D-Link®

Version 1.00 | 12/07/2017

User Manual

Tri-Band Wireless AC5300 Gigabit VDSL Modem Router

DSL-5300

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	December 6, 2017	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.

Apple®, Apple logo®, Safari®, iPhone®, iPad®, iPod touch® and Macintosh® are trademarks of Apple Inc., registered in the U.S. and other countries. App Store℠ is a service mark of Apple Inc.

Chrome™ browser, Google Play™ and Android™ are trademarks of Google Inc.

Internet Explorer®, Windows® and the Windows logo are trademarks of the Microsoft group of companies.

Copyright © 2017 by D-Link Corporation, Inc.

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

Table of Contents

Preface ..... **i**

Product Overview **1**
- Package Contents 1
- System Requirements 2
- Introduction 3
- Features 4
- Antenna Setup 5
- Hardware Overview 6
  - Connections 6
  - LEDs 7

Installation **8**
- Before you Begin 8
- Wireless Installation Considerations 9
- Manual Setup 10

Getting Started **13**
- Setup Wizard 14

Configuration **20**
- Home 20
  - Internet 21
    - IPv4 22
    - IPv6 23
    - DSL 24
  - DSL-5300 25
  - Connected Clients 26
  - Connected Clients (Cont) 27
  - USB Device 28
- Settings 29
  - Wizard 29
  - Internet 29
    - IPv4 31
    - DSL 41
    - ATM 42
    - PTM 43
    - VLAN 44
    - IPv6 45
  - Wireless 59
    - Guest Zone 61
    - Advanced Settings 62
  - Network 65
  - SharePort 67
    - Create User 68
- Features 69
  - QoS Engine 69
  - Firewall Settings 70
    - IPv4/IPv6 Rules 72
  - Port Forwarding 73
    - Virtual Server 74
  - Website Filter 75
  - Static Routes 76
    - IPv6 77

Dynamic DNS 78
IPv6 Host 79
VPN....80
Management....82
Time & Schedule 82
Time 82
Schedule 83
System Log....84
Admin 85
System 87
Upgrade 88
Statistics 89

Connect a Wireless Client to your Router 90
WPS Button....90
Windows® 10....91
Windows® 8....93
WPA/WPA2 93
Windows® 7....95
WPA/WPA2 95
WPS....98
Windows Vista®....102
WPA/WPA2 103
Windows® XP....105
WPA/WPA2 106

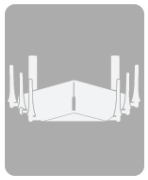
Troubleshooting 108

Wireless Basics 112
What is Wireless?....113
Tips....115
Wireless Modes....116

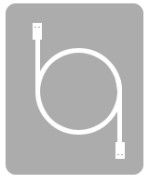
Networking Basics 117
Check your IP address....117
Statically Assign an IP address....118
Wireless Security 119
What is WPA? 119

Technical Specifications 120

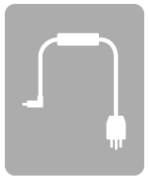
Package Contents



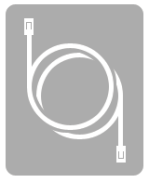
DSL-5300 Tri Band Wireless AC5300
Gigabit VDSL Modem Router



DSL Phone Cable



Splitter



Ethernet Cable

Power Adapter

Wi-Fi Configuration Card

D-Link Cloud Service Mobile Apps Guide

Quick Installation Guide

Wall Mount Hardware

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

Note: *Using a power supply with a different voltage rating than the one included with the DSL-5300 will cause damage and void the warranty for this product.*

System Requirements

Network Requirements	• An Ethernet-based cable or DSL modem • 802.11ac/n/g/b/a wireless or Ethernet port
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 9 or higher • Firefox 20 or higher • Safari 5.1 or higher • Chrome 25 or higher **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

Introduction

The D-Link DSL-5300 Tri-Band Wireless AC5300 Gigabit VDSL Modem Router shares your DSL Internet connection over a blazing-fast Wireless AC connection using advanced AC beamforming technology to maximize the speed and range of your wireless signal to significantly outperform 802.11n and other 802.11ac devices. It also comes equipped with four Gigabit ports to provide speeds up to 10x faster than standard 10/100 ports. With the addition of Advanced Quality of Service (QoS), data streams are separated, which helps organize and prioritize your network traffic so your video streaming, gaming, and VoIP calls run smoother over both your wired and wireless network.

The Tri-Band Wireless AC5300 Gigabit VDSL Modem Router supports VDSL2 to help you make the most of your broadband subscription. With download speeds of up to 100Mbps, the DSL-5300 provides more than enough bandwidth for multiple devices streaming HD video, playing intense online games, or multiple simultaneous file transfers. With VDSL2 and a compatible ISP, you can say goodbye to buffering, queuing, and compromises for bandwidth-intensive applications.

File sharing technology lets you take advantage of the USB 3.0 port found on the back of your DSL-5300 (as well as an additional USB 2.0 port). Plug in a USB storage drive and you can use the access files, stream videos, view photos, or listen to music on your laptop or mobile devices.

The DSL-5300 Tri-Band Wireless AC5300 Gigabit VDSL Modem Router provides incredible speeds, smart antenna technology, fast ports, and cloud features. It also features an innovative design and easy installation options.

Features

- **Faster Wireless Networking** - The DSL-5300 uses Smart Connect, a D-Link feature, when combined with additional 5 GHz antennas, can provide up to a full 5300 Mbps* wireless connection with concurrent 801.11ac and 802.11n wireless clients. It operates on both the 2.4 GHz and 5 GHz bands to allow separation of traffic so users can participate in high-bandwidth activities, such as video streaming, online gaming, and real-time audio, without affecting low-priority traffic like email and web surfing.

- **Compatible with 802.11n/g/b/a Devices** - The DSL-5300 is fully compatible with the 802.11n, IEEE 802.11g and 802.11a standards, so it can connect with existing 802.11n, 802.11g, 802.11b, and 802.11a wireless devices.

- **Advanced Firewall Features** - The web-based user interface displays a number of advanced network management features including:
    - **Content Filtering** - Easily applied content filtering based on MAC address, URL, and/or domain name.
    - **Scheduling** - The Firewall, wireless, and port forwarding features can be scheduled to be active on certain days, or for a duration of a set number of hours.

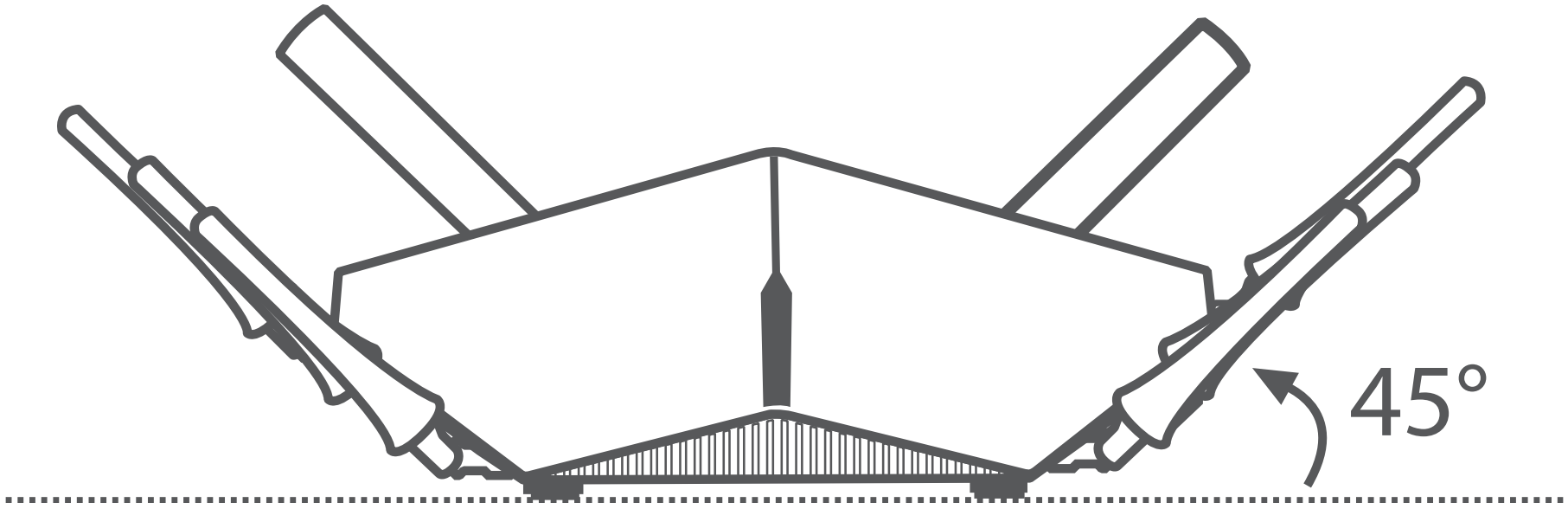
- **User-friendly Setup Wizard** - Through its easy-to-use web-based user interface, the DSL-5300 lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.

- **Fast VDSL2** - VDSL2 support for up to 100 mbps broadband speeds lets you make the most of your high-speed connection. Plenty of bandwidth for every family member to each stream their own HD content and ultra-responsive for the most intense games, real-time video conferencing, or large file transfers.

* Maximum wireless signal rate derived from IEEE Standard 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac 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 conditions will adversely affect wireless signal range.

Antenna Setup

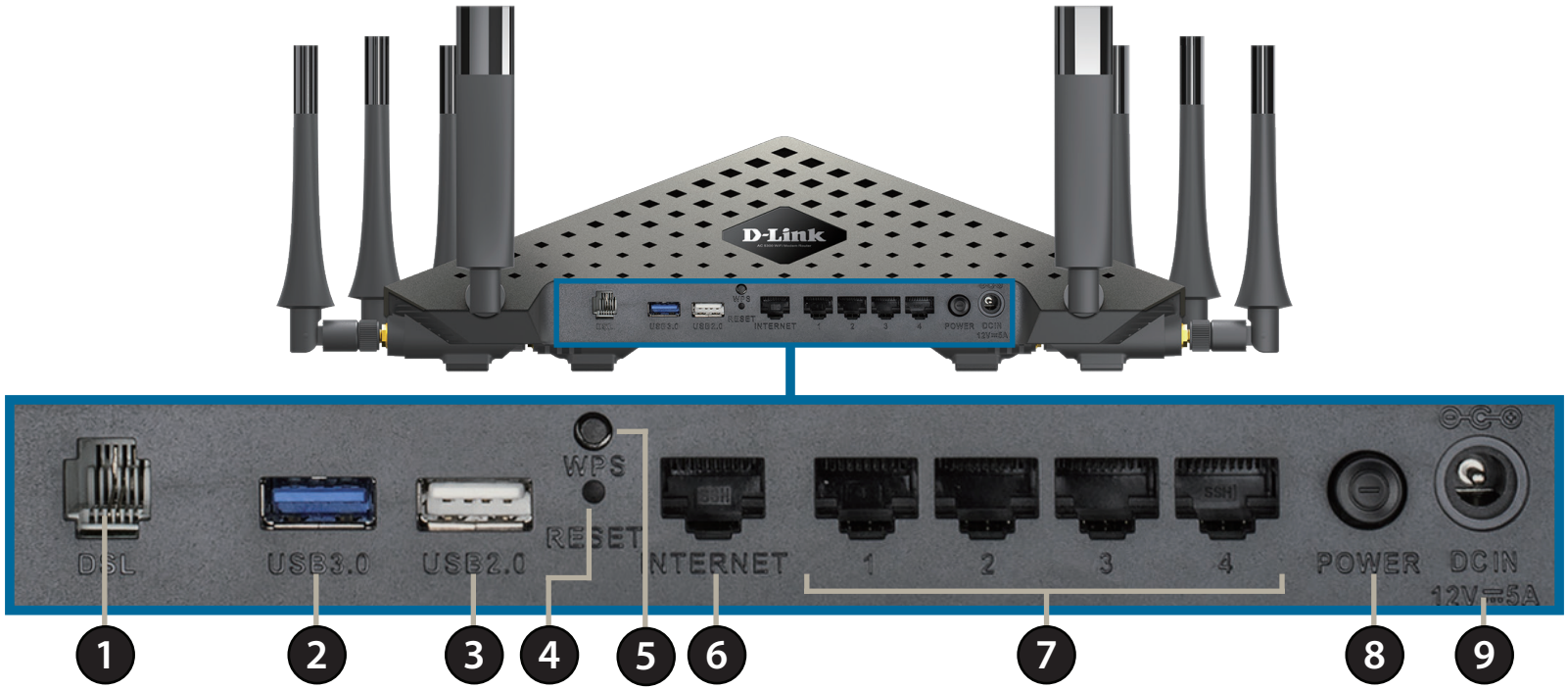
The DSL-5300 is designed to give you the fastest, most stable network connection possible. In order to maximize performance, potition the antennas at an angle, pointing outward and away from the base unit.



NOTE: Attach the antennas to the router before powering it on.

Hardware Overview

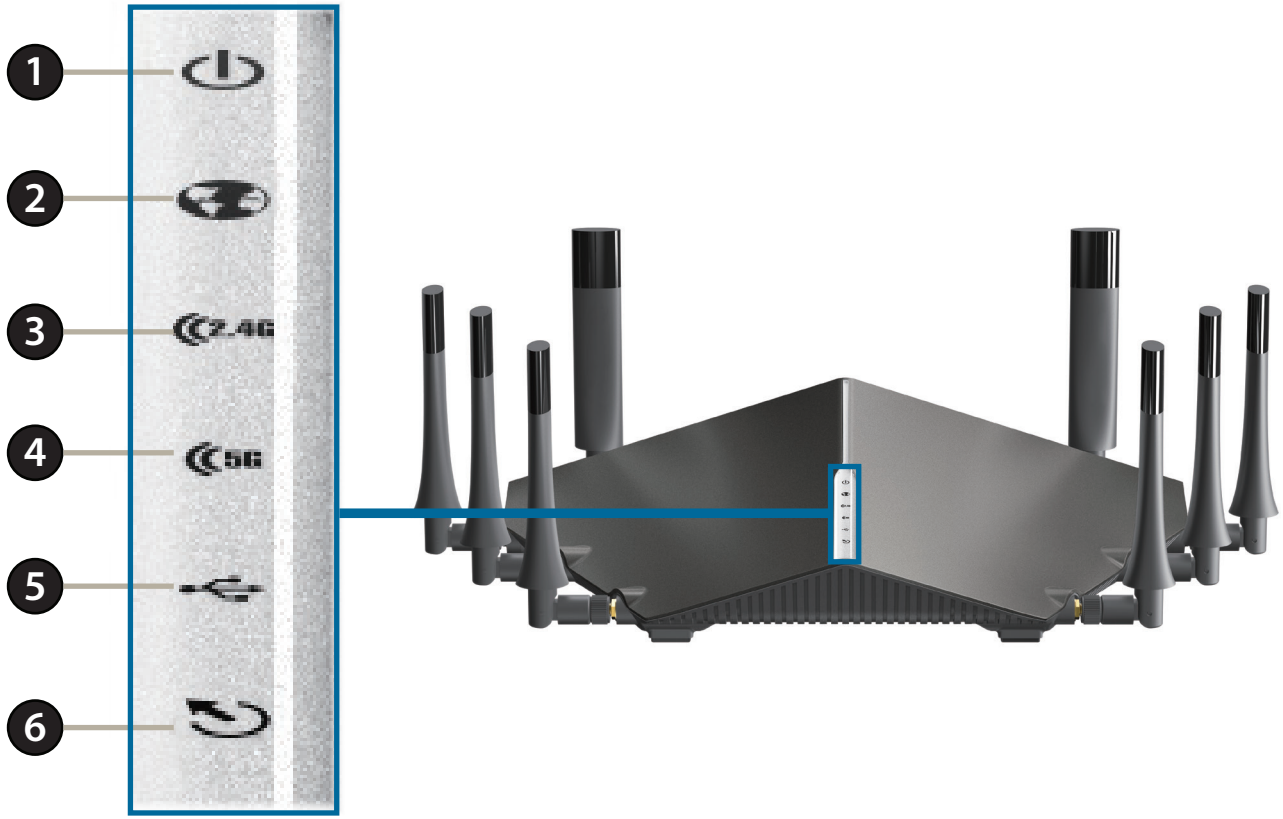
Connections



1	**DSL Port**	Connect to a DSL-enabled telephone line with the supplied microfilter/splitter.
2	**USB 3.0 Port**	Connect a USB flash drive to share content or connect it to a USB printer to share it on your network.
3	**USB 2.0 Port**	Connect a USB flash drive to share content or connect it to a USB printer to share it on your network.
4	**Reset Button**	Insert a paperclip in the hole and wait for several seconds to reset the router to default settings.
5	**WPS Button**	Press to start the WPS process and automatically create a secure connection to a WPS client.
6	**Gigabit WAN Port**	Connects to Ethernet WAN devices.
7	**Gigabit LAN Ports (1-4)**	Connect Ethernet devices such as computers, switches, storage (NAS) devices, and game consoles.
8	**Power Button**	Press the power button to turn the router on or off.
9	**Power Connector**	Connector for the supplied power adapter.

Hardware Overview

LEDs



1	**Power LED**	A solid green light indicates a proper connection to the power supply. The light will be solid red during boot up.
2	**USB 3.0/2.0 LED**	A solid green light indicates that a USB device was detected in the USB 3.0 port. A solid orange light indicates that a USB device was detected in the USB 2.0 port.
3	**Wireless (2.4 GHz) LED**	A solid green light indicates that the 2.4 GHz wireless band is enabled.
4	**Wireless (5 GHz) LED**	A solid green light indicates that the 5 GHz wireless band is enabled.
5	**DSL LED**	A solid green light indicates a proper connection to a DSL-enabled telephone line.
6	**Internet LED**	A solid green light indicates a proper connection to a broadband service.

Installation

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

Note: This installation section is written for users who are setting up their home Internet service with the DSL-5300 Tri-Band Wireless AC5300 Gigabit VDSL Modem Router for the first time. If you are replacing an existing DSL modem and/or router, you may need to modify these steps.

Before you Begin

- Make sure to have your DSL service information provided by your Internet Service Provider handy. This information is likely to include your DSL account's Username and Password. Your ISP may also supply you with additional WAN configuration settings necessary to establish a connection. This information may include the connection type (DHCP IP, Static IP, PPPoE, or PPPoA) and/or ATM PVC details.

- If you are connecting a considerable amount of networking equipment, it may be a good idea to take the time to label each cable or take a picture of your existing setup before making any changes.

- We suggest setting up your DSL-5300 from a single device and verifying that it is connected to the Internet before connecting additional devices.

- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE connection software such as WinPoET, BroadJump, or EnterNet 300 from your computer as the DSL-5300 will provide functionality.

Wireless Installation Considerations

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

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

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

3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.

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

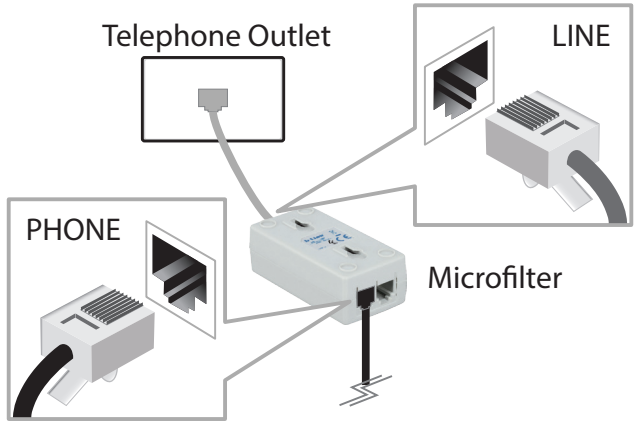
5. If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Manual Setup

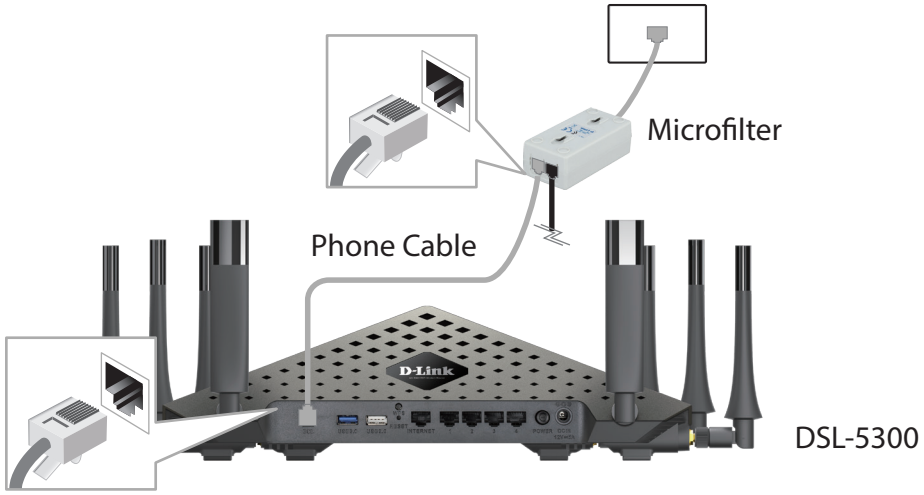
1. Position your router close to a wall jack that provides DSL service. Place the router in an open area of your intended work area for better wireless coverage.

2. Connect your existing phone cable from a telephone outlet to the LINE port on the microfilter and your telephone handset into the PHONE port.

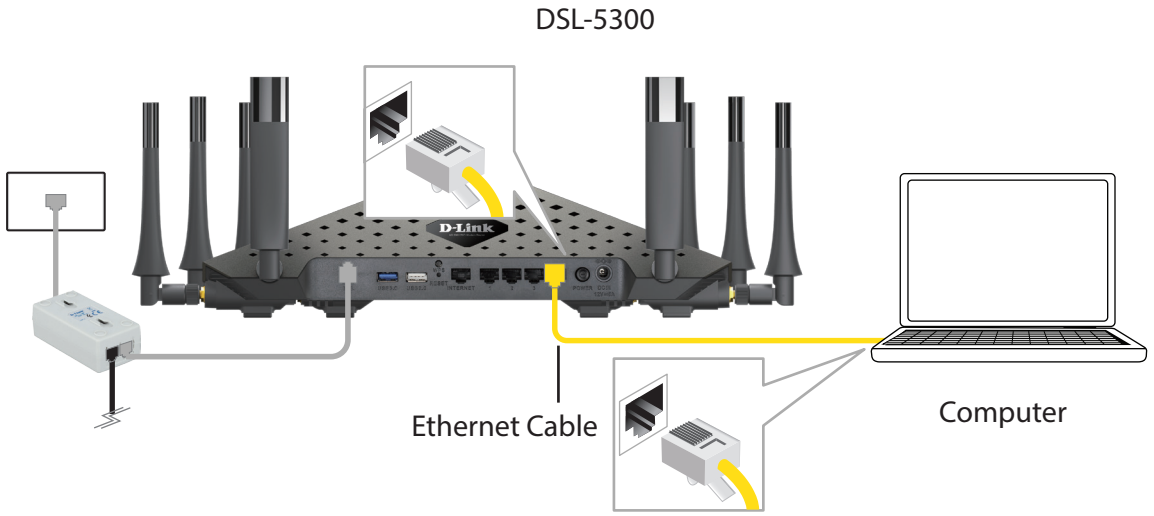
   Caution: *- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.*



3. Connect the phone cable from the DSL port on the Microfilter to the ADSL port of the modem router.

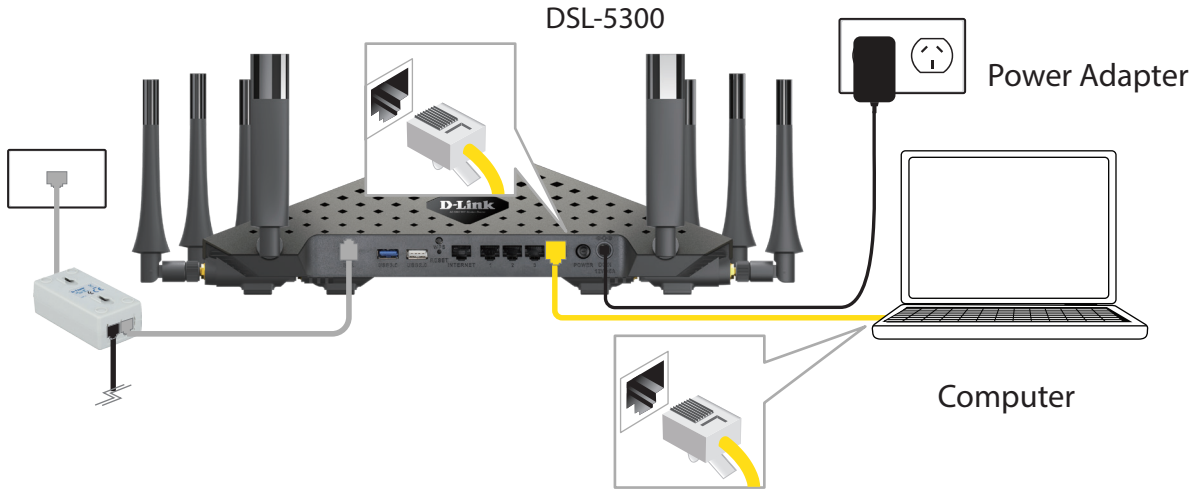


4 If you wish to use a wired connection, connect the Ethernet cable from a LAN port of the DSL-5300 to the Ethernet port on your computer.



