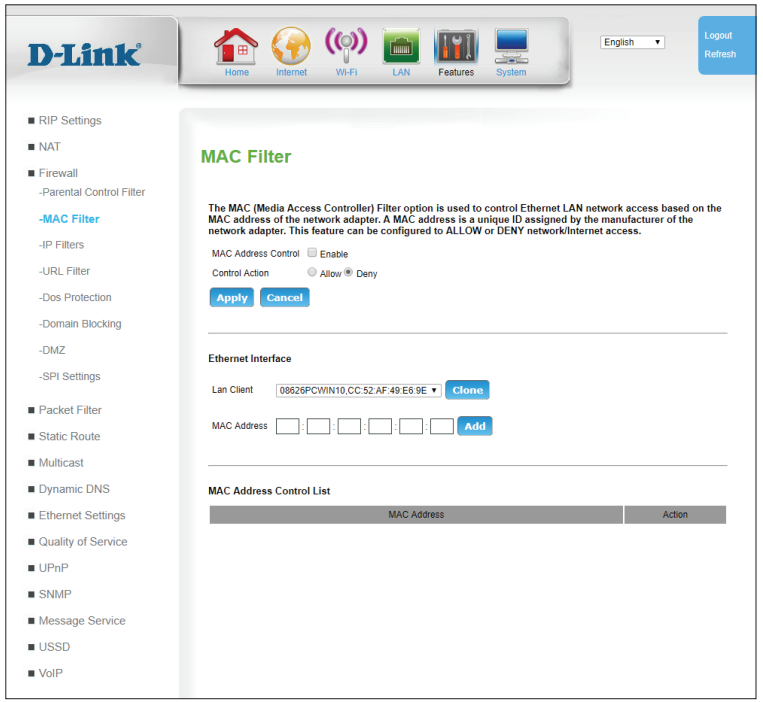
Action: Click the trash can icon (🗑) to delete the rule.

MAC Filter

The **MAC (Media Access Controller) Filter** option is used to control Ethernet LAN 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.

MAC Address Control: Select **Enable** to enable MAC Address filtering.

Control Action: Select **Allow** to allow only clients on the list to connect, creating a white list. Select **Deny** to allow all connections except to the clients on the list, creating a black list.



Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Ethernet Interface

Lan Client: You can optionally select a LAN client from the list of clients. Once selected, click **Clone** to auto-fill the field below.

MAC Address: Enter a MAC address or edit one cloned from the **Lan Client** field. Click **Add** to

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

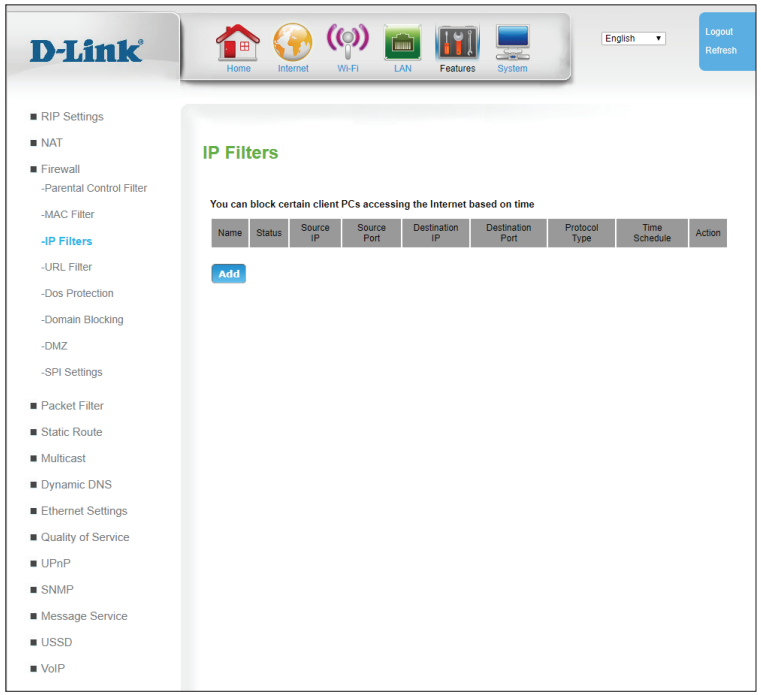
MAC Address list

MAC Address Displays the MAC Address(es) to be filtered.

Action: Click the trash can icon (🗑) to delete the rule.

IP Filters

An **IP Filter** is an advanced feature that allows you to drop IP traffic based on specific rules. Each IP packet is marked with a source address, destination address, and ports.



Name: Indicates the name of the filter. The name is for reference purposes only and does not affect functionality.

Status: Indicates whether the filter is set to **Enable** or **Disable**.

Source IP: Indicates the source IP or IP range to which the rule will apply

Source Port: Indicates the source port or port range to which the rule will apply.

Destination IP: Indicates the destination IP or IP range to which the rule will apply

Destination Port: Indicates the destination port or port range to which the rule will apply.

Protocol Type: Indicates protocol types affected by the filter.

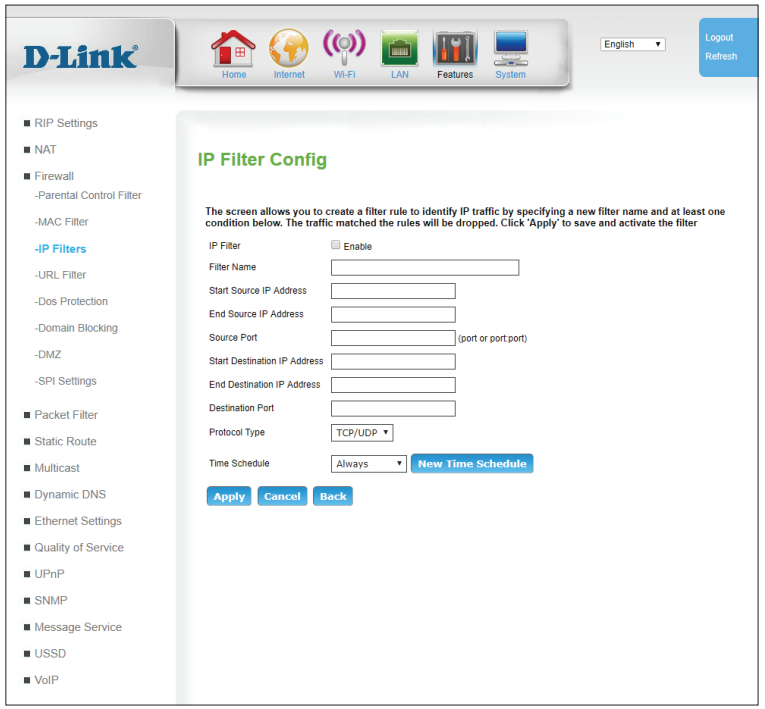
Time Schedule: Indicates the schedule used by the filter.

Action: Click the pencil (✎) icon to edit the filter, click the trash can icon (🗑) to delete the filter.

Click **Add** to add a new filter, described in **IP Filter Config** on page **58**.

IP Filter Config

An **IP Filter** is an advanced feature that allows you to drop IP traffic based on specific rules. Each IP packet is marked with a source address, destination address, and ports.



IP Filter: Tick the **Enable** box to activate this filter.

Name: Input the name of the filter. The name is for reference purposes only and does not affect functionality.

Start Source IP: Specify the source IP or IP range to which the rule will apply. To specify a range, enter the start of the range in this box. To specify a single IP, enter the same address in the Start and End boxes.

End Source IP: Specify the source IP or IP range to which the rule will apply. To specify a range, enter the end of the range in this box. To specify a single IP, enter the same address in the Start and End boxes.

Source Port: Indicates the source port or port range to which the rule will apply. To specify a port range, enter in the format of **Start:End**.

Start Destination IP Address: Specify the destination IP or IP range start to which the rule will apply. To specify a range, enter the start of the range in this box. To specify a single IP, enter the same address in the Start and End boxes.

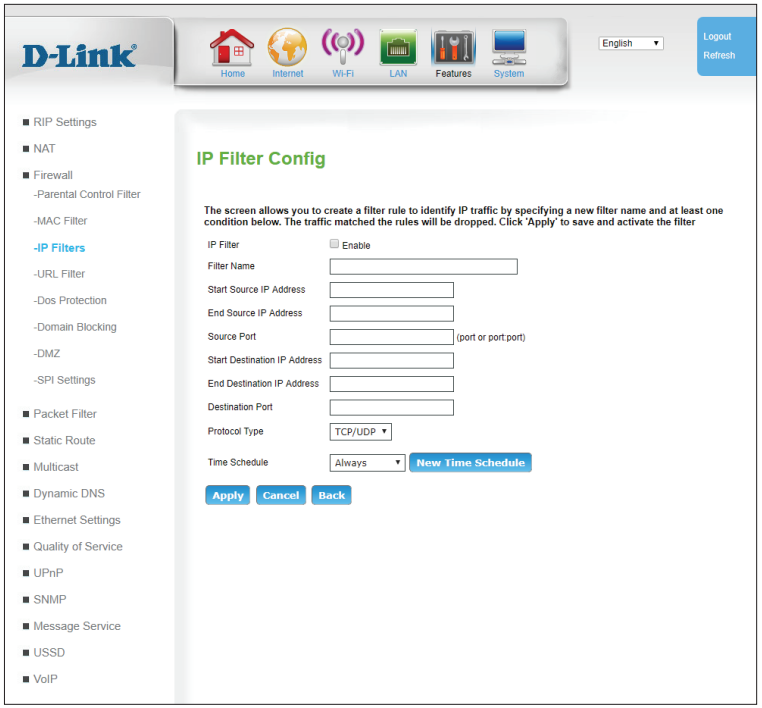
End Destination IP Address: Specify the destination IP or IP range end to which the rule will apply. To specify a range, enter the end of the range in this box. To specify a single IP, enter the same address in the Start and End boxes.

Destination Port: Specify the destination port or port range to which the rule will apply. To specify a port range, enter in the format of **Start:End**.

Protocol Type: Specify the protocol type(s) to be filtered.

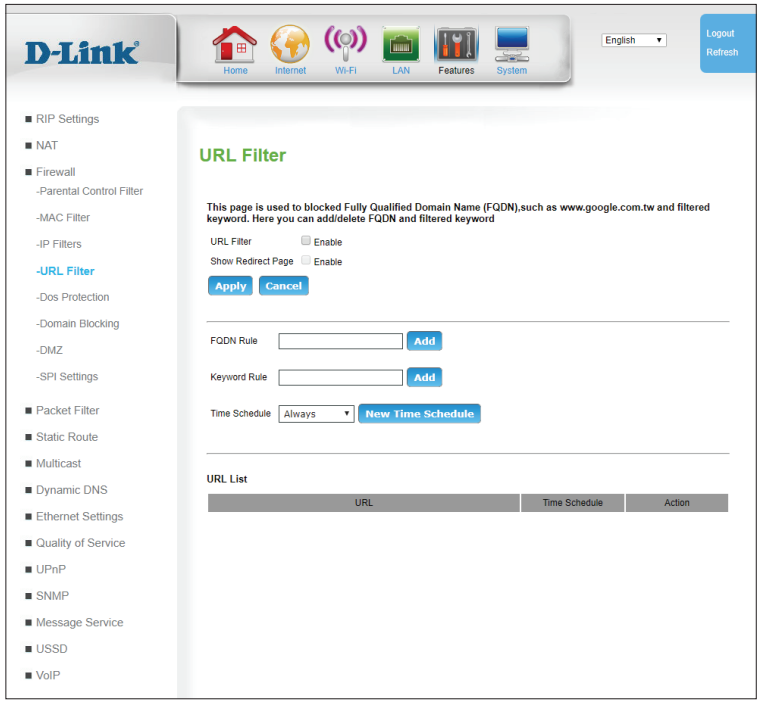
Time Schedule: Select a time schedule to apply to the filter. To create a new filter, click **New Time Schedule** and see **Time Schedule** on page **109**.

Click **Apply** to save your settings, **Cancel** to revert to your previous settings, or **Back** to return to the previous screen.



URL Filter

URL Filter allows you to set up a list of websites that will be blocked from users on your network.



URL Filter: Check the box to enable URL Filtering.

Show Redirect Page: Check this box to show a redirect page when a page is blocked.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

FQDN Rule: The fully qualified domain name (**FQDN**) that you would like to block. All URLs that begin with this address will be blocked. Click **Add** to add a new filter.

Keyword Rule: Enter keywords you want to filter. Click **Add** to add a new filter.

Time Schedule: Select a time schedule to apply to the filter. To create a new filter, click **New Time Schedule** and see **Time Schedule** on page **109**.

URL List

URL: Indicates the URL or keyword to which the filter will apply.

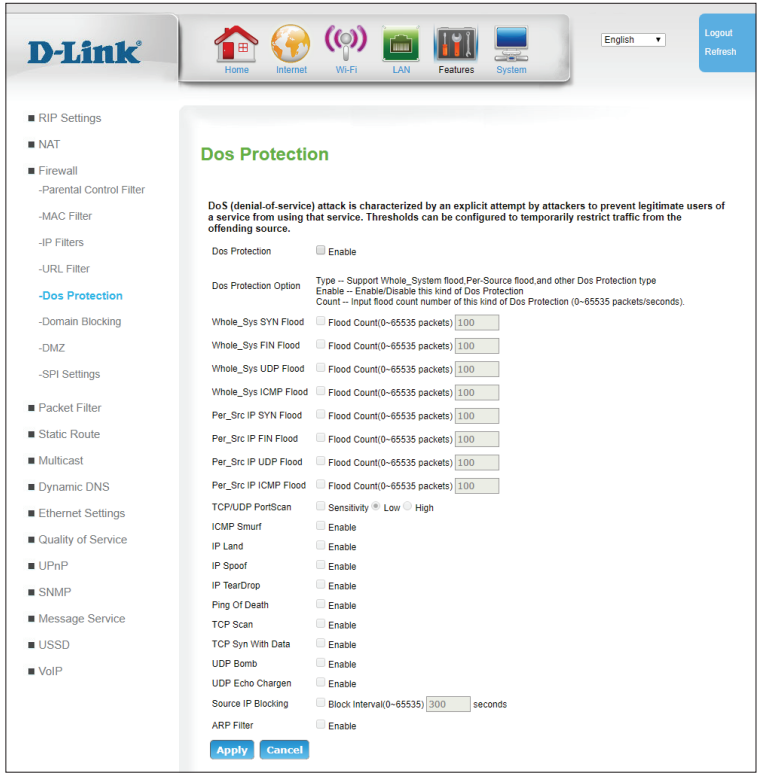
Time Schedule: Indicates the time schedule during which the filter will apply.

Action: Click the trash can icon (🗑) to delete the filter.

Dos Protection

A denial-of-service (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Attacks can be malicious security breaches or unintentional network issues that render the router unusable. Attack checks allow you to manage WAN security threats such as continual ping requests and discovery via ARP scans. Certain Denial-of-Service (DoS) attacks can be blocked. These attacks, if uninhibited, can use up processing power and bandwidth and prevent regular network services from running normally. Thresholds can be configured to temporarily restrict traffic from the offending source.

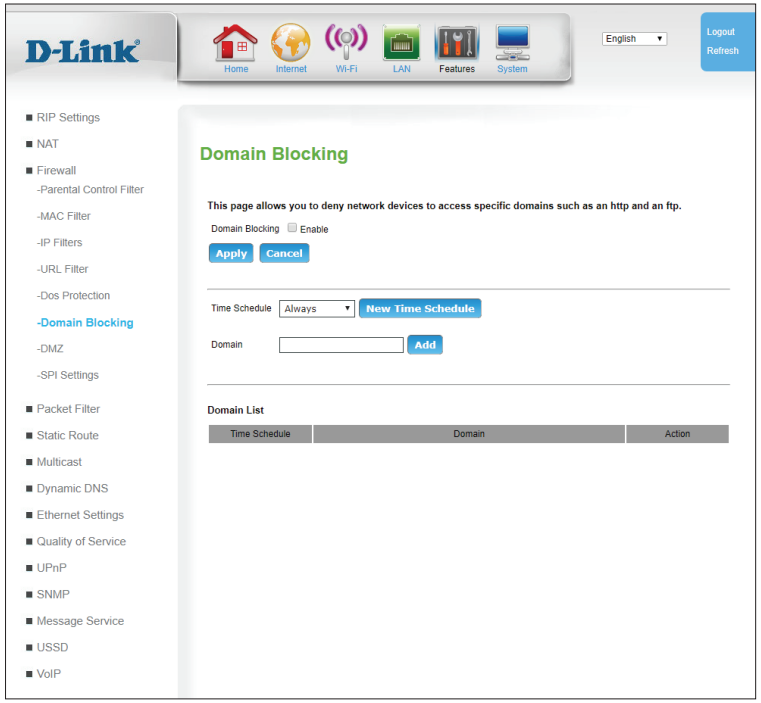
Dos Protection: Check this box to enable DoS prevention. Attack types may be individually enabled and thresholds (if applicable) manually configured.



Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Domain Blocking

Domain Filter allows you to set up a list of domains that will be blocked from users on your network.



Domain Filter: Check the box to enable Domain Filtering.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Time Schedule: Select a time schedule to apply to the filter. To create a new filter, click **New Time Schedule** and see **Time Schedule** on page **109**.

Domain Rule: Enter domain you want to filter. Click **Add** to add a new filter.

Domain List

Time Schedule: Indicates the time schedule during which the filter will apply.

Domain: Indicates the domain to which the filter will apply.

Action: Click the trash can icon (🗑) to delete the filter.

DMZ

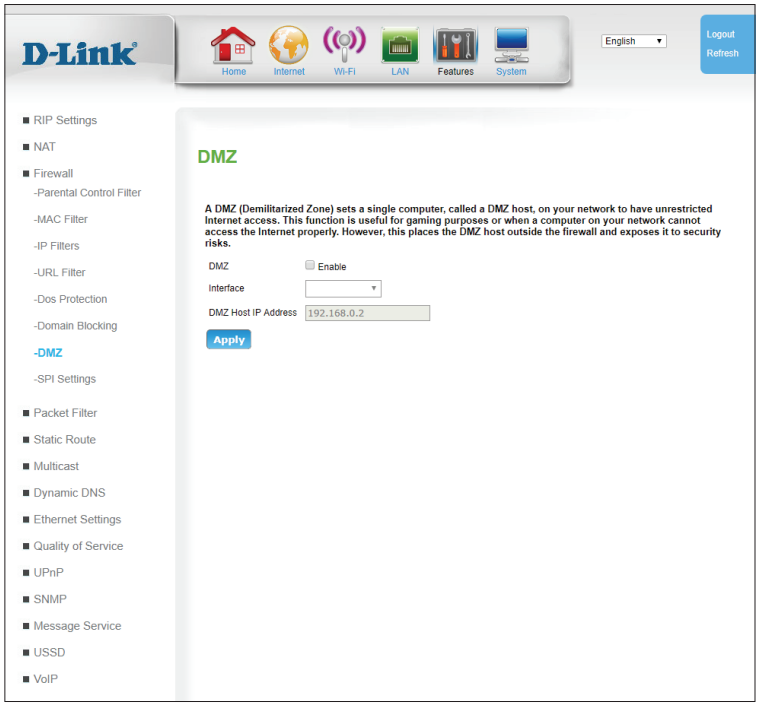
Sometimes you may want a computer exposed to the Internet for certain types of applications. If you choose to expose a computer, you can enable Demilitarized Zone (DMZ). This option will expose the chosen computer completely to the Internet. This is not recommended for normal use.

DMZ: Check the box to enable DMZ.

Interface: Select a WAN interface to which the DMZ will be applied.

DMZ Host IP Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication.

Click **Apply** to save your settings.



SPI Settings

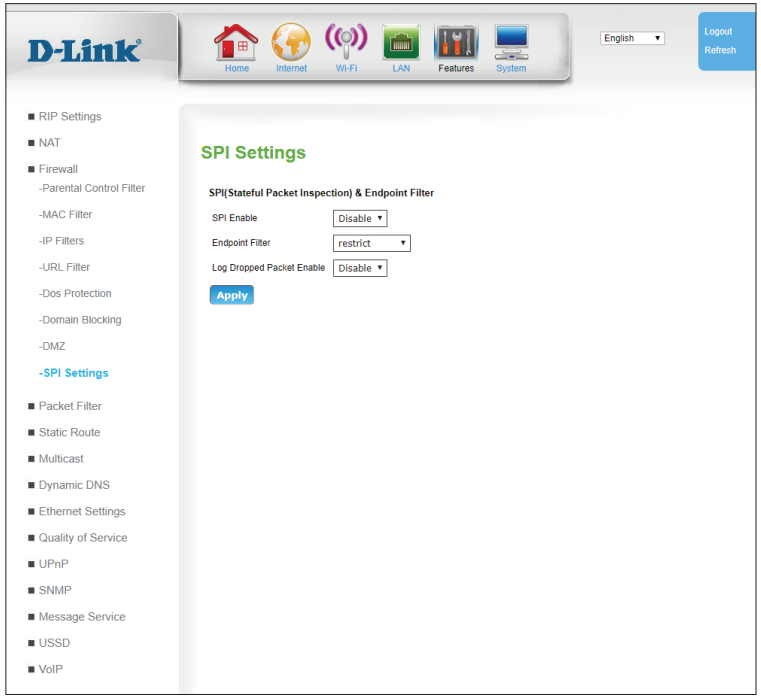
Stateful Packet Inspection (SPI) checks traffic against known protocols, and drops packets that do not conform to known patterns. SPI is also known as dynamic packet inspection.

SPI Enable: Check the Enable SPI box to enable the SPI (Stateful Packet Inspection) feature.

Endpoint Filter: Select the appropriate endpoint filter setting.

Log Dropped Packet Enable: Select **Enable** to log all dropped packets. The default setting is **Disable**.

Click **Apply** to save your settings.



Packet Filter

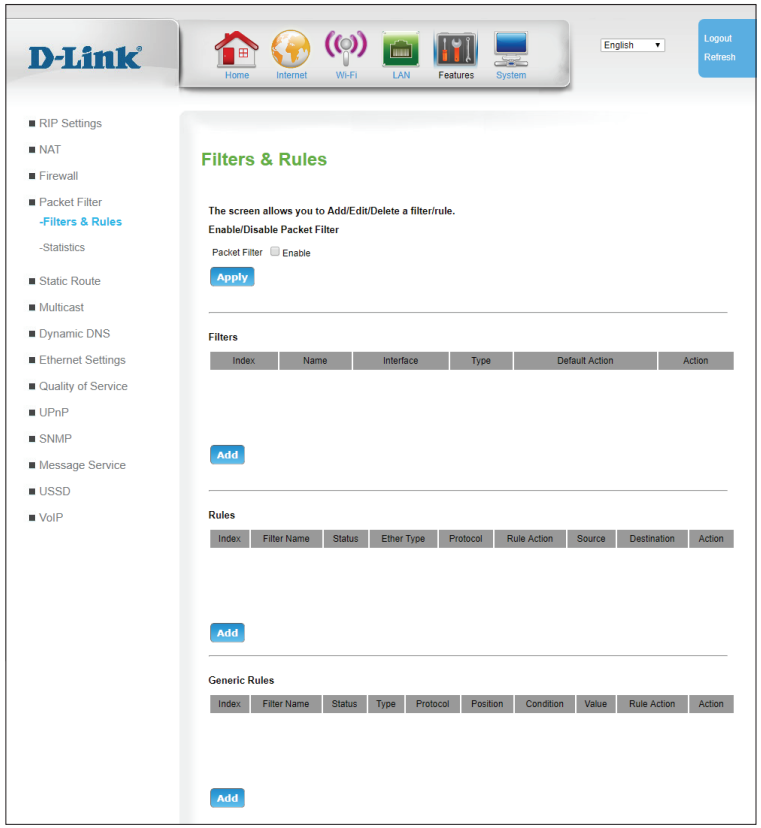
Filters & Rules

The router has the ability to filter packets based on specific characteristics of Ethernet frames. Filters are used to specify interfaces and broad guidelines, while rules allow very fine, protocol-specific control over packets. Generic Rules look for a particular pattern within any Ethernet frame. These features are intended for advanced users and network professionals only, and can safely be ignored by most users.

Enable/Disable Packet Filter

Packet Filter: Check this box to enable the packet filter.

Click **Apply** to save your settings.



Filters

Index: Indicates the index of the filter.

Name: Indicates the user assigned name of the filter.

Interface: Indicates the WAN interface to which the filter applies.

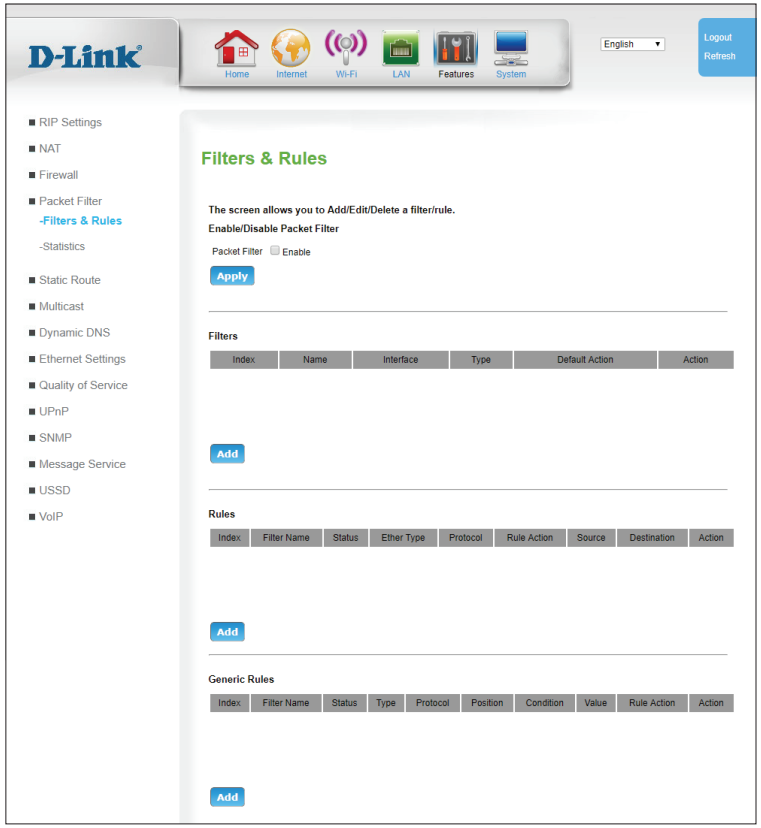
Type: Indicates whether the filter applies to inbound or outbound packets.