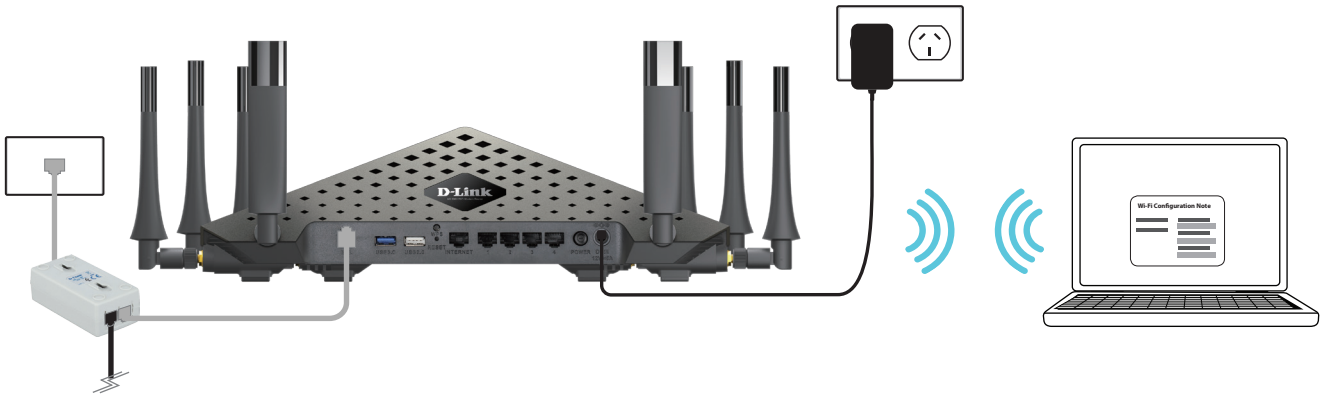
5 Plug the power adapter into your modem router and connect it to an available power outlet or surge protector.

Caution: *- Use only the included power adapter with this product.*



6 Press the power button and verify that the power LED is lit. Allow 1 minute for the router to boot up.

7 If connecting to the DSL-5300 wirelessly, access the wireless utility on your computer or mobile device. Scan for available Wi-Fi networks (SSID). Select and join a Wi-Fi network and use the password corresponding to the information on the supplied Wi-Fi Configuration Card.



Getting Started

There are two ways you can configure your router to connect to the Internet and connect to your clients:

- **D-Link Setup Wizard** - This wizard will launch when you log into the router for the first time. Refer to page "Setup Wizard" on page 14.

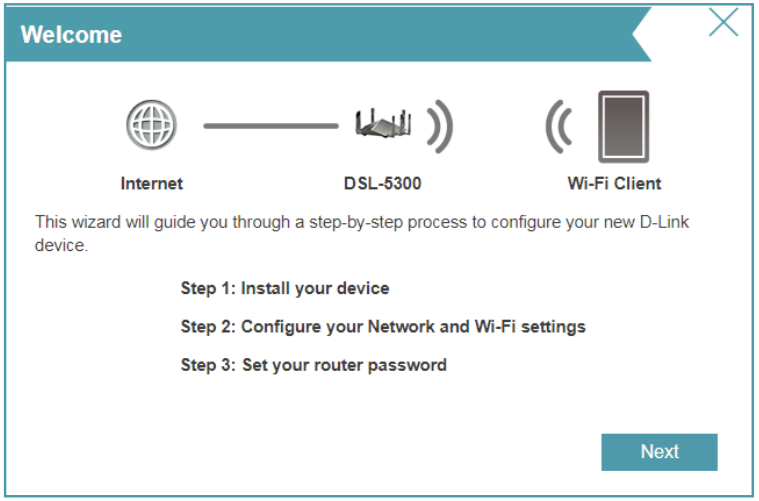
- **Manual Setup** - Log into the router and manually configure your router. Refer to "Configuration" on page 20.

Setup Wizard

If this is your first time installing the router, open your web browser and enter **http://dlinkrouter.local./** in the address bar. Alternatively, enter the IP address of the router (default: **http://192.168.1.1**).

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

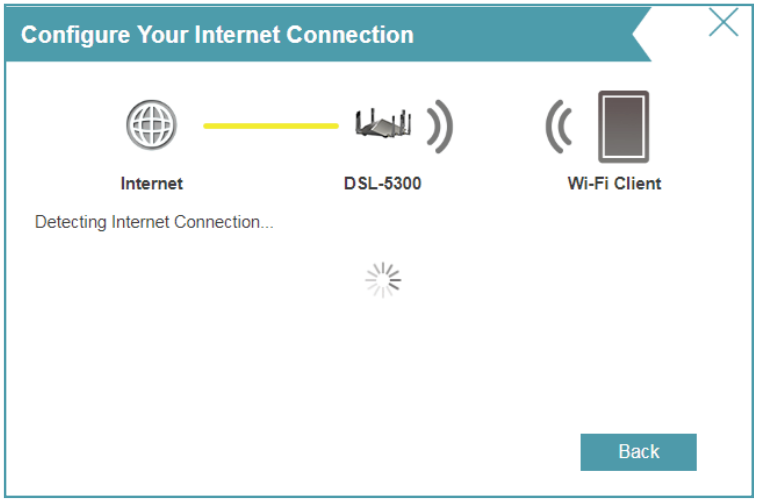
Click **Next** to continue.



Ensure that your DSL phone cable is connected to both the router and the wall jack.

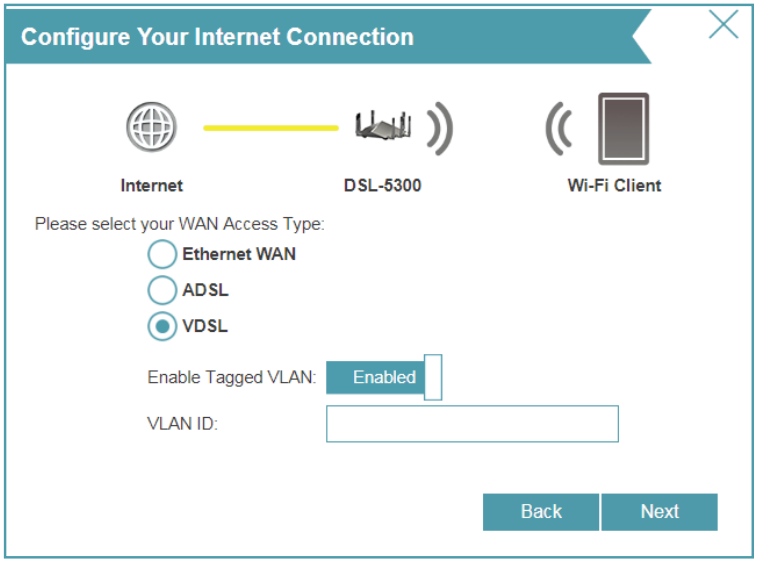
Click **Next** to continue.

Please wait while your router detects your Internet connection type. If the router detects your Internet connection, you may need to enter your ISP information such as username and password.



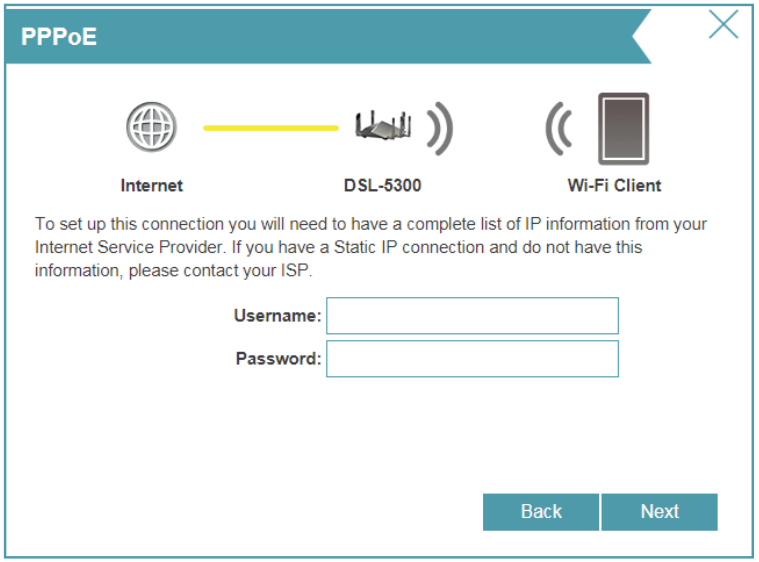
If the router does not detect a valid Internet connection, a list of connection types to choose from will be displayed.

Select your Internet connection type (this information can be obtained from your Internet Service Provider) and click **Next** to continue.



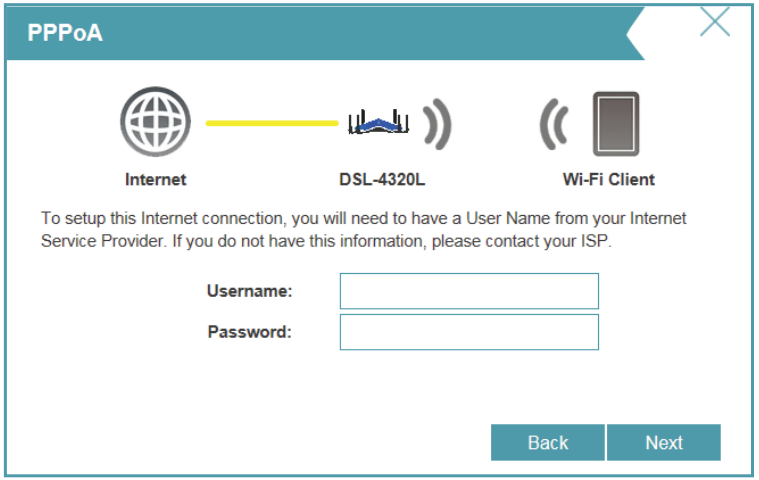
If the router detected or you selected **PPPoE**, enter your PPPoE username and password and click **Next** to continue.

Note: *Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.*

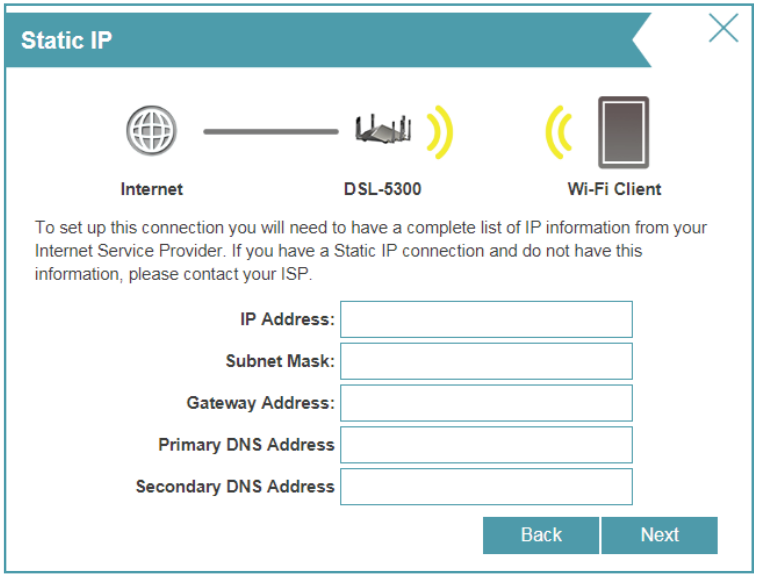


If the router detected or you selected **PPPoA**, enter your PPPoA username and password and click **Next** to continue.

Note: *Make sure to remove your PPPoA software from your computer. The software is no longer needed and will not work through a router.*



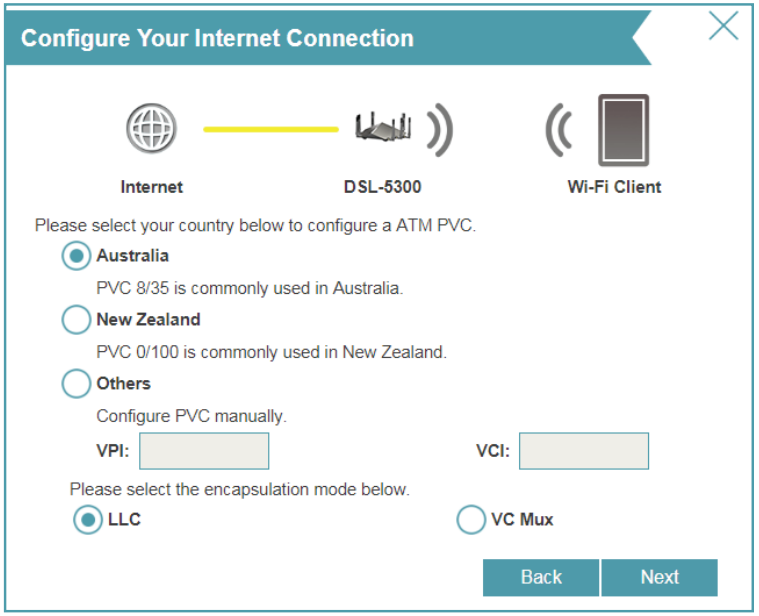
If the router detected or you selected **Static**, enter the IP and DNS settings supplied by your ISP. Click **Next** to continue.



You may be prompted to select a country. If you are not in Australia or New Zealand, select **Others** and configure the Asynchronous Transfer Mode Permanent Virtual Circuit (ATM PVC) settings manually. We suggest using the default Virtual Path Identifier (VPI), Virtual Channel Identifier(VCI), and Logical Link Control (LLC) encapsulation settings unless directed by your ISP.

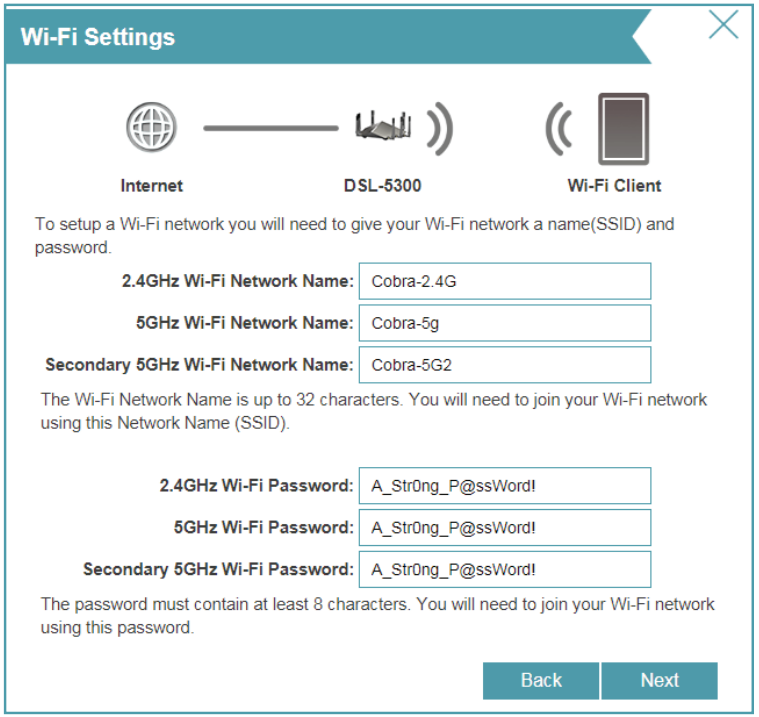
These settings may be adjusted later from the Web Configuration Utility. For more information refer to "ATM" on page 42.

Click **Next** to continue.

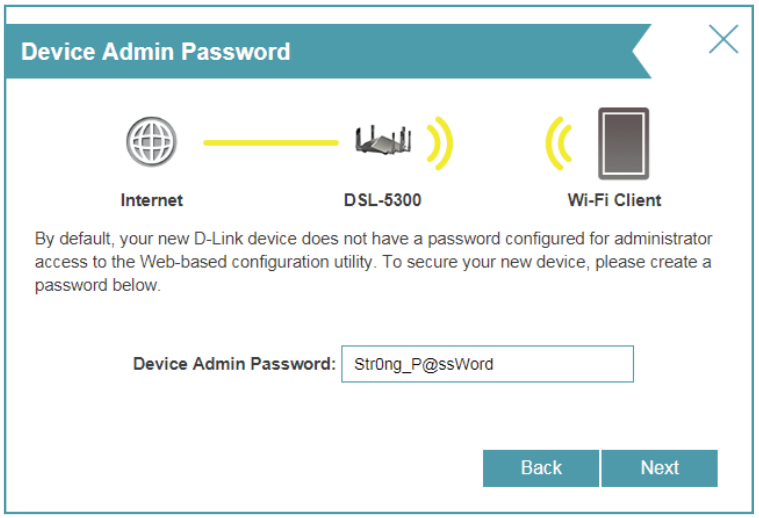


Create a Wi-Fi password (between 8-63 characters). Your wireless clients will need to have this passphrase or key entered to be able to connect to your wireless network.

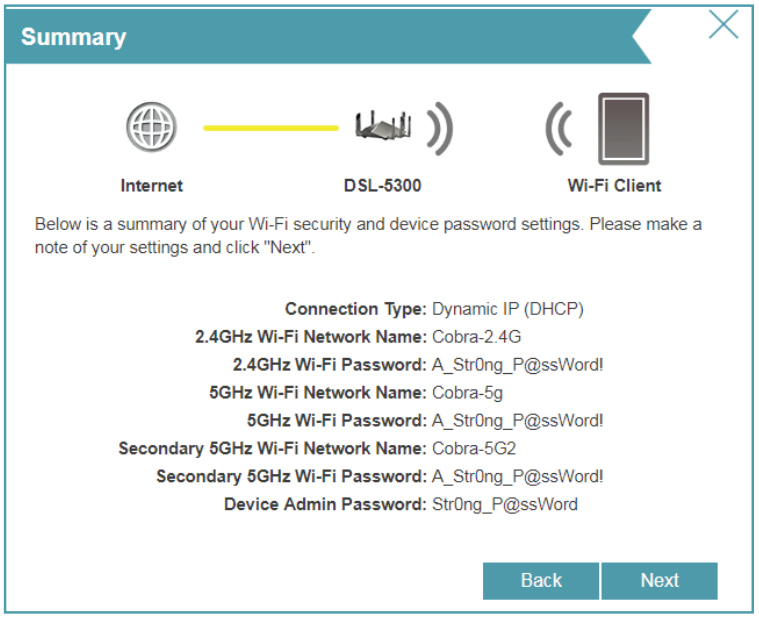
Click **Next** to continue.



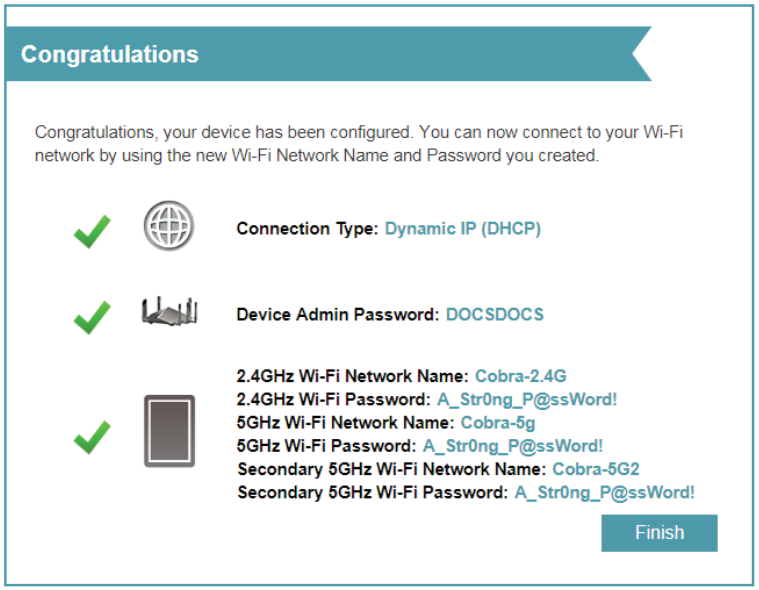
Enter a new administrator password. You will be prompted for this password every time you want to use the router's web configuration utility. Click **Next** to continue.



The Summary window will display your settings. Click **Next** if you are satisfied, or click **Back** to make changes to them.



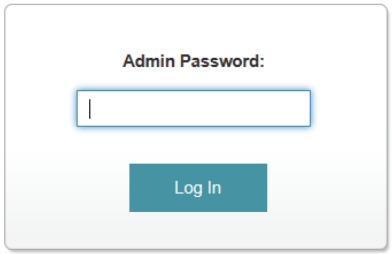
At the end of the wizard, you will be presented with a final summary of your settings. Click **Finish** to close the wizard.



Configuration

To access the configuration utility, open a web-browser such as Internet Explorer and enter **http://192.168.1.1** in the address bar.

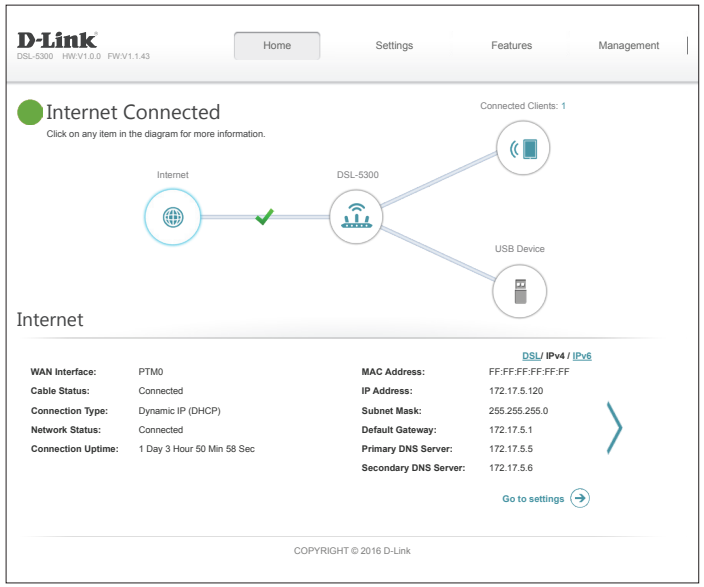
Enter your password. If you previously followed the Setup Wizard (see page 14), please use the admin password you entered during the wizard. Otherwise, leave the password blank. Click **Log In** to proceed.