Default Action: Indicates the default action - permitting packets or dropping them.

Action: Click the pencil (✎) icon to edit the filter, click the trash can icon (🗑) to delete the filter.

Click **Add** to add a new filter, described in **Packet Filter -- Filters** on page **68**.

Rules



Index: Indicates the index of the rule.

Filter Name: Indicates the name of the filter to which the rule is applied.

Status: Indicates the current status of the rule (usually **Enabled** or **Disabled**).

Ether Type: Indicates the EtherType to which the rule applies.

Protocol: Indicates the protocol to which the rule applies

Rule Action: Indicates whether the incoming packet will be dropped, permitted, rejected (return an error), logged and dropped, or logged and permitted.

Origin: Indicates the origin to which the rule applies.

Destination: Indicates the destination to which the rule applies.

Action: Click the pencil (✎) icon to edit the rule, click the trash can icon (🗑) to delete the rule.

Click **Add** to add a new rule, described in **Packet Filter -- Rules** on page **69.**

Generic Rules

Index: Indicates the index of the rule.

Filter Name: Indicates the name of the filter to which the rule is applied.

Status: Indicates the current status of the rule (usually **Enabled** or **Disabled**).

Type: Select an EtherType from the dropdown menu to which the rule will apply.

Protocol: Select a protocol from the dropdown menu to which the rule will apply.

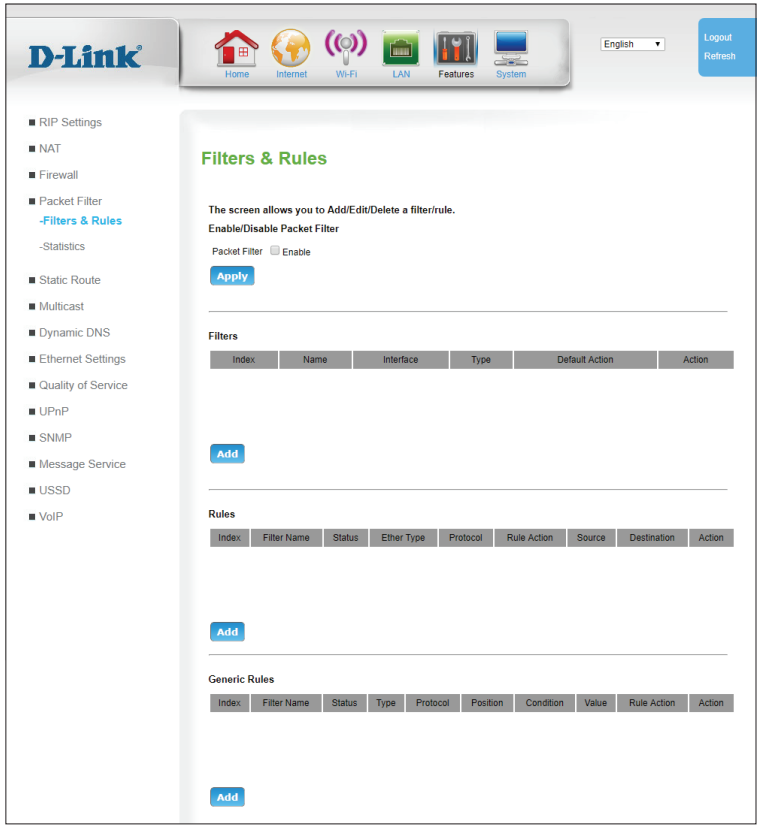
Position: Rules are evaluated based on position starting with rule 0. The rules are applied from lowest to highest until the rules are exhausted or one is triggered.

Condition: Indicates a python logical operator to be performed on the value.

Value: Indicates the value the rule will use to evaluate trigger conditions.

Rule Action: Indicates the action taken when the rule is triggered.

Action: Click the pencil (✎) icon to edit the rule, click the trash can icon (🗑) to delete the rule.



Click **Add** to add a new generic rule, described in **Packet Filter -- Generic Rules** on page **71.**

Packet Filter -- Filters

Filter allow you to specify broad rules that apply to all packet classes across a single interface. Other, more specific rules will be based on these filters.

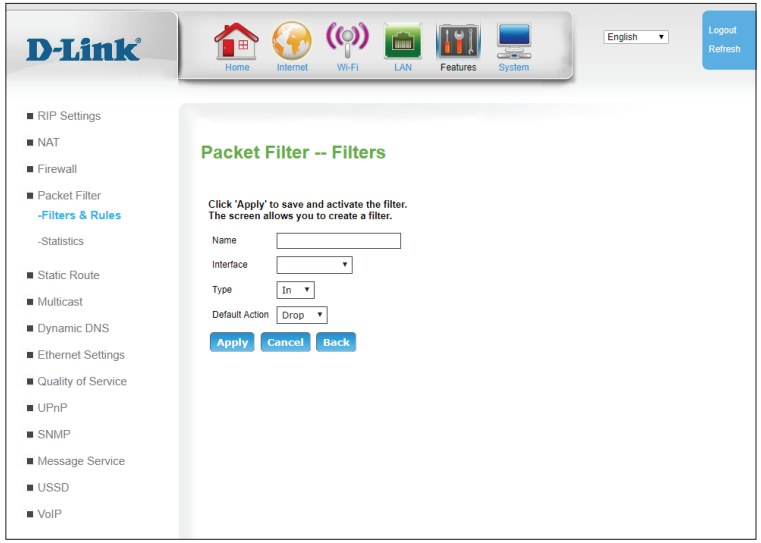
Name: Enter the user assigned name of the filter. This is for reference only and does not affect functionality.

Interface: Specify the WAN interface to which the filter applies.

Type: Specify whether the filter applies to inbound or outbound packets.

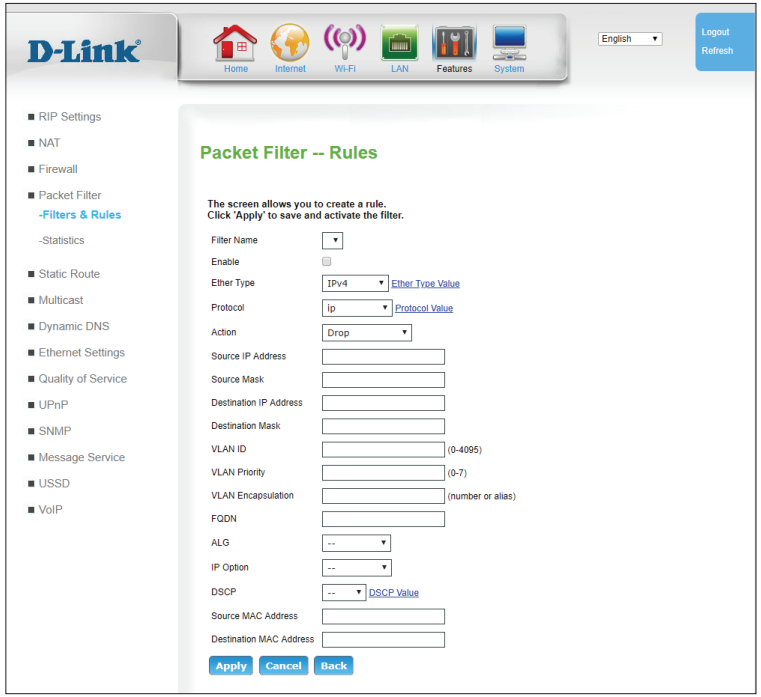
Default Action: Specify the default action - permitting packets or dropping them.

Click **Apply** to save your settings, **Cancel** to clear settings, or **Back** to return to the previous page.



Packet Filter -- Rules

The rules page allows you to assign rules for specific protocols attached to existing filters.



Filter Name: Select the filter to which to apply the rule.

Enable: Check this box to enable the rule. This can be changed later.

Ether Type Select an Ether Type from the dropdown menu to which the rule will apply.

Protocol: Select a protocol from the dropdown menu to which the rule will apply.

Action: Specify whether the incoming packet should be dropped, permitted, rejected (return an error), logged and dropped, or logged and permitted.

ICMP Type: If **ICMP** has been selected for **Port** above and if **Ether Type** has been set to **IPv4** or **IPv6**, select an ICMP type from the dropdown list. (Optional)

Source IP Address: If **Ether Type** has been set to **IPv4**, enter the source IP address to which the rule will be applied. (Optional)

Source Mask: If **Ether Type** has been set to **IPv4**, enter a source mask/subnet prefix length to which the rule will apply. (Optional)

Destination IP Address: If **Ether Type** has been set to **IPv4**, specify a destination IP address to which the rule will be applied. (Optional)

VLAN ID: Enter the VLAN ID to which the rule will apply. (Optional)

VLAN Priority: Enter the VLAN priority to which the rule will apply. (Optional)

VLAN Encapsulation: Enter the VLAN encapsulation to which the rule will apply. (Optional)

FWDN: Enter the fully qualified domain name (FWDN) to which the rule will be applied. (Optional)

ALG: Enter the application layer gateway (ALG) to which the rule will apply. (Optional)

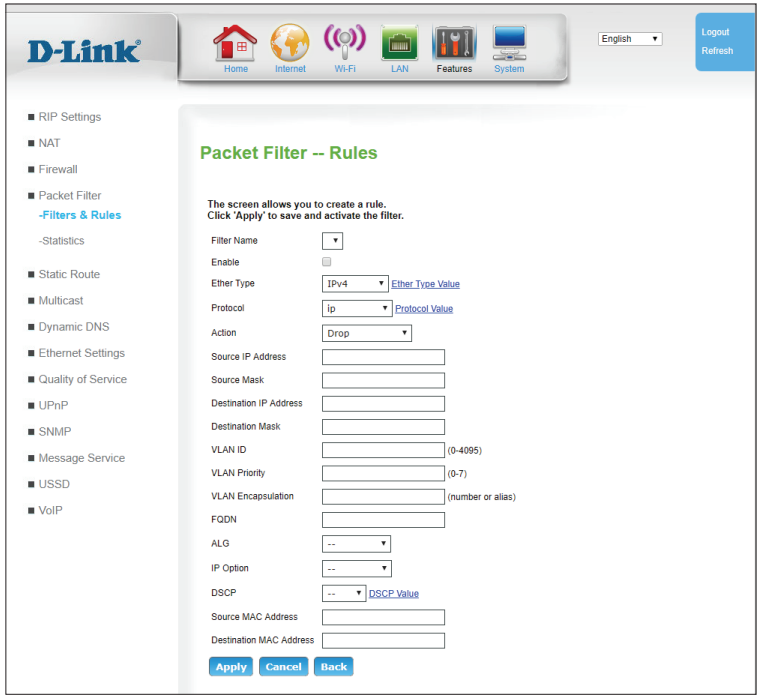
IP Option: Select an IP Option from the dropdown list to which the rule will apply. (Optional)

DSCP: Select a differentiated services code point from the dropdown menu to which the rule will apply. (Optional)

Source MAC Address: Enter a source MAC address to which the rule will apply. (Optional)

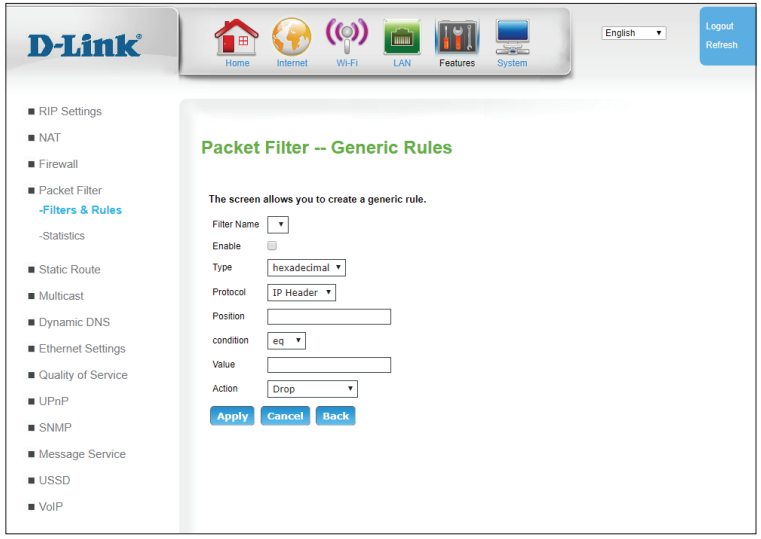
Destination MAC Address: Enter a destination MAC address to which the rule will apply. (Optional)

Click **Apply** to save your settings, **Cancel** to clear settings, or **Back** to return to the previous page.



Packet Filter -- Generic Rules

Generic rules are more general than the rules listed in **Packet Filter -- Rules** on page **69**, and can be applied broadly to any EtherType.



Filter Name: Select the filter to which to apply the rule.

Enable: Check this box to enable the rule. This can be changed later.

Type: Select an EtherType from the dropdown menu to which the rule will apply.

Proto: Select a protocol from the dropdown menu to which the rule will apply.

Position: Enter a non-negative integer value. Rules are evaluated based on position starting with rule 0. The rules are applied from lowest to highest until the rules are exhausted or one is triggered.

Condition: Specific a python logical operator to be performed on the value.

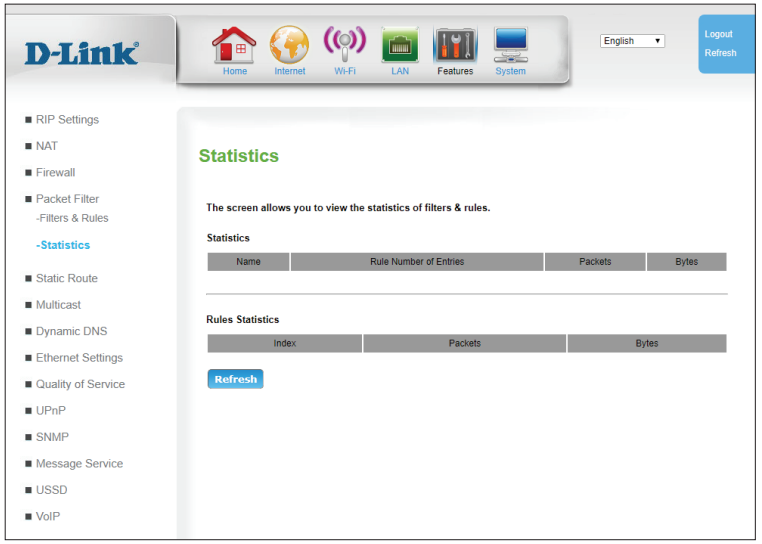
Value: Enter a value the rule will use to evaluate.

Action: Specify the action taken when the rule is triggered.

Click **Apply** to save your settings, **Cancel** to clear settings, or **Back** to return to the previous page.

Statistics

The screen allows you to view the statistics of filters and rules.



Statistics

Name: Indicates the name of the statistic.

Rule Number of Entries: The number of entries for the rule.

Packets: The amount of packets that pass through the router.

Bytes: The amount of bytes that pass through the router.

Rules Statistics

Index: Indicates the index of the rule.

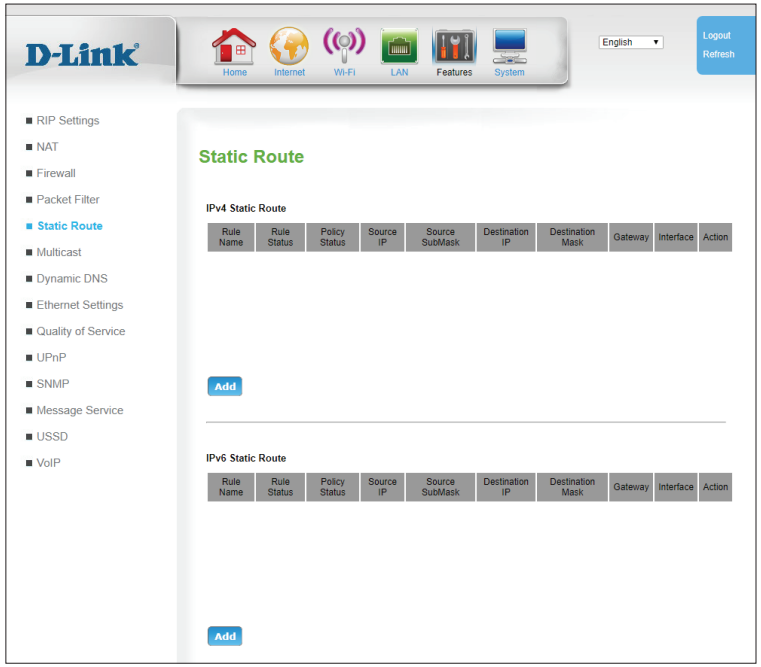
Packets: The amount of packets that pass through the router.

Bytes: The amount of bytes that pass through the router.

Click **Refresh** to refresh the statistics.

Static Route

The **Static Route** page allows you to specify custom routes that determine how data is moved around your network. Static routes can be specified separately for IPv4 and IPv6.



Rule Name: Indicates the name of the static route.

Rule Status: Indicates whether the rule is **enabled** or **disabled**.

Policy Status: Indicates the policy of the route. If enabled, all packets matching the destination will always follow the specified route. If disabled, no packet will be sent along this route.

Source IP: Indicates the source IP of the static route. (Optional)

Source SubMask: Indicates the source subnet of the static route. (Optional)

Destination IP: Indicates the destination IP of the static route.

Destination Mask: Indicates the destination mask of the static route.

Gateway: Indicates the gateway that will be used (or avoided) by the static rout.

Interface: Indicates the interface used by the static route.

Action: Click the pencil (✎) icon to edit the filter, click the trash can icon (🗑) to delete the static route.

Click **Apply** to save your settings.

Static Route Set

Rule Enable: Specify whether the rule is **enabled** or **disabled**.

Forwarding Policy Option: Specify the policy of the route. If enabled, all packets matching the destination will always follow the specified route. If disabled, no packet will be sent along this route.

Rule Name: Specify the name of the static route for reference

Source IP: Specify the source IP of the static route. (Optional)

Source SubMask: Specify the source subnet of the static route. (Optional)

Destination IP: Specify the destination IP of the static route.

Destination Mask: Specify the destination mask of the static route.

Gateway: Specify the gateway that will be used (or avoided) by the static route.

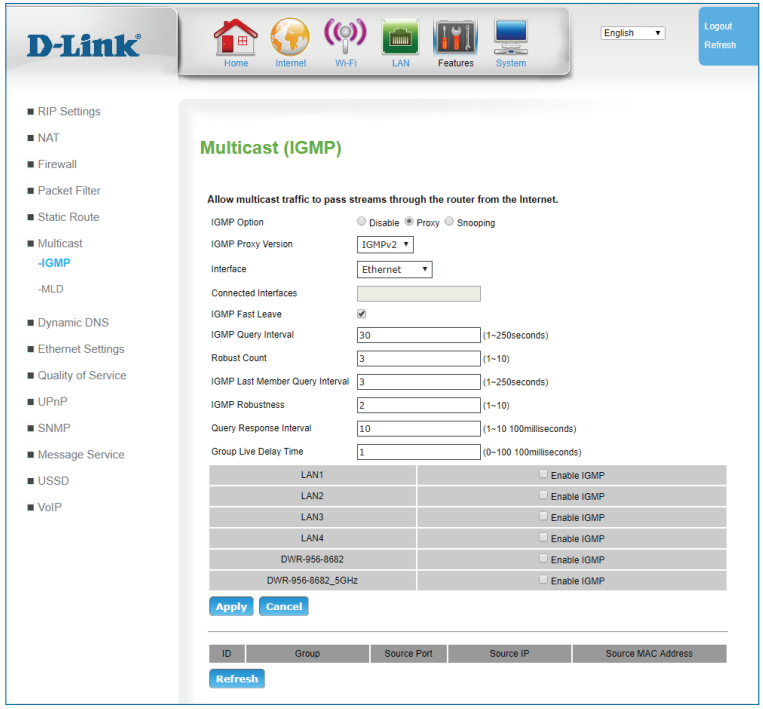
Interface Name: Specify the interface used by the static route.

Click **Apply** to save your settings.

Multicast

IGMP

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. Multicast allows for the transmission of identical content, such as multimedia, from a source to a number of recipients, and is commonly used for applications like IP TV. This setting should be disabled unless you use a service that explicitly relies on multicast.



IGMP Option: Select **Disable**, **Proxy**, or **Snooping**. If you select **Disable**, no additional configuration is required.

If you have selected Proxy:

IGMP Proxy Version: Select **IGMPv2** or **IGMPv3**.

Interface: Specify a WAN interface over which the proxy will be used.

Connected Interfaces: Specify connected interfaces. This option is greyed out for 4G connections.

IGMP Fast Leave: Check the box to enable the fast leave feature.

IGMP Query Interval: The query interval is the amount of time in seconds between General Query messages sent by the router (if the router is querying on this subnet).

Robust Count: Set robustness value to account for packet loss on congested networks.

IGMP last Member Query Interval: The last member query interval is the amount of time in seconds that the router waits to receive a response to a Group-Specific Query message. It is also the amount of time in seconds between successive Group-Specific Query messages.

IGMP Robustness: The robustness variable is a way of indicating how susceptible the subnet is to lost packets. The router can recover from the robustness variable minus 1 lost packet.

Query Response Interval: The query response interval is the maximum amount of time in seconds that the router waits to receive a response to a General Query message. It is the Maximum Response Time field in the message header. The default query response interval is 10 seconds and must be less than the query interval.

Group Live Delay Time: Specify the group live delay time in milliseconds. The default setting is 1.

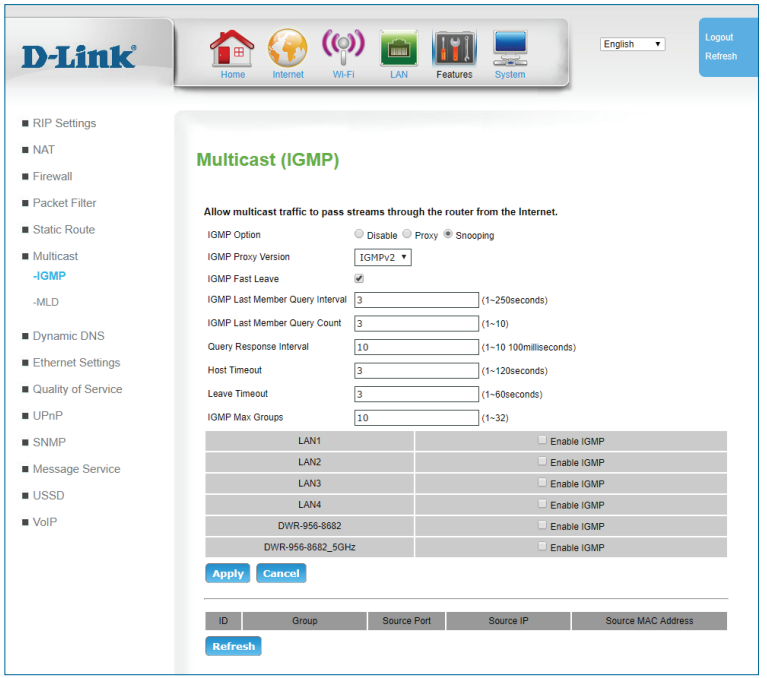
If you have selected Snooping:

IGMP Proxy Version: Select **IGMPv2** or **IGMPv3**.

IGMP Fast Leave: Check the box to enable the fast leave feature.

IGMP Last Member Query Interval: The last member query interval is the amount of time in seconds that the router waits to receive a response to a Group-Specific Query message. It is also the amount of time in seconds between successive Group-Specific Query messages.

IGMP Last Member Query Count: The last member query count is the number of messages the router sends out during the **Last Member Query Interval**. If no host responds to those messages, the IGMP state is removed from those hosts.



Query Response Interval: Specify the Query Response Interval which is the maximum amount of time in seconds that the router waits to receive a response to a General Query message. It is the Maximum Response Time field in the message header. The default query response interval is 10 seconds and must be less than the query interval.

Host Timeout: Specify the time in which hosts must reply to queries within this value in seconds or be dropped from the group.

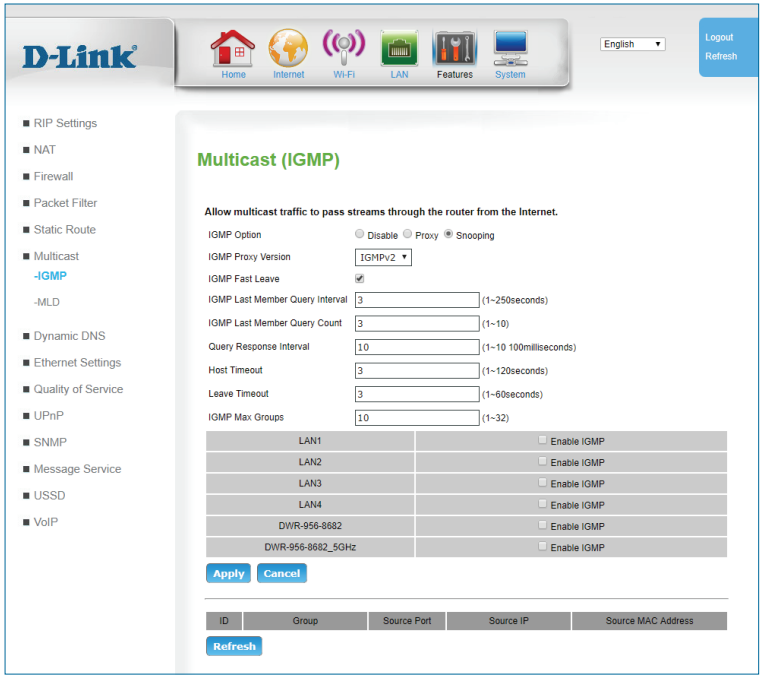
Leave Timeout: Specify the amount of time the host waits to receive an new IGMP join message after leaving the current group. If it does not receive a join message in the specified time, it times out.

IGMP Max Groups: Specify the maximum number of groups a host can join.

For Snooping and Proxy:

LAN1-4, 2.4, and 5 GHz Wireless: Select **Enable** to enable IGMP on this interface.

Click **Apply** to save your settings.



MLD

The Multicast Listener Discovery (MLD) is a communications protocol used by hosts and adjacent routers on IPv6 networks to establish multicast group memberships. Multicast allows for the transmission of identical content, such as multimedia, from a source to a number of recipients, and is commonly used for applications like IP TV. This setting should be disabled unless you use a service that explicitly relies on multicast.