Note: *If you cannot remember your password and cannot log in, press the reset button (see page 6) to restore the router to its default settings.*

Home

The Home page displays the current status of the router in the form of an interactive diagram. There are four main sections: **Internet**, **DSL-5300**, **Connected Clients**, and **USB Device**. You can click each icon to display information about each section at the bottom of the screen. The menu bar at the top of the page will allow you to quickly navigate to the Settings and Management functions. You may quickly jump back Home at any time.



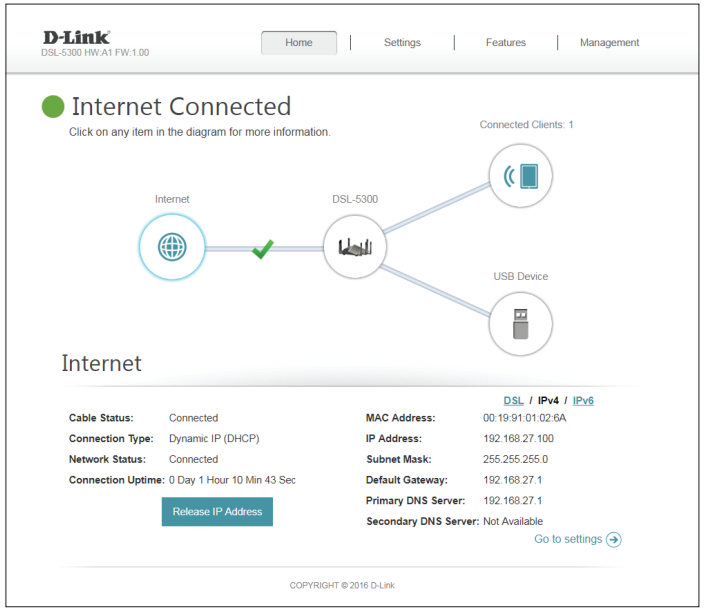
Note: *The system will automatically log out after a period of inactivity.*

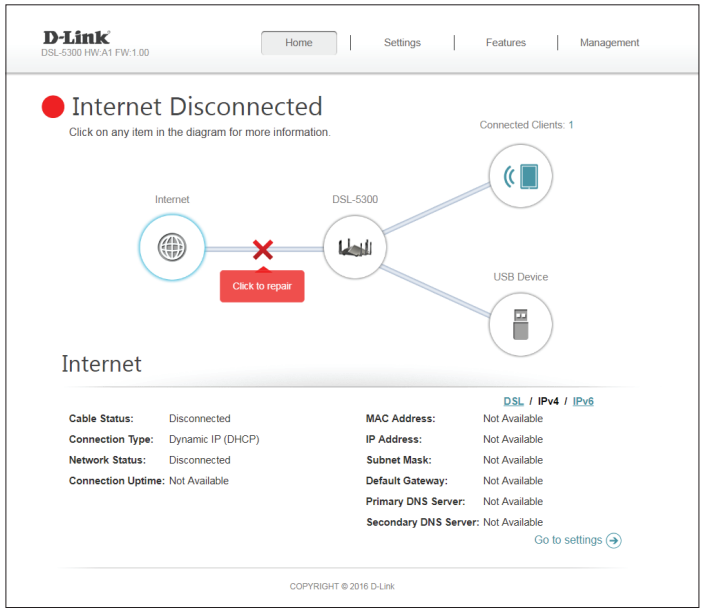
Internet

To bring up more details about your Internet connection, click on the **Internet** icon. You may cycle through the WAN interfaces at the bottom of the page by clicking on the arrows on the left and right sides of the screen. The Internet Connection status at the top of the diagram will reflect the status of the currently selected WAN interface.

If your Internet is disconnected, you can click **Click to repair** to bring up the Setup Wizard.

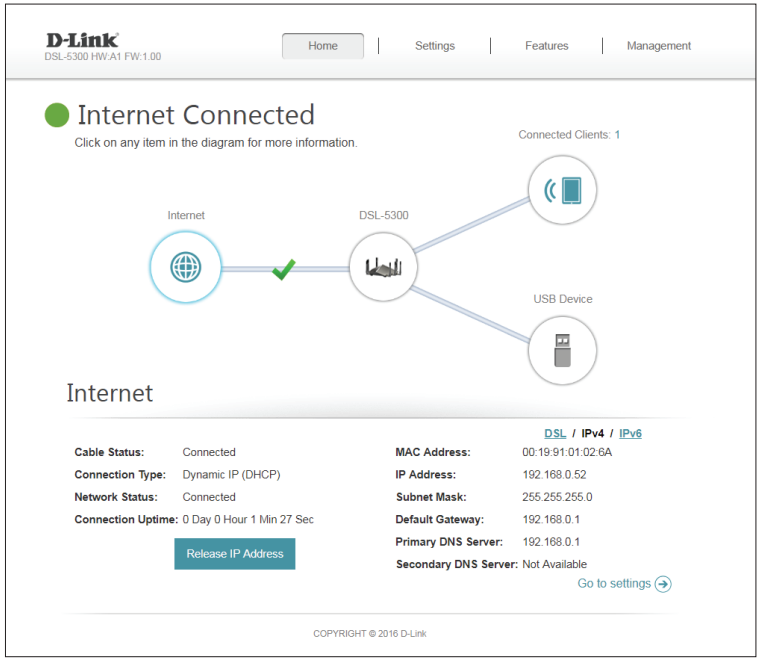
For each of the WAN interfaces, you can see the connection status, IPv4, and IPv6 information. Clicking the DSL button will display DSL port information.





IPv4

Click the **IPv4** button to see the IPv4 information for each WAN interface.



Cable Status: Displays the current cable connection status.

Connection Type: Displays the network protocol used to obtain an IP address.

Network Status: Displays the current network connection status.

Connection Uptime: Displays the amount of time the connection has been connected.

Release/Renew IP Address: Releases/Renews the current WAN IP address.

MAC Address: The WAN interface's MAC address is listed here.

IP Address: The WAN IP address is listed here.

Default Gateway: The default gateway IP address is listed here.

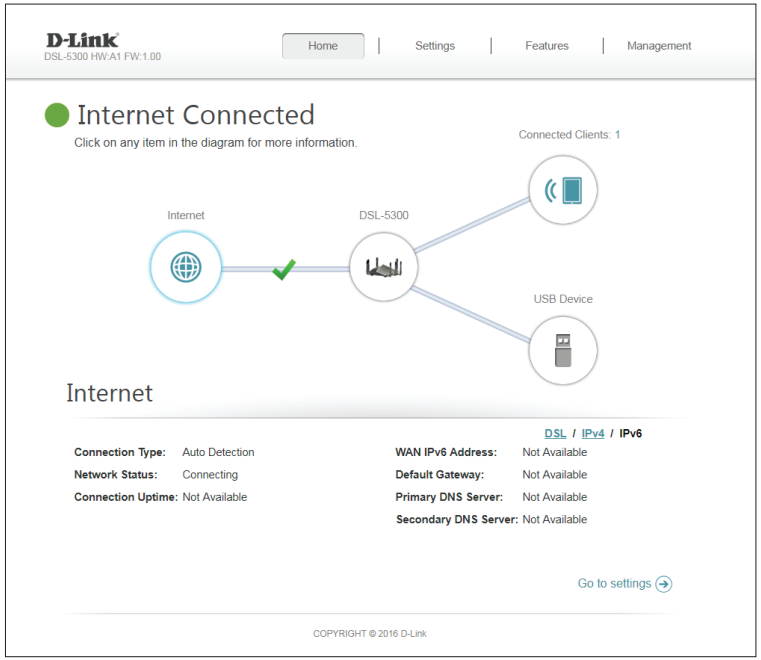
Primary DNS Server: Displays the current primary DNS server.

Secondary DNS Server: Displays the current secondary DNS server.

Click the **Go to settings** button to be taken to **Internet on page 29.**

IPv6

Click the **IPv6** button to see the IPv6 information for each WAN interface.



Connection Type: Displays the network protocol used to obtain an IP address.

Network Status: Displays the current network connection status.

Connection Uptime: Displays the amount of time the connection has been connected.

WAN IPv6 Address: The WAN IPv6 address is listed here.

Default Gateway: The default gateway IP address is listed here.

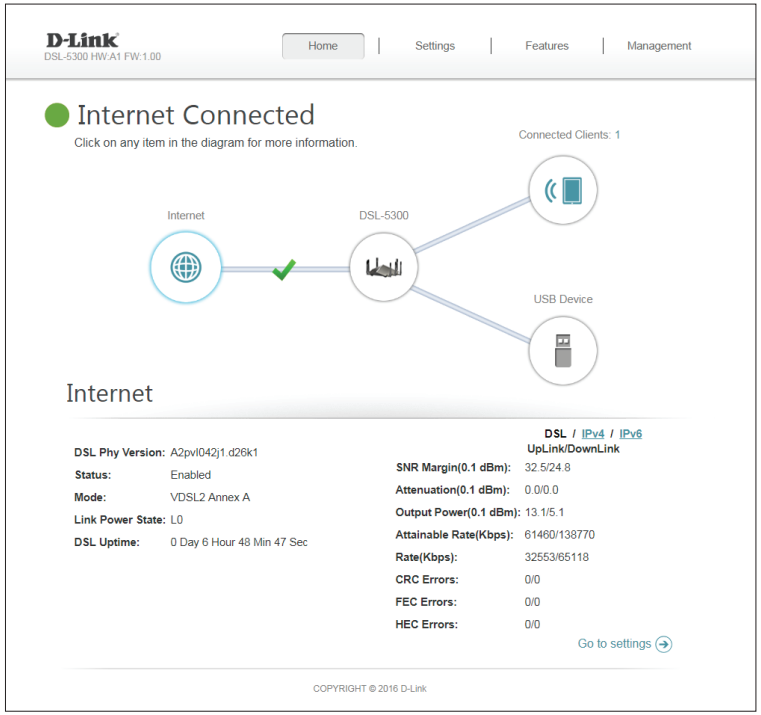
Primary DNS Server: The primary DNS server IP address is listed here.

Secondary DNS Server: The secondary DNS server IP address is listed here.

Click the **Go to settings** button to be taken to **IPv6 on page 45.**

DSL

Click the **DSL** button to see the DSL hardware connection information.



DSL Phy Version: Displays the DSL Phy version.

Cable Status: Displays the current cable status.

DSL Status: Displays the current negotiation state of the DSL port.

Mode: Displays the current DSL mode.

Link Power State: Displays the current link power state.

SNR Margin (0.1 dB): The DSL connection's signal-to-noise ratio is listed here.

Attenuation (0.1 dB): The DSL connection's attenuation is listed here.

Output Power (0.1 dBm): The DSL connection's power output is listed here.

Attainable Rate (Kbps): The measured maximum attainable rate is listed here.

Rate (Kbps): The negotiated connection speed is listed here.

CRC Errors: Displays the number of Cyclic Redundancy Check errors.

FEC Errors: Displays the number Forward Error Correction Errors.

HEC Errors: Displays the number of Header Error Control Errors.

Click the **Go to settings** button to be taken to **Internet on page 29.**

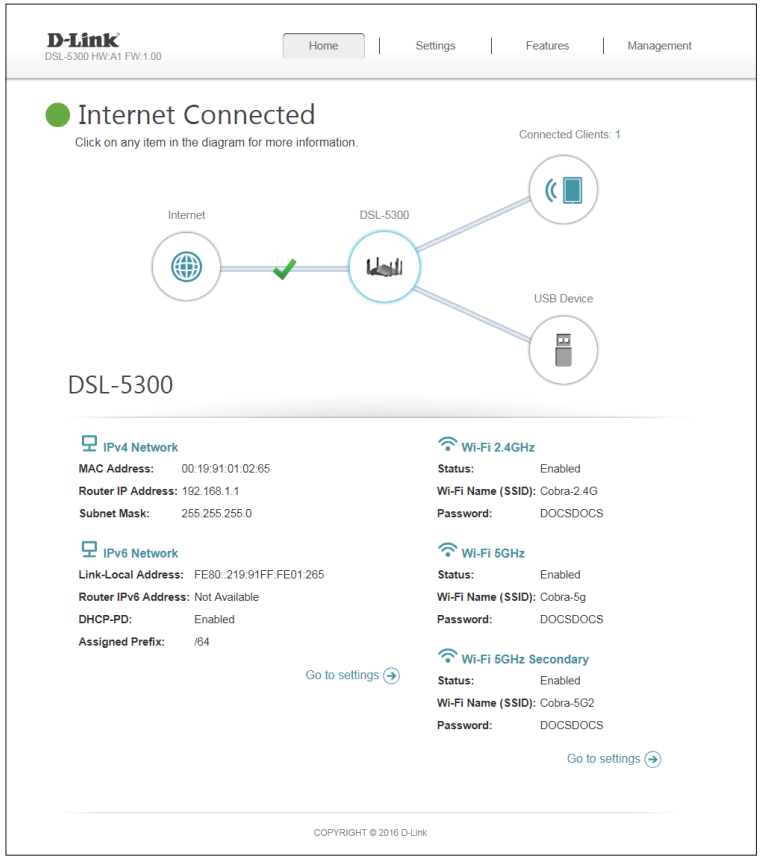
DSL-5300

Click on the **DSL-5300** icon to view details about the router and its wireless settings.

Here you can see the router's current wireless networks and passwords, as well as the local area network MAC, IPv4, and IPv6 addresses.

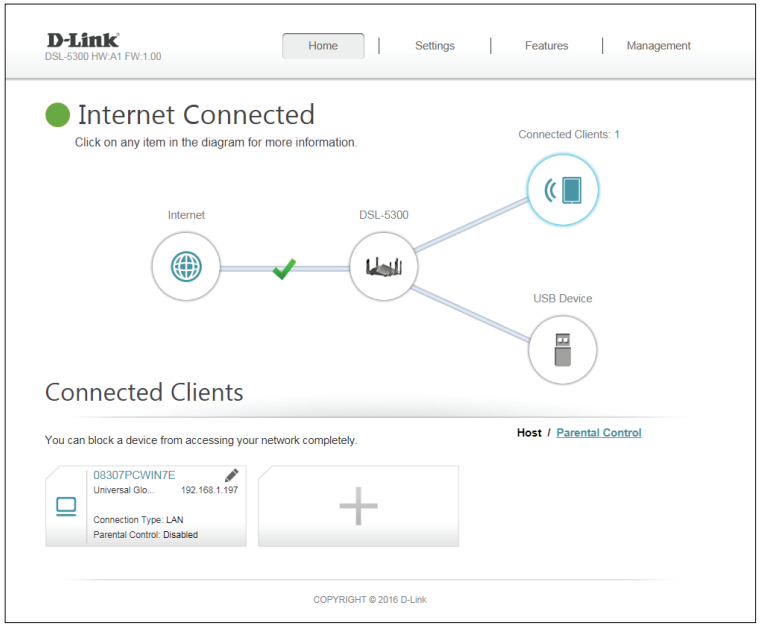
To reconfigure the network settings, click the **Go to settings** link, from the **Settings** menu at the top of the page, select **Network**. Refer to page 65 for more information.

To reconfigure the wireless settings, click the **Go to settings** link, from the **Settings** menu at the top of the page, select **Wireless**. Refer to page 59 for more information.



Connected Clients

Click on the **Connected Clients** icon to view details about the router and its wireless settings.



On this page, you can see all the clients currently connected to the router and their IP addresses.

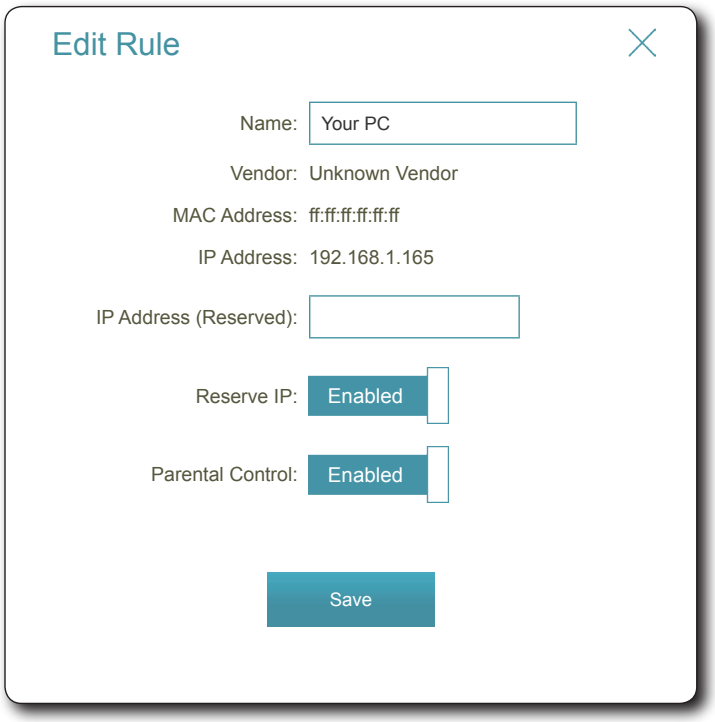
To edit each client's settings, click the pencil icon on the client you want to edit.

Connected Clients (Cont)

Click on the **Connected Clients** icon to view details about the router and its wireless settings.

On this page. you can see all the clients currently connected to the router and their IP addresses.

To edit each client's settings, click the pencil icon on the client you want to edit.



Edit Rule

Name: Enter a custom name for this client.

Vendor: Displays the vendor of the device.

MAC Address: Displays the MAC address of the device.

IP Address: Enter a specific IP address for this client if **Reserve IP** is enabled.

Reserve IP: Enable to reserve this IP address for this client.

Parental Control: Allow or Block access to the router.

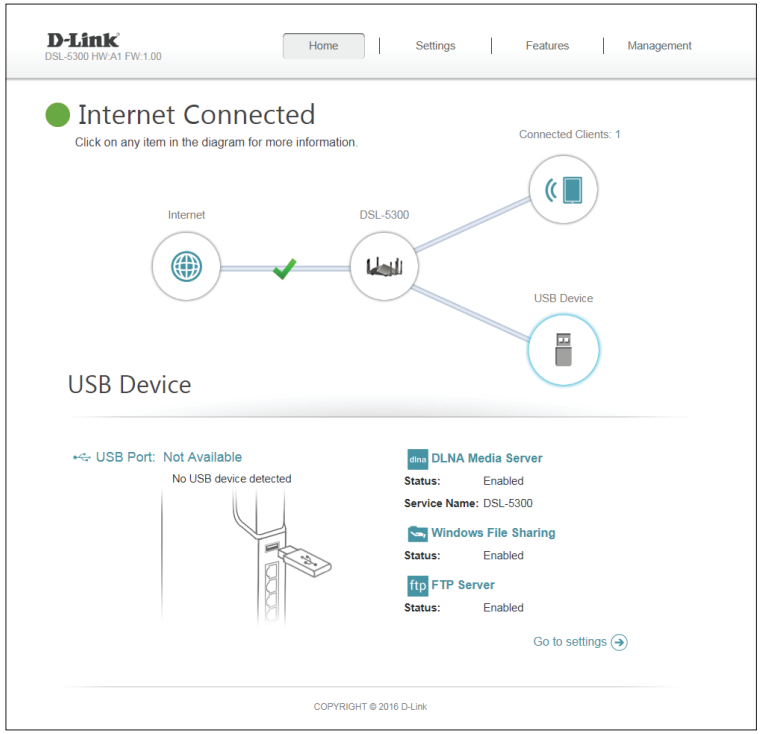
Click **Save** when you are done.

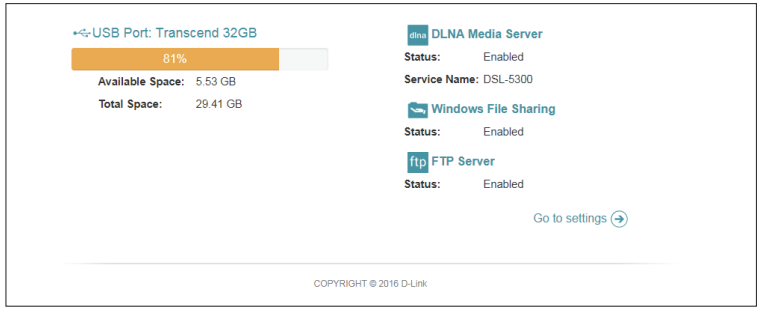
USB Device

Click on the **USB Device** icon to view details about the currently connected USB device, SharePort, and Windows File Sharing.

If you have a USB device connected, you can see its name and how much free space it has.

To configure your SharePort settings, click **Go to settings** and refer to page 67 for more information.





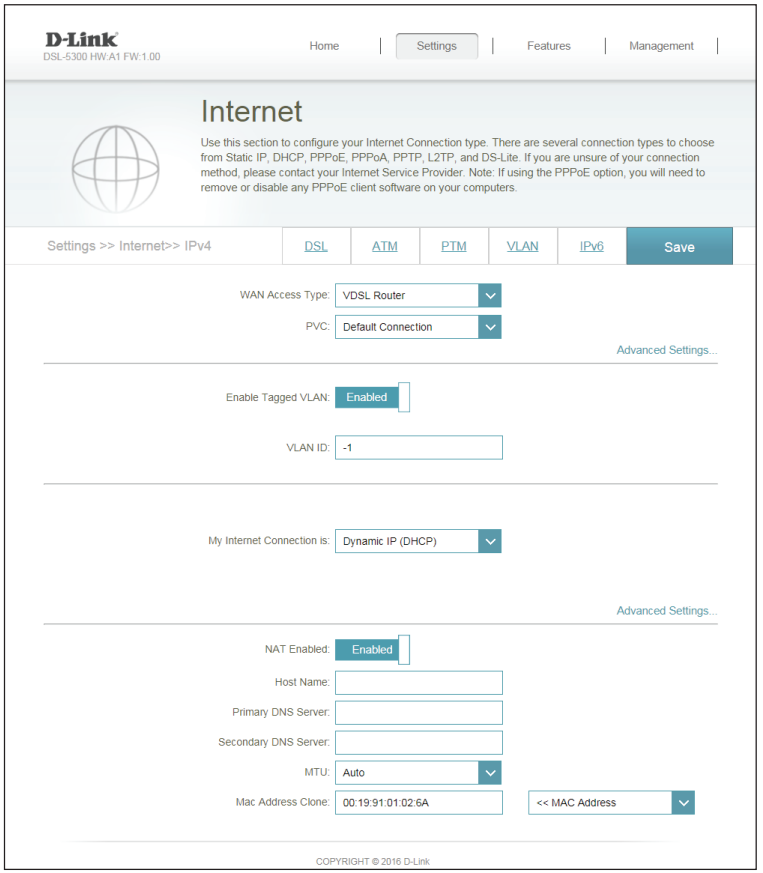
Settings

Wizard

In the Settings menu on the bar on the top of the page, click **Wizard** to open the setup wizard. This is the same wizard that appears when you start the router for the first time. Refer to **Setup Wizard** on page 14 for more information.

Internet

In the Settings menu on the bar on the top of the page, click **Internet** to see the Internet configuration options. Click **Advanced Settings...** to expand the list and see all of the options.



You will see the settings for your **IPv4** connection.

To configure the advanced DSL settings, click the **DSL** link. Refer to **DSL on page 41**.