MLD Option: Select **Disable**, **Proxy**, or **Snooping**. If you select **Disable**, no additional configuration is required.

If you have selected Proxy:

Interface: Specify a WAN interface over which the

Connected Interfaces: Specify connected interfaces. This option is greyed out for 4G connections.

Fast Leave: Check the box to enable the fast leave feature.

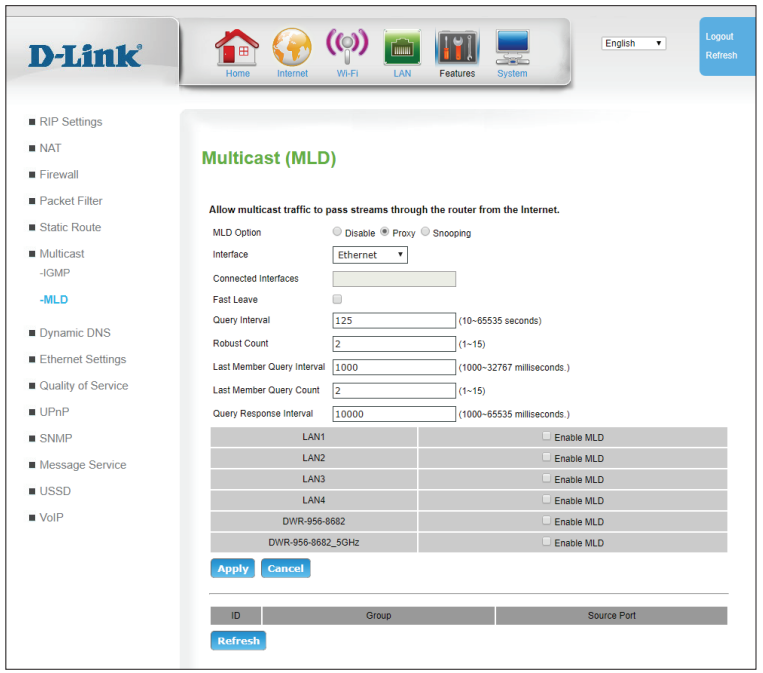
Query Interval: Specify the query interval which is the amount of time in seconds between General Query messages sent by the router (if the router is querying on this subnet).

Robust Count: Set a robustness value to account for packet loss on congested networks.

Last Member Query Interval: Specify the last member query interval which is the amount of time in seconds that the router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.

Last Member Query Count: Specify the last member query count which is the number of messages the router sends out during the **Last Member Query Interval**. If no host responds to those messages, the MLD state is removed from those hosts.

Query Response Interval: Specify the query response interval which is the maximum amount of time in seconds that the router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the message header. The default query response interval is 10 seconds and must be less than the query interval.

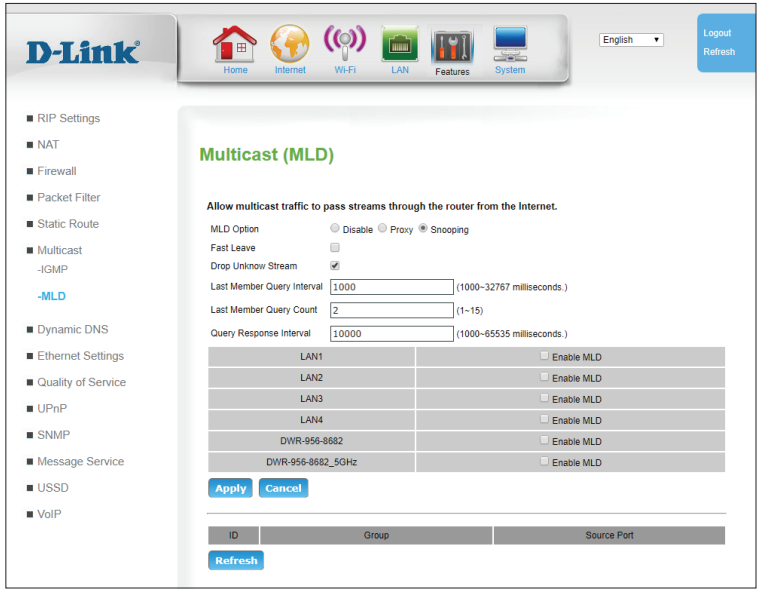


If you have selected Snooping:

Fast Leave: Check the box to enable the fast leave feature.

Drop Unknown Stream: Check this box to drop unknown streams.

Last Member Query Interval: Specify the last member query interval which is the amount of time in milliseconds that the router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.



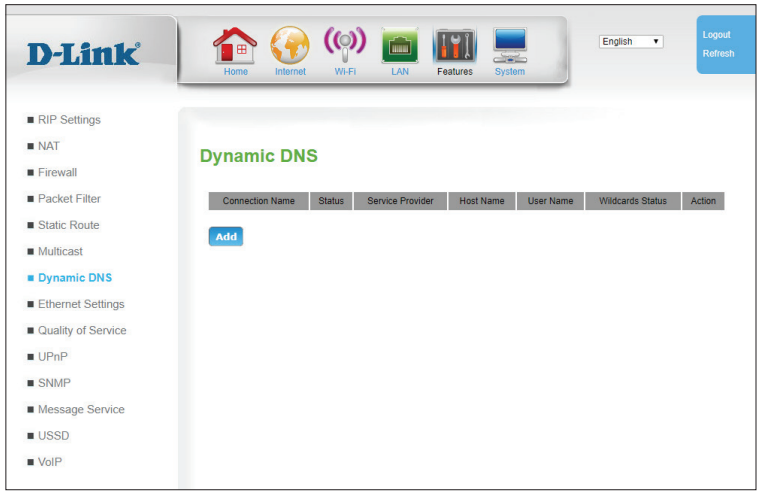
Last Member Query Count: Specify the last member query count which is the number of messages the router sends out during the **Last Member Query Interval**. If no host responds to those messages, the MLD state is removed from those hosts.

Query Response Interval: Specify the query response interval which is the maximum amount of time in seconds that the router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the message header. The default query response interval is 10 seconds and must be less than the query interval.

Click **Apply** to save your settings.

Dynamic DNS

The Router supports DDNS (Dynamic Domain Name Service). Dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specified host from various locations on the Internet. This is enabled to allow remote access to a host by clicking on a hyperlinked URL in the form hostname.dyndns.org, Many ISPs assign public IP addresses using DHCP, and this can make it difficult to locate a specific host on the LAN using standard DNS. If for example you are running a public web server or VPN server on your LAN, this ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be setup with one of the supported DDNS service providers.



Connection Name: Indicates the interface (connection) over which DDNS is operating.

Status: Indicates whether the DDNS connection is enabled or disabled.

Service Provider: Indicates which DDNS service provider is being used.

Host Name: Indicates the host name chosen by the user.

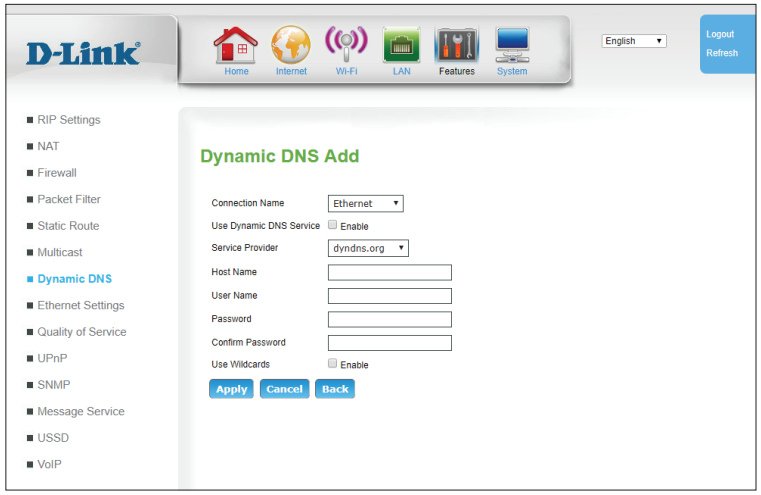
User name: Indicates the user account being used to access the DDNS service.

Wildcards Status: Indicates whether wildcards are **Enabled** or **Disabled**. Wildcards allows anything before the hostname to be resolved into an IP address. For example, if your hostname is *hostname.ddns.com*, typing *www.hostname.ddns.com* or *lakjsdfhlkadf.hostname.ddns.com* would both resolve to the same IP address. Note that not all DDNS providers support wildcards.

Action: Click the pencil (✎) icon to edit the DDNS entry, click the trash can icon (🗑) to delete the DDNS entry.

Add: Click **Add** to add a new DDNS service. This will launch the **Dynamic DNS Add** screen, described on the next page.

Dynamic DNS Add



Connection Name: Specify the interface (connection) over which DDNS will operate.

Use Dynamic DNS Service: Check this box to enable the DDNS service.

Service Provider: Specify the DDNS service provider to be used.

Host Name: Enter the host name that will be used.

User name: Specify the user account to be used to access the DDNS service.

Password: Enter the password to be used to connect to the DDNS service.

Confirm Password: Re-enter the password to be used to connect to the DDNS service.

Use Wildcards: Specify if the use of wildcards is **Enabled** or **Disabled**. Wildcards allows anything before the host name to be resolved into an IP address. For example, if your host name is *hostname.ddns.com*, typing *www.hostname.ddns.com* or *lakjsdfhlkadf.hostname.ddns.com* would both resolve to the same IP address.

Click **Apply** to save your settings, **Cancel** to clear current settings, or **Back** to return to the previous page.

Ethernet Settings

This page allows you to configure low-level features of the LAN Ethernet ports.. These features are intended for advanced users and network professionals only, and can safely be ignored by most users.

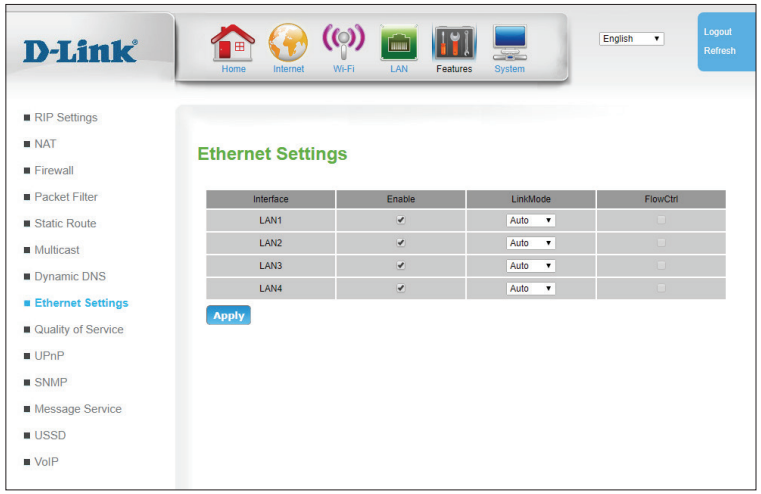
Interface: Indicates the LAN interface.

Enable: Check this box to enable this Ethernet port. This setting is enabled by default.

LinkMode: Indicates the speed and duplex mode used by the Ethernet port. The default and recommended setting is **Auto**.

FlowCtrl: Check this box to enable flow control on the connection. This setting is only available in some modes.

Click **Apply** to save your settings.



Quality of Service

The **QoS Engine** improves your online gaming or streaming media experience by ensuring that your game or media traffic is prioritized over other network traffic, such as FTP or web.

Queue Management

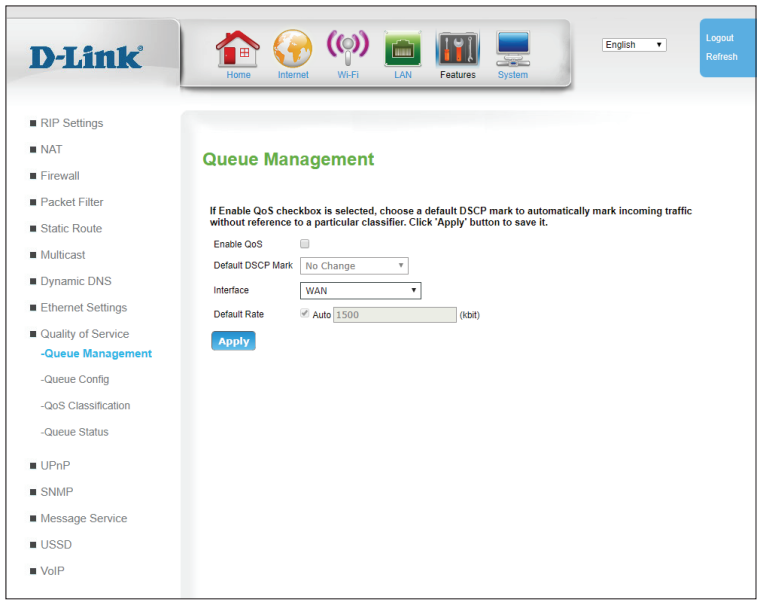
Enable QoS: Check this box to enable the QoS engine.

Default DSCP Mark: Specify a default Differentiated Services Code Point (DSCP) mark for queues.

Interface: Select an interface to which the Queue settings will apply.

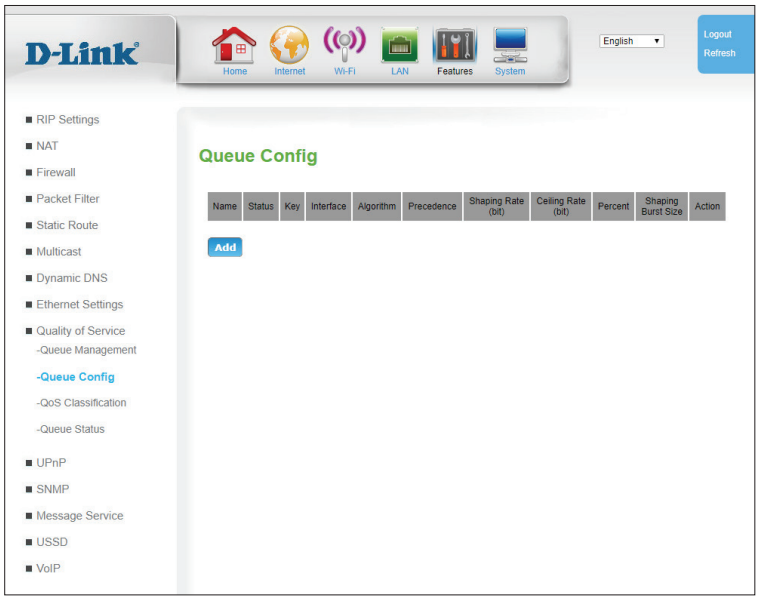
Default Rate: Specify a default rate in kilobits per second.

Click **Apply** to save your settings.



Queue Config

This screen lists all queues currently saved. Queues are assigned to specific network interfaces and assigned a precedence. The Queue entry can then be used by **QoS Classification** to direct ingress packets accordingly. This section is intended for network professionals and advanced users only, and can safely be ignored by a majority of users.



Name: Indicates the name of the queue.

Status: Indicates the status of the queue.

Key: Indicates the key or index of the queue.

Interface: Indicates the interface the queue applies to.

Algorithm: Indicates the algorithm employed by the queue.

Precedence: Indicates the precedent of packets sorted by the queue.

Shaping Rate (bit): Indicates the shaping rate set on the queue. -1 indicates no shaping.

Ceiling Rate (bit): Indicates the ceiling rate set on the queue.

Percent: Indicates the percent of total bandwidth assigned to the queue.

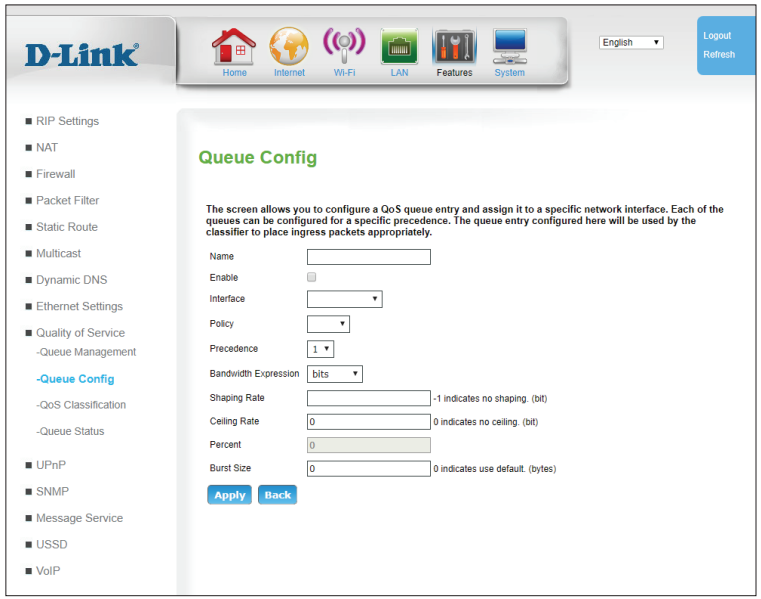
Shaping Burst Size: Indicates maximum burst size permitted in the queue.

Action: Click the pencil (✎) icon to edit the queue, click the trash can icon (🗑) to delete the queue. Select the **C** icon to clone the queue.

Add: Click **Add** to add a new queue, described in **Queue Config - Add** on page 86.

Queue Config - Add

This screen allows you to create a new queue.



Name: Enter the name of the queue. This is for user reference only, and does not affect functionality.

Enable: Check this box to enable the queue.

Interface: Specify the interface this queue will apply to from the dropdown menu.

Policy: Select whether the queue will employ Strict Priority (**SP**) or Weighted Fair Queuing (**WFQ**).

Precedence: Select the precedence from 1-8. A lower value indicates higher priority.

Bandwidth Expression: If you have selected a **WFQ** policy, specify if bandwidth will be expressed as a percentage over overall bandwidth or as an absolute bit rate.

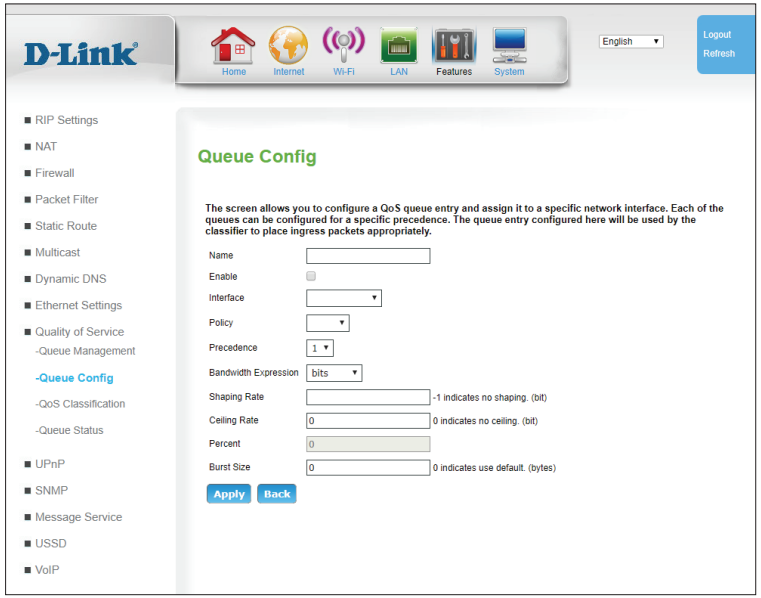
Shaping Rate (bit): If you have selected **bits** for bandwidth expression, enter a shaping rate in bits to specify a maximum bandwidth for the queue. Indicates the shaping rate set on the queue. -1 indicates no shaping.

Ceiling Rate (bit): If you have selected **bits** for bandwidth expression, specify a ceiling rate. The ceiling rate is the maximum bandwidth while bursting.

Percent: If you have selected **percent** for bandwidth expression, specify the percent of total bandwidth assigned to the queue.

Shaping Burst Size: If you have selected **percent** for bandwidth expression, specify the maximum burst size permitted in the queue. The maximum burst size is the total number of bytes permitted to be transferred at burst speeds.

Click **Apply** to save your settings or **Back** to return to the previous page without saving.



QoS Classification

QoS classes are subfilters that feed into the larger QoS Queues.

Class Name: Indicates the name of the queue. This is for user reference only, and does not affect functionality.

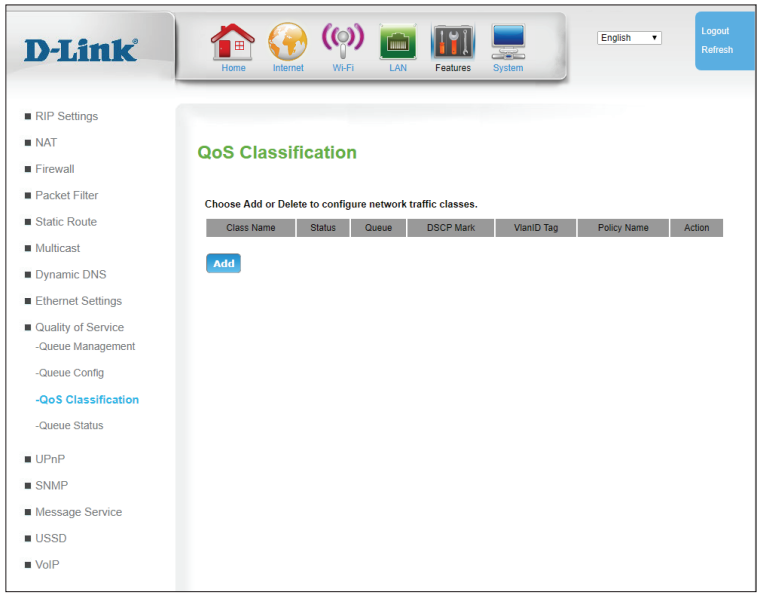
Status: Indicates the current status of the class.

Queue: Indicates which the queue to which the class forwards packets..

DSCP Mark: Indicates the Differentiated Services Code Point (DSCP) mark used in the class

VlanID Tag: Indicates the VLAN ID of the class.

Policy Name: Indicate the policy or algorithm used in the class.

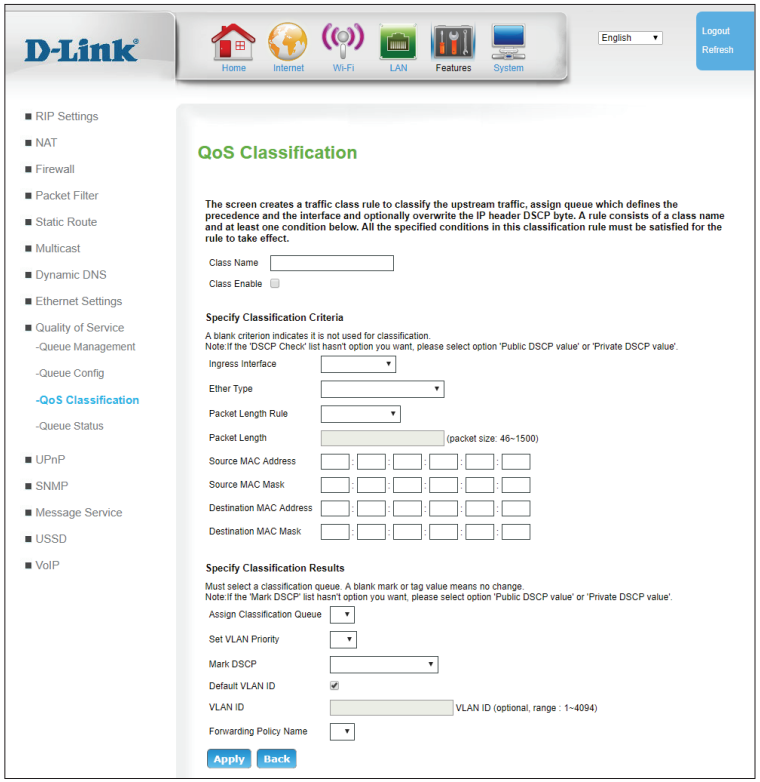


Action: Click the pencil (✎) icon to edit the queue, click the trash can icon (🗑) to delete the queue. Select the **C** icon to clone the queue.

Add: Click **Add** to add a new QoS class, described on **QoS Classification - Add** on page <OV>.

QoS Classification - Add

QoS classes are subfilters that feed into the larger QoS Queues.



Class Name: Enter the name of the queue. This is for user reference only, and does not affect functionality.

Class Enable: Check this box to enable the queue.

Ingress Interface: Specify the inbound interface to which classification will apply.

Ether Type: Select an Ether Type from the dropdown menu. Depending on the type selected, the other options on this page may change.

Packet Length Rule: Specify whether the class will be triggered by a packet length of **Greater than**, **Less than**, or **Equal to** the length specified in **Packet Length**.

Packet Length: Enter a packet length in bytes between 46 and 1500 that will trigger the above classification.