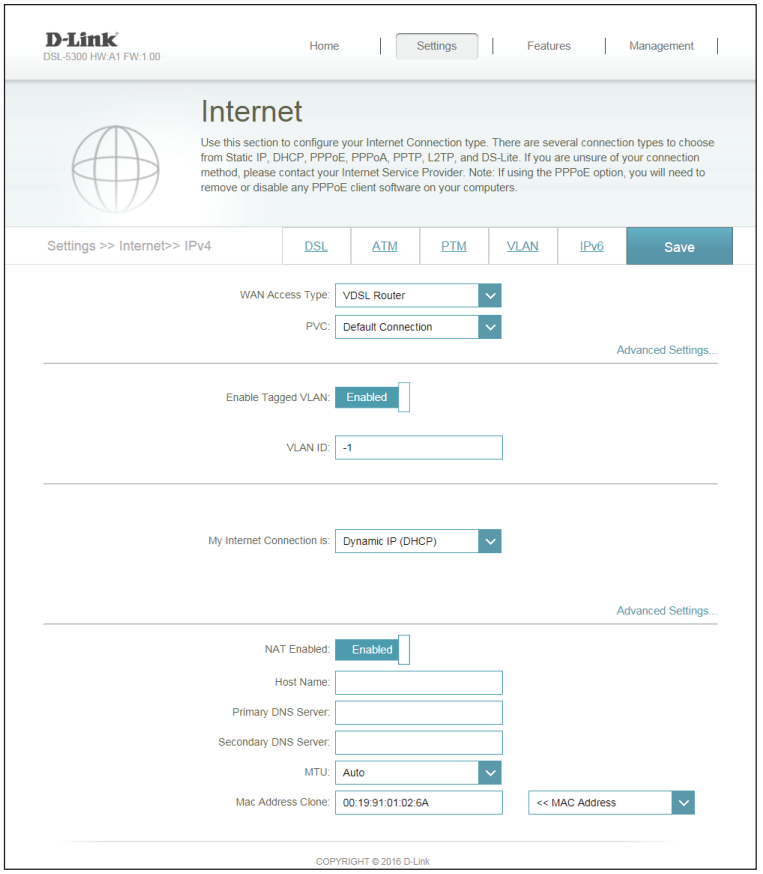
To configure the ATM settings, click the **ATM** link. Refer to **ATM on page 42**.

To configure the PTM settings, click the **PTM** link. Refer to **PTM on page 43**.

To configure the VLAN settings, click the **VLAN** link. Refer to **VLAN on page 44.**

To configure an IPv6 connection, click the **IPv6** link. Refer to **IPv6 on page 45**.

In the Settings menu on the bar on the top of the page, click **Internet** to see the Internet configuration options. Click **Advanced Settings...** to expand the list and see all of the options.



WAN Access Type: Select whether the device should act as an **ADSL Router**, a **VDSL Router**, a **Residential Gateway**, or a **3G/4G Dongle**.

PVC: Use the default setting unless otherwise instructed by your ISP.

Ether WAN Port: If you selected **Residential Gateway**, select the Ethernet port that will connect to the WAN. Use this setting if you do not intend to use the built-in DSL modem.

Enable Tagged VLAN: Enable or disable Tagged VLAN.

VLAN ID: Enter the VLAN ID.

My Internet Connection Is: Choose your Internet connection type from the drop-down menu. You will be presented with the appropriate options for your connection type.

For **Dynamic IP (DHCP)** refer to **Dynamic IP (DCHP) on page 31**.

For **Static IP** refer to **Static IP on page 32.**

For **PPPoE** refer to **PPPoE on page 33.**

For **PPPoA** refer to **PPPoA on page 34.**

For **PPTP** refer to **PPTP on page 35.**

For **L2TP** refer to **L2TP on page 37.**

For **DS-Lite** refer to **DS-Lite on page 39**

For **Bridge** refer to **Bridge on page 40.**

IPv4

Dynamic IP (DCHP)

Select **Dynamic IP (DHCP)** to obtain IP address information automatically from your Internet Service Provider (ISP). Select this option if your ISP does not give you an IP address to use.

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

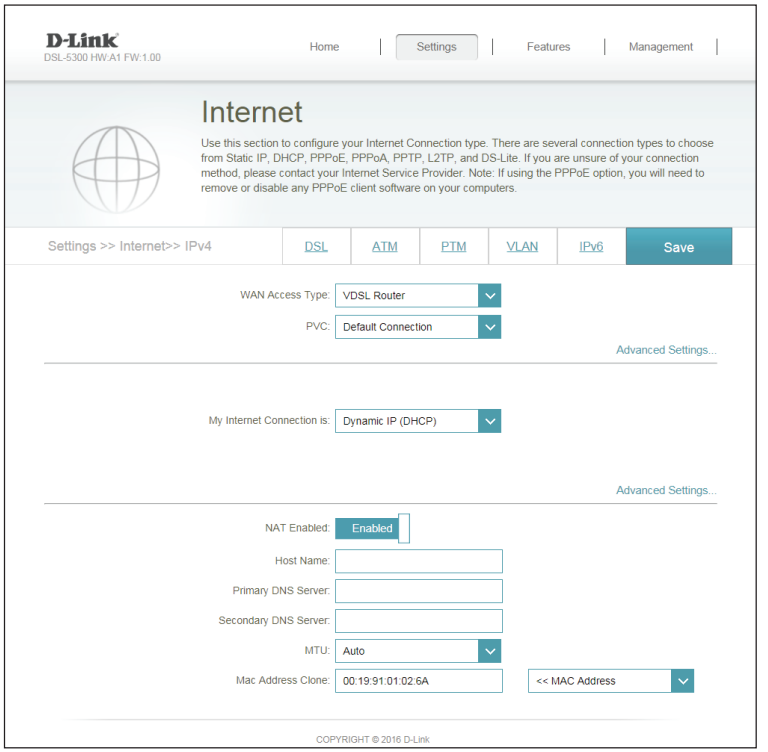
Primary DNS Server: Enter the primary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

Secondary DNS Server: Enter the secondary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

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

MAC Address Clone: The default MAC address is set to the Internet port's physical interface MAC address on the router. You can use the drop-down menu to replace the Internet port's MAC address with the MAC address of a connected client.

Click **Save** when you are done.



Static IP

Select **Static IP** if your IP information is provided by your Internet Service Provider (ISP).

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

Subnet Mask: Enter the subnet mask provided by your ISP.

Default Gateway: Enter the default gateway address provided by your ISP.

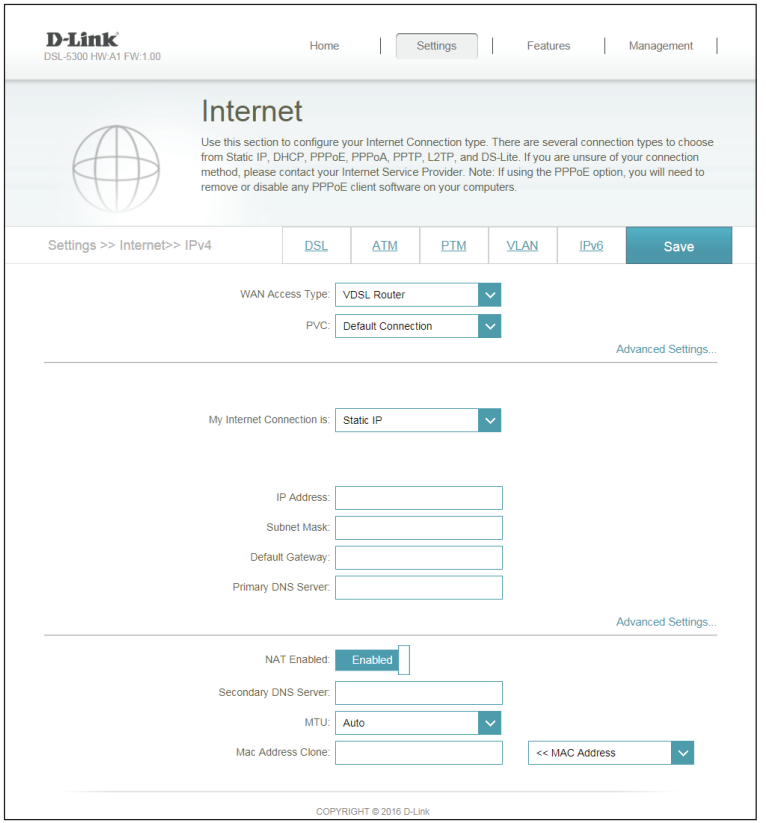
Primary DNS Server: Enter the primary DNS server IP address assigned by your ISP.

Secondary DNS Server: Enter the secondary DNS server IP address assigned by your ISP.

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

MAC Address Clone: The default MAC address is set to the Internet port's physical interface MAC address on the router. You can use the drop-down menu to replace the Internet port's MAC address with the MAC address of a connected client.

Click **Save** when you are done.



PPPoE

Select **PPPoE** if your Internet connection requires you to enter a PPPoE username and password. This information is provided by your Internet Service Provider (ISP).

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

Reconnect Mode: Select either **Always-on**, **On-Demand**, or **Manual**.

Address Mode: Select **Static IP** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic IP**.

IP Address: Enter the IP address provided by your ISP (Static IP only).

Service Name: Enter the ISP service name (optional).

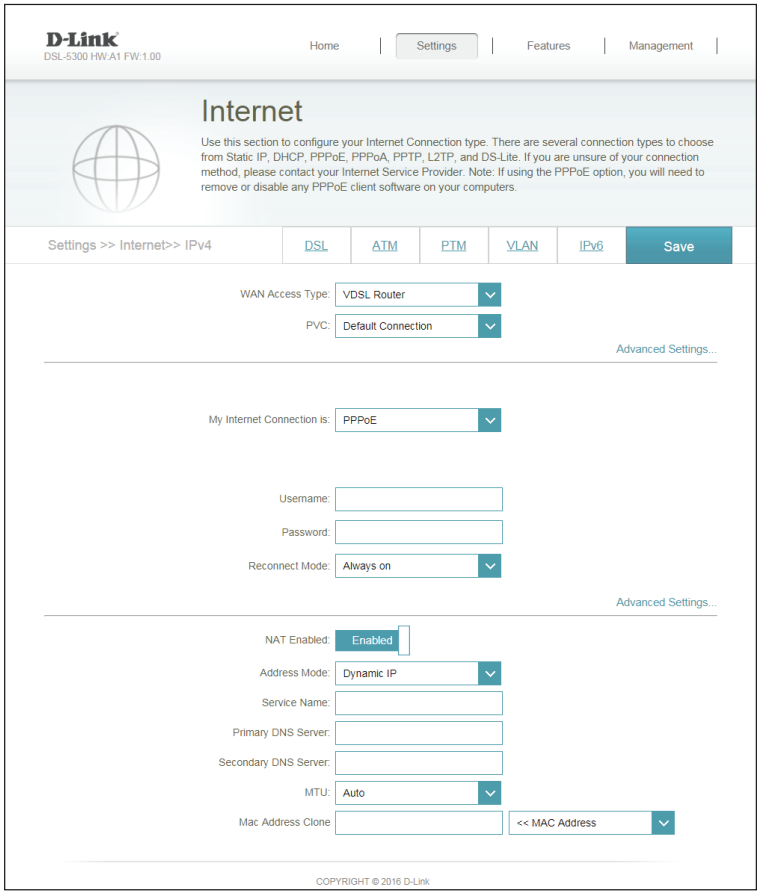
Primary DNS Server: Enter the primary DNS server IP address assigned by your ISP.

Secondary DNS Server: Enter the secondary DNS server IP address assigned by your ISP.

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

MAC Address Clone: The default MAC address is set to the Internet port's physical interface MAC address on the router. You can use the drop-down menu to replace the Internet port's MAC address with the MAC address of a connected client.

Click **Save** when you are done.



PPPoA

Choose **PPPoA** if your Internet connection requires you to enter a PPPoA username and password. This information is provided by your Internet Service Provider (ISP).

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

Reconnect Mode: Select either **Always-on**, **On-Demand**, or **Manual**.

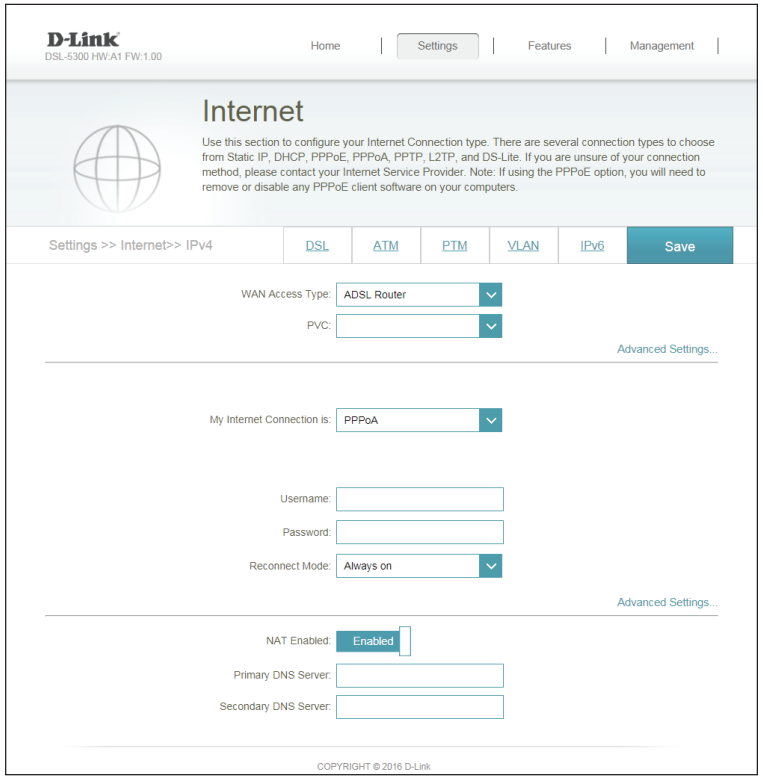
Address Mode: Select **Static IP** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic IP**.

IP Address: Enter the IP address provided by your ISP (Static IP only).

Primary DNS Server: Enter the primary DNS server IP address assigned by your ISP.

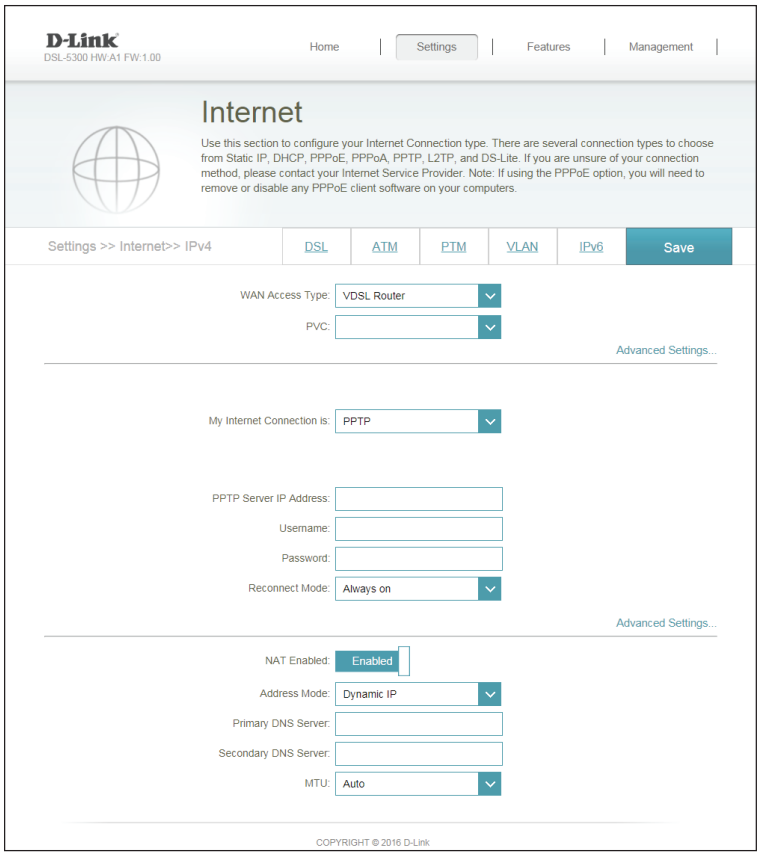
Secondary DNS Server: Enter the secondary DNS server IP address assigned by your ISP.

Click **Save** when you are done.



PPTP

Choose **PPTP** (Point-to-Point-Tunneling Protocol) if your Internet Service Provider (ISP) uses a PPTP connection. Your ISP will provide you with a username and password.



PPTP Server IP Address: Enter the PPTP server IP address provided by your ISP.

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

Reconnect Mode: Select either **Always-on**, **On-Demand**, or **Manual**.

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

Address Mode: Select **Static IP** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic IP**.

PPTP IP Address: Enter the IP address provided by your ISP (Static IP only).

PPTP Subnet Mask: Enter the subnet mask provided by your ISP (Static IP only).

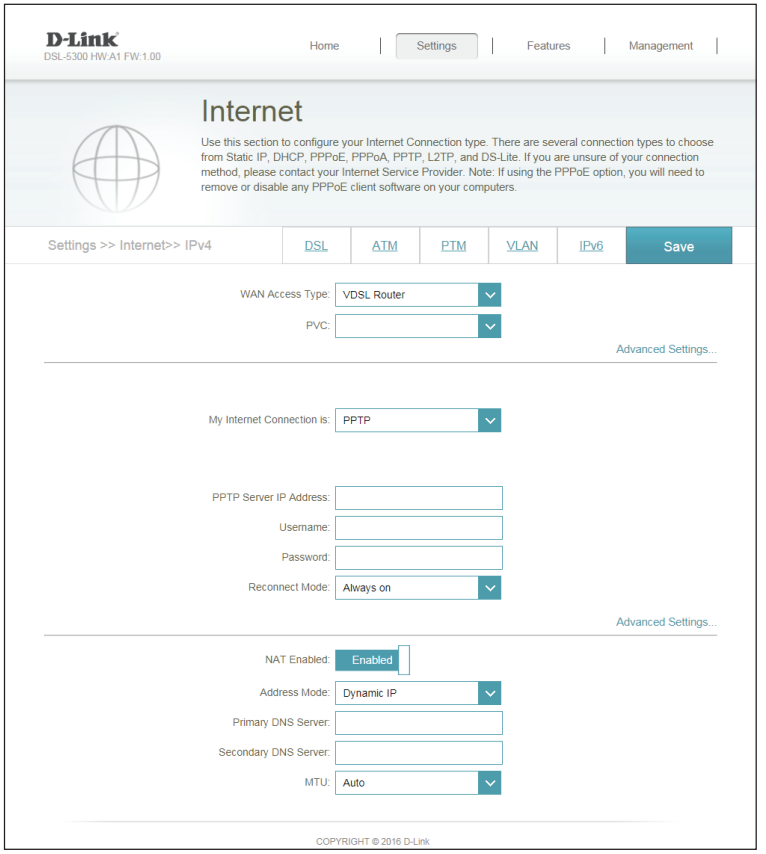
PPTP Gateway IP Address: Enter the gateway IP address provided by your ISP (Static IP only).

Primary DNS Server: Enter the primary DNS server IP address assigned by your ISP.

Secondary DNS Server: Enter the secondary DNS server IP address assigned by your ISP.

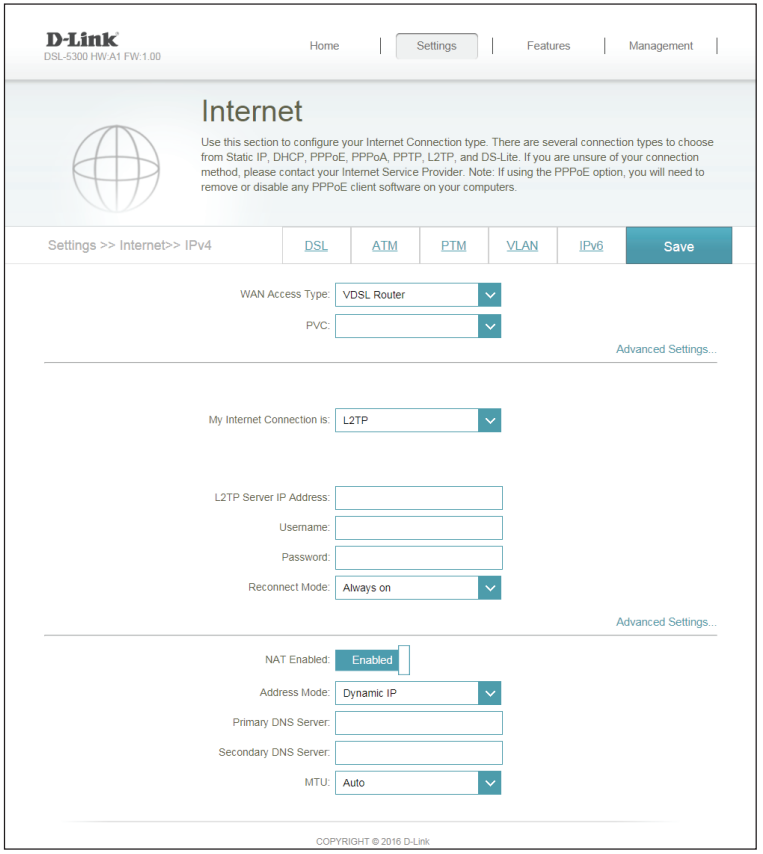
MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your ISP.

Click **Save** when you are done.



L2TP

Choose **L2TP** (Layer 2 Tunneling Protocol) if your Internet Service Provider (ISP) uses an L2TP connection. Your ISP will provide you with a username and password.



L2TP Server IP Address: Enter the L2TP server IP address provided by your ISP.

Username: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

Reconnect Mode: Select either **Always-on**, **On-Demand**, or **Manual**.

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

Address Mode: Select **Static IP** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic IP**.

L2TP IP Address: Enter the IP address provided by your ISP (Static IP only).

L2TP Subnet Mask: Enter the subnet mask provided by your ISP (Static IP only).

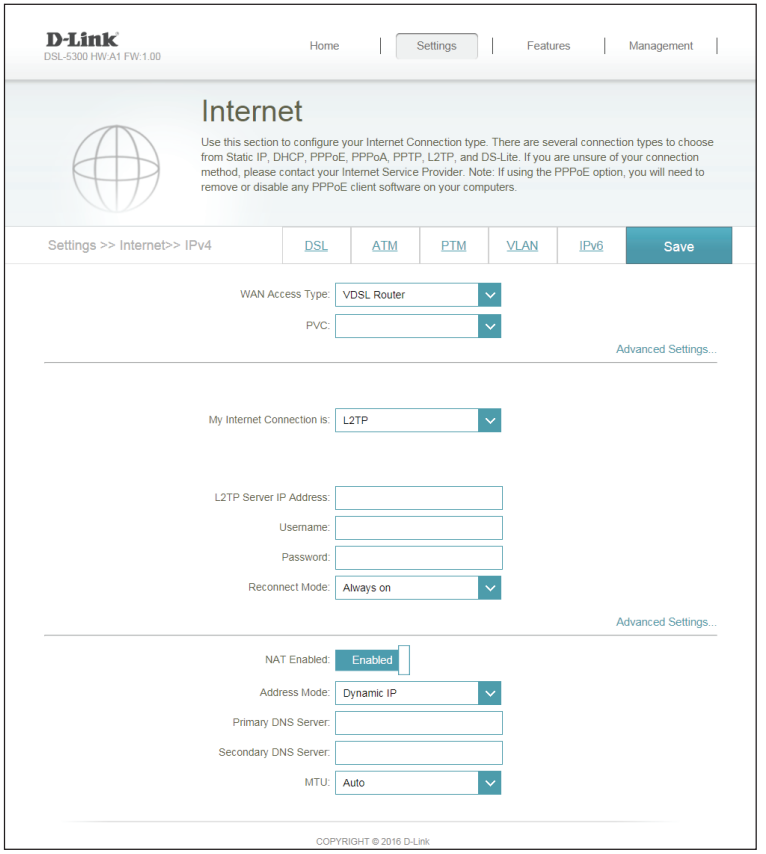
L2TP Gateway IP Address: Enter the gateway IP address provided by your ISP (Static IP only).

Primary DNS Server: Enter the primary DNS server IP address assigned by your ISP.

Secondary DNS Server: Enter the secondary DNS server IP address assigned by your ISP.

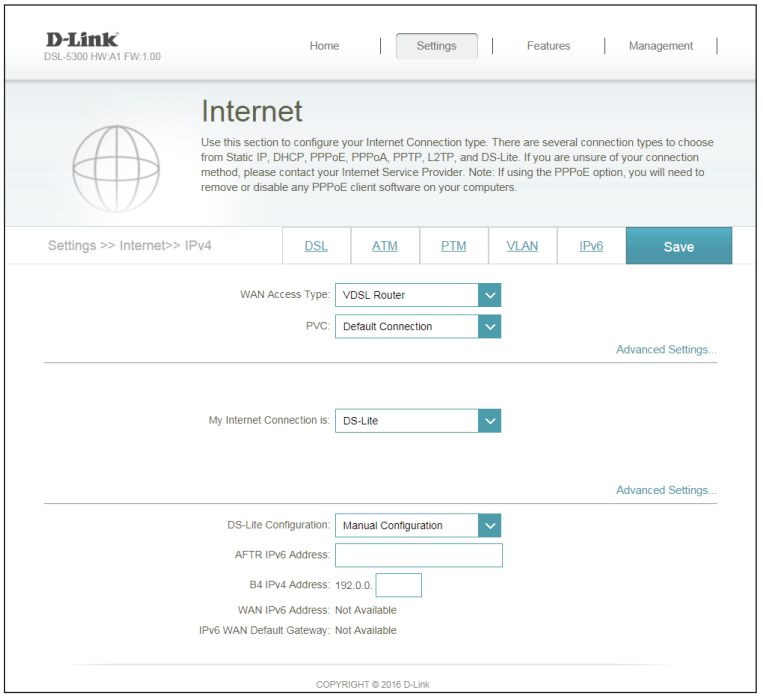
MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your ISP.

Click **Save** when you are done.



DS-Lite

Choose **DS-Lite** if your ISP uses a Dual Stack Lite connection. Your ISP will provide you with the required information. Thisoption is typically used for DSL services.



DS-Lite Configuration: Select **DS-Lite DHCPv6 Option** to have the DS-Lite IPv6 address automatically assigned by the DHCPv6 server. Select **Manual Configuration** to enter the IPv6 information manually.

AFTR IPv6 Address: Enter the AFTR IPv6 address provided by your ISP (Manual configuration only).

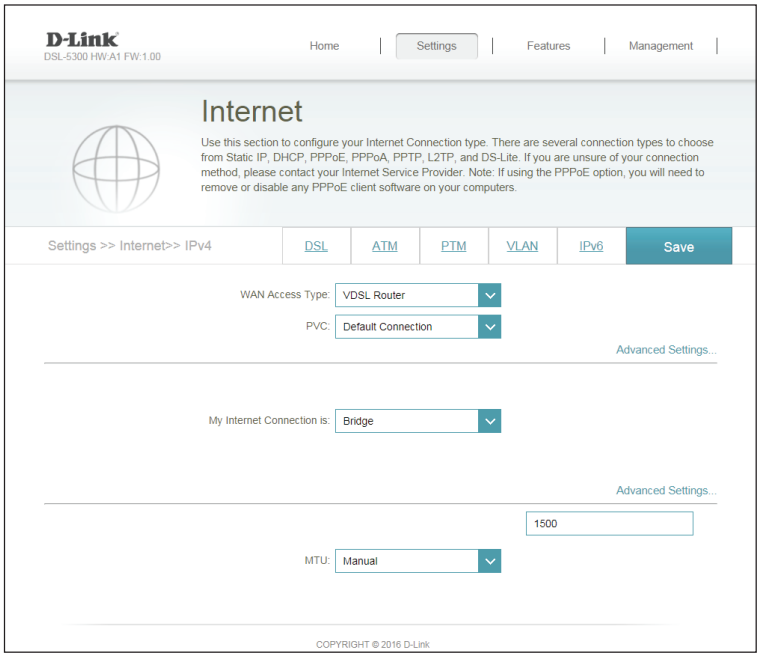
B4 IPv6 Address: Enter the B4 IPv6 address provided by your ISP (optional).

Click **Save** when you are done.

Bridge

Choose **Bridge** to configure the device as a network bridge.

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

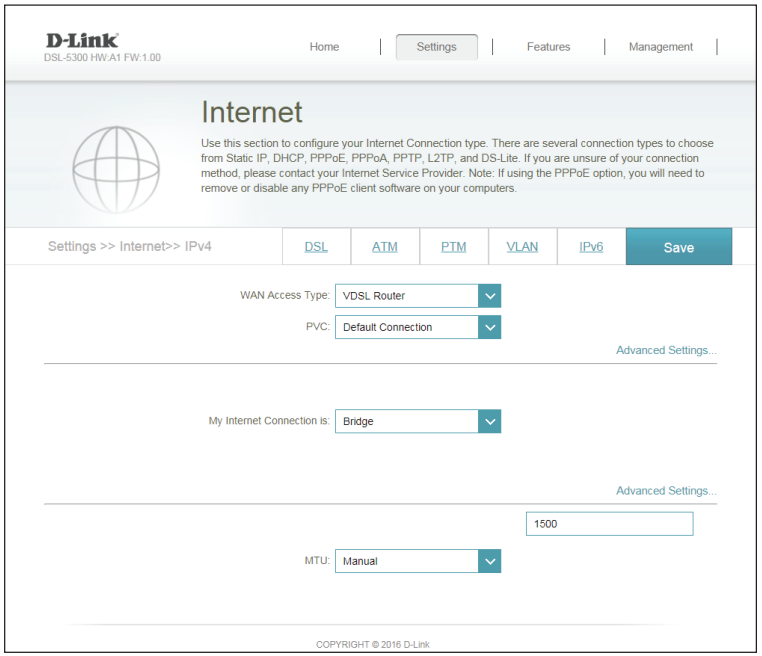


DSL

On this page, you can configure your DSL settings. If you are unsure, you can obtain these settings from your ISP.

DSL Modulation: Select whether to enable or disable each DSL modulation option. Usually, it is best to use the default settings, unless otherwise instructed by your ISP.

Click **Save** when you are done.



ATM

On this page, you can configure your Asynchronous Transfer Mode (ATM) settings. If you are unsure, you can obtain these settings from your ISP.

Interface: Select the ATM interface from the drop-down menu.

VPI: Enter the Virtual Path Indicator (0 - 255).

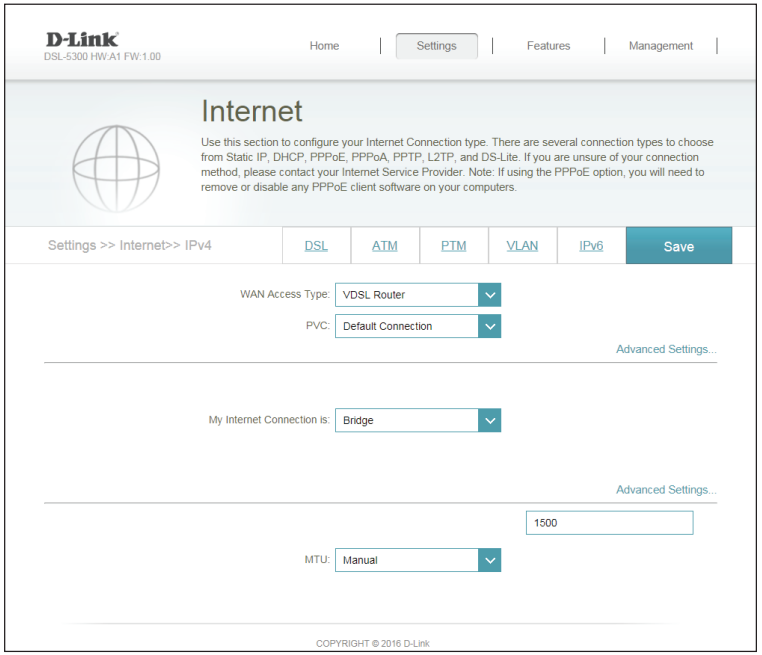
VCI: Enter the Virtual Channel Indicator (32 - 65535).

Latency: Select the latency from the drop-down menu.

Encapsulation: Select the method of encapsulation provided by your ISP. You can select **LLC** or **VCMUX**.

ATM QoS: Select the Quality of Service type from the drop-down menu.

Click **Save** when you are done.



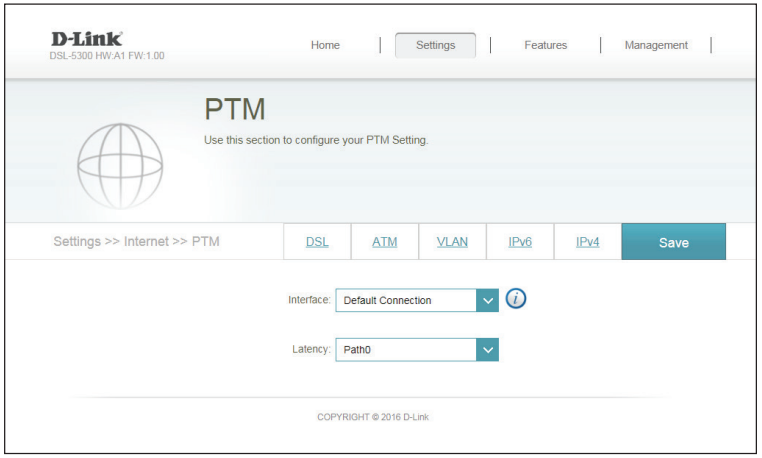
PTM

On this page, you can configure your Packet Transfer Mode (ATM) settings. If you are unsure, you can obtain these settings from your ISP.

Interface: Select the PTM interface from the drop-down menu.

Latency: Select the latency from the drop-down menu.

Click **Save** when you are done.



VLAN

The VLAN bridging feature allows advanced users to enable 802.1Q VLAN tagging on the WAN interface. If you have an Ultra Fast Broadband (UFB) fiber optic connection, your ISP may offer High Priority Committed Information Rate (CIR). This guarantees the bandwidth required for real-time voice and video applications.

In order to utilize the CIR, you must know the proper 802.1Q VLAN tags that your ISP uses. To enable this functionality, define the VLAN IDs, apply the VLAN to the desired interface, and connect your devices.

VLAN: Select **Enable** to enable VLAN support.

Internet VLAN ID: Enter a VLAN ID between 2 and 4094 that will be used for your Internet connection.

IPTV VLAN ID: Enter a VLAN ID between 2 and 4094 that will be used to connect to IPTV services

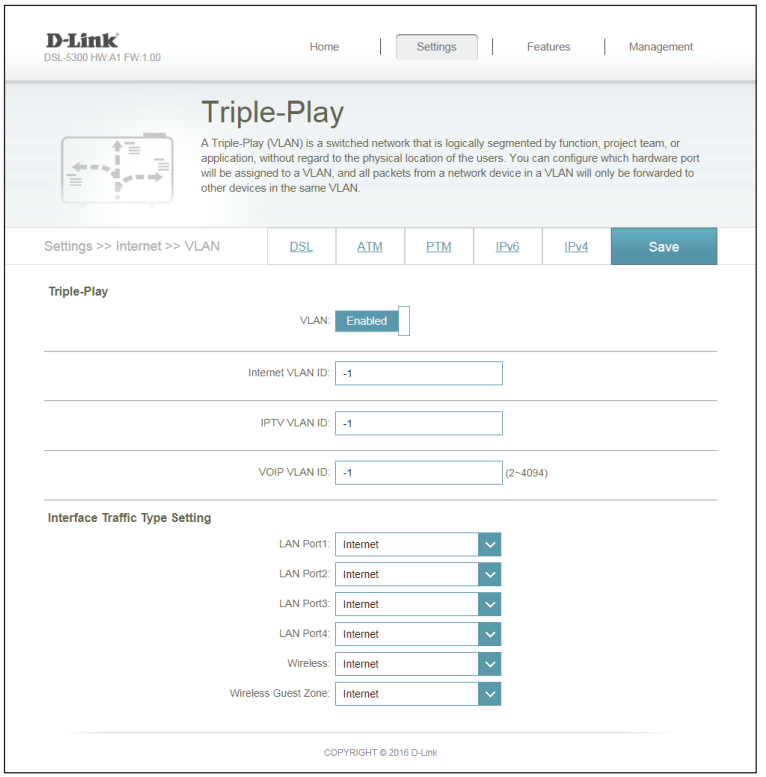
VOIP VLAN ID Enter a VLAN ID between 2 and 4094 that will be used for VoIP services.

LAN Port1-4: Assign a VLAN identifier to each LAN port.

Wireless: Assign a VLAN identifier to the main wireless connections.

Wireless Guest Zone: Assign a VLAN identifier to the Wireless Guest Zone (if enabled).

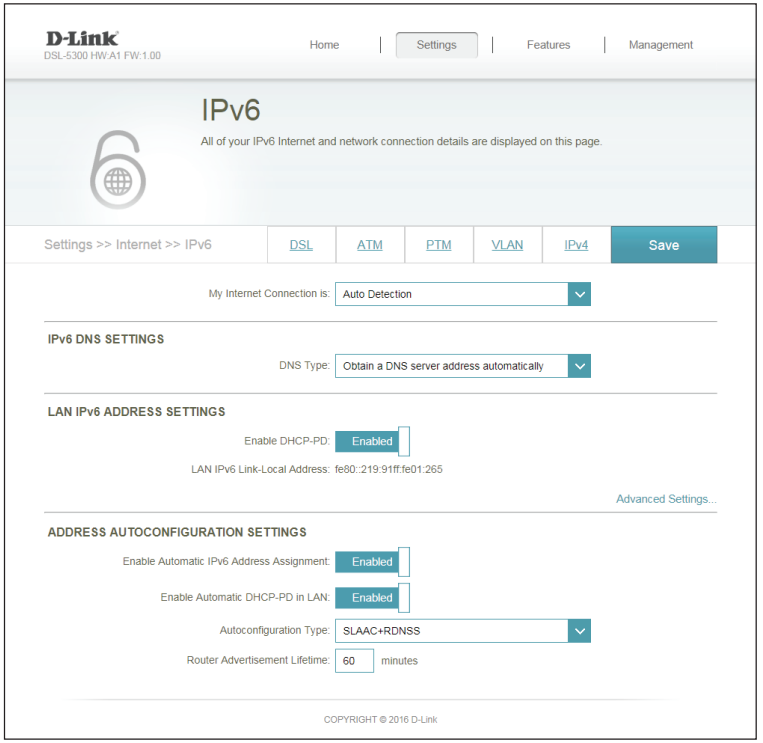
Click **Save** when you are done.



IPv6

To configure an IPv6 connection, click the **IPv6** link. To return to the IPv4 settings, click **IPv4**.

My Internet Connection Is: Choose your IPv6 connection type from the drop-down menu. You will be presented with the appropriate options for your connection type. Click **Advanced Settings...** to expand the list and see all of the options.



For **Auto Detection** refer to **Auto Detection on page 46.**

For **Static IPv6** refer to **Static IPv6 on page 47**.

For **Auto Configuration (SLAAC/DHCPv6)** refer to **Auto Configuration (SLAAC/DHCPv6) on page 49**.

For **PPPoE** refer to **PPPoE on page 51**.

For **IPv6 in IPv4 Tunnel** refer to **IPv6 in IPv4 Tunnel on page 53**.

For **6 to 4** refer to **6 to 4 on page 55.**

For **6rd** refer to **6rd on page 56.**

For **Local Connectivity Only** refer to **Local Connectivity Only on page 58.**

Auto Detection

Auto Detection mode (not Auto-Configuration mode) automatically detects IPv6 the connection method used by your Internet Service Provider (ISP). If your ISP provides an IPv6 service and Auto Detection failed to detect it, the user must manually select another IPv6 connection type (such as PPPoE, Auto Configuration, 6rd, DS-Lite etc.)

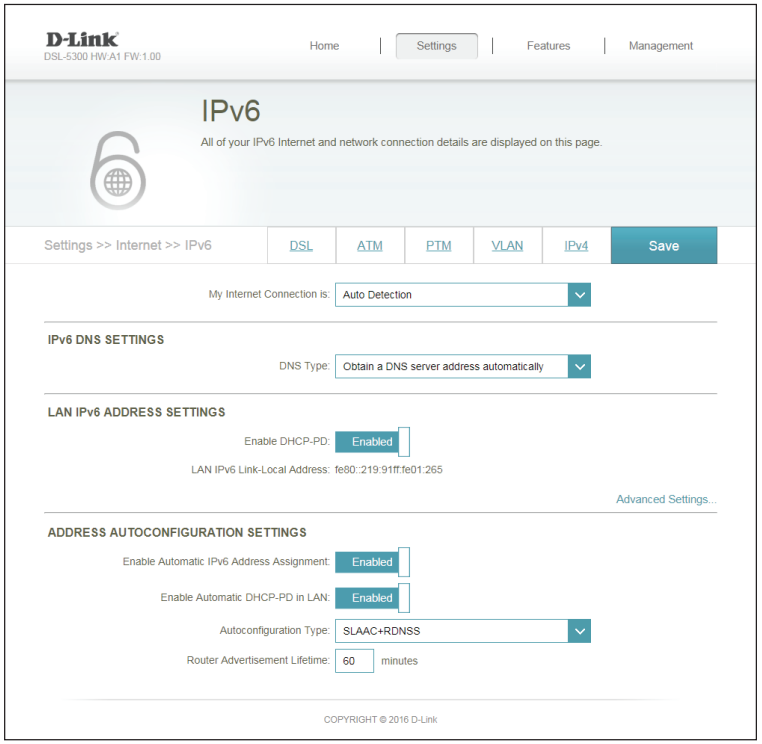
Enable Automatic IPv6 Address Assignment: Enable or disable the Automatic IPv6 Address Assignment feature.

Enable Automatic DHCP-PD in LAN: Enable or disable automatic DHCP-PD services.

Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

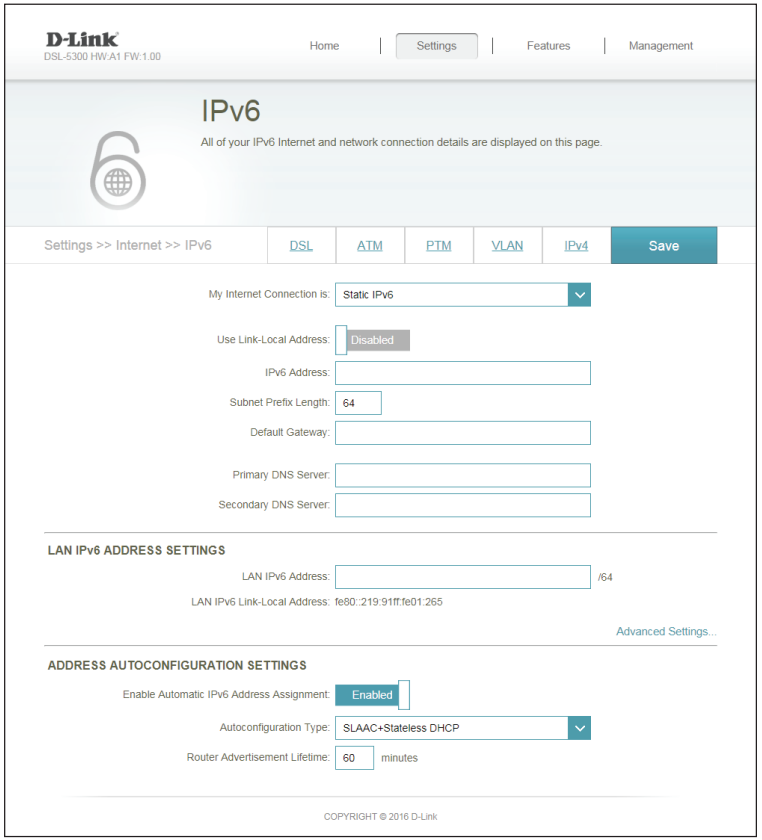
Router Advertisement Lifetime: Enter the IPv6 address lifetime (in minutes).

Click **Save** when you are done.



Static IPv6

Select **Static IP** if your IPv6 information is provided by your Internet Service Provider (ISP).



Use Link-Local Address: Enable or disable a link-local address.

IPv6 Address: If you disabled **Use Link-Local Address**, enter the address supplied by your ISP.

Subnet Prefix Length: If you disabled **Use Link-Local Address**, enter the subnet prefix length supplied by your ISP.

Default Gateway: Enter the default gateway for your IPv6 connection.

Primary DNS Server: Enter the primary DNS server address.

Secondary DNS Server: Enter the secondary DNS server address.

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

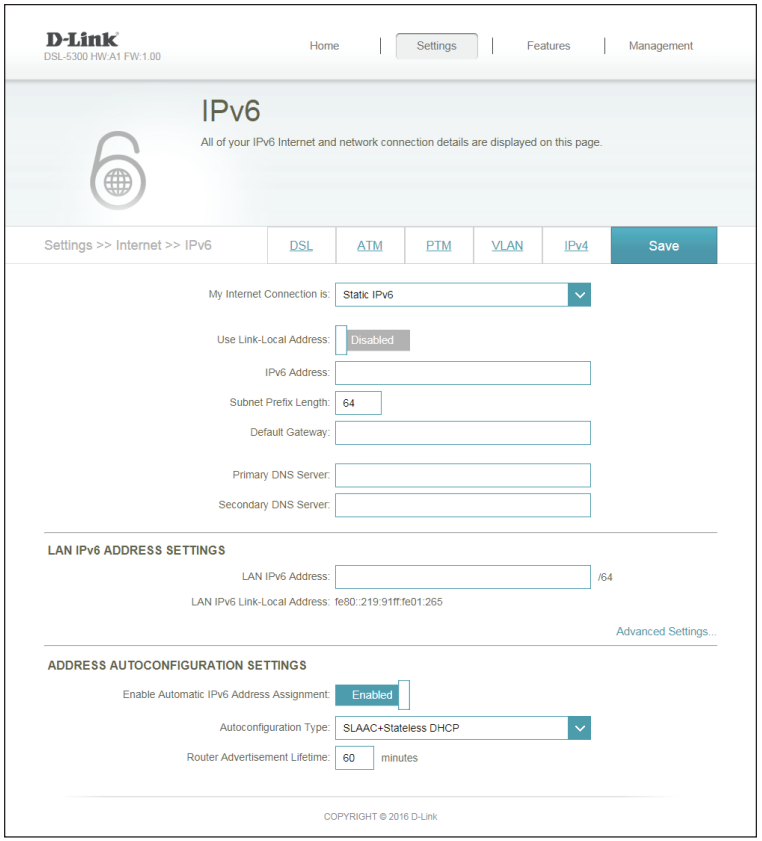
LAN IPv6 Link-Local Address: Displays the router's LAN link-local address.

Enable Automatic IPv6 Address Assignment: Check to enable the Automatic IPv6 Address Assignment feature.

Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

Router Advertisement Lifetime: Enter the IPv6 address lifetime (in minutes).

Click **Save** when you are done.



Auto Configuration (SLAAC/DHCPv6)

This is a connection method where the ISP assigns your IPv6 address when your router requests one from the ISP's server. Some ISPs require you to make some settings on your side before your router can connect to the IPv6 Internet.

DNS Type: Select either **Obtain DNS server address automatically** or **Use the following DNS address**.

Enable IANA: Enable this option to enable Internet Assigned Numbers Authority IPv6 Compatibility.

Primary DNS Server: If you selected **Use the following DNS address** above, enter the primary DNS server address.

Secondary DNS Server: If you selected **Use the following DNS address** above, enter the secondary DNS server address.