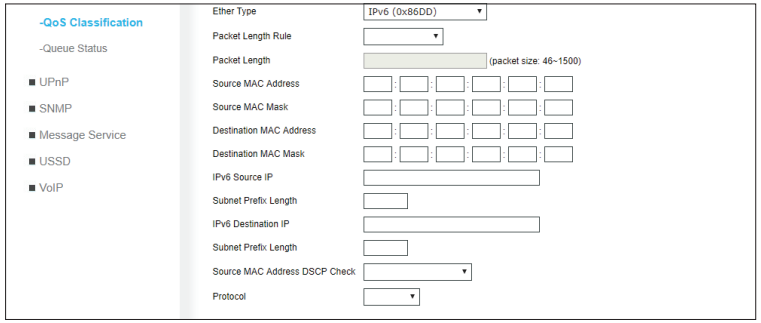
Source MAC Address: Enter a source MAC address to which the class will apply. (Optional)

Source MAC Mask: Specify the MAC Mask used to filter MAC addresses. (Optional)

Destination MAC Address: Enter a destination MAC address to which the rule will apply. (Optional)class

Destination MAC Mask: Specify the MAC Mask used to filter MAC addresses. (Optional)

If Ether Type is set to IP or IPv6:



Source IP/ Vendor Class/ User Class: Specify whether the class will be applied to the **Source IP**, **Vendor Class,** or **User Class** from the drop-down manu, and then enter the corresponding value.
If **Ether Type** has been set to **IPv6**, enter the source IPv6 address. (Optional)

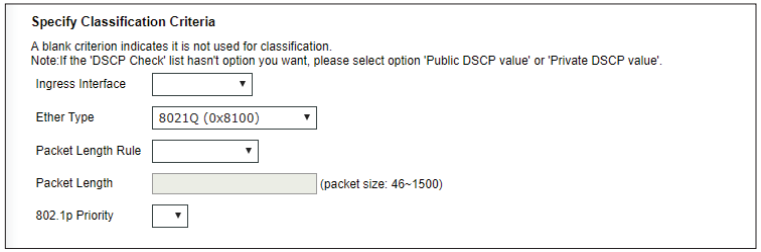
Destination IP/IPv6 Destination IP: Specify a destination IP address to which the class will be applied. (Optional)

Subnet Mask/ Subnet Prefix Length: Enter an destination mask/subnet prefix length to which the rule will apply. (Optional)

Source MAC Address DSCP Check: Specify a Differentiated Services Code Point (DSCP) for the source MAC address. (Optional)

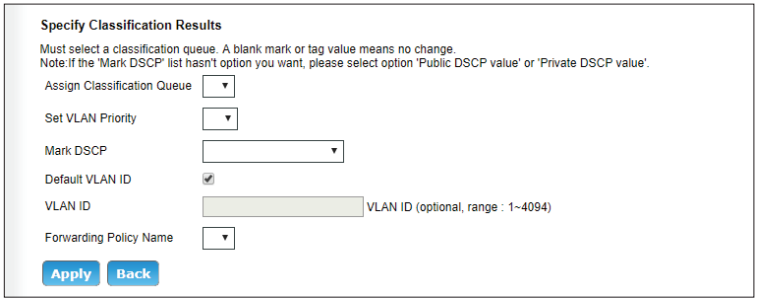
Protocol: Select a protocol from the list to classify. If you select **TCP** or **UDP**, additional options will appear. (Optional)

If Ether Type is set to 8021Q:



802.1p Priority: Enter the priority code point assigned to filtered frames. 1 is lowest priority, 0 is default priority, and 2-7 are increasing priority, with 7 being highest. (Optional)

Specify Classification Results:



Assign Classification Queue: For packets that trigger this classification, specify in which queue they should be placed. (Required)

Set VLAN Priority: For classified packets, specify the VLAN priority. (Optional)

Mark DSCP: For classified packets, specify if they should be marked with DSCP. (Optional)
Note: If the default dropdown list does not contain the required value, select **Public DSCP value** or **Private DSCP value** to toggle additional options in the dropdown menu.

Default VLAN ID: Check this box to specify classified packets be tagged with the default VLAN ID. If this box is unchecked, specify the VLAN ID in the box below. (Optional)

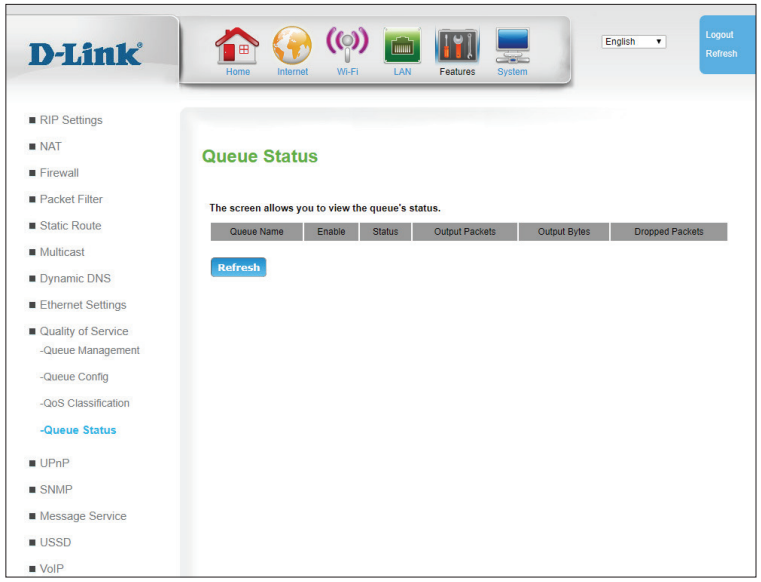
VLAN ID: If **Default VLAN ID** is not checked, specify the VLAN ID for classified packets. (Optional)

Forwarding Policy Name: Select a forwarding policy from the dropdown box. (Optional)

Click **Apply** to save your settings, or click **Back** to return to the previous screen.

Queue Status

The Queue Status screen lists the current status of each queue.



Queue Name: Indicates the name of the queue.

Enable: Indicates whether the queue is enabled (**True**) or disabled (**False**).

Status: Indicates the status of the queue.

Output Packets: Indicates the number of packets output from the queue.

Output Bytes: Indicates the number of bytes output from the queue.

Dropped Packets: Indicates the number of dropped packets.

Click **Refresh** to refresh this list.

UPnP

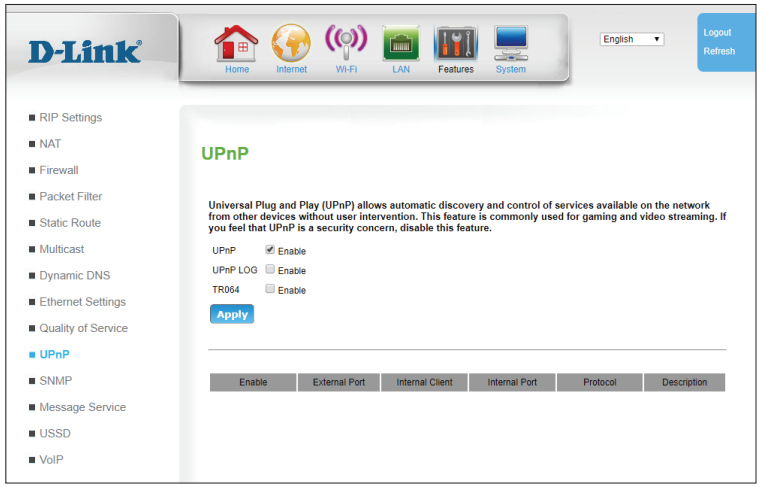
UPnP (Universal Plug and Play) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. UPnP broadcasts are only allowed on the LAN. UPnP is often used for popular audio visual software. It allows automatic discovery of your device in the network. If you are concerned about UPnP security, you can disable it.

UPnP Check this box to enable Universal Plug and Play (UPnP).

UPnP LOG: Check this box to enable logging of UPnP activity.

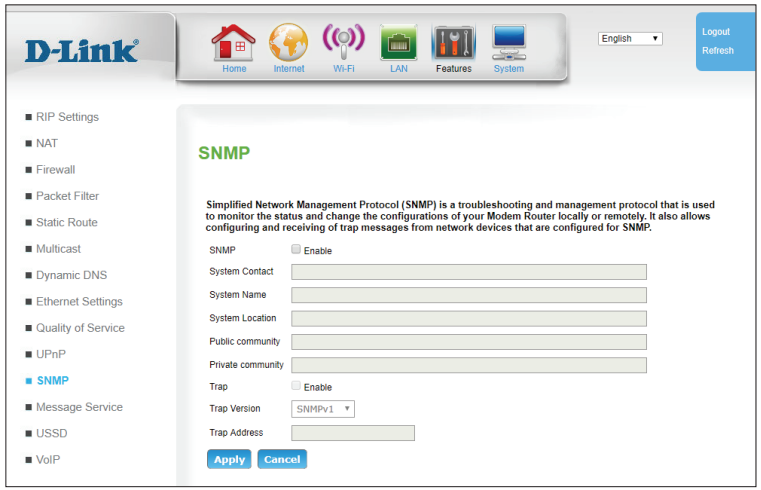
TR064: TR-064 is used by service providers to automatically update and configure end-user equipment. Check this box to enable it.

Click **Apply** to save your settings.



SNMP

SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol that reports activity on each network device to the administrator of the network. SNMP can be used to monitor traffic and statistics of the DWR-956. The DWR-956 supports SNMP v1 and v2c.



SNMP: Check this box to enable SNMP.

System Contact/ Name/ Location: Enter contact and reference information. This information is for reference only and will be displayed when administering the router over SNMP.

Public community: Enter the password **public** in this field to allow read-only access to network administration using SNMP. You can view the network, but no configuration is possible with this setting.

Private community: Enter the password **private** in this field to enable read/write access to the network using SNMP.

Trap: Traps are short messages sent to remote controllers about SNMP status. Check this box to enable them.

Trap Version: Specify **SNMPv1** or **SNMPv2c**.

Trap Address: Specify the IP address to which the traps will be sent.

Click **Apply** to save your settings.

Message Service

SMS Inbox

This page shows all messages that are stored on the SIM card. Select a message to display its contents in the SMS window. After you read it, you can delete it, or reply to the sender. Click the Refresh button to update the list.

Delete: Click this button to go to the first page.

Reply: Click this button to go to the previous page.

Forward: Click this button to go to the next page.

Refresh: Click this button to go to the last page.

Create Message

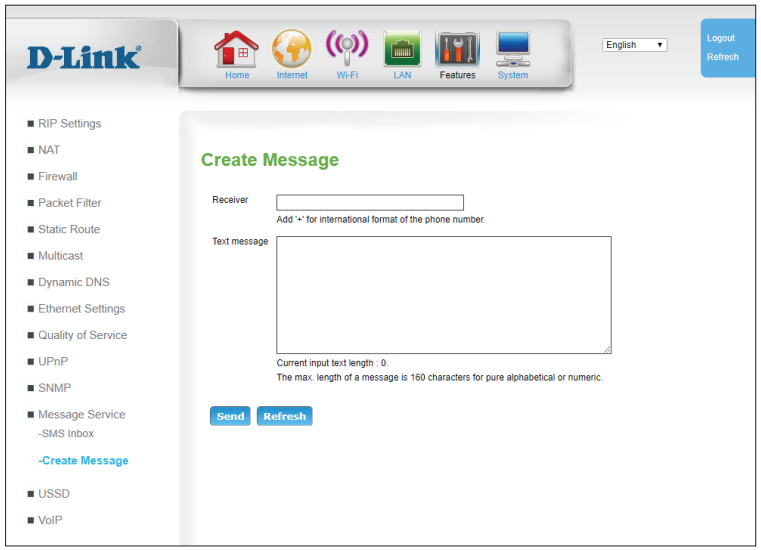
This page allows you to send SMS messages.

Receiver: Type in the phone number of the person you want to send your message to.

Text Message: Type in your message here.

Send: Click this button to send the message.

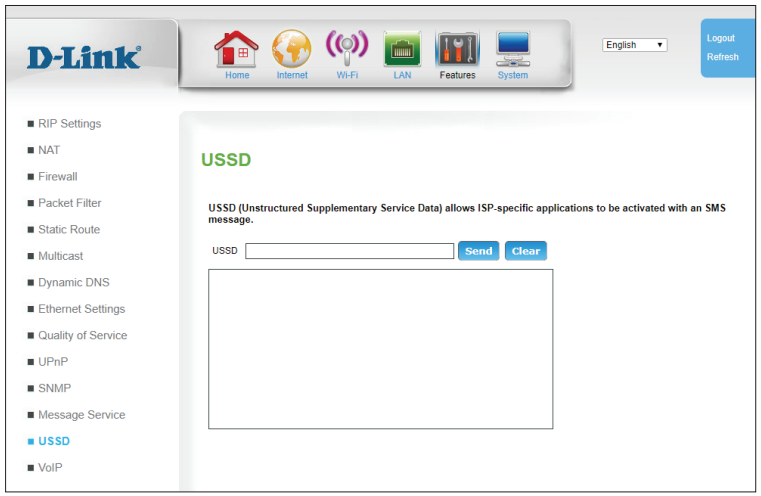
Refresh: Click this button to go to refresh the page.



USSD

Unstructured Supplementary Service Data (USSD) allows ISP-specific applications to be activated with an SMS message.

USSD: Enter an application activation code and click **Send**. This will allow you to activate applications by sending an SMS message to your ISP.



VoIP
SIP Setting

This section will allow you to configure advanced VoIP (Voice over Internet Protocol) settings. Most users can safely ignore this section. Your ISP or VoIP service should provide you with this information. Please check with your phone provider, or leave the settings at their defaults if you are not sure.

SIP Account

SIP is a VoIP protocol, a networking language which allows your VoIP devices and servers to communicate with one another.

Account: Enable or disable this account.

Display: Display name on the IP phone.

Number: The number is your user name.

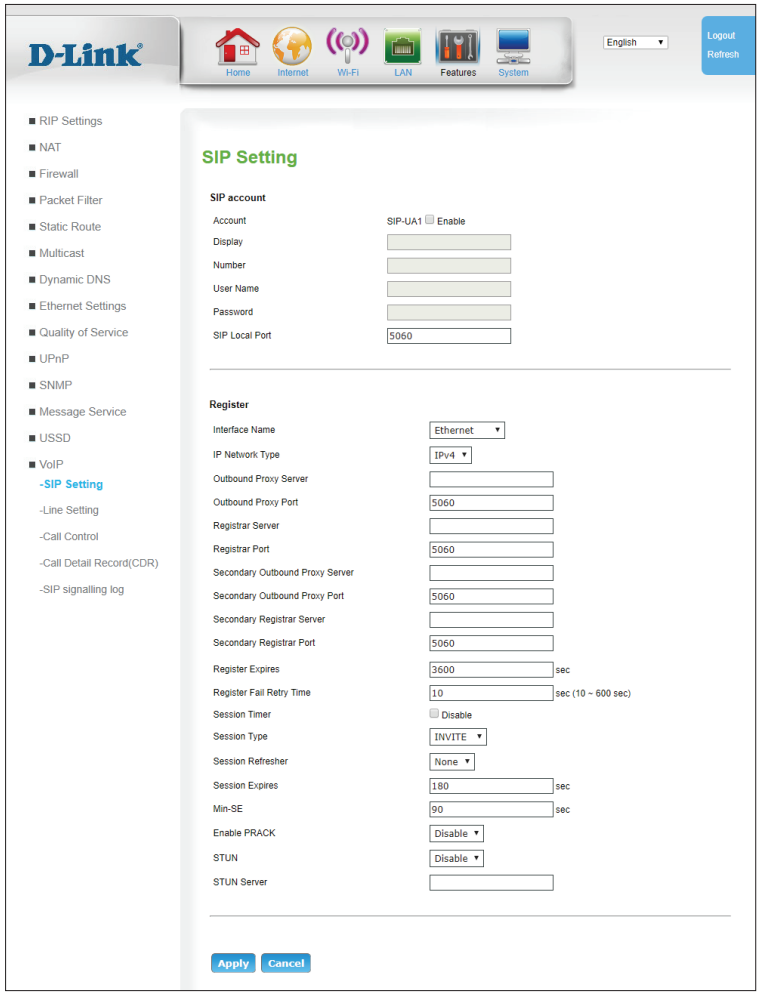
User Name: Name used to access SIP server.

Password: Password to access SIP server.

SP Local Port: Specify the local SIP initiation port. The default port is 5060.

Register

Enter the information of the primary VoIP registration servers in these sections. This information should be provided by your VoIP provider.



Line Setting

Here you can see your Line Settings for your VoIP line. Please check with your phone provider for the correct settings.

Line 1 Settings

TX Gain: Increase or decrease the transmitting power.

RX Volume: Increase or decrease the receiving sensitivity.

Anonymous: If **Disable** is selected, the full URI and name will be sent to the receiver's phone when the user makes a phone call. The URI and name of the caller are displayed on the receiver's phone. When **Enable: Full URI** is selected, only the user name will be displayed on the receiver's phone when the user makes a phone call. When **Enable: Display Name** is selected, only the name is displayed on the receiver's phone when the user makes a phone call.

Anonymous Reject: Select Enable to reject anonymous calls.

Do Not Disturb: Reject all incoming calls.

Call Forward: Check **No Answer** to enable call forward to another number when no one answers the phone.
Check **Busy** to enable call forward to another number when the user is busy on the phone.
Check **Unconditional** to transfer all incoming calls to another number.
Enter the call forwarding number in the text boxes.

Call Forward Timer(sec): Set the call forwarding timer in seconds.

Call Waiting: Enable or disable call waiting.

T38: Select Enable to enable T.38 for fax over IP.

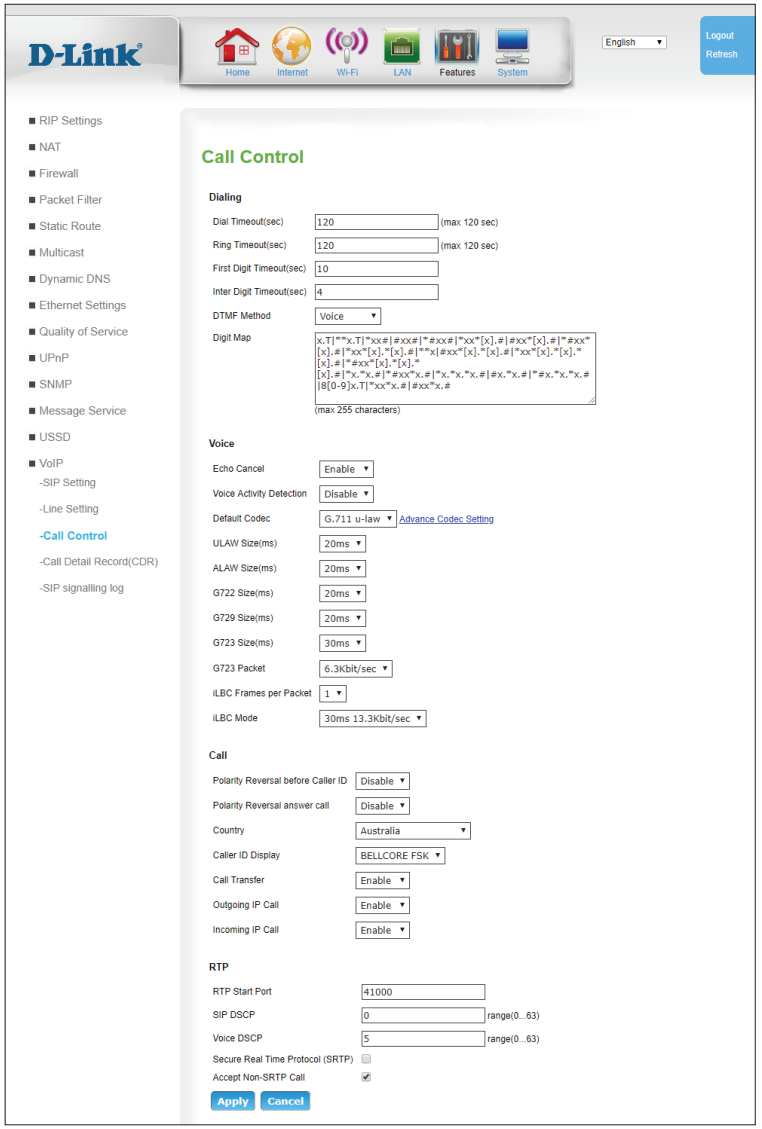
Hot Line: Check to enable Hot Line. Type a number into the text field.

DTMF Supplementary service codes

User can define a dialer code to use for the services listed.

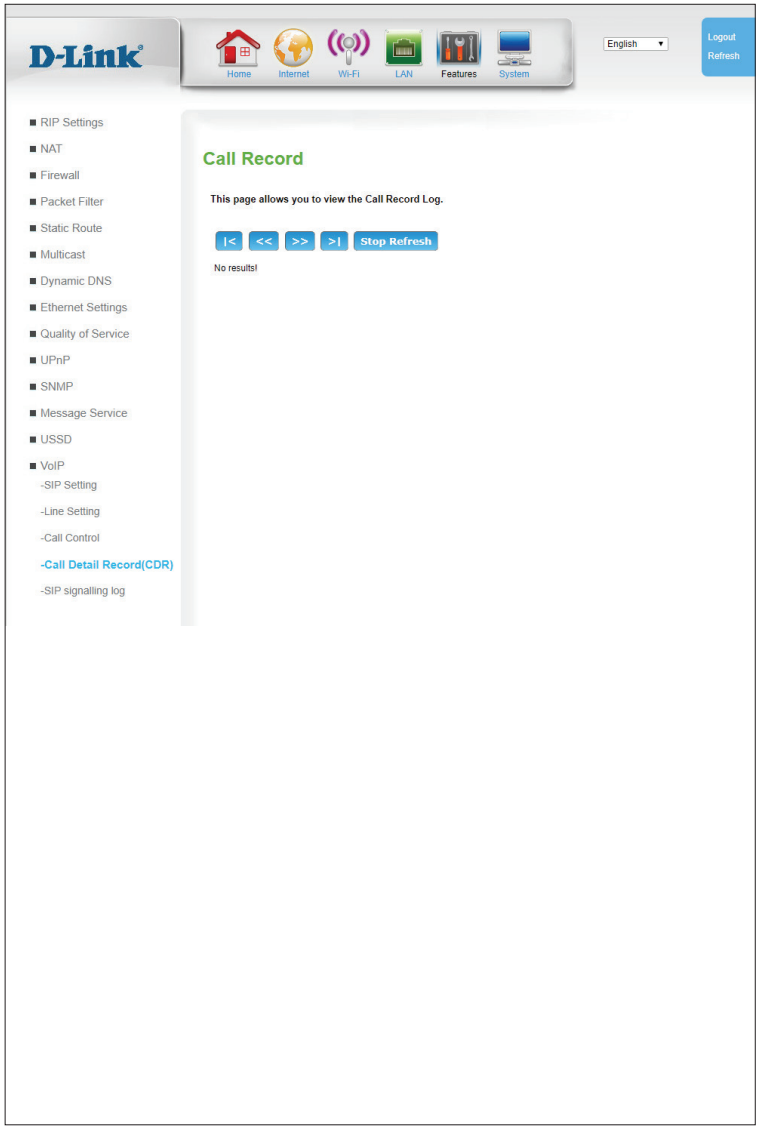
Call Control

Here you can see the Call Control settings for the VoIP function. Please check with your phone provider for the correct settings.



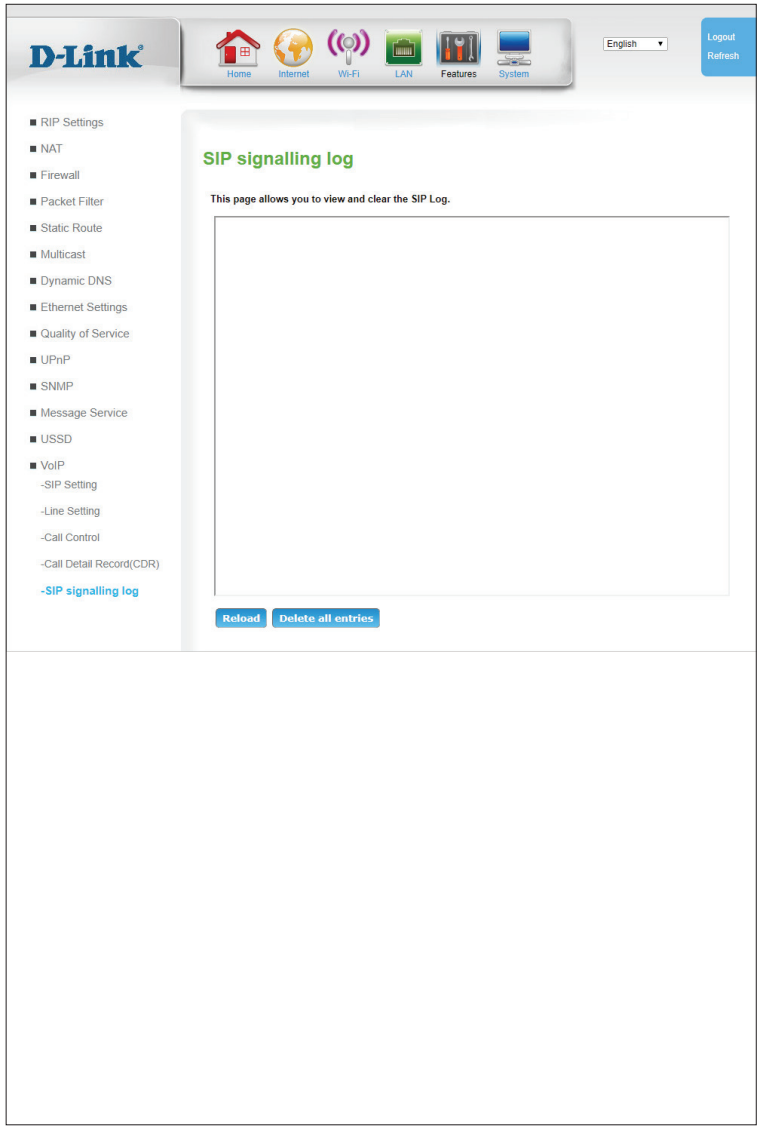
Call Record

The call record log keeps a record of all the phone activities.



SIP Signalling Log

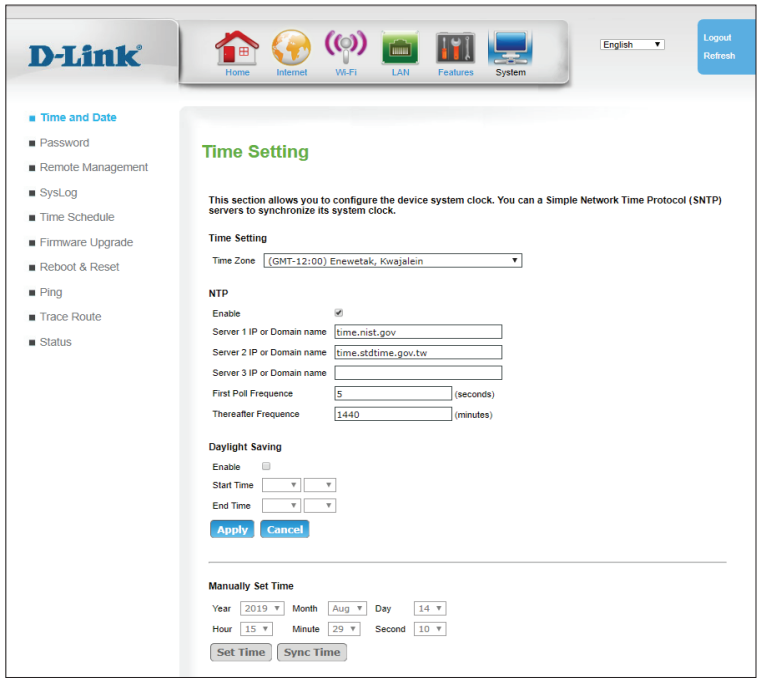
This page allows you to view and clear the SIP Signalling Log.



System

Time Settings

This section will help you set the time zone that you are in and an NTP (Network Time Protocol) server to use. Daylight Saving can also be configured to adjust the time when needed.



Ethernet Interface

Time Zone: Select the appropriate **Time Zone** from the drop-down box.

NTP

Enable: Check the box to allow the router to use an NTP server to update the router's internal clock.

Server 1/2/3 IP or Domain name: Enter an NTP server to use for time synchronization, or use the drop-down box to select one.

First Poll Frequence: Specify the initial poll after connectivity established.

Thereafter Frequence: Specify the frequency of updates in minutes.

Daylight Saving

Enable: Check the box to allow for daylight saving adjustments.

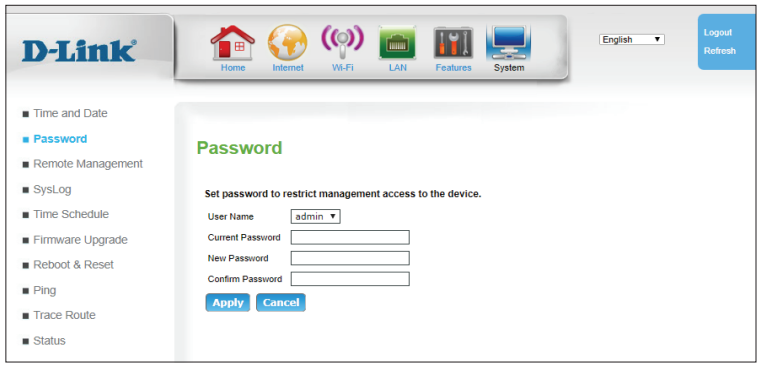
Start Time: Specify a start date for daylight saving time adjustments.

End Time: Specify an start date for daylight saving time adjustments.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Password

The **Password** page allows you to change the Administrator password. The admin has read/write access while users only have read-only access. Only the admin has the ability to change both admin and user account passwords.



User Name: Select a user name for which to edit the password.

Current Password: Enter the current password for the account.

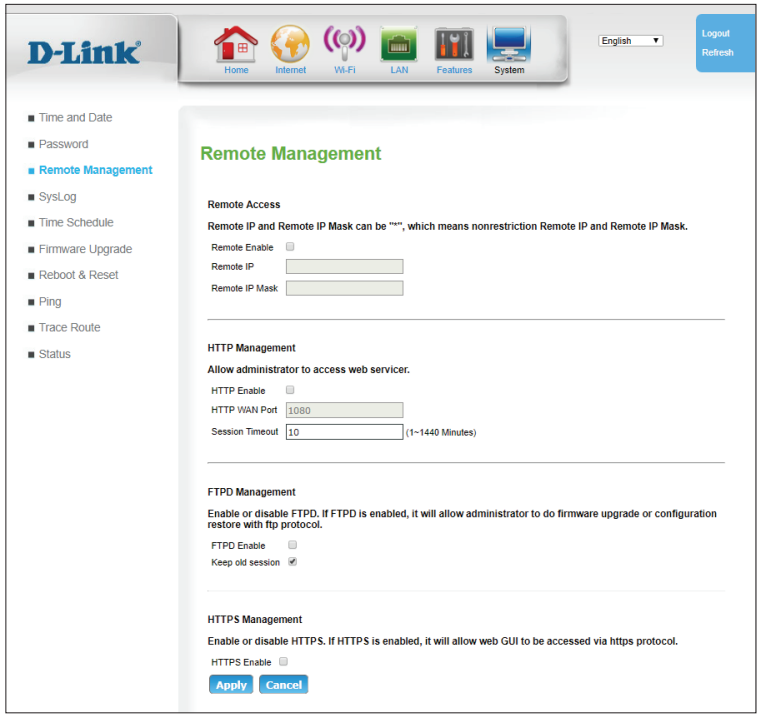
New Password: Enter the new password for the account.

Confirm Password: Confirm the new password for the account.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Remote Management

The Remote Management page allows configuration of the router from a remote location, usually over WAN.



Remote Access

Remote Enable: Check **Enable** to enable remote access.
Note: this setting could allow remote attackers to access your router. Use with caution.

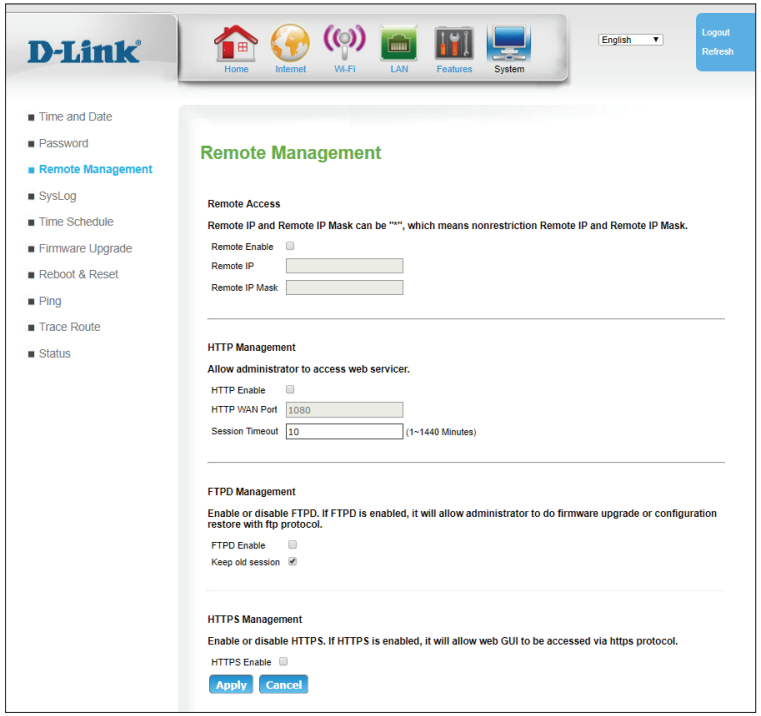
Remote IP: You can specify an authorized IP address for remote management. Packets appearing from other sources will be dropped. Enter an asterisk (*****) to allow remote access from any IP. Adding an asterisk (*) into this field could present a security risk and is not recommended.
Note: This method does not provide packet authentication, and provides only basic security.

Remote IP Mask: You can specify an authorized subnet mask for remote management. Packets appearing from other sources will be dropped. Enter an asterisk (*) to allow remote access from any mask. Adding an asterisk (*) into this field could present a security risk and is not recommended.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

Http Management

Http Enable: Check this check box to enable remote management. Remote management allows the DWR-956 to be configured over the Internet through a web browser. A username and password will still be required to access the web-management interface.



HTTP WAN Port: This is the port number used to access the router.

Session Timeout: Specify a time in minutes before the web interface will auto logout.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

FTPD Management

FTPD Enable: Check this box to enable the FTP Daemon for remote firmware updates.

Keep old session: Maintain previous sessions when new ones connect. Disabling this feature will allow only one FTP connection at a time.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

HTTPS Management

HTTPS Enable: Enables HTTPS access to the router.
Note that this does not disable unencrypted LAN access.

Click **Apply** to save your settings, or **Cancel** to revert to your previous settings.

SysLog

The DWR-956 keeps a running log of events and activities occurring on the router. You may download these logs as a file.

|<: Click this button to go to the first page.

<<: Click this button to go to the previous page.

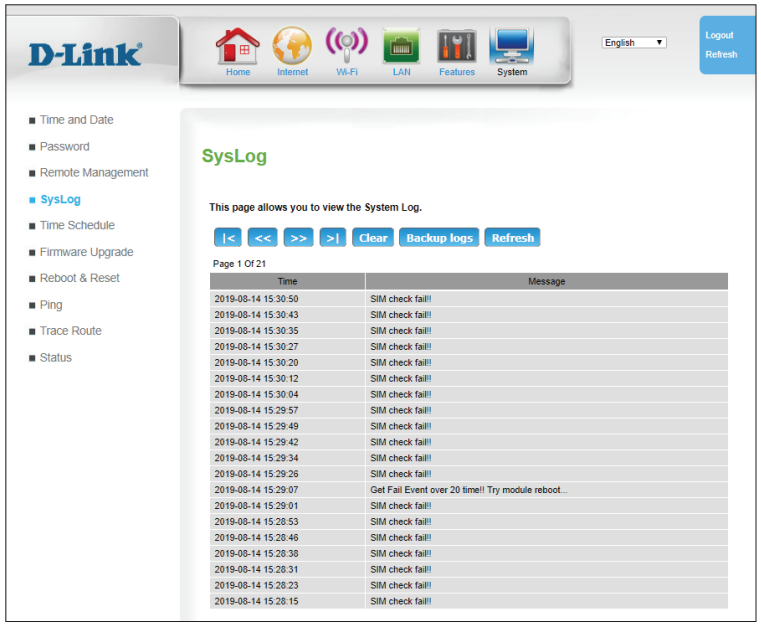
>>: Click this button to go to the next page.

>|: Click this button to go to the last page.

Clear: Click this button to clear the log.

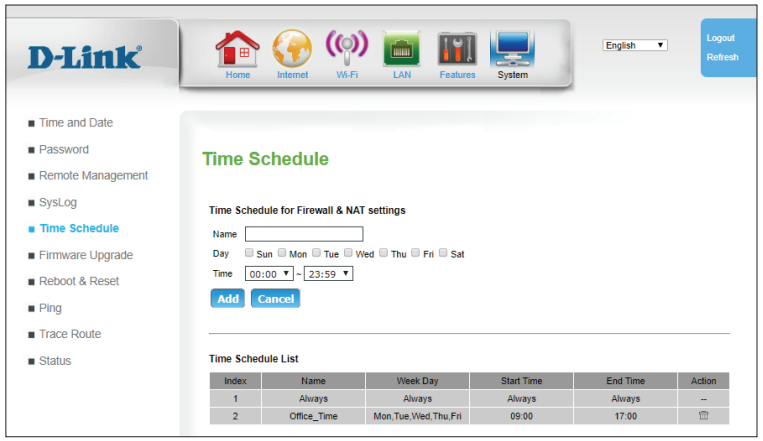
Backup Logs: Click this button to download the log.

Refresh: Click this button to refresh the current page.



Time Schedule

This section allows you to manage schedule rules for various firewall and parental control features. Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



Time Schedule for Firewall & NAT settings

Name: Enter a name for your new schedule.

Day: Select a day of the week for the start time and end time.

Time: Enter a start and end time for the schedule to apply. Note the settings use 24 hour time.

Click **Add** to create your schedule, or **Cancel** to revert to your previous settings.

Time Schedule List

Index: Indicates the index of the schedule.

Name: Indicates the name of your schedule.

Week Day: Indicates the day of the week for the start time and end time.

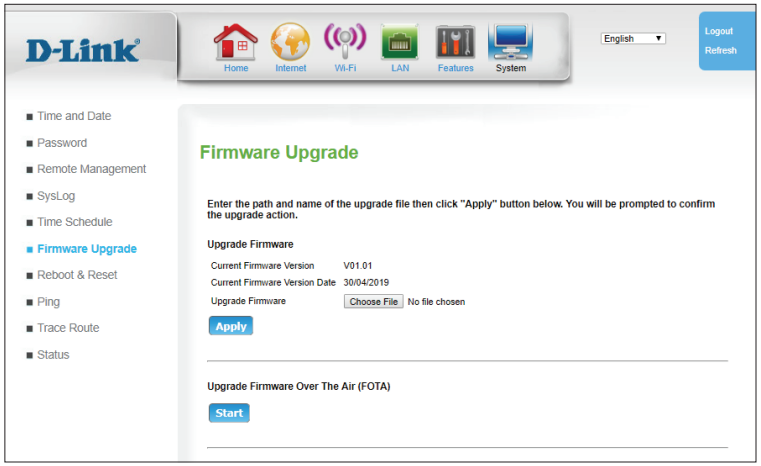
Star Time: Indicates the time when the schedule will become active.

End Time: Indicates the time when the schedule will become inactive.

Action: Click the trash can icon (🗑) to delete the schedule.

Firmware Upgrade

Here, you can upgrade the firmware of your router. Make sure the firmware you want to use is on the local hard drive of the computer and then click **Browse** to upload the file. You can check for and download firmware updates at the D-Link support site at **http://support.dlink.com**.



Upgrade Firmware

Current Firmware Version: Displays the current firmware version.

Upgrade Firmware: After you have downloaded a new firmware, click **Choose File** to locate the firmware on your computer, then click **Apply** to start the firmware upgrade.

Click **Apply** to start the firmware upgrade.

Upgrade Firmware by FOTA

Start: Click **Start** to begin the Firmware Over the Air (FOTA) upgrade process. Note that this requires an active Internet connection.

Reboot & Reset

Here, you can save the current system settings to a local hard drive.

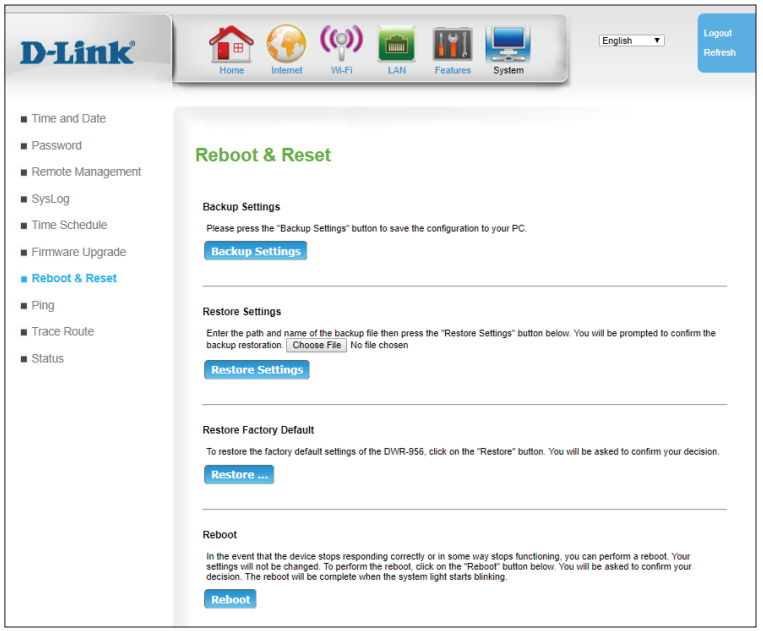
Time Schedule for Firewall & NAT settings

Backup Settings: Use this option to save your current router configuration settings to a file. Click **Backup Settings** to download your settings.

Restore Settings: Use this option to load previously saved router configuration settings. Click **Choose File** and select the saved file and then click the **Restore Settings** button to upload the settings to the router.

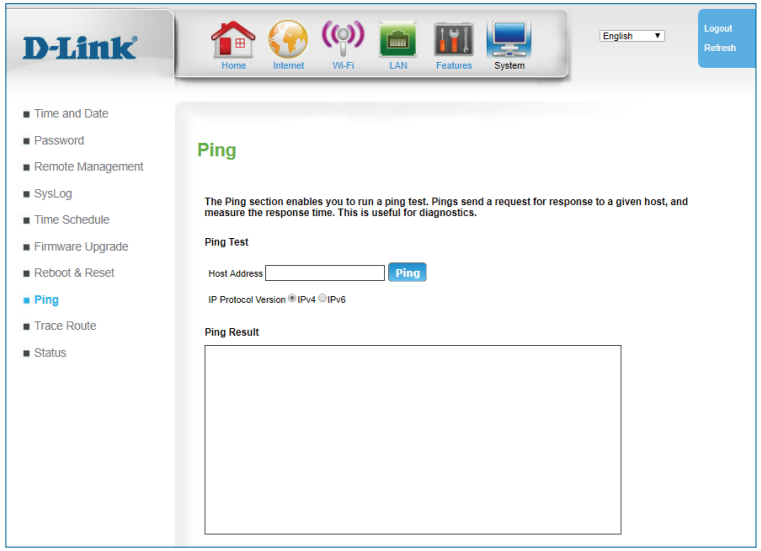
Restore Factory Default: This option will restore all settings back to their defaults. Any settings that have not been backed up will be lost, including any rules that you have created.

Reboot: This option will reboot the router.



Ping

The Ping section enables you to run a ping test. Pings send a request for response to a given host, and measure the response time. This is useful for diagnostics.



Ping Test

Host Address: Enter host name or IP address to be pinged. Click **Ping** to start the ping test, or click **Stop** to stop the ping.

IP Protocol Version: Specify whether the ping test will traverse **IPv4** or **IPv6**.

Ping Test

Ping Result: This section displays the result of the ping.

Trace Route

This feature allows you to run a traceroute. Traceroute tracks every node between your router and the destination IP. This is useful for diagnostics.

Trace Route

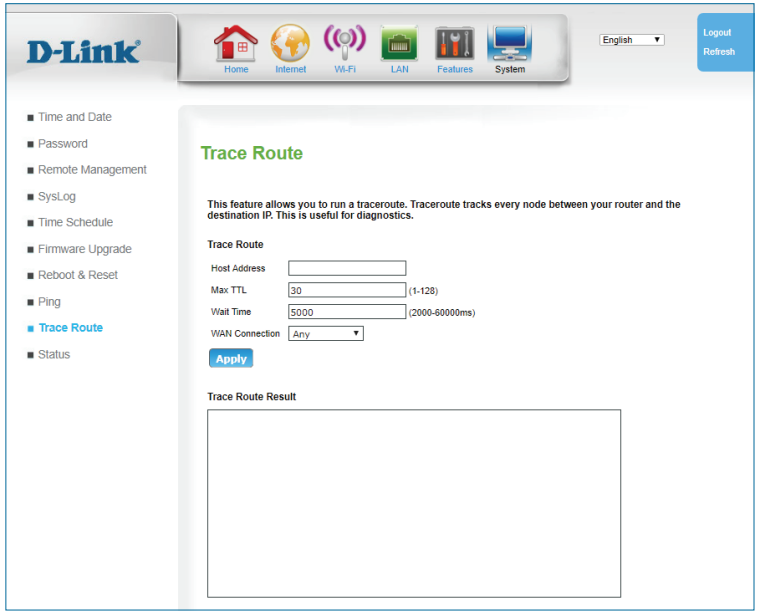
Host Address: Enter the host address to traceroute.

Max TTL: Specify a time to live (TTL) in hops from 1-125.

Wait Time: Enter a wait time in milliseconds. Nodes exceeding this limit will have their packets dropped.

WAN Connection: Specify a WAN interface over which the trace route will be run.

Click **Apply** to start the traceroute.



Trace Route Result

Trace Route Result: This section displays the results of the traceroute.

Status

Wireless 5G/2.4G Clients

This page displays a list of currently-connected wireless clients, their IP address, MAC addresses, and signal strength measured by received signal strength indicator (RSSI). This screen refreshes itself automatically unless you click **Stop Refresh**.

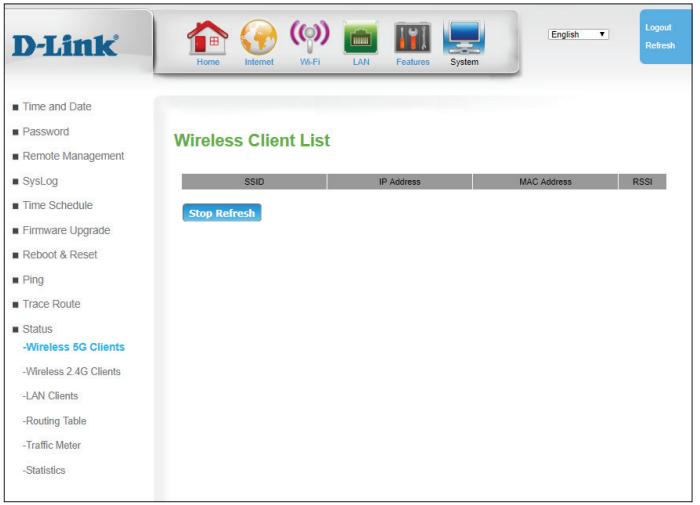
SSID: Indicates which SSID the device is connected to.

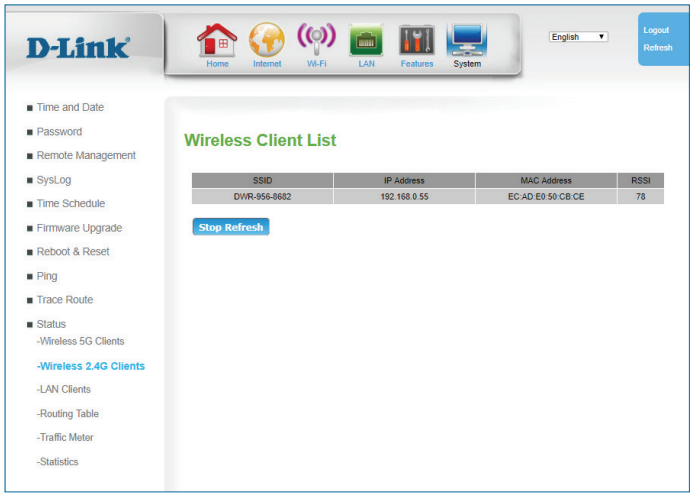
IP Address: Indicates the IP address of the client.

MAC Address: Indicates the MAC address of the client

RSSI: Indicates signal strength measured by received signal strength indicator (RSSI). In this case, higher numbers indicate stronger signal.

Stop Refresh: This screen refreshes automatically unless you click **Stop Refresh**.





LAN Clients

This page displays the details of connected Ethernet clients. This screen refreshes itself automatically unless you click **Stop Refresh**.

Host Name: Indicates the host name of the client, if applicable.

IP Address: Indicates the IP address of the client.

MAC Address: Indicates the MAC address of the client

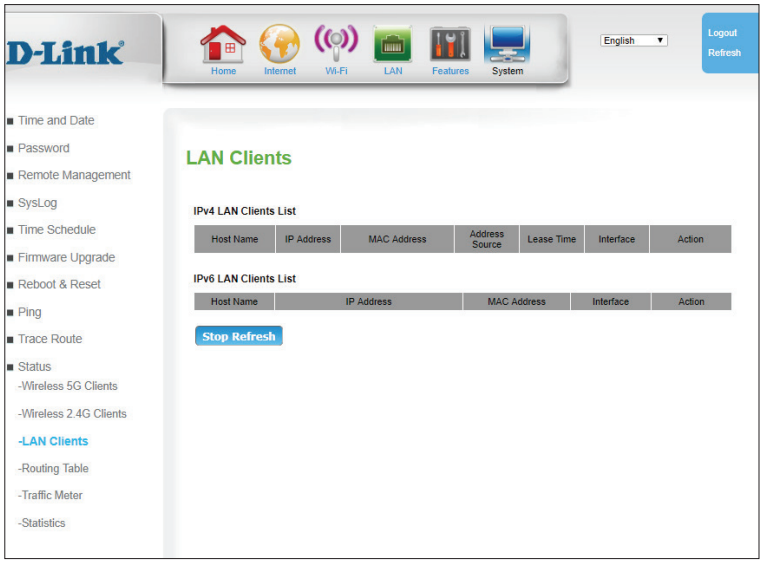
Address Source (IPv4 Only): Indicates the source of the address (DHCP, static, etc...).

Lease Time: Indicates the lease time in minutes.

Interface: Indicates the interface over which the connection is established

Action: Click the trash can icon (🗑) to delete inactive IP entries.

Stop Refresh: This screen refreshes automatically unless you click **Stop Refresh**.



Routing Table

This page displays the current routing table. This screen refreshes itself automatically unless you click **Stop Refresh**.

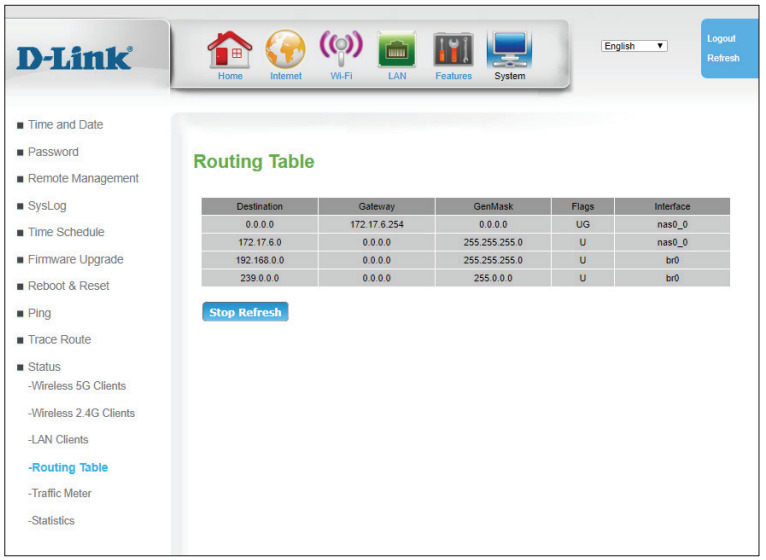
Destination: Indicates the destination IP of the route.

Gateway: Indicates the gateway used by the route.

GenMask: Indicates the subnet mask of the destination IP.

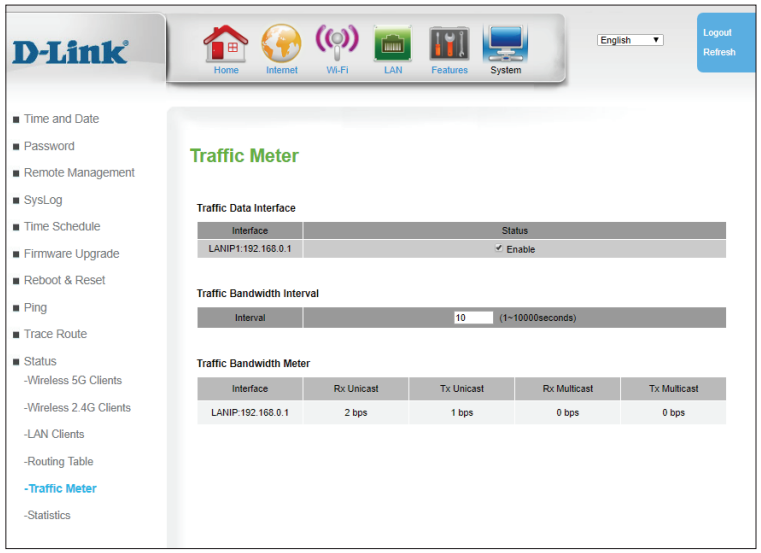
Flags: Indicates any flags used on this route.