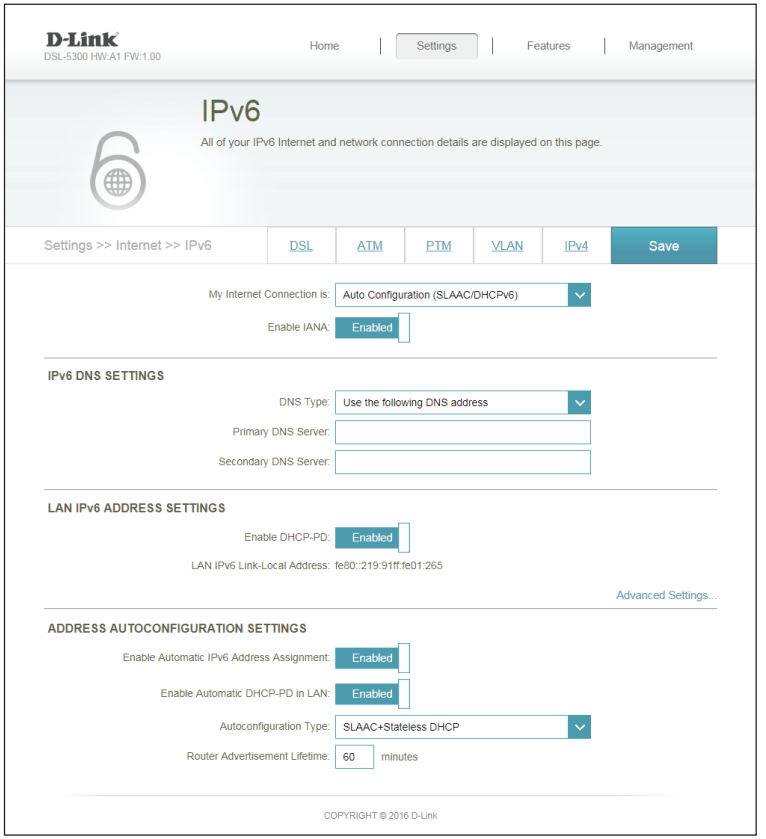
Enable DHCP-PD: Enable or disable prefix delegation services.

LAN IPv6 Address: If you disabled DHCP-PD, enter the LAN (local) IPv6 address for the router.

LAN IPv6 Link-Local Address: Displays the router's LAN link-local address.

Enable Automatic IPv6 Address Assignment: Enable or disable the Automatic IPv6 Address Assignment feature.

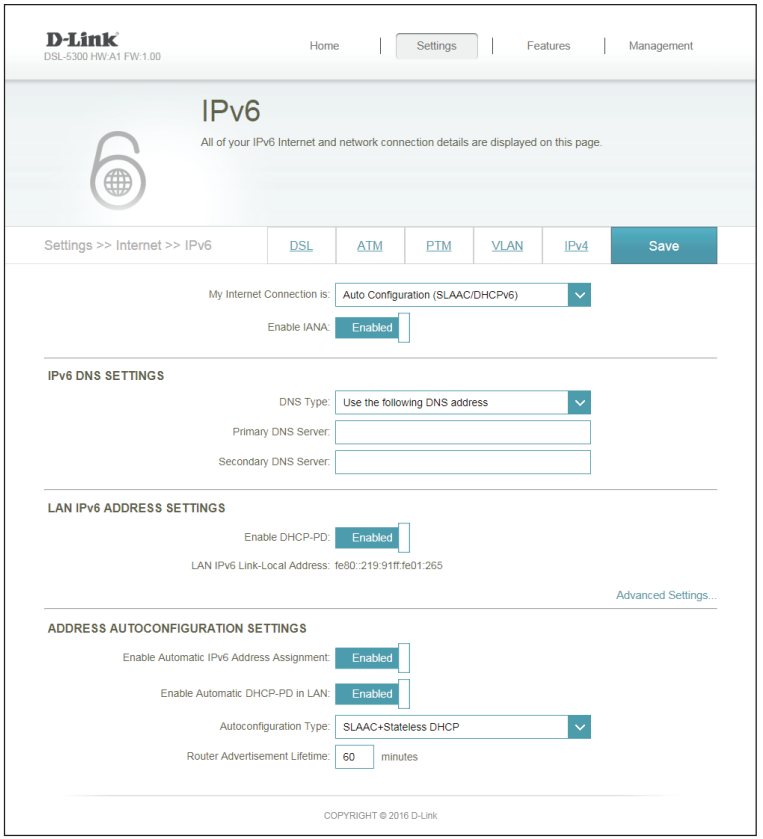
Enable Automatic DHCP-PD in LAN: Enable or disable automatic DHCP-PD services.



Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

Router Advertisement Lifetime: Enter the IPv6 address lifetime (in minutes).

Click **Save** when you are done.



PPPoE

Select **PPPoE** if your Internet connection requires you to enter a username and password. This information is provided by your Internet Service Provider (ISP).

PPPoE Session: Choose **Share with IPv4** to re-use your IPv4 PPPoE username and password, or **Create a new session**.

Enable IANA: Enable this option to enable Internet Assigned Numbers Authority IPv6 Compatibility.

Username: If you selected **Create a new session** above, enter the PPPoE username provided by your ISP here.

Password: If you selected **Create a new session** above, enter the PPPoE password provided by your ISP here.

Address Mode: Select **Static IP** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic IP**.

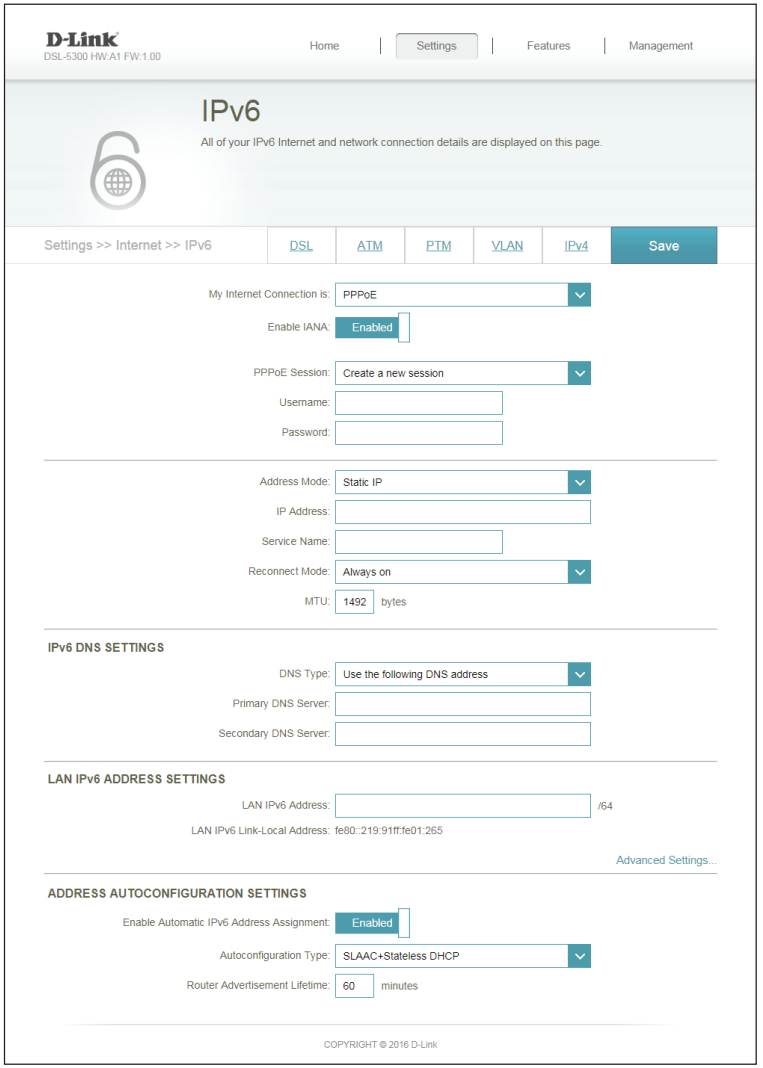
IP Address: Enter the IP address provided by your ISP (Static IP only).

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

DNS Type: Select either **Obtain DNS server address automatically** or **Use the following DNS address**.

Primary DNS Server: If you selected **Use the following DNS address** above, enter the primary DNS server address.

Secondary DNS Server: If you selected **Use the following DNS address** above, enter the secondary DNS server address.



Enable DHCP-PD: Enable or disable prefix delegation services.

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

LAN IPv6 Link-Local Address: Displays the router's LAN link-local address.

Enable Automatic IPv6 Address Assignment: Enable or disable the Automatic IPv6 Address Assignment feature.

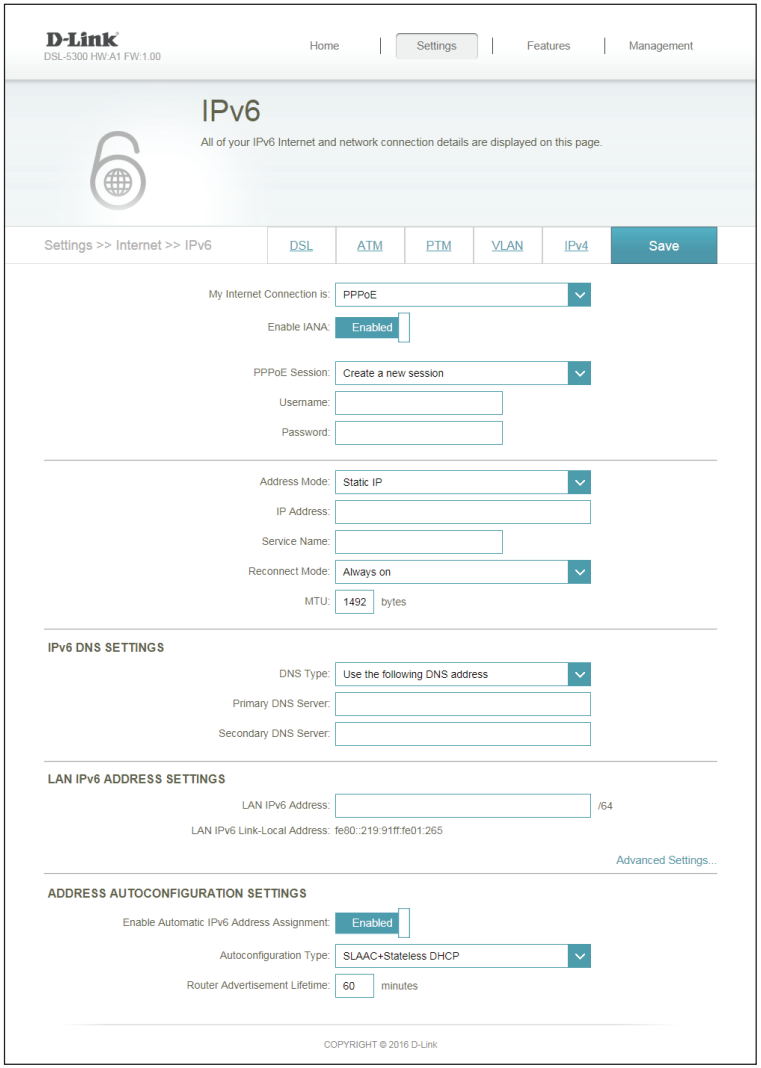
Enable Automatic DHCP-PD in LAN: Enable or disable DHCP-PD for other IPv6 routers connected to the LAN interface.

Note: *This feature requires a smaller subnet prefix than /64 (i.e. allowing for a larger address allocation), such as /63. Contact your ISP for more information.*

Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

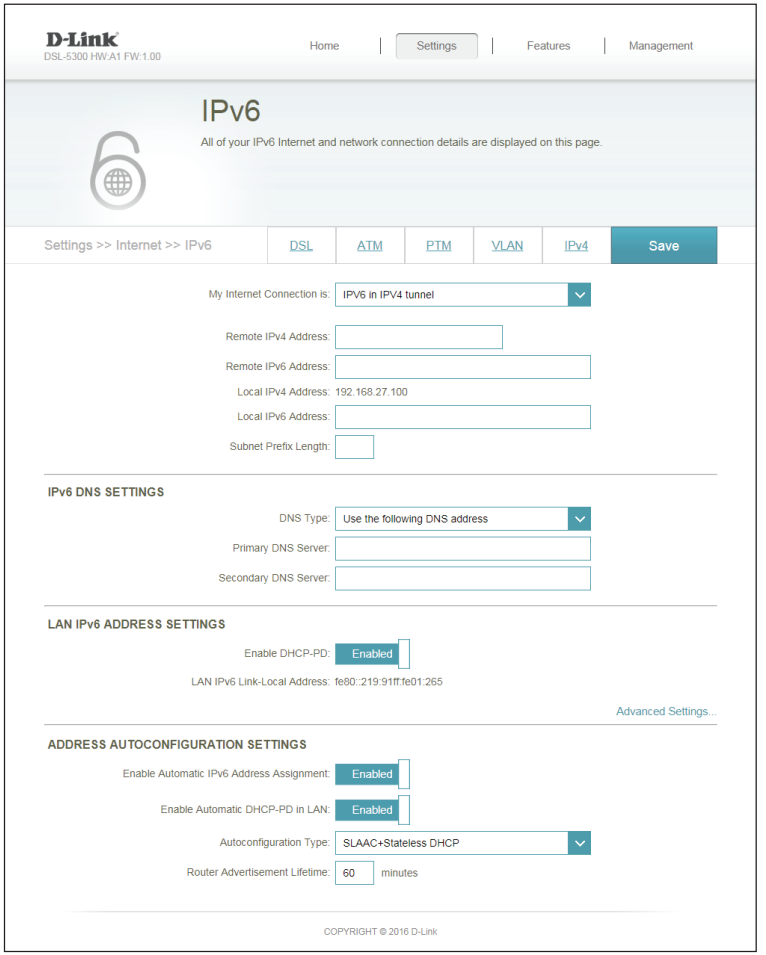
Router Advertisement Lifetime: Enter the IPv6 address lifetime (in minutes).

Click **Save** when you are done.



IPv6 in IPv4 Tunnel

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



Remote IPv4 Address: Enter the IPv4 remote address you will use.

Remote IPv6 Address: Enter the IPv6 remote address you will use.

Local IPv4 Address: Enter the IPv4 local address you will use.

Local IPv6 Address: Enter the IPv6 local address you will use.

Subnet Prefix Length: Enter the subnet prefix length supplied by your ISP.

DNS Type: Select either **Obtain DNS server address automatically** or **Use the following DNS address**.

Primary DNS Server: If you selected **Use the following DNS address** above, enter the primary DNS server address.

Secondary DNS Server: If you selected **Use the following DNS address** above, enter the secondary DNS server address.

Enable DHCP-PD: Enable or disable prefix delegation services.

LAN IPv6 Address: If you disabled DHCP-PD, enter the LAN (local) IPv6 address for the router.

LAN IPv6 Link-Local Address: Displays the router's LAN link-local address.

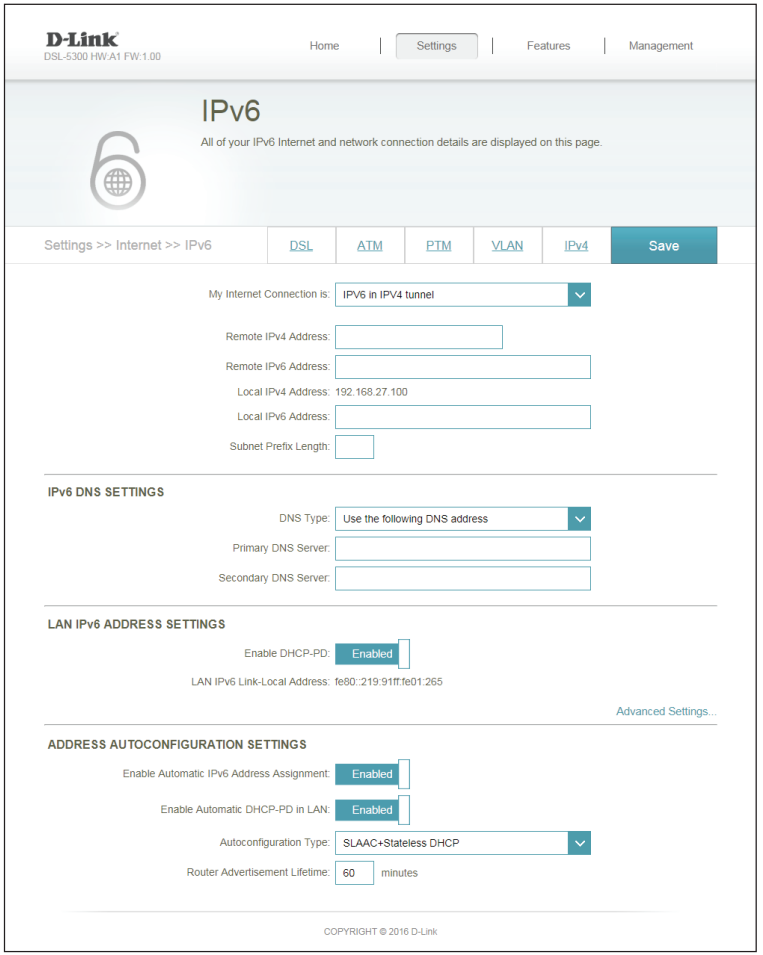
Enable Automatic IPv6 Address Assignment: Enable or disable the Automatic IPv6 Address Assignment feature.

Enable Automatic DHCP-PD in LAN: Enable or disable automatic DHCP-PD services.

Auto Configuration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

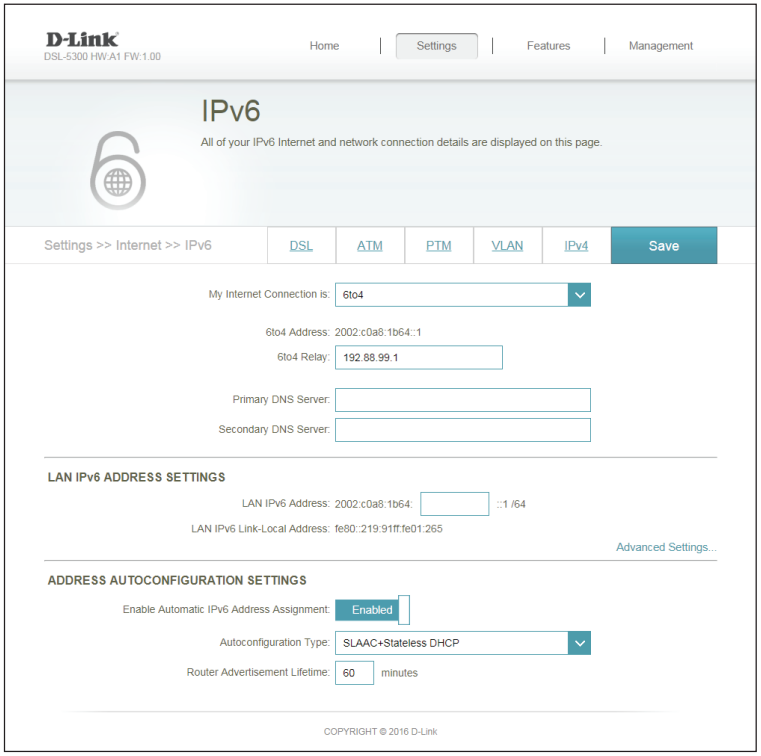
Router Advertisement Lifetime: Enter the IPv6 address lifetime (in minutes).

Click **Save** when you are done.



6 to 4

In this section the user can configure the IPv6 6 to 4 connection settings. 6to4 is an IPv6 address assignment and automatic tunneling technology that is used to provide unicast IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet.



6 to 4 Address: Displays the 6 to 4 address.

6 to 4 Relay: Enter the 6 to 4 relay supplied by your ISP.

Primary DNS Server: Enter the primary DNS server address.

Secondary DNS Server: Enter the secondary DNS server address.

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

LAN IPv6 Link-Local Address: Displays the router's LAN link-local address.

Enable Automatic IPv6 Address Assignment: Check to enable the Automatic IPv6 Address Assignment feature.

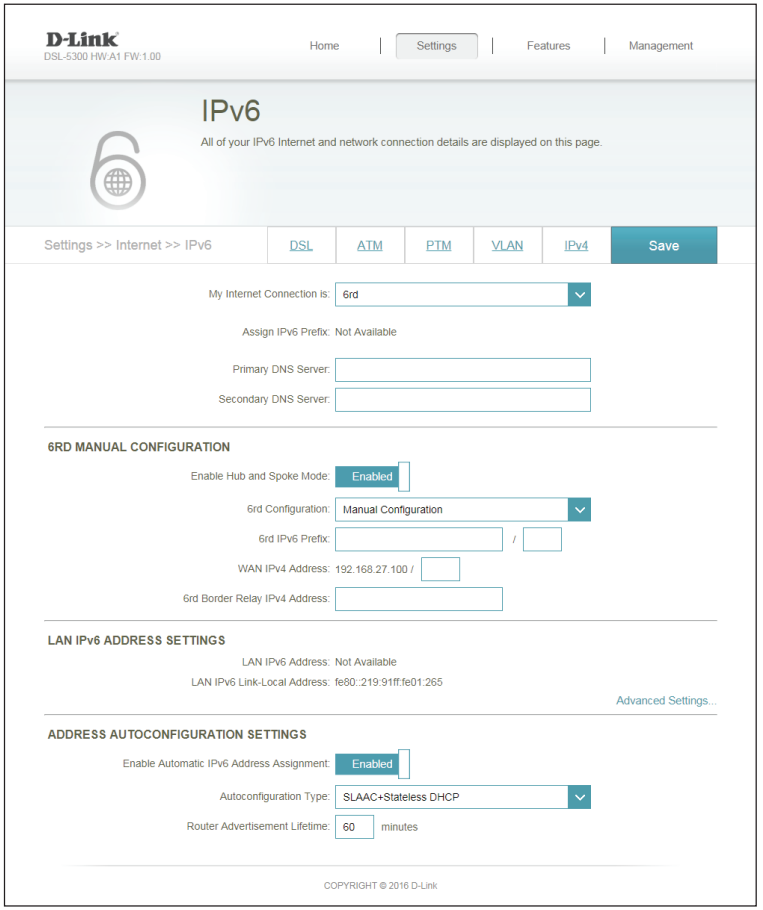
Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

Router Advertisement Lifetime: Enter the IPv6 address lifetime (in minutes).

Click **Save** when you are done.

6rd

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



Assign IPv6 Prefix: Enter the IPv6 prefix.

Primary DNS Server: Enter the primary DNS server address.

Secondary DNS Server: Enter the secondary DNS server address.

Enable Hub and Spoke Mode: Enable if you want to minimize the number of routes to the destination by using a hub and spoke method of networking.

6rd Configuration: Choose the **6rd DHCPv4 Option** to automatically discover and populate the data values, or **Manual Configuration** to enter the settings yourself.

6rd IPv6 Prefix: Enter the 6rd IPv6 prefix and mask length supplied by your ISP (manual configuration only).

6rd Border Relay IPv4 Address: Enter the 6rd border relay IPv4 address settings supplied by your ISP (manual configuration only).

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

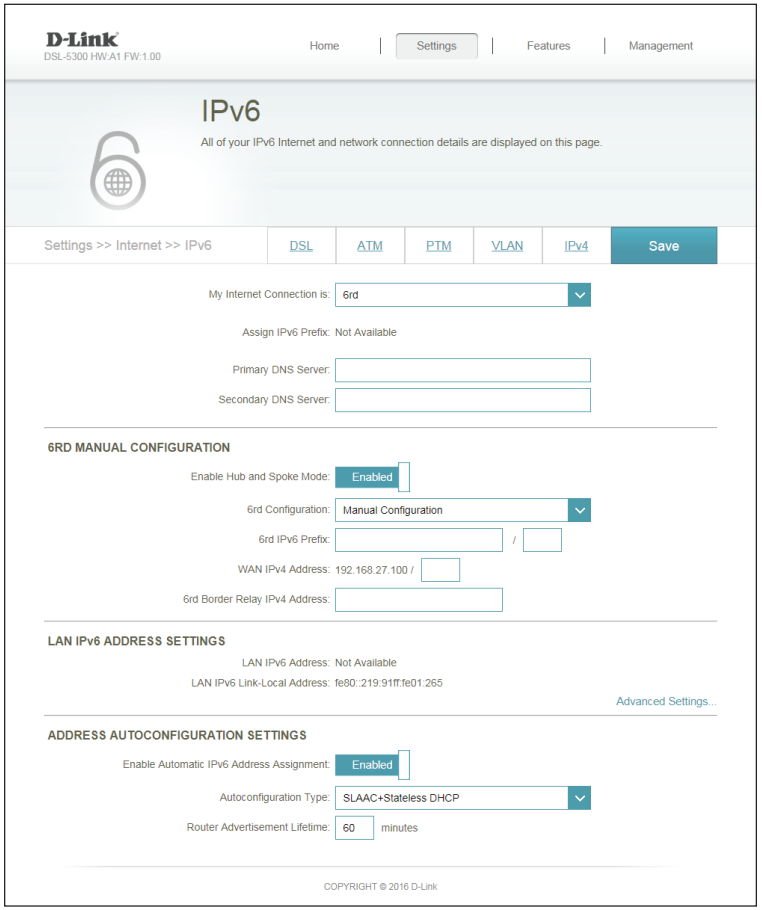
LAN IPv6 Link-Local Address: Displays the router's LAN link-local address.

Enable Automatic IPv6 Address Assignment: Check to enable the Automatic IPv6 Address Assignment feature.

Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

Router Advertisement Lifetime: Enter the IPv6 address lifetime (in minutes).

Click **Save** when you are done.



Local Connectivity Only

Local Connectivity Only allows you to set up an IPv6 connection that will not connect to the Internet.

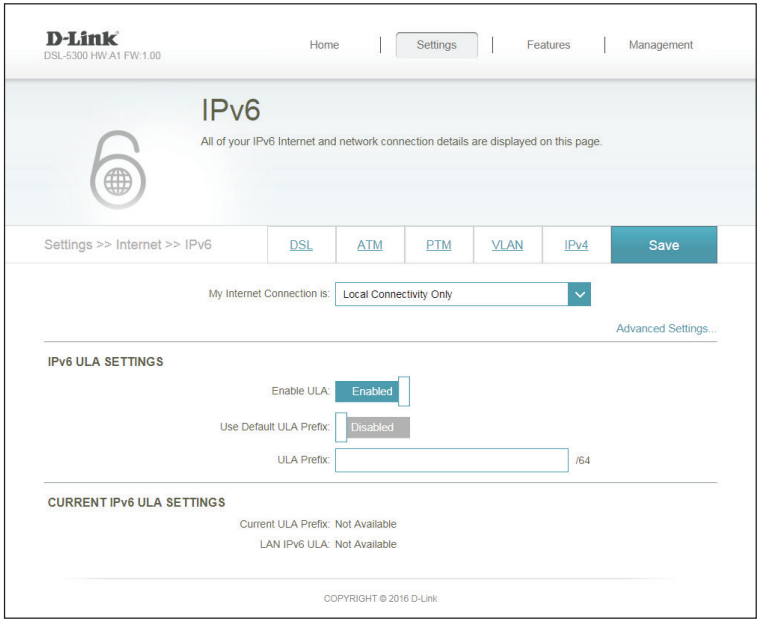
Enable ULA: Click here to enable Unique Local IPv6 Unicast Addresses settings.

Use Default ULA Prefix: Checking this box will automatically configure the ULA prefix for the default setting.

ULA Prefix: If you wish to choose your own ULA prefix, enter it here.

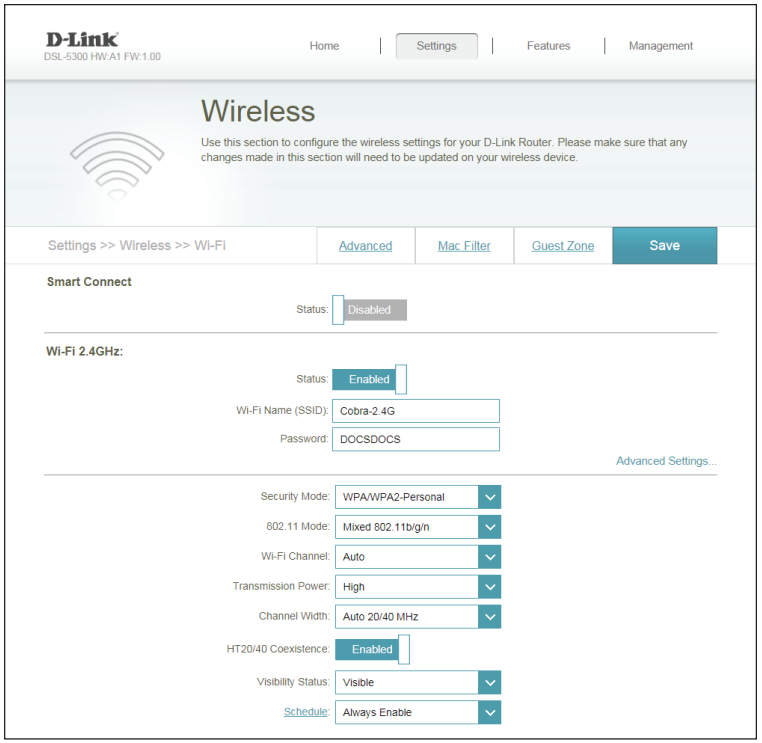
Current IPv6 ULA Settings: This section will display the current settings for your IPv6 ULA.

Click **Save** when you are done.



Wireless

In the Settings menu on the bar on the top of the page, click **Wireless** to see the wireless configuration options. To configure the router's guest zone, click the **Guest Zone** link. Refer to 61 for details. Click **Advanced Settings...** to expand the list and see all of the options. The following options apply to both the 2.4 GHz and the 5 GHz wireless frequency bands:



Smart Connect: Enable this option to have the DSL-5300 automatically manage the 2.4 GHz and 5 GHz wireless networks. Disable this option if you want to manually configure the 2.4 GHz and 5 GHz wireless networks.

Status: Enable or disable the wireless frequency band.

Wi-Fi Name (SSID): Create a name for your wireless network using up to 32 characters.

Password: Create a password to use for wireless security. Wireless clients will need to enter this password to successfully connect to the network.

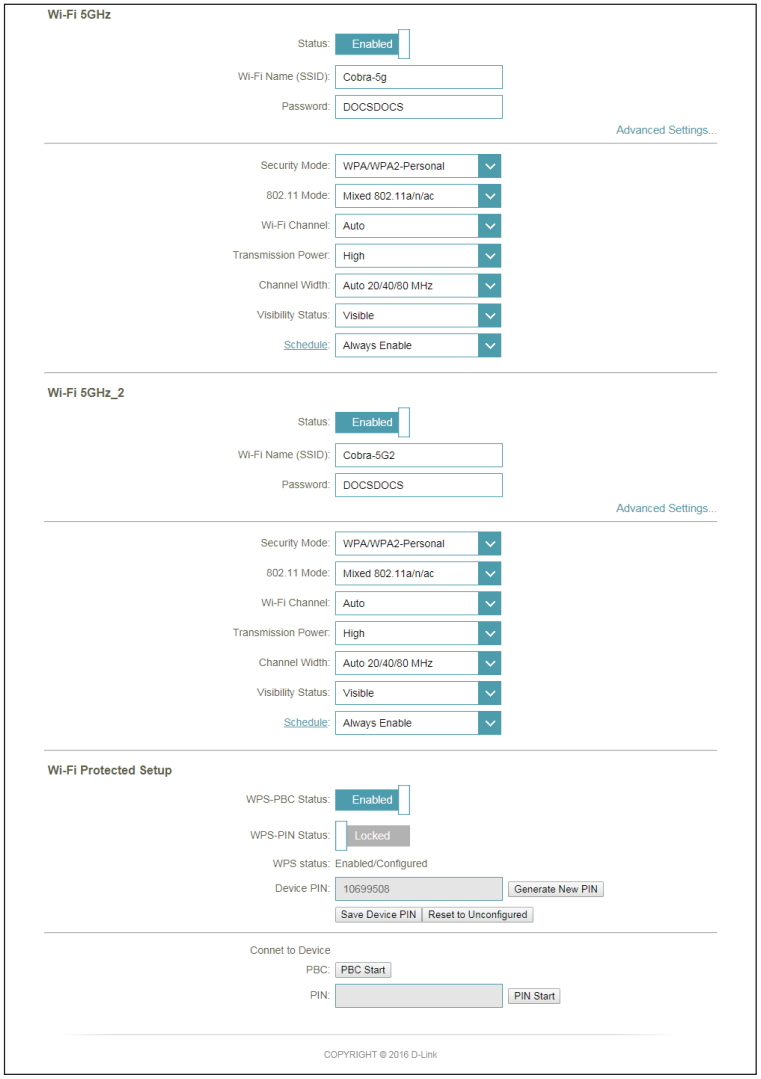
Security Mode: Choose **None**, **WEP**, or **WPA/WPA2-(Personal)** (recommended).

802.11 Mode: Select the desired wireless networking standards to use. The available options will depend on the wireless frequency band, as well as the currently selected security mode.

Wi-Fi Channel: Select the desired channel. The default is **Auto** (recommended).

Transmission Power: Select the desired wireless transmission power.

Channel Width: Select **Auto 20/40** if you are using both 802.11n and non-802.11n wireless devices, or select **20 MHz** if you are not using any 802.11n wireless clients.



Visibility Status: The default setting is **Visible**. Select **Invisible** if you do not want to broadcast the SSID of your wireless network.

Schedule: Use the drop-down menu to select the time schedule that the rule will be enabled on. The schedule may be set to **Always Enable**, or you can create your own schedules in the **Schedules** section. Refer to page 83 for more information.

WPS-PBC Status: Enable or disable Wi-Fi Protected Setup Push Button Configuration (WPS-PBC) functionality.

WPS-PIN Status: Enable or disable WPS-PIN functionality.

Note: WPS-PIN functionality has known security vulnerabilities and is disabled by default for your protection. It is provided for compatibility only.

WPS status: Displays WPS status.

Device PIN: Displays the current PIN. Use of WPS-PIN is not recommended.

Generate New PIN: Generates a new, random PIN. Use of WPS-PIN is not recommended.

PBC Start Enables you to start PBC pairing from the web UI.

PIN Start: Allows you to pair a *client device* configured with a PIN without enabling PIN support on your router.

Click **Save** when you are done.

Guest Zone

The guest zone feature will allow you to create temporary zones that can be used by guests to access the Internet. These zones will be separate from your main wireless network. You may configure different zones for the 2.4 GHz, primary, and secondary 5 GHz wireless bands.

In the Settings menu on the bar on the top of the page, click **Wireless**, then click the **Guest Zone** link. Click **Advanced Settings...** to expand the list and see all of the options. Each band can be configured separately:

Status: Enable or disable the guest zone for each wireless frequency band.

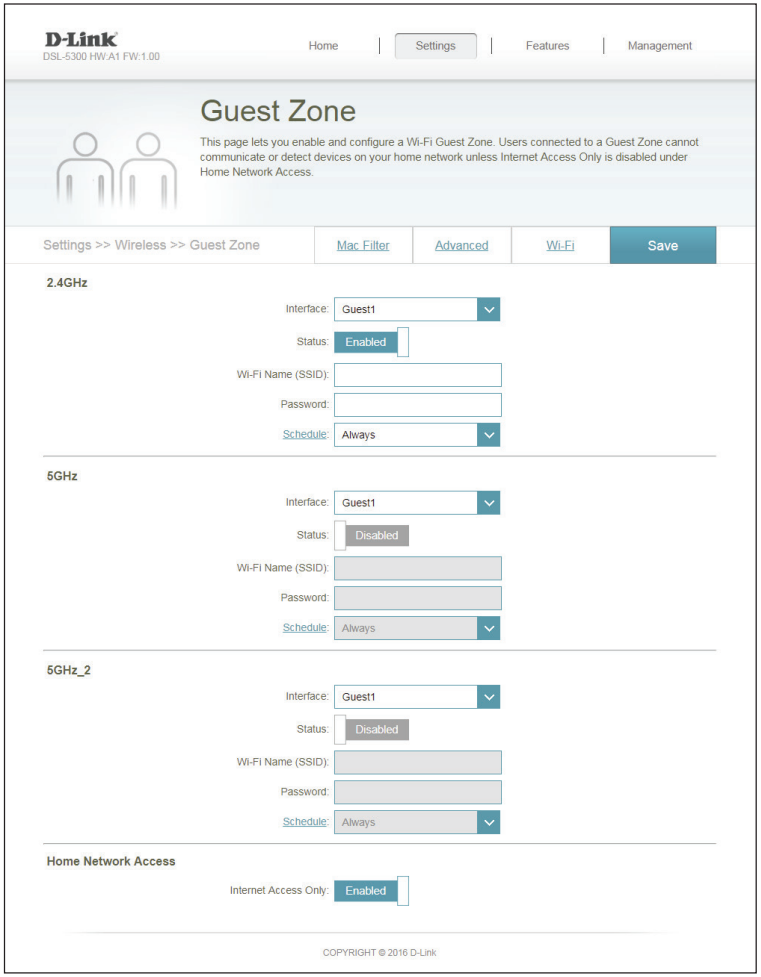
Wi-Fi Name (SSID): Enter a wireless network name (SSID) that is different from your main wireless network.

Password: Create a password to use for wireless security. Wireless clients will need to enter this password to successfully connect to the guest zone.

Schedule: Use the drop-down menu to select the time schedule followed by the guest zone.. The schedule may be set to **Always Enable**, or you can create your own schedules in the **Schedules** section. Refer to page 83 for more information.

Internet Access Only: Enabling this option will confine connectivity to the Internet, disallowing guests from accessing other local network devices.

Click **Save** when you are done.



Advanced Settings

The Advanced Settings menu allows you to configure advanced wireless features to optimize performance and compatibility. These are advanced settings that can safely be ignored by most users.

Enable Radio: Select this option to enable the Wireless radio. Disabling will disable for the specified band. This feature is enabled by default

Set AP Isloated: Select this option to prevent wireless clients from communicating with each other. This feature is disabled by default.

Roaming Assistant: The roaming assistant allows clients to more easily move between APs or repeaters. This feature disconnects the client bellow a certain RSSI (Received Signal Strength Indicator) threshold to connect to a stronger signal (see below). This feature is enabled by default.

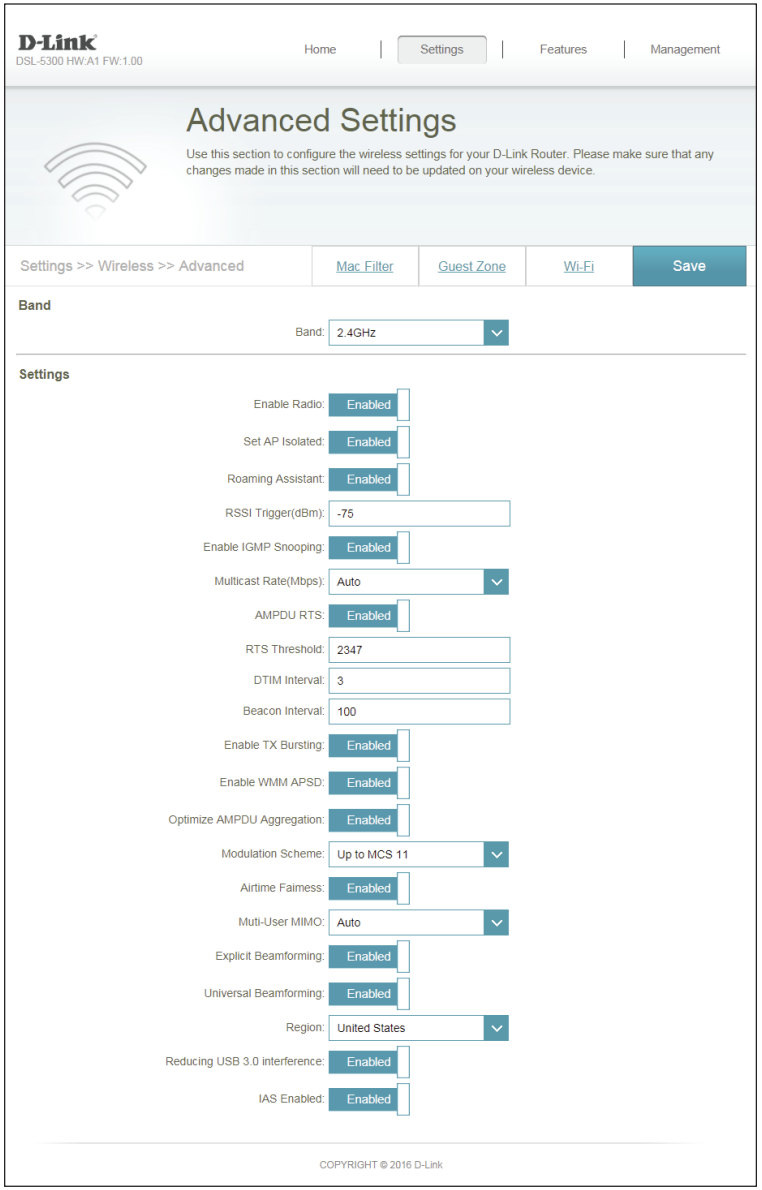
RSSI Trigger(dBm): Sets the RSSI (Received Signal Strength Indicator) to drop the client from the network to allow it to reconnect to a repeater or AP.

Enable IGMP Snooping: Allows monitoring of IGMP (Internet Group management Protocol) to optimize wireless multicast traffic. The feature is enabled by default.

Multicast Rate (Mbps): Allows you to specify the maximum speed which multicast packets are sent. **Auto** is the default and recommended setting.

AMPDU RTSL: The AMPDU (Aggregated-MAC Packet Data Unit) is a feature of the 802.11e and 802.11n standards that allows groups of frames to be transmitted together. The default and recommended setting is **Enable.**

RTS Threshold: RTS (Request to Send) indicates the maximum number of bytes per packet. Reducing this may improve communication in crowded wireless environments. The default and recommended setting is **2347**.



DTIM Interval: The DTIM (Delivery Traffic Indication Message) interval set the wake-up interval in power saving mode. The default and recomended setting is **3 ms**.

Beacon Interval: The Beacon Interval is the time in milliseconds between one DTIM and the next. Lower this for unstable connections and roaming devices. The default and recommended setting is **100 ms.**

Enable TX Bursting: Transmission Bursting improves transmission speed between the router and 802.11g devices. The default and recommended setting is **Enable.**

Enable WMM APSD: Enable WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) to improve power management between wireless devices.

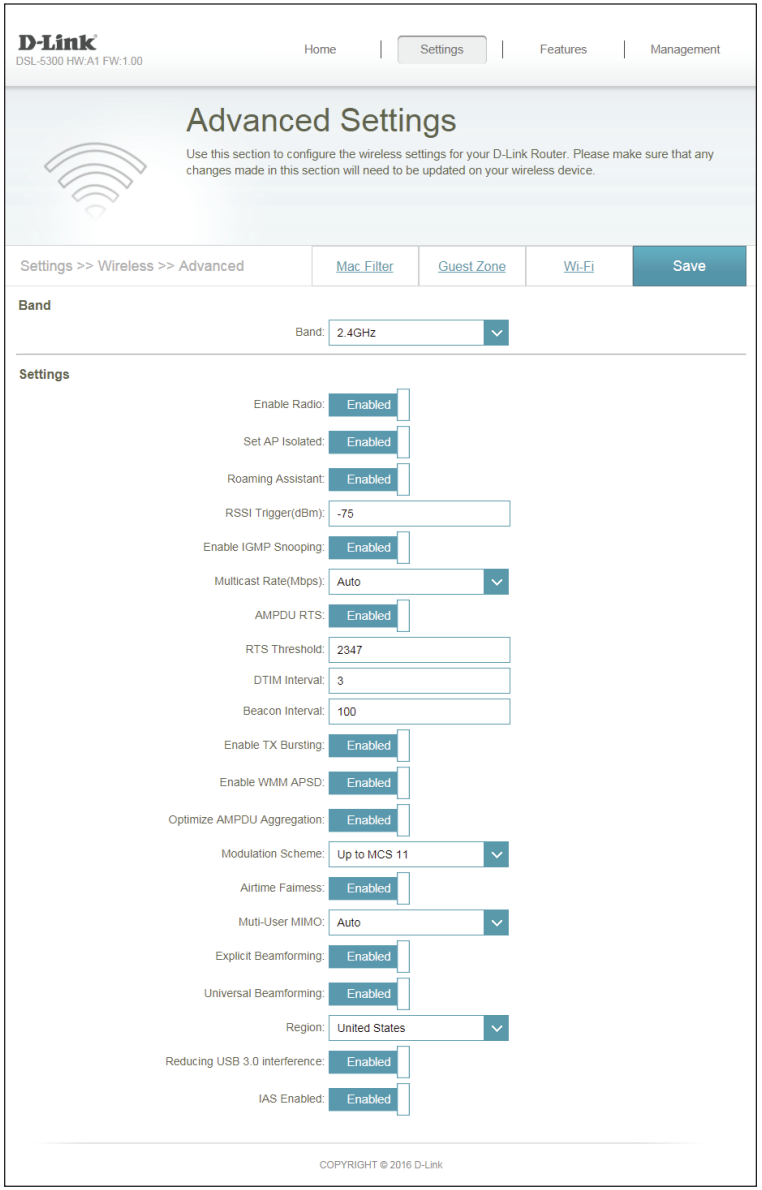
Optimize AMPDU Aggregation: AMPDU (Aggregated-MAC Packet Data Unit) optimizes the number of MSDUs (MAC Service Data Units) to avoid packet loss in error-prone wireless channels.

Modulation Scheme: Specifies the modulation scheme used for wireless transmission.

Aitrime Fairness: By default, wireless networks reduce speed to the slowest client. This setting allocates time equally among clients, each running at their highest speeds. The default setting is **disabled.**

Multi-User MIMO: Multi-User MIMO (Multiple Input Multiple Output) allows transmissions to take multiple paths using multiple antennas, dramatically increasing throughput. The default and recommended setting is **Auto**.

Explicit Beamforming: Explicit Beamforming can be used when all clients support beam forming, and allows use of channel estimation and direction steering to improve link speeds.



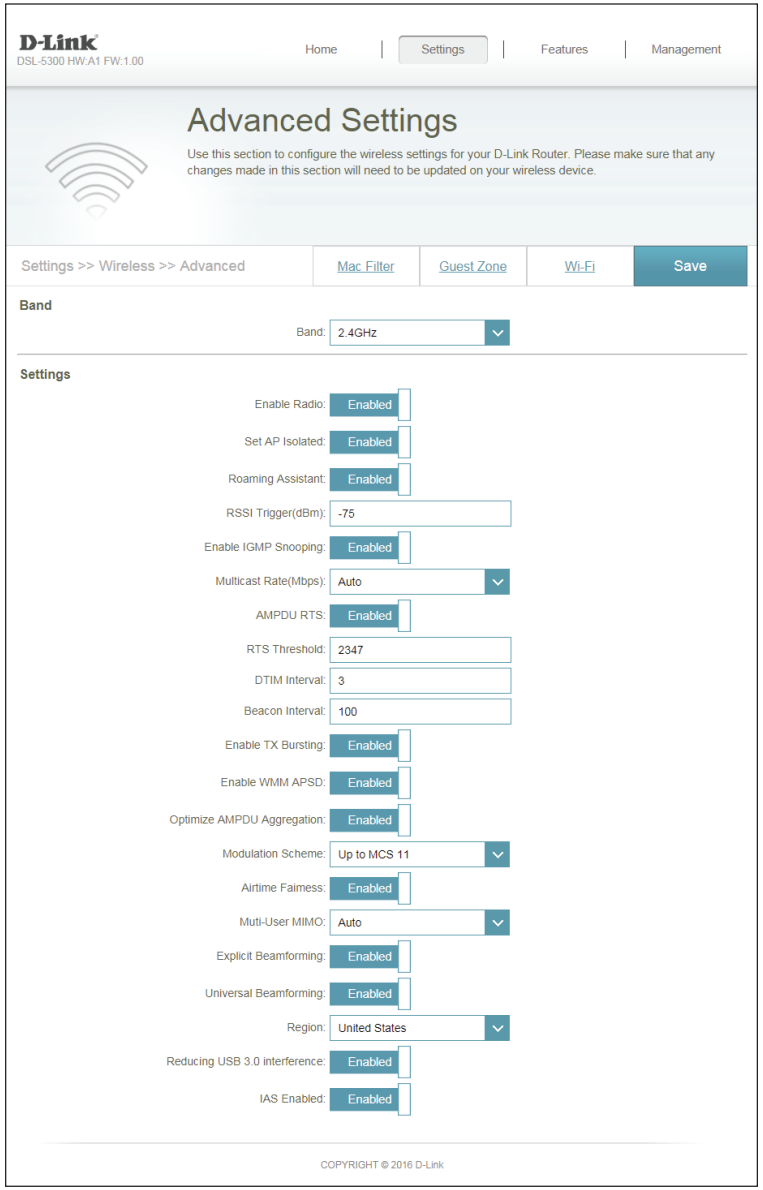
Universal Beamforming: Universal beamforming allows basic beamforming features in compatibility mode to support legacy adaptors. This feature is **disabled** by default.