Interface: Indicates the interface over which the route exits the router.



Traffic Meter

This page displays the meters for data traffic across all the devices connected to the router.



Traffic Data Interface

Interface: Indicates the physical interface and IP address of the devices being metered.

Status: Check this box to enable metering of the selected device.

Traffic Bandwidth Interval

Interval: Specify the update interval in seconds.

Traffic Bandwidth Meter

Interface: Indicates which interface is being metered.

Rx Unicast: Indicates received unicast data rates in bits per second.

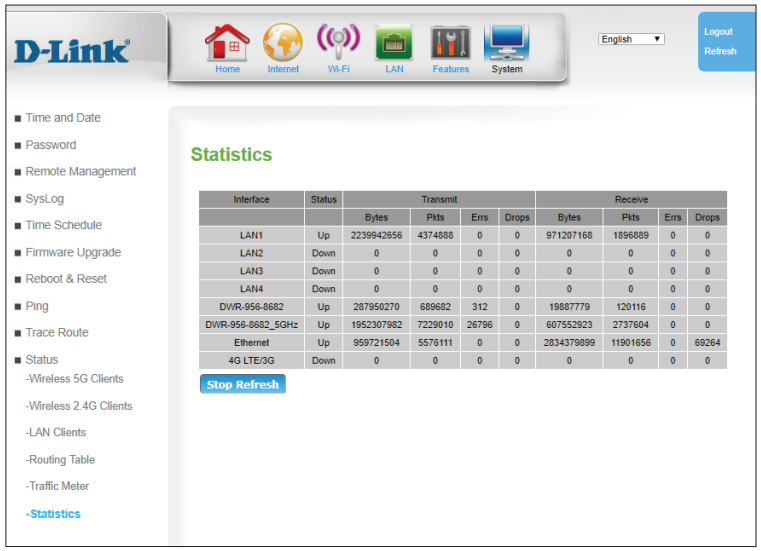
Tx Unicast: Indicates transmitted unicast data rates in bits second.

Rx Multicast: Indicates received unicast data rates in bits per second.

Tx Multicast: Indicates received unicast data rates in bits per second.

Statistics

This page displays packet totals for each interface on the router. All information is totalled since the router was last restarted.



Connect a Wireless Client to your Router

WPS Button

The easiest way to connect your wireless devices to the router is with WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DWR-956 router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the WPS button on the DWR-956 for about 6 seconds. The WLAN LED on the front will start to blink.

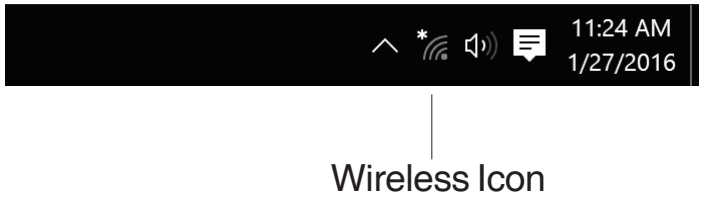
Step 2 - Within 2 minutes, press the WPS button on your wireless client (or launch the software utility and start the WPS process).

Step 3 - Allow up to 1 minute for your connection to be configured. Once the Internet light stops blinking, you will be connected and your wireless connection will be encrypted with WPA2.

Connecting to a Wireless Network
Windows® 10

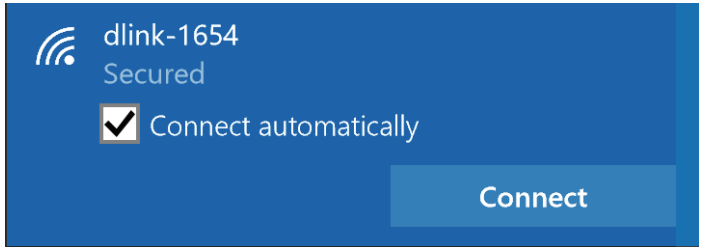
To connect to a wireless network using Windows 10, you will need to know the wireless network name (SSID) and Wi-Fi password (security key) of the device you are connecting to.

To join an existing network, locate the wireless network icon in the taskbar, next to the time display and click on it.



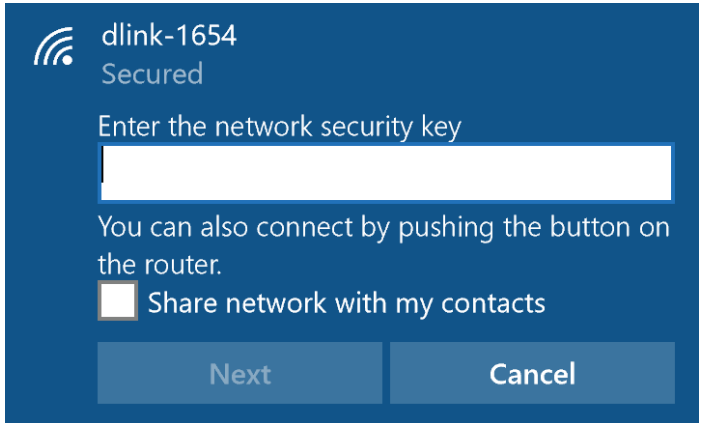
Clicking on this icon will display a list of wireless networks which are within range of your computer. Select the desired network by clicking on its SSID.

To connect to the network, click **Connect.**



To automatically connect when your device is in range, click the **Connect Automatically** check box**.** Your computer will now automatically connect to this wireless network whenever it is detected.

You will then be prompted to enter the Wi-Fi password (network security key) for the wireless network. Enter the password into the box and click **Next** to connect to the network.



You can also use Wi-Fi Protected Setup (WPS) to connect to the wireless network. Press the WPS button on your device and you will be automatically connected.

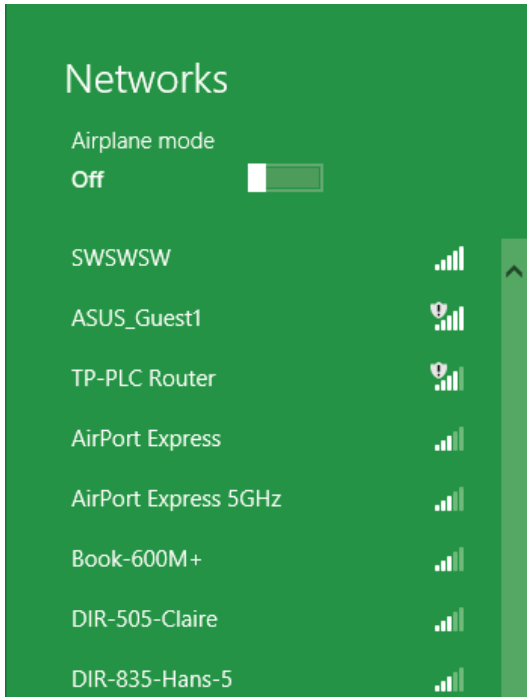
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as the one on the wireless router.

Windows® 8
WPA/WPA2

It is recommended that you 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 (Wi-Fi password) being used.

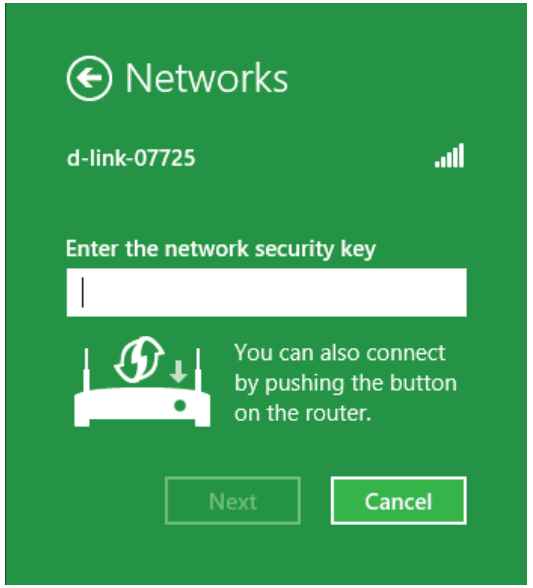
To join an existing network, locate the wireless network icon in the taskbar next to the time display.

Clicking on this icon will display a list of wireless networks that are within connecting proximity of your computer. Select the desired network by clicking on the network name.

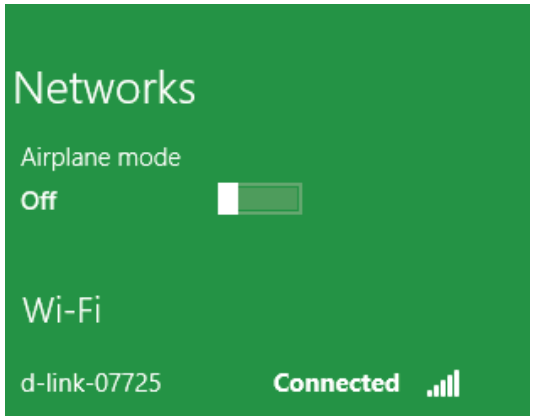


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

If you wish to use Wi-Fi Protected Setup (WPS) to connect to the router, you can also press the WPS button on your router during this step to enable the WPS function.



When you have established a successful connection to a wireless network, the word **Connected** will appear next to the name of the network to which you are connected to.



Windows® 7
WPA/WPA2

It is recommended that you 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.

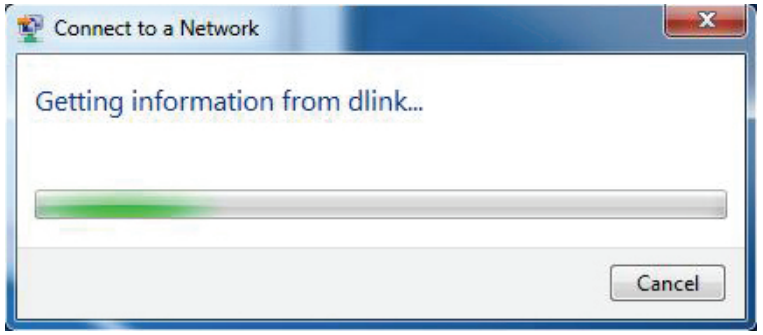
1. Click on the wireless icon in your system tray (lower-right corner).

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

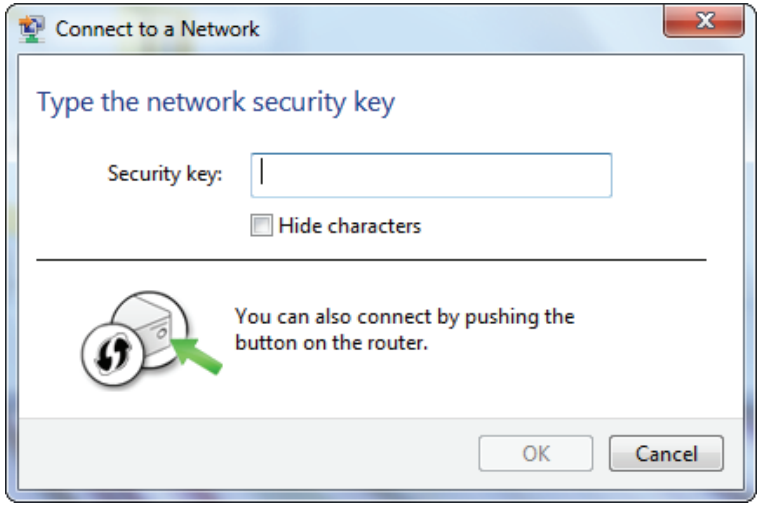
3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

   If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to **Networking Basics** on page 146 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 (Wi-Fi password) that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.

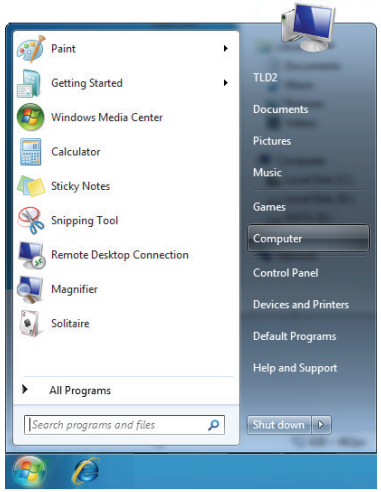


It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as the one on the wireless router.

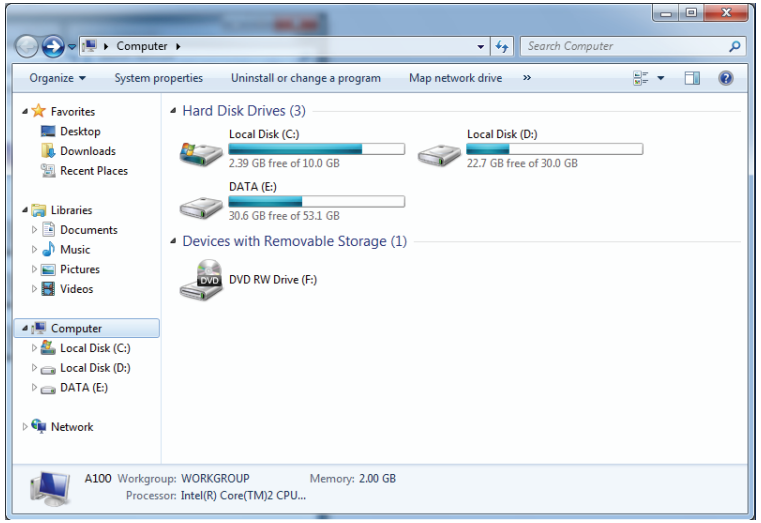
WPS

The WPS feature of the DWR-956 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

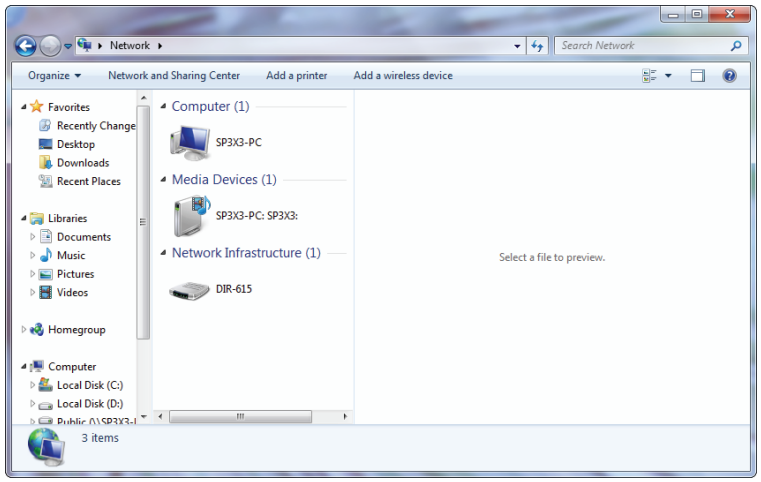
1. Click the **Start** button and select **Computer** from the Start menu.



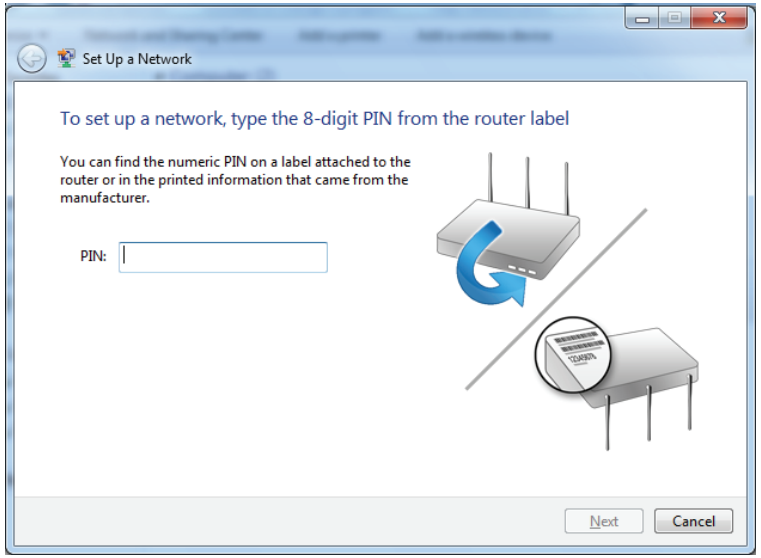
2. Click **Network** on the left side.



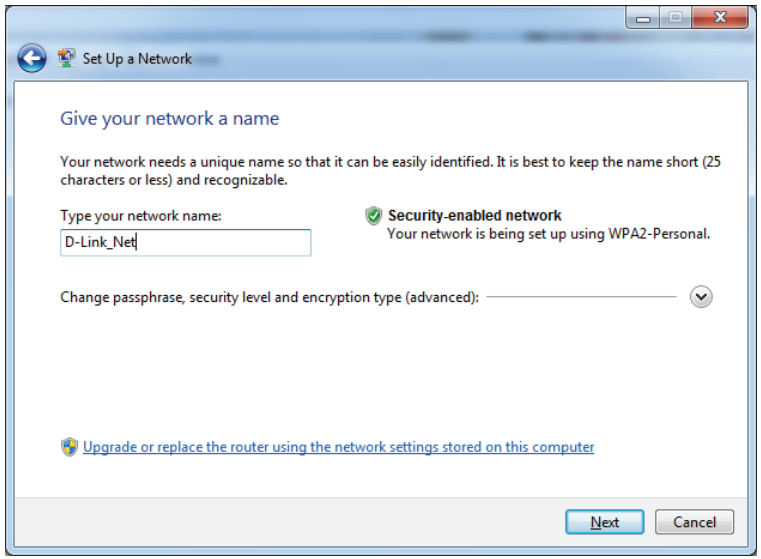
3. Double-click the DWR-956.



4. Input the WPS PIN number (on the router label) in the **Setup** > **Wireless Setup** menu in the Router's Web UI) and click **Next**.

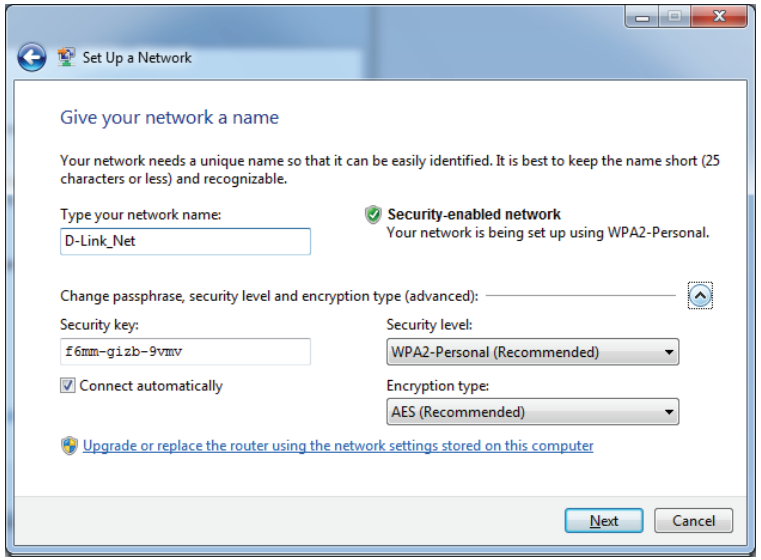


5. Type a name to identify the network.



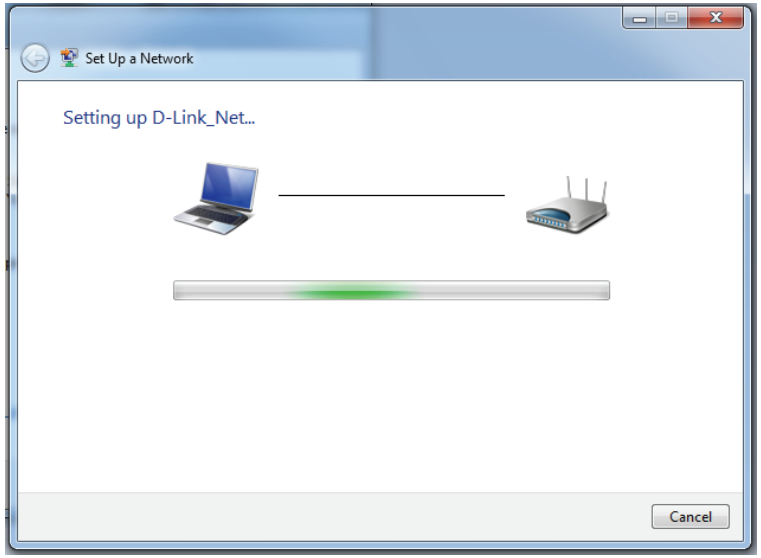
6. To configure advanced settings, click the icon.

Click **Next** to continue.



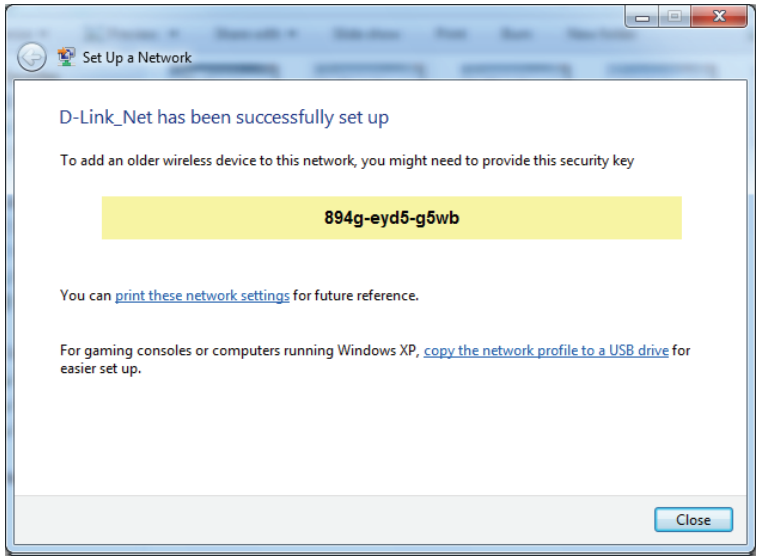
7. The following window appears while the router is being configured.

   Wait for the configuration to complete.



8. The following window informs you that WPS on the router has been set up 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.

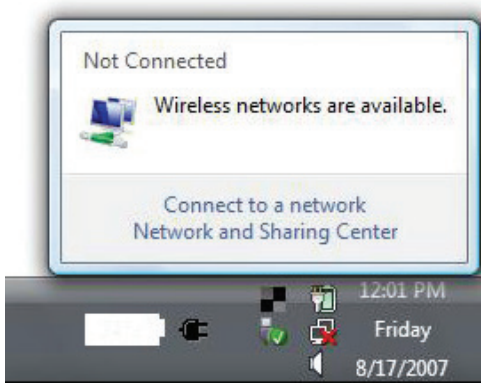
Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's wireless utility, please refer to the user manual of your wireless adapter for help connecting to a wireless network. Most wireless 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.

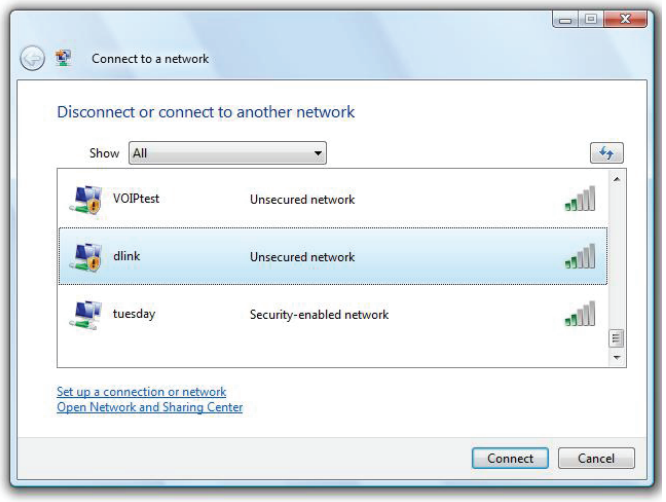
or

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 a network (displayed using the SSID) and click the **Connect** button.

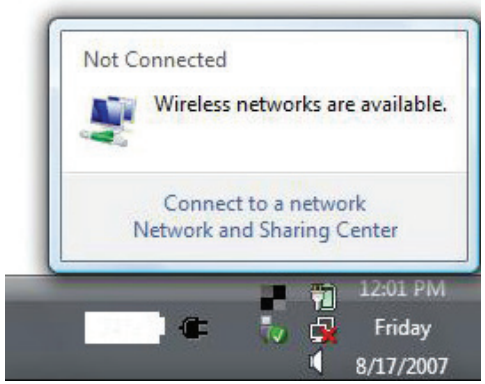
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



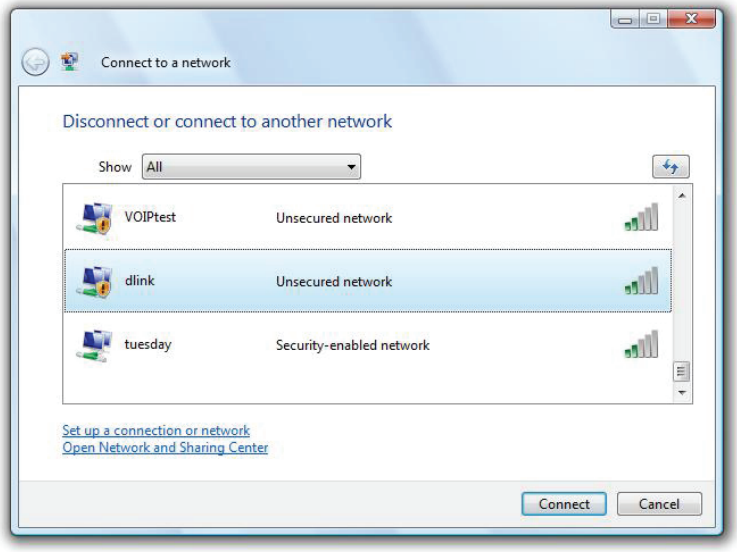
WPA/WPA2

It is recommended that you 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 Wi-Fi name (SSID) you would like to connect to and click **Connect**.



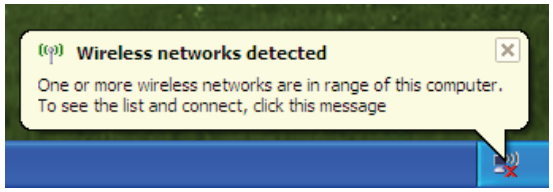
3. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**.

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 the one on the wireless router.

Windows® XP

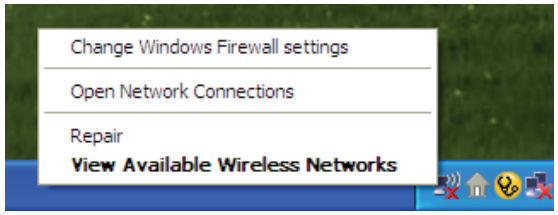
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities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



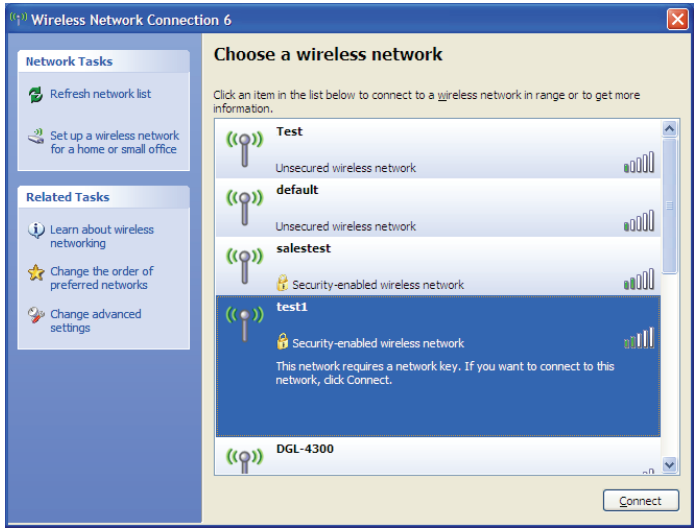
or

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 Wi-Fi network (displayed using the SSID) and click the **Connect** button.

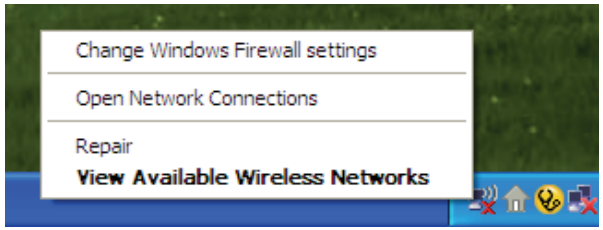
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



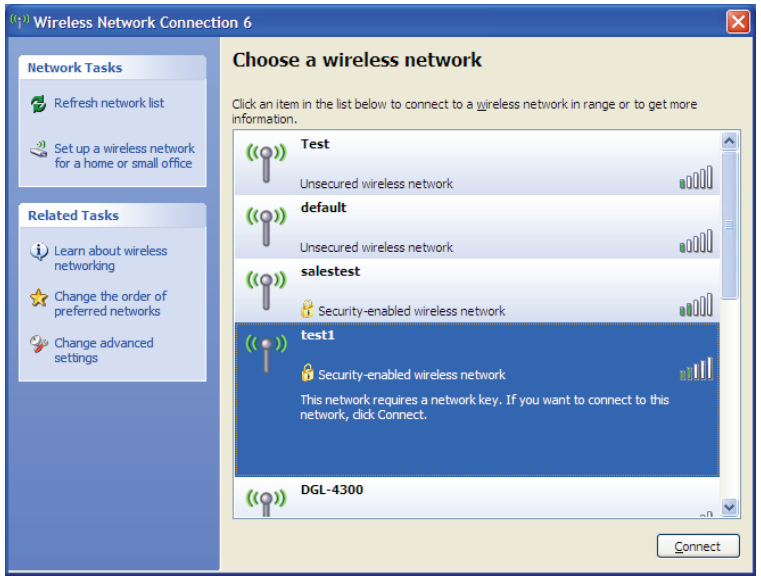
WPA/WPA2

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.

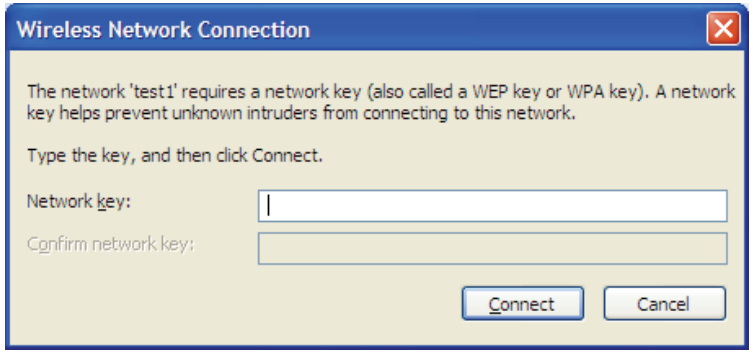
1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.



2. Highlight the Wi-Fi network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK Wi-Fi password 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 Wi-Fi password 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 DWR-956. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to these examples.

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

When entering the IP address of the D-Link 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® 7 or higher
  - Mozilla Firefox 3.5 or higher
  - Google™ Chrome 8 or higher
  - Apple Safari 4 or 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 ZoneAlarm, BlackICE, 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 D-Link 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.

2. What can I do if I forgot my password?

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

To reset the router, locate the reset button (hole) on the rear 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, leave the password box empty.

3. 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, XP, Vista®, and 7 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**

```
C:\>ping yahoo.com -f -l 1482

Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ping yahoo.com -f -l 1472

Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:

Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 93ms, Maximum =  203ms, Average =  132ms

C:\>
```

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:

- Navigate to the Internet configuration page (see **Internet** on page 10 for details).
- To change the MTU, enter the number in the MTU field and click **Apply** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

D-Link 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 D-Link wireless family of products will allow you to 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 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.

Why D-Link Wireless?

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

Wireless works similarly to how cordless phones work, through radio signals that 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 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, university 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. This 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, D-Link has a wireless solution for it.

Home Uses/Benefits

- 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 Uses/Benefits

- 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 D-Link CardBus Adapter with your laptop, you can access the hotspot to connect to the 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

Turn on WPA2 encryption on the router to help protect your wireless network from unwanted access by people close to your network, such as neighbors or intruders. Refer to the product manual for detailed 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 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 adapters. All the adapters must be in ad hoc mode to communicate.

Networking Basics

Check your IP address

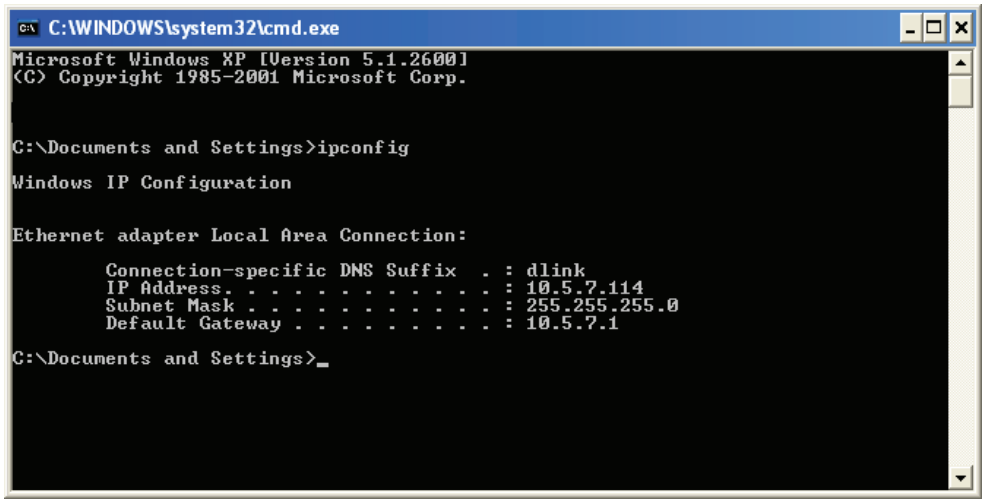
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

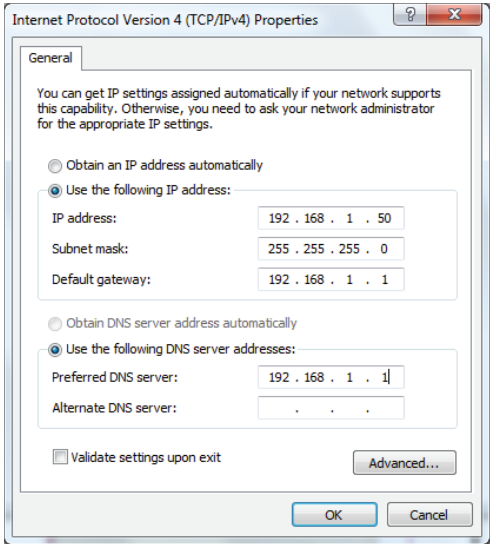
Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

Step 3

Highlight **Internet Protocol Version 4 (TCP/IPv4)** 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 192.168.1.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 the Default Gateway the same as the LAN IP address of your router (I.E. 192.168.0.1).

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

Step 5

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

Wireless Security

This section will show you the different levels of security you can use to help protect your data from intruders. The DWR-956 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

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. 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 stronger public-key encryption system so that only authorized network users should be able to 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. This is the technique typically used on home networks.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on an even stronger key encryption system to make it much more difficult for unauthorized network users to access the network. EAP is often used in corporate or university environments.

Technical Specifications

Cellular Bands[1]
- FDD-LTE: 2600/2100/1800/900/800/700 MHz (B1/3/7/8/20/28)
- UMTS: 2100/900 MHz (B1/8)
- GSM: 1800/900 MHz (B3/8)

Data Rates[2]
- Up to 866 Mbps with 802.11ac clients
- Up to 300 Mbps with 802.11n clients
- 6/9/11/12/18/24/36/48/54 Mbps in 802.11g mode
- 1/2/5.5/11 Mbps in 802.11b mode
- LTE Downlink: Up to 150 Mbps

Standards
- IEEE 802.11ac/n/g/b/a
- IEEE 802.3i
- IEEE 802.3u

Wireless Security
- 64 / 128-bit WEP (Wired Equivalent Privacy)
- WPA & WPA2 (Wi-Fi Protected Access)

Firewall
- Network Address Translation (NAT)
- Stateful Packet Inspection (SPI)

VPN
- L2TP/PPTP/IPSEC/VPN Pass-through

Antenna
- Two detachable 4G antennas

SIM/UICC Slot
- Standard Mini-SIM/UICC slot

Ports
- Four LAN ports (RJ-45)
- WAN port (RJ-45)
- Phone port (RJ-11)

LED Status Indicators
- Power
- Internet
- 5 GHz
- 2.4 GHz
- 4G
- 2G/3G
- LAN
- WAN
- Voice
- SMS
- Signal Strength

Dimensions
- 170 x 180 x 80 mm (6.7 x 7.1 x 3.15 in)

Operating Temperature
- 0 to 40 ˚C (32 to 104 ˚F)

Operating Humidity
- 10% to 90% (Non-condensing)

Certifications
- CE
- RCM

[1] Supported frequency band is dependent upon regional hardware version.
[2] Data rates are theoretical. Data transfer rate depends on network capacity, signal strength, and environmental factors.
[3] Maximum wireless signal rate derived from IEEE Standard 802.11ac/n/g/b/a 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.

Regulatory Information

CE EMI Class A Warning

This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

CE

	Frequency Band(s) **Frequenzband** **Fréquence bande(s)** **Bandas de Frecuencia** **Frequenza/e** **Frequentie(s)**	**Max. Output Power (EIRP)** **Max. Output Power** **Consommation d'énergie max.** **Potencia máxima de Salida** **Potenza max. Output** **Max. Output Power**
5 G	5.15 – 5.25 GHz	200 mW
	5.25 – 5.35 GHz	200 mW
	5.47 – 5.725 GHz	1 W
2.4 G	2.4 – 2.4835 GHz	100 mW

European Community Declaration of Conformity:

Česky [Czech]	Tímto D-Link Corporation prohlašuje, že tento produkt, jeho příslušenství a software jsou v souladu se směrnicí 2014/53/EU. Celý text ES prohlášení o shodě vydaného EU a o firmwaru produktu lze stáhnout na stránkách k produktu www.dlink.com.
Dansk [Danish]	D-Link Corporation erklærer herved, at dette produkt, tilbehør og software er i overensstemmelse med direktiv 2014/53/EU. Den fulde tekst i EU-overensstemmelseserklæringen og produktfirmware kan wnloades fra produktsiden hos www.dlink.com.
Deutsch [German]	Hiermit erklärt die D-Link Corporation, dass dieses Produkt, das Zubehör und die Software der Richtlinie 2014/53/EU entsprechen. Der vollständige Text der Konformitätserklärung der Europäischen Gemeinschaft sowie die Firmware zum Produkt stehen Ihnen zum Herunterladen von der Produktseite im Internet auf www.dlink.com zur Verfügung.
Eesti [Estonian]	Käesolevaga kinnitab D-Link Corporation, et see toode, tarvikud ja tarkvara on kooskõlas direktiiviga 2014/53/EL. Euroopa Liidu vastavusdeklaratsiooni täistekst ja toote püsivara on allalaadimiseks saadaval tootelehel www.dlink.com.
English	Hereby, D-Link Corporation, declares that this product, accessories, and software are in compliance with directive 2014/53/EU. The full text of the EU Declaration of Conformity and product firmware are available for download from the product page at www.dlink.com
Español [Spanish]	Por la presente, D-Link Corporation declara que este producto, accesorios y software cumplen con las directivas 2014/53/UE. El texto completo de la declaración de conformidad de la UE y el firmware del producto están disponibles y se pueden descargar desde la página del producto en www.dlink.com.
Ελληνική [Greek]	Με την παρούσα, η D-Link Corporation δηλώνει ότι αυτό το προϊόν, τα αξεσουάρ και το λογισμικό συμμορφώνονται με την Οδηγία 2014/53/ΕΕ. Το πλήρες κείμενο της δήλωσης συμμόρφωσης της ΕΕ και το υλικολογισμικό του προϊόντος είναι διαθέσιμα για λήψη από τη σελίδα του προϊόντος στην τοποθεσία www.dlink.com.
Français [French]	Par les présentes, D-Link Corporation déclare que ce produit, ces accessoires et ce logiciel sont conformes aux directives 2014/53/UE.Le texte complet de la déclaration de conformité de l'UE et le icroprogramme du produit sont disponibles au téléchargement sur la page des produits à www.dlink.com.
Italiano [Italian]	Con la presente, D-Link Corporation dichiara che questo prodotto, i relativi accessori e il software sono conformi alla direttiva 2014/53/UE. Il testo completo della dichiarazione di conformità UE e il firmware del prodotto sono disponibili per il download dalla pagina del prodotto su www.dlink.com.

Latviski [Latvian]	Ar šo uzņēmums D-Link Corporation apliecina, ka šis produkts, piederumi un programmatūra atbilst direktīvai 2014/53/ES. ES atbilstības deklarācijas pilno tekstu un produkta aparātprogrammatūru var lejupielādēt attiecīgā produkta lapā vietnē www.dlink.com.
Lietuvių [Lithuanian]	Šiuo dokumentu „D-Link Corporation“ pareiškia, kad šis gaminys, priedai ir programinė įranga atitinka direktyvą 2014/53/ES. Visą ES atitikties deklaracijos tekstą ir gaminio programinę aparatinę įrangą galima atsisiųsti iš gaminio puslapio adresu www.dlink.com.
Nederlands [Dutch]	Hierbij verklaart D-Link Corporation dat dit product, accessoires en software voldoen aan de richtlijnen 2014/53/EU. De volledige tekst van de EU conformiteitsverklaring en productfirmware is beschikbaar voor download van de productpagina op www.dlink.com.
Malti [Maltese]	Bil-preżenti, D-Link Corporation tiddikjara li dan il-prodott, l-aċċessorji, u s-software huma konformi mad-Direttiva 2014/53/UE. Tista' tniżżel it-test sħiħ tad-dikjarazzjoni ta' konformità tal-UE u l-firmware tal-prodott mill-paġna tal-prodott fuq www.dlink.com.
Magyar [Hungarian]	Ezennel a D-Link Corporation kijelenti, hogy a jelen termék, annak tartozékai és szoftvere megfelelnek a 2014/53/EU sz. rendeletek rendelkezéseinek. Az EU Megfelelőségi nyilatkozat teljes szövege és a termék firmware a termék oldaláról tölthető le a www.dlink.com címen.
Polski [Polish]	D-Link Corporation niniejszym oświadcza, że ten produkt, akcesoria oraz oprogramowanie są zgodne z dyrektywami 2014/53/EU. Pełen tekst deklaracji zgodności UE oraz oprogramowanie sprzętowe do produktu można pobrać na stronie produktu w witrynie www.dlink.com.
Português [Portuguese]	Desta forma, a D-Link Corporation declara que este produto, os acessórios e o software estão em conformidade com a diretiva 2014/53/UE. O texto completo da declaração de conformidade da UE e do firmware
Slovensko[Slovenian]	Podjetje D-Link Corporation s tem izjavlja, da so ta izdelek, dodatna oprema in programska oprema skladni z direktivami 2014/53/EU. Celotno besedilo izjave o skladnosti EU in vdelana programska oprema sta na voljo za prenos na strani izdelka na www.dlink.com.
Slovensky [Slovak]	Spoločnosť D-Link týmto vyhlasuje, že tento produkt, príslušenstvo a softvér sú v súlade so smernicou 214/53/EÚ. Úplné znenie vyhlásenia EÚ o zhode a firmvéri produktu sú k dispozícii na prevzatie zo stránky produktu www.dlink.com.
Suomi [Finnish]	D-Link Corporation täten vakuuttaa, että tämä tuote, lisävarusteet ja ohjelmisto ovat direktiivin 2014/53/EU vaatimusten mukaisia. Täydellinen EU-vaatimustenmukaisuusvakuutus samoin kuin tuotteen laiteohjelmisto ovat ladattavissa osoitteesta www.dlink.com.

Svenska[Swedish]	D-Link Corporation försäkrar härmed att denna produkt, tillbehör och programvara överensstämmer med direktiv 2014/53/EU. Hela texten med EU-försäkran om överensstämmelse och produkt-firmware kan hämtas från produktsidan på www.dlink.com.
Íslenska [Icelandic]	Hér með lýsir D-Link Corporation því yfir að þessi vara, fylgihlutir og hugbúnaður eru í samræmi við tilskipun 2014/53/EB. Sækja má ESB-samræmisyfirlýsinguna í heild sinni og fastbúnað vörunnar af vefsíðu vörunnar á www.dlink.com.
Norsk [Norwegian]	Herved erklærer D-Link Corporation at dette produktet, tilbehøret og programvaren er i samsvar med direktivet 2014/53/EU. Den fullstendige teksten i EU-erklæring om samsvar og produktets fastvare er tilgjengelig for nedlasting fra produktsiden på www.dlink.com.

Warning Statement:

The power outlet should be near the device and easily accessible.

NOTICE OF WIRELESS RADIO LAN USAGE IN THE EUROPEAN COMMUNITY (FOR WIRELESS PRODUCT ONLY):

- This device is restricted to indoor use when operated in the European Community using channels in the 5.15-5.35 GHz band to reduce the potential for interference.
- This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries. This equipment may be operated in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, and CY.

Usage Notes:

- To remain in conformance with European National spectrum usage regulations, frequency and channel limitations will be applied on the products according to the country where the equipment will be deployed.
- This device is restricted from functioning in Ad-hoc mode while operating in 5 GHz. Ad-hoc mode is direct peer-to-peer communication between two client devices without an Access Point.
- Access points will support DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control) functionality as required when operating in 5 GHz band within the EU.
- Please refer to the product manual or datasheet to check whether your product uses 2.4 GHz and/or 5 GHz wireless.

HINWEIS ZUR VERWENDUNG VON DRAHTLOS-NETZWERK (WLAN) IN DER EUROPÄISCHEN GEMEINSCHAFT (NUR FÜR EIN DRAHTLOSES PRODUKT)

- Der Betrieb dieses Geräts in der Europäischen Gemeinschaft bei Nutzung von Kanälen im 5,15-5,35 GHz Frequenzband ist ausschließlich auf Innenräume beschränkt, um das Interferenzpotential zu reduzieren.
- Bei diesem Gerät handelt es sich um ein zum Einsatz in allen EU-Mitgliedsstaaten und in EFTA-Ländern - ausgenommen Frankreich. Der Betrieb dieses Geräts ist in den folgenden Ländern erlaubt: AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Gebrauchshinweise:

- Um den in Europa geltenden nationalen Vorschriften zum Nutzen des Funkspektrums weiterhin zu entsprechen, werden Frequenz und Kanalbeschränkungen, dem jeweiligen Land, in dem das Gerät zum Einsatz kommt, entsprechend, auf die Produkte angewandt.
- Die Funktionalität im Ad-hoc-Modus bei Betrieb auf 5 GHz ist für dieses Gerät eingeschränkt. Bei dem Ad-hoc-Modus handelt es sich um eine Peer-to-Peer-Kommunikation zwischen zwei Client-Geräten ohneeinen Access Point.
- Access Points unterstützen die Funktionen DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) wie erforderlich bei Betrieb auf 5 GHz innerhalb der EU.
- Bitte schlagen Sie im Handbuch oder Datenblatt nach nach, ob Ihr Gerät eine 2,4 GHz und / oder 5 GHz Verbindung nutzt.

AVIS CONCERNANT L'UTILISATION DE LA RADIO SANS FIL LAN DANS LA COMMUNAUTÉ EUROPÉENNE (UNIQUEMENT POUR LES PRODUITS SANS FIL)

- Cet appareil est limité à un usage intérieur lorsqu'il est utilisé dans la Communauté européenne sur les canaux de la bande de 5,15 à 5,35 GHz afin de réduire les risques d'interférences.
- Cet appareil est un système de transmission à large bande (émetteur-récepteur) de 2,4 GHz, destiné à être utilisé dans tous les États-membres de l'UE et les pays de l'AELE. Cet équipement peut être utilisé dans les pays suivants : AL, AD, BE , BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT , MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Notes d'utilisation:

- Pour rester en conformité avec la réglementation nationale européenne en matière d'utilisation du spectre, des limites de fréquence et de canal seront appliquées aux produits selon le pays où l'équipement sera déployé.
- Cet appareil ne peut pas utiliser le mode Ad-hoc lorsqu'il fonctionne dans la bande de 5 GHz. Le mode Adhoc fournit une communication directe pair à pair entre deux périphériques clients sans point d'accès.
- Les points d'accès prendront en charge les fonctionnalités DFS (Dynamic Frequency Selection) et TPC (Transmit Power Control) au besoin lors du fonctionnement dans la bande de 5 GHz au sein de l'UE.
- Merci de vous référer au guide d'utilisation ou de la fiche technique afin de vérifier si votre produit utilise 2.4 GHz et/ou 5 GHz sans fil.

AVISO DE USO DE LA LAN DE RADIO INALÁMBRICA EN LA COMUNIDAD EUROPEA (SOLO PARA EL PRODUCTO INALÁMBRICO)

- El uso de este dispositivo está restringido a interiores cuando funciona en la Comunidad Europea utilizando canales en la banda de 5,15-5,35 GHz, para reducir la posibilidad de interferencias.
- Este dispositivo es un sistema de transmisión (transceptor) de banda ancha de 2,4 GHz, pensado para su uso en todos los estados miembros de la UE y en los países de la AELC. Este equipo se puede utilizar en AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Notas de uso:

- Para seguir cumpliendo las normas europeas de uso del espectro nacional, se aplicarán limitaciones de frecuencia y canal en los productos en función del país en el que se pondrá en funcionamiento el equipo.
- Este dispositivo tiene restringido el funcionamiento en modo Ad-hoc mientras funcione a 5 Ghz. El modo Ad-hoc es la comunicación directa de igual a igual entre dos dispositivos cliente sin un punto de acceso.
- Los puntos de acceso admitirán la funcionalidad DFS (Selección de frecuencia dinámica) y TPC (Control de la potencia de transmisión) si es necesario cuando funcionan a 5 Ghz dentro de la UE.
- Por favor compruebe el manual o la ficha de producto para comprobar si el producto utiliza las bandas inalámbricas de 2.4 GHz y/o la de 5 GHz.

AVVISO PER L'USO DI LAN RADIO WIRELESS NELLA COMUNITÀ EUROPEA (SOLO PER PRODOTTI WIRELESS)

- Nella Comunità europea, l'uso di questo dispositivo è limitato esclusivamente agli ambienti interni sui canali compresi nella banda da 5,15 a 5,35 GHz al fine di ridurre potenziali interferenze. Questo dispositivo è un sistema di trasmissione a banda larga a 2,4 GHz (ricetrasmittente), destinato all'uso in tutti gli stati membri dell'Unione europea e nei paesi EFTA.
- Questo dispositivo può essere utilizzato in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Note per l'uso

- Al fine di mantenere la conformità alle normative nazionali europee per l'uso dello spettro di frequenze, saranno applicate limitazioni sulle frequenze e sui canali per il prodotto in conformità alle normative del paese in cui il dispositivo viene utilizzato.
- Questo dispositivo non può essere attivato in modalità Ad-hoc durante il funzionamento a 5 Ghz. La modalità Ad-hoc è una comunicazione diretta peer-to-peer fra due dispositivi client senza un punto di accesso.
- I punti di accesso supportano le funzionalità DFS (Dynamic Frequency Selection) e TPC (Transmit Power Control) richieste per operare a 5 Ghz nell'Unione europea.
- Ti invitiamo a fare riferimento al manuale del prodotto o alla scheda tecnica per verificare se il tuo prodotto utilizza le frequenze 2,4 GHz e/o 5 GHz.

KENNISGEVING VAN DRAADLOOS RADIO LAN-GEBRUIK IN DE EUROPESE GEMEENSCHAP (ALLEEN VOOR DRAADLOOS PRODUCT)

- Dit toestel is beperkt tot gebruik binnenshuis wanneer het wordt gebruikt in de Europese Gemeenschap gebruik makend van kanalen in de 5.15-5.35 GHz band om de kans op interferentie te beperken.
- Dit toestel is een 2.4 GHz breedband transmissiesysteem (transceiver) dat bedoeld is voor gebruik in alle EU lidstaten en EFTA landen. Deze uitrusting mag gebruikt worden in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

Gebruiksaanwijzingen:

- Om de gebruiksvoorschriften van het Europese Nationale spectrum na te leven, zullen frequentie- en kanaalbeperkingen worden toegepast op de producten volgens het land waar de uitrusting gebruikt zal worden.
- Dit toestel kan niet functioneren in Ad-hoc mode wanneer het gebruikt wordt in 5 GHz. Ad-hoc mode is directe peer-to-peer communicatie tussen twee klantenapparaten zonder een toegangspunt.
- Toegangspunten ondersteunen DFS (Dynamic Frequency Selection) en TPC (Transmit Power Control) functionaliteit zoals vereist bij gebruik in 5 GHz binnen de EU.
- Raadpleeg de handleiding of de datasheet om te controleren of uw product gebruik maakt van 2.4 GHz en/of 5 GHz.

SAFETY INSTRUCTIONS

The following general safety guidelines are provided to help ensure your own personal safety and protect your product from potential damage. Remember to consult the product user instructions for more details.

- Static electricity can be harmful to electronic components. Discharge static electricity from your body (i.e. touching grounded bare metal) before touching the product.
- Do not attempt to service the product and never disassemble the product. For some products with a user replaceable battery, please read and follow the instructions in the user manual.
- Do not spill food or liquid on your product and never push any objects into the openings of your product.
- Do not use this product near water, areas with high humidity, or condensation unless the product is specifically rated for outdoor application.
- Keep the product away from radiators and other heat sources.
- Always unplug the product from mains power before cleaning and use a dry lint free cloth only.

SICHERHEITSVORSCHRIFTEN

Die folgenden allgemeinen Sicherheitsvorschriften dienen als Hilfe zur Gewährleistung Ihrer eigenen Sicherheit und zum Schutz Ihres Produkts. Weitere Details finden Sie in den Benutzeranleitungen zum Produkt.

- Statische Elektrizität kann elektronischen Komponenten schaden. Um Schäden durch statische Aufladung zu vermeiden, leiten Sie elektrostatische Ladungen von Ihrem Körper ab,
  (z. B. durch Berühren eines geerdeten blanken Metallteils), bevor Sie das Produkt berühren.
- Unterlassen Sie jeden Versuch, das Produkt zu warten, und versuchen Sie nicht, es in seine Bestandteile zu zerlegen. Für einige Produkte mit austauschbaren Akkus lesen Sie bitte das Benutzerhandbuch und befolgen Sie die dort beschriebenen Anleitungen.
- Vermeiden Sie, dass Speisen oder Flüssigkeiten auf Ihr Produkt gelangen, und stecken Sie keine Gegenstände in die Gehäuseschlitze oder -öffnungen Ihres Produkts.
- Verwenden Sie dieses Produkt nicht in unmittelbarer Nähe von Wasser und nicht in Bereichen mit hoher Luftfeuchtigkeit oder Kondensation, es sei denn, es ist speziell zur Nutzung in Außenbereichen vorgesehen und eingestuft.
- Halten Sie das Produkt von Heizkörpern und anderen Quellen fern, die Wärme erzeugen.
- Trennen Sie das Produkt immer von der Stromzufuhr, bevor Sie es reinigen und verwenden Sie dazu ausschließlich ein trockenes fusselfreies Tuch.

CONSIGNES DE SÉCURITÉ

Les consignes générales de sécurité ci-après sont fournies afin d'assurer votre sécurité personnelle et de protéger le produit d'éventuels dommages. Veuillez consulter les consignes d'utilisation du produit pour plus de détails.

- L'électricité statique peut endommager les composants électroniques. Déchargez l'électricité statique de votre corps (en touchant un objet en métal relié à la terre par exemple) avant de toucher le produit.
- N'essayez pas d'intervenir sur le produit et ne le démontez jamais. Pour certains produits contenant une batterie remplaçable par l'utilisateur, veuillez lire et suivre les consignes contenues dans le manuel d'utilisation.
- Ne renversez pas d'aliments ou de liquide sur le produit et n'insérez jamais d'objets dans les orifices.
- N'utilisez pas ce produit à proximité d'un point d'eau, de zones très humides ou de condensation sauf si le produit a été spécifiquement conçu pour une application extérieure.
- Éloignez le produit des radiateurs et autres sources de chaleur.
- Débranchez toujours le produit de l'alimentation avant de le nettoyer et utilisez uniquement un chiffon sec non pelucheux.

INSTRUCCIONES DE SEGURIDAD

Las siguientes directrices de seguridad general se facilitan para ayudarle a garantizar su propia seguridad personal y para proteger el producto frente a posibles daños. No olvide consultar las instrucciones del usuario del producto para obtener más información.

- La electricidad estática puede resultar nociva para los componentes electrónicos. Descargue la electricidad estática de su cuerpo (p. ej., tocando algún metal sin revestimiento conectado a tierra) antes de tocar el producto.
- No intente realizar el mantenimiento del producto ni lo desmonte nunca. Para algunos productos con batería reemplazable por el usuario, lea y siga las instrucciones del manual de usuario.
- No derrame comida o líquidos sobre el producto y nunca deje que caigan objetos en las aberturas del mismo.
- No utilice este producto cerca del agua, en zonas con humedad o condensación elevadas a menos que el producto esté clasificado específicamente para aplicación en exteriores.
- Mantenga el producto alejado de los radiadores y de otras fuentes de calor.
- Desenchufe siempre el producto de la alimentación de red antes de limpiarlo y utilice solo un paño seco sin pelusa.

ISTRUZIONI PER LA SICUREZZA

Le seguenti linee guida sulla sicurezza sono fornite per contribuire a garantire la sicurezza personale degli utenti e a proteggere il prodotto da potenziali danni. Per maggiori dettagli, consultare le istruzioni per l'utente del prodotto.

- L'elettricità statica può essere pericolosa per i componenti elettronici. Scaricare l'elettricità statica dal corpo (ad esempio toccando una parte metallica collegata a terra) prima di toccare il prodotto.
- Non cercare di riparare il prodotto e non smontarlo mai. Per alcuni prodotti dotati di batteria sostituibile dall'utente, leggere e seguire le istruzioni riportate nel manuale dell'utente.
- Non versare cibi o liquidi sul prodotto e non spingere mai alcun oggetto nelle aperture del prodotto.
- Non usare questo prodotto vicino all'acqua, in aree con elevato grado di umidità o soggette a condensa a meno che il prodotto non sia specificatamente approvato per uso in ambienti esterni.
- Tenere il prodotto lontano da caloriferi e altre fonti di calore.
- Scollegare sempre il prodotto dalla presa elettrica prima di pulirlo e usare solo un panno asciutto che non lasci filacce.

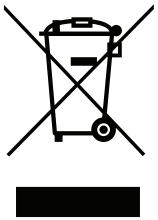
VEILIGHEIDSINFORMATIE

De volgende algemene veiligheidsinformatie werd verstrekt om uw eigen persoonlijke veiligheid te waarborgen en uw product te beschermen tegen mogelijke schade. Denk eraan om de gebruikersinstructies van het product te raadplegen voor meer informatie.

- Statische elektriciteit kan schadelijk zijn voor elektronische componenten. Ontlaad de statische elektriciteit van uw lichaam (d.w.z. het aanraken van geaard bloot metaal) voordat uhet product aanraakt.
- U mag nooit proberen het product te onderhouden en u mag het product nooit demonteren. Voor sommige producten met door de gebruiker te vervangen batterij, dient u de instructies in de gebruikershandleiding te lezen en te volgen.
- Mors geen voedsel of vloeistof op uw product en u mag nooit voorwerpen in de openingen van uw product duwen.
- Gebruik dit product niet in de buurt van water, gebieden met hoge vochtigheid of condensatie, tenzij het product specifiek geclassificeerd is voor gebruik buitenshuis.
- Houd het product uit de buurt van radiators en andere warmtebronnen.
- U dient het product steeds los te koppelen van de stroom voordat u het reinigt en gebruik uitsluitend een droge pluisvrije doek.

Disposing of and Recycling Your Product

ENGLISH **EN**



This symbol on the product or packaging means that according to local laws and regulations this product should be not be disposed of in household waste but sent for recycling. Please take it to a collection point designated by your local authorities once it has reached the end of its life, some will accept products for free. By recycling the product and its packaging in this manner you help to conserve the environment and protect human health.

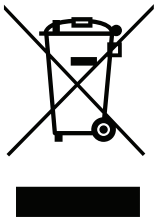
D-Link and the Environment

At D-Link, we understand and are committed to reducing any impact our operations and products may have on the environment. To minimise this impact D-Link designs and builds its products to be as environmentally friendly as possible, by using recyclable, low toxic materials in both products and packaging.

D-Link recommends that you always switch off or unplug your D-Link products when they are not in use. By doing so you will help to save energy and reduce CO2 emissions.

To learn more about our environmentally responsible products and packaging please visit **www.dlinkgreen.com**.

DEUTSCH **DE**



Dieses Symbol auf dem Produkt oder der Verpackung weist darauf hin, dass dieses Produkt gemäß bestehender örtlicher Gesetze und Vorschriften nicht über den normalen Hausmüll entsorgt werden sollte, sondern einer Wiederverwertung zuzuführen ist. Bringen Sie es bitte zu einer von Ihrer Kommunalbehörde entsprechend amtlich ausgewiesenen Sammelstelle, sobald das Produkt das Ende seiner Nutzungsdauer erreicht hat. Für die Annahme solcher Produkte erheben einige dieser Stellen keine Gebühren. Durch ein auf diese Weise durchgeführtes Recycling des Produkts und seiner Verpackung helfen Sie, die Umwelt zu schonen und die menschliche Gesundheit zu schützen.

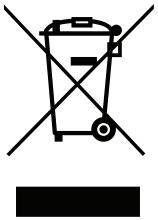
D-Link und die Umwelt

D-Link ist sich den möglichen Auswirkungen seiner Geschäftstätigkeiten und seiner Produkte auf die Umwelt bewusst und fühlt sich verpflichtet, diese entsprechend zu mindern. Zu diesem Zweck entwickelt und stellt D-Link seine Produkte mit dem Ziel größtmöglicher Umweltfreundlichkeit her und verwendet wiederverwertbare, schadstoffarme Materialien bei Produktherstellung und Verpackung.

D-Link empfiehlt, Ihre Produkte von D-Link, wenn nicht in Gebrauch, immer auszuschalten oder vom Netz zu nehmen. Auf diese Weise helfen Sie, Energie zu sparen und CO2-Emissionen zu reduzieren.

Wenn Sie mehr über unsere umweltgerechten Produkte und Verpackungen wissen möchten, finden Sie entsprechende Informationen im Internet unter **www.dlinkgreen.com**.

FRANÇAIS FR



Ce symbole apposé sur le produit ou son emballage signifie que, conformément aux lois et règlementations locales, ce produit ne doit pas être éliminé avec les déchets domestiques mais recyclé. Veuillez le rapporter à un point de collecte prévu à cet effet par les autorités locales; certains accepteront vos produits gratuitement. En recyclant le produit et son emballage de cette manière, vous aidez à préserver l'environnement et à protéger la santé de l'homme.

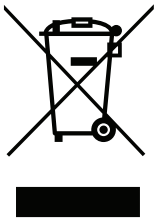
D-Link et l'environnement

Chez D-Link, nous sommes conscients de l'impact de nos opérations et produits sur l'environnement et nous engageons à le réduire. Pour limiter cet impact, D-Link conçoit et fabrique ses produits de manière aussi écologique que possible, en utilisant des matériaux recyclables et faiblement toxiques, tant dans ses produits que ses emballages.

D-Link recommande de toujours éteindre ou débrancher vos produits D-Link lorsque vous ne les utilisez pas. Vous réaliserez ainsi des économies d'énergie et réduirez vos émissions de CO2.

Pour en savoir plus sur les produits et emballages respectueux de l'environnement, veuillez consulter le **www.dlinkgreen.com**.

ESPAÑOL ES



Este símbolo en el producto o el embalaje significa que, de acuerdo con la legislación y la normativa local, este producto no se debe desechar en la basura doméstica sino que se debe reciclar. Llévelo a un punto de recogida designado por las autoridades locales una vez que ha llegado al fin de su vida útil; algunos de ellos aceptan recogerlos de forma gratuita. Al reciclar el producto y su embalaje de esta forma, contribuye a preservar el medio ambiente y a proteger la salud de los seres humanos.

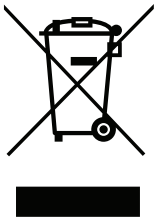
D-Link y el medio ambiente

En D-Link, comprendemos y estamos comprometidos con la reducción del impacto que puedan tener nuestras actividades y nuestros productos en el medio ambiente. Para reducir este impacto, D-Link diseña y fabrica sus productos para que sean lo más ecológicos posible, utilizando materiales reciclables y de baja toxicidad tanto en los productos como en el embalaje.

D-Link recomienda apagar o desenchufar los productos D-Link cuando no se estén utilizando. Al hacerlo, contribuirá a ahorrar energía y a reducir las emisiones de CO2.

Para obtener más información acerca de nuestros productos y embalajes ecológicos, visite el sitio **www.dlinkgreen.com**.

ITALIANO IT



La presenza di questo simbolo sul prodotto o sulla confezione del prodotto indica che, in conformità alle leggi e alle normative locali, questo prodotto non deve essere smaltito nei rifiuti domestici, ma avviato al riciclo. Una volta terminato il ciclo di vita utile, portare il prodotto presso un punto di raccolta indicato dalle autorità locali. Alcuni questi punti di raccolta accettano gratuitamente i prodotti da riciclare. Scegliendo di riciclare il prodotto e il relativo imballaggio, si contribuirà a preservare l'ambiente e a salvaguardare la salute umana.

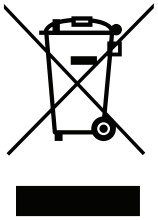
D-Link e l'ambiente

D-Link cerca da sempre di ridurre l'impatto ambientale dei propri stabilimenti e dei propri prodotti. Allo scopo di ridurre al minimo tale impatto, D-Link progetta e realizza i propri prodotti in modo che rispettino il più possibile l'ambiente, utilizzando materiali riciclabili a basso tasso di tossicità sia per i prodotti che per gli imballaggi.

D-Link raccomanda di spegnere sempre i prodotti D-Link o di scollegarne la spina quando non vengono utilizzati. In questo modo si contribuirà a risparmiare energia e a ridurre le emissioni di anidride carbonica.

Per ulteriori informazioni sui prodotti e sugli imballaggi D-Link a ridotto impatto ambientale, visitate il sito all'indirizzo **www.dlinkgreen.com**.

NEDERLANDS NL



Dit symbool op het product of de verpakking betekent dat dit product volgens de plaatselijke wetgeving niet mag worden weggegooid met het huishoudelijk afval, maar voor recyclage moeten worden ingeleverd. Zodra het product het einde van de levensduur heeft bereikt, dient u het naar een inzamelpunt te brengen dat hiertoe werd aangeduid door uw plaatselijke autoriteiten, sommige autoriteiten accepteren producten zonder dat u hiervoor dient te betalen. Door het product en de verpakking op deze manier te recyclen helpt u het milieu en de gezondheid van de mens te beschermen.

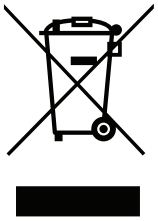
D-Link en het milieu

Bij D-Link spannen we ons in om de impact van onze handelingen en producten op het milieu te beperken. Om deze impact te beperken, ontwerpt en bouwt D-Link zijn producten zo milieuvriendelijk mogelijk, door het gebruik van recycleerbare producten met lage toxiciteit in product en verpakking.

D-Link raadt aan om steeds uw D-Link producten uit te schakelen of uit de stekker te halen wanneer u ze niet gebruikt. Door dit te doen bespaart u energie en beperkt u de CO2-emissies.

Breng een bezoek aan **www.dlinkgreen.com** voor meer informatie over onze milieuverantwoorde producten en verpakkingen.

POLSKI PL



Ten symbol umieszczony na produkcie lub opakowaniu oznacza, że zgodnie z miejscowym prawem i lokalnymi przepisami niniejszego produktu nie wolno wyrzucać jak odpady czy śmieci z gospodarstwa domowego, lecz należy go poddać procesowi recyklingu. Po zakończeniu użytkowania produktu, niektóre odpowiednie do tego celu podmioty przyjmą takie produkty nieodpłatnie, dlatego prosimy dostarczyć go do punktu zbiórki wskazanego przez lokalne władze. Poprzez proces recyklingu i dzięki takiemu postępowaniu z produktem oraz jego opakowaniem, pomogą Państwo chronić środowisko naturalne i dbać o ludzkie zdrowie.

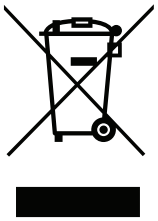
D-Link i środowisko

D-Link podchodzimy w sposób świadomy do ochrony otoczenia oraz jesteśmy zaangażowani w zmniejszanie wpływu naszych działań i produktów na środowisko naturalne. W celu zminimalizowania takiego wpływu firma D-Link konstruuje i wytwarza swoje produkty w taki sposób, aby były one jak najbardziej przyjazne środowisku, stosując do tych celów materiały nadające się do powtórnego wykorzystania, charakteryzujące się małą toksycznością zarówno w przypadku samych produktów jak i opakowań.

Firma D-Link zaleca, aby Państwo zawsze prawidłowo wyłączali z użytku swoje produkty D-Link, gdy nie są one wykorzystywane. Postępując w ten sposób pozwalają Państwo oszczędzać energię i zmniejszać emisje CO2.

Aby dowiedzieć się więcej na temat produktów i opakowań mających wpływ na środowisko prosimy zapoznać się ze stroną Internetową **www.dlinkgreen.com**.

ČESKY CZ



Tento symbol na výrobku nebo jeho obalu znamená, že podle místně platných předpisů se výrobek nesmí vyhazovat do komunálního odpadu, ale odeslat k recyklaci. Až výrobek doslouží, odneste jej prosím na sběrné místo určené místními úřady k tomuto účelu. Některá sběrná místa přijímají výrobky zdarma. Recyklací výrobku i obalu pomáháte chránit životní prostředí i lidské zdraví.

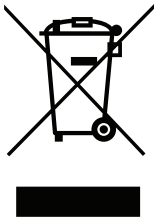
D-Link a životní prostředí

Ve společnosti D-Link jsme si vědomi vlivu našich provozů a výrobků na životní prostředí a snažíme se o minimalizaci těchto vlivů. Proto své výrobky navrhujeme a vyrábíme tak, aby byly co nejekologičtější, a ve výrobcích i obalech používáme recyklovatelné a nízkotoxické materiály.

Společnost D-Link doporučuje, abyste své výrobky značky D-Link vypnuli nebo vytáhli ze zásuvky vždy, když je nepoužíváte. Pomůžete tak šetřit energii a snížit emise CO2.

Více informací o našich ekologických výrobcích a obalech najdete na adrese **www.dlinkgreen.com**.

MAGYAR **HU**



Ez a szimbólum a terméken vagy a csomagoláson azt jelenti, hogy a helyi törvényeknek és szabályoknak megfelelően ez a termék nem semmisíthető meg a háztartási hulladékkal együtt, hanem újrahasznosításra kell küldeni. Kérjük, hogy a termék élettartamának elteltét követően vigye azt a helyi hatóság által kijelölt gyűjtőhelyre. A termékek egyes helyeken ingyen elhelyezhetők. A termék és a csomagolás újrahasznosításával segíti védeni a környezetet és az emberek egészségét.

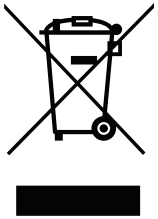
A D-Link és a környezet

A D-Linknél megértjük és elkötelezettek vagyunk a műveleteink és termékeink környezetre gyakorolt hatásainak csökkentésére. Az ezen hatás csökkentése érdekében a D-Link a lehető leginkább környezetbarát termékeket tervez és gyárt azáltal, hogy újrahasznosítható, alacsony károsanyag-tartalmú termékeket gyárt és csomagolásokat alkalmaz.

A D-Link azt javasolja, hogy mindig kapcsolja ki vagy húzza ki a D-Link termékeket a tápforrásból, ha nem használja azokat. Ezzel segít az energia megtakarításában és a széndioxid kibocsátásának csökkentésében.

Környezetbarát termékeinkről és csomagolásainkról további információkat a **www.dlinkgreen.com** weboldalon tudhat meg.

NORSK **NO**



Dette symbolet på produktet eller forpakningen betyr at dette produktet ifølge lokale lover og forskrifter ikke skal kastes sammen med husholdningsavfall, men leveres inn til gjenvinning. Vennligst ta det til et innsamlingssted anvist av lokale myndigheter når det er kommet til slutten av levetiden. Noen steder aksepteres produkter uten avgift. Ved på denne måten å gjenvinne produktet og forpakningen hjelper du å verne miljøet og beskytte folks helse.

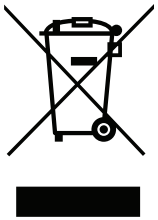
D-Link og miljøet

Hos D-Link forstår vi oss på og er forpliktet til å minske innvirkningen som vår drift og våre produkter kan ha på miljøet. For å minimalisere denne innvirkningen designer og lager D-Link produkter som er så miljøvennlig som mulig, ved å bruke resirkulerbare, lav-toksiske materialer både i produktene og forpakningen.

D-Link anbefaler at du alltid slår av eller frakobler D-Link-produkter når de ikke er i bruk. Ved å gjøre dette hjelper du å spare energi og å redusere CO2-utslipp.

For mer informasjon angående våre miljøansvarlige produkter og forpakninger kan du gå til **www.dlinkgreen.com**.

DANSK DK



Dette symbol på produktet eller emballagen betyder, at dette produkt i henhold til lokale love og regler ikke må bortskaffes som husholdningsaffald, mens skal sendes til genbrug. Indlever produktet til et indsamlingssted som angivet af de lokale myndigheder, når det er nået til slutningen af dets levetid. I nogle tilfælde vil produktet blive modtaget gratis. Ved at indlevere produktet og dets emballage til genbrug på denne måde bidrager du til at beskytte miljøet og den menneskelige sundhed.

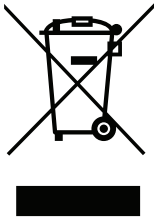
D-Link og miljøet

Hos D-Link forstår vi og bestræber os på at reducere enhver indvirkning, som vores aktiviteter og produkter kan have på miljøet. For at minimere denne indvirkning designer og producerer D-Link sine produkter, så de er så miljøvenlige som muligt, ved at bruge genanvendelige materialer med lavt giftighedsniveau i både produkter og emballage.

D-Link anbefaler, at du altid slukker eller frakobler dine D-Link-produkter, når de ikke er i brug. Ved at gøre det bidrager du til at spare energi og reducere CO2-udledningerne.

Du kan finde flere oplysninger om vores miljømæssigt ansvarlige produkter og emballage på **www.dlinkgreen.com**.

SUOMI FI



Tämä symboli tuotteen pakkauksessa tarkoittaa, että paikallisten lakien ja säännösten mukaisesti tätä tuotetta ei pidä hävittää yleisen kotitalousjätteen seassa vaan se tulee toimittaa kierrätettäväksi. Kun tuote on elinkaarensa päässä, toimita se lähimpään viranomaisten hyväksymään kierrätyspisteeseen. Kierrättämällä käytetyn tuotteen ja sen pakkauksen autat tukemaan sekä ympäristön että ihmisten terveyttä ja hyvinvointia.

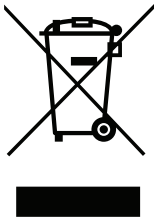
D-Link ja ympäristö

D-Link ymmärtää ympäristönsuojelun tärkeyden ja on sitoutunut vähentämään tuotteistaan ja niiden valmistuksesta ympäristölle mahdollisesti aiheutuvia haittavaikutuksia. Nämä negatiiviset vaikutukset minimoidakseen D-Link suunnittelee ja valmistaa tuotteensa mahdollisimman ympäristöystävällisiksi käyttämällä kierrätettäviä, alhaisia pitoisuuksia haitallisia aineita sisältäviä materiaaleja sekä tuotteissaan että niiden pakkauksissa.

Suosittelemme, että irrotat D-Link-tuotteesi virtalähteestä tai sammutat ne aina, kun ne eivät ole käytössä. Toimimalla näin autat säästämään energiaa ja vähentämään hiilidioksiidipäästöjä.

Lue lisää ympäristöystävällisistä D-Link-tuotteista ja pakkauksistamme osoitteesta **www.dlinkgreen.com**.

SVENSKA SE



Den här symbolen på produkten eller förpackningen betyder att produkten enligt lokala lagar och föreskrifter inte skall kastas i hushållssoporna utan i stället återvinnas. Ta den vid slutet av dess livslängd till en av din lokala myndighet utsedd uppsamlingsplats, vissa accepterar produkter utan kostnad. Genom att på detta sätt återvinna produkten och förpackningen hjälper du till att bevara miljön och skydda människors hälsa.

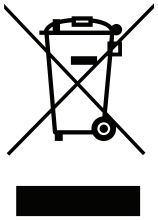
D-Link och miljön

På D-Link förstår vi och är fast beslutna att minska den påverkan våra verksamheter och produkter kan ha på miljön. För att minska denna påverkan utformar och bygger D-Link sina produkter för att de ska vara så miljövänliga som möjligt, genom att använda återvinningsbara material med låg gifthalt i både produkter och förpackningar.

D-Link rekommenderar att du alltid stänger av eller kopplar ur dina D-Link produkter när du inte använder dem. Genom att göra detta hjälper du till att spara energi och minska utsläpp av koldioxid.

För mer information om våra miljöansvariga produkter och förpackningar **www.dlinkgreen.com**.

PORTUGUÊS PT



Este símbolo no produto ou embalagem significa que, de acordo com as leis e regulamentações locais, este produto não deverá ser eliminado juntamente com o lixo doméstico mas enviado para a reciclagem. Transporte-o para um ponto de recolha designado pelas suas autoridades locais quando este tiver atingido o fim da sua vida útil, alguns destes pontos aceitam produtos gratuitamente. Ao reciclar o produto e respectiva embalagem desta forma, ajuda a preservar o ambiente e protege a saúde humana.

A D-Link e o ambiente

Na D-Link compreendemos e comprometemo-nos com a redução do impacto que as nossas operações e produtos possam ter no ambiente. Para minimizar este impacto a D-Link concebe e constrói os seus produtos para que estes sejam o mais inofensivos para o ambiente possível, utilizando meteriais recicláveis e não tóxicos tanto nos produtos como nas embalagens.

A D-Link recomenda que desligue os seus produtos D-Link quando estes não se encontrarem em utilização. Com esta acção ajudará a poupar energia e reduzir as emissões de CO2.

Para saber mais sobre os nossos produtos e embalagens responsáveis a nível ambiental visite **www.dlinkgreen.com**.