Region: Set your region correctly to ensure compatibility with local equipment and compliance with local laws. The default setting is **Australia**.

Reducing USB 3.0 Interference: USB 3.0 sometimes interferes with 2.4 GHz wireless transmissions. This setting moderates the speed of the included USB 3.0 port to reduce interference. This setting is **enabled** by default.

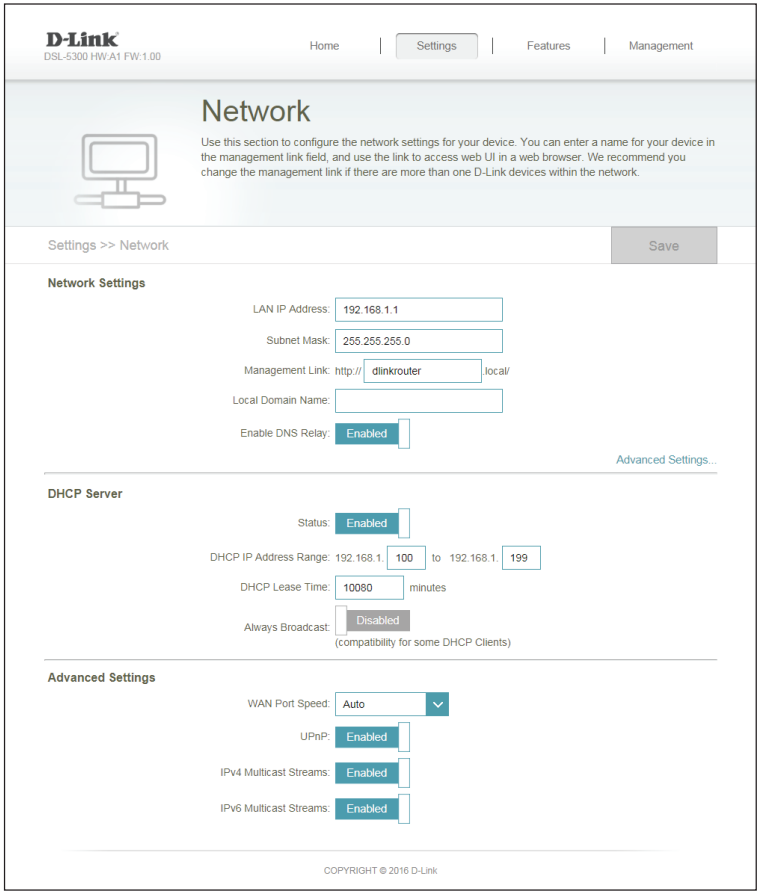
IAS Enabled: Select to enable IAS (Internet Authentication Service). This feature is disabled by default.

Click **Save** when you are done.



Network

This section will allow you to change the local network settings of the router and to configure the DHCP settings. In the Settings menu on the bar on the top of the page, click **Network**. Click **Advanced Settings...** to expand the list and see all of the options.



LAN IP Address: Enter the IP address of the router. The default IP address is **192.168.0.1**.

If you change the IP address, once you click **Save**, you will need to enter the new IP address in your browser to get back into the configuration utility.

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

Management Link: The default address to access the router's configuration is **http://dlinkrouter.local./** Here, you can replace **dlinkrouter** with a name of your choice.

Local Domain Name: Enter the domain name (optional).

Enable 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.

Status: Enable or disable the DHCP server.

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

Note: *If you statically (manually) assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.*

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

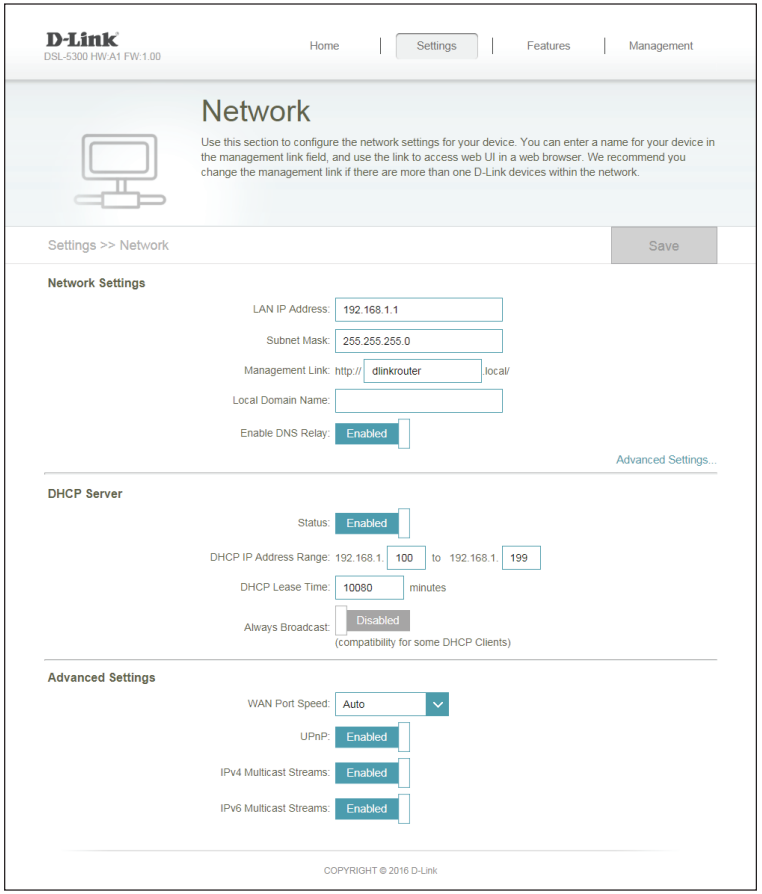
Always Broadcast: Enable this feature to broadcast your networks DHCP server to LAN/WLAN clients.

UPnP: Enable or disable Universal Plug and Play (UPnP). UPnP provides compatibility with networking equipment, software, and peripherals.

IPv4 Multicast Stream: Enable to allow IPv4 multicast traffic to pass through the router from the Internet.

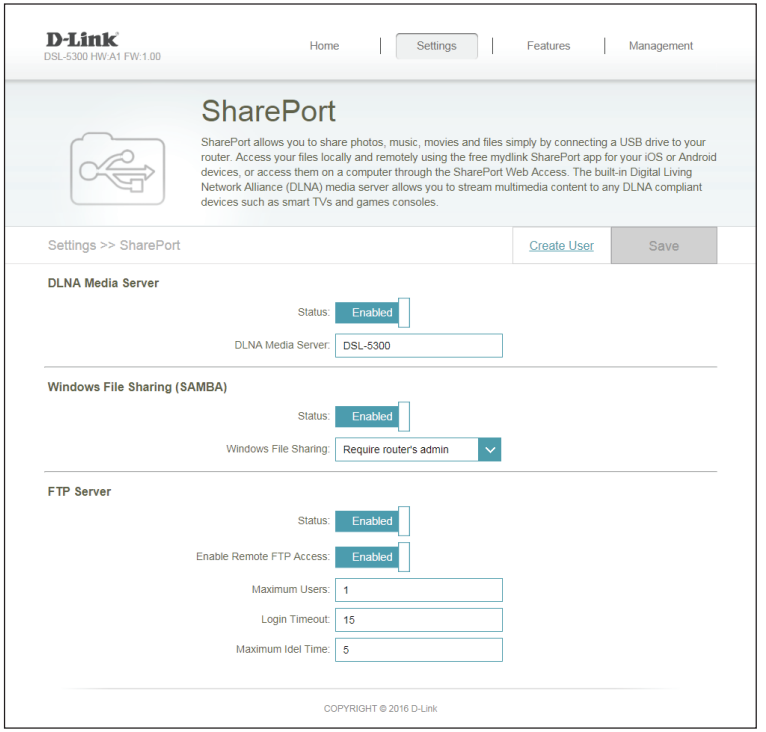
IPv6 Multicast Stream: Enable to allow IPv6 multicast traffic to pass through the router from the Internet.

Click **Save** when you are done.



SharePort

This page will allow you to set up access to files on an external USB device plugged into the router. You can do this through the local network or from the Internet using either a web browser or an app on your smartphone or tablet. In the Settings menu on the bar on the top of the page, click **SharePort**.



Status: Check to enable the media server functions, allowing connected clients access to media files over the network.

UPnP Media Server: Choose a name for your media server so that it can be found.

Windows File Sharing (SAMBA): Choose either **Allow all users to access (no password)** or **Require router's admin password** to specify whether the router's password will be required for access.

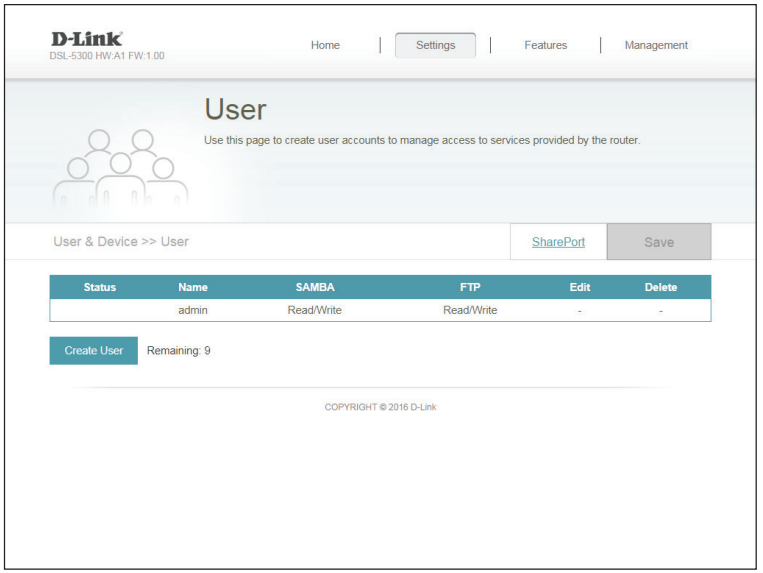
FTP File Access: To allow file access via FTP, ensure that the **Status** is **Enabled**. **Enable Remote FTP Access** allows users to access files from outside the network via FTP. If this is enabled, enter the **Maximum Users**, **Login Timeout**, and the **Maximum Idle Time**.

Click **Save** when you are done.

To manage user accounts for SharePort access, click **Create User** and refer to the next page for details.

Create User

The Create User page allows you to manage your SharePort user accounts. The current list of user accounts will be displayed, along with their current permissions and access path. If they do not have an account set up, users will be restricted to guest access; only having access to the "Guest" folder on the media server. The router can store a maximum of ten accounts (including the "Admin" account).



If you wish to remove an account, click on its trash can icon in the Delete column. If you wish to edit an account, click on its pencil icon in the Edit column. If you wish to create a new account, click the **Create User** button. If you edit or create a user, the following options will appear:

User Name: Enter the desired user name for the new account.

Password: Enter the password the user will need to enter when logging in.

Status: For each connection type, choose to **Enable** or **Disable**

Permission: Select either **Read Only** or **Read/Write** to control whether the user can edit, add, or delete files on the device.

Folder: Choose the parent folder that the user will be able to access. Files and folders on a higher level will be unavailable. "root" means that the user can access all files on the device. To change the selected folder, click **Browse** and browse to the desired folder.

Click **OK** when you are done. The new user should be added to the list of user accounts. To save the new list, click **Save**. To return to the SharePort page, click **SharePort**.

Features

QoS Engine

This section will allow you to prioritize particular clients over others so that those clients receive higher bandwidth. For example, if one client is streaming a movie and another is downloading a non-urgent file, you might wish to assign the former device a higher priority than the latter so that the movie streaming is not disrupted by the traffic of the other devices on the network.

In the Features menu on the bar on the top of the page, click **QoS Engine**.

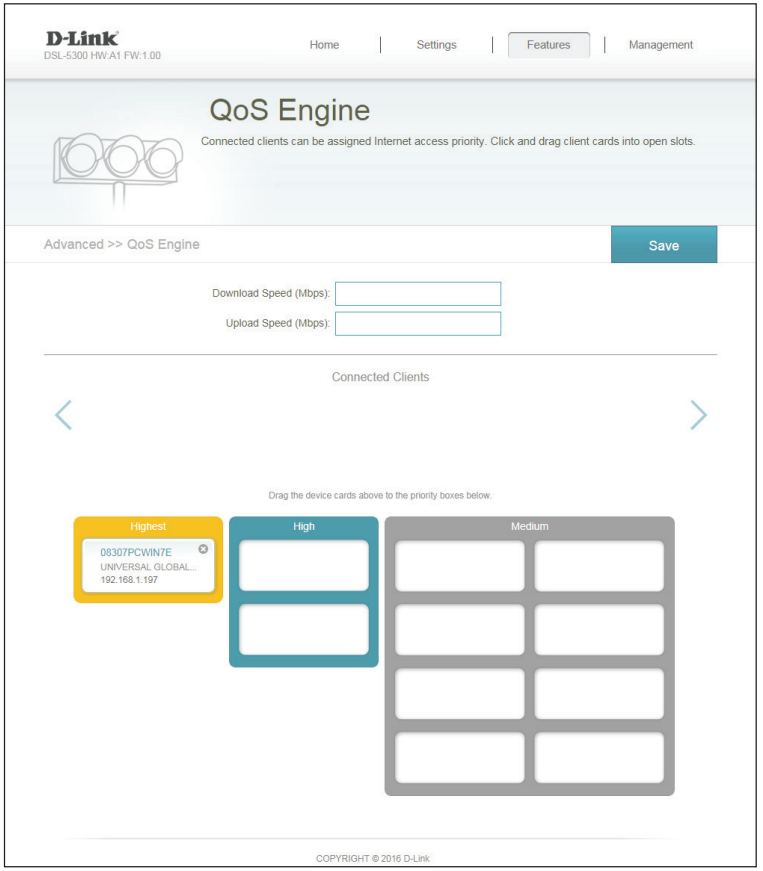
Under All Devices, you will see device cards representing each connected client. If some are off-screen, you can use the **<** and **>** buttons to scroll through the cards.

A maximum of **one** device can be assigned **Highest** priority.

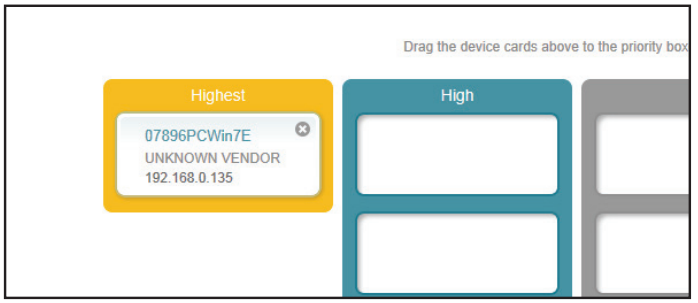
A maximum of **two** devices can be assigned **High** priority.

A maximum of **eight** devices can be assigned **Medium** priority.

If no devices are explicitly assigned a priority, they will all be treated with equal priority. If some devices are not assigned a priority and others are, the unassigned devices will be treated with the lowest priority.



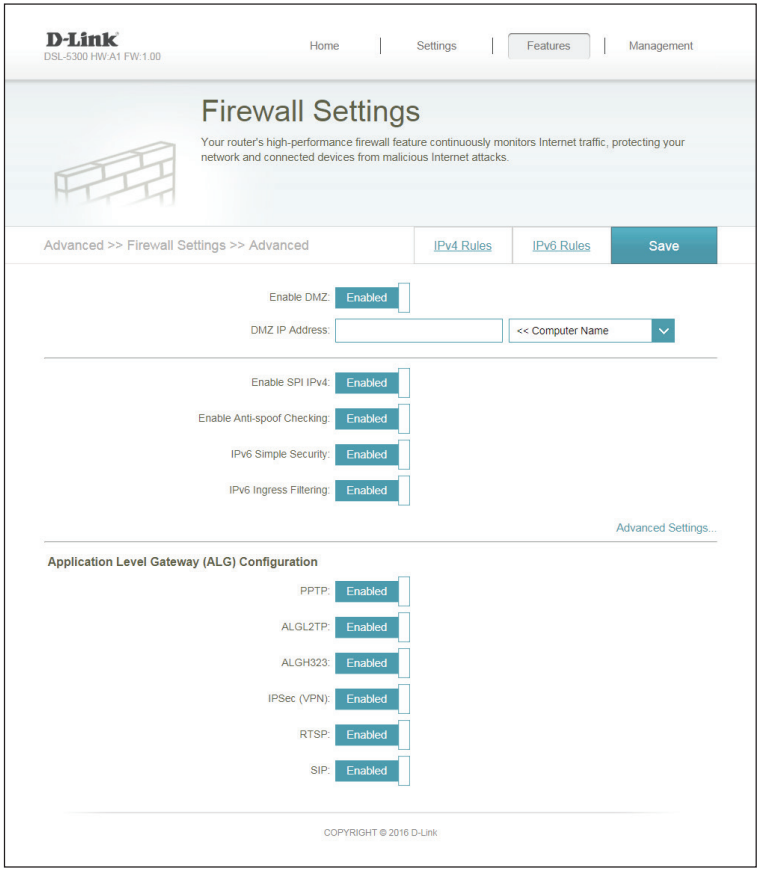
To assign a priority level to a device, drag the device card from the All Devices list over an empty slot and release the mouse button. The card will remain in the slot. If you want to remove a priority assignment from a device and return it to the All Devices list, click the cross icon in the top right of the device card.



Click **Save** when you are done.

Firewall Settings

The router's firewall protects your network from malicious attacks over the Internet. In the Features menu on the bar on the top of the page, click **Firewall Settings**. Click **Advanced Settings...** to expand the list and see all of the options.



Enable DMZ: Enable or disable Demilitarized Zone (DMZ). This completely exposes the client to threats over the Internet, and is not recommended in ordinary situations.

DMZ IP Address: If you enabled DMZ, enter the IP address of the client you wish to expose, or use the drop-down menu to quickly select it.

Enable SPI IPv4: Enabling Stateful Packet Inspection (SPI) helps to prevent cyber attacks by validating that the traffic passing through the session conforms to the protocol.

Enable Anti-Spoof Checking: Enable this feature to protect your network from certain kinds of "spoofing" attacks.

IPv6 Simple Security: Enable or disable IPv6 simple security.

IPv6 Ingress Filtering: Enable or disable IPv6 ingress filtering.

PPTP: Allows multiple machines on the LAN to connect to their corporate network using the PPTP protocol.

IPSec (VPN): Allows multiple VPN clients to connect to their corporate network using IPSec. Some VPN clients support traversal of IPSec through NAT. This Application Level Gateway (ALG) may interfere with the operation of such VPN clients. If you are having trouble connecting to your corporate network, try turning this ALG off. Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

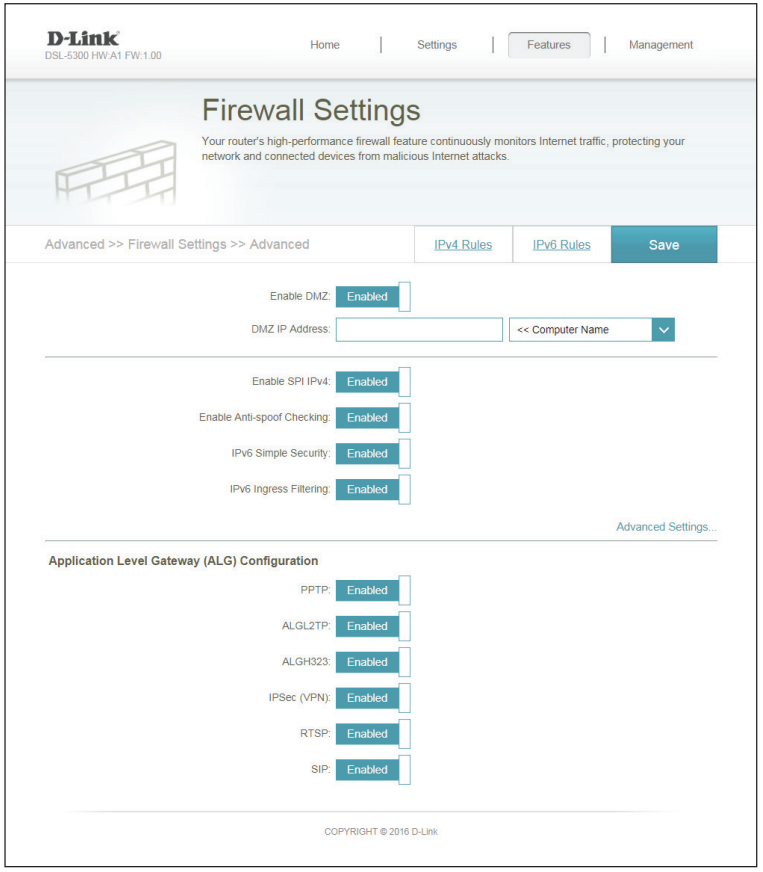
ALGL2TP: Allows multiple VPN clients to connect to their corporate network using L2TP. Some VPN clients support traversal of IPSec through NAT. This Application Level Gateway (ALG) may interfere with the operation of such VPN clients. If you are having trouble connecting to your corporate network, try turning this ALG off. Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

ALGH323 Enable pass-through for the H.323 protocol often used for VoIP calls.

RTSP: Allows applications that use the Real Time Streaming Protocol (RTSP) to receive streaming media from the Internet.

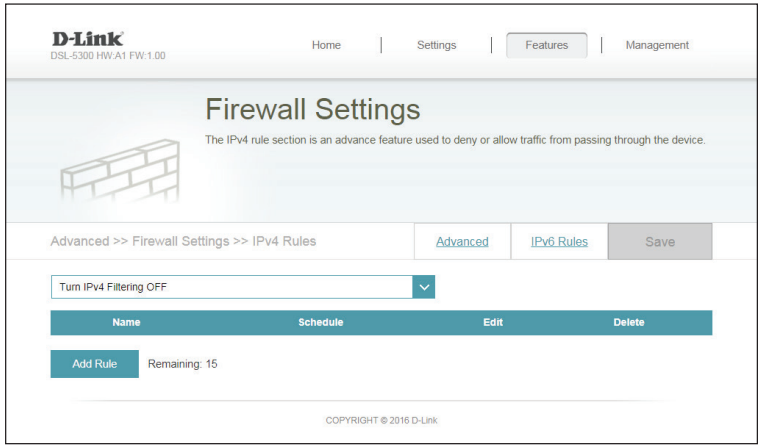
SIP: Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

Click **Save** when you are done.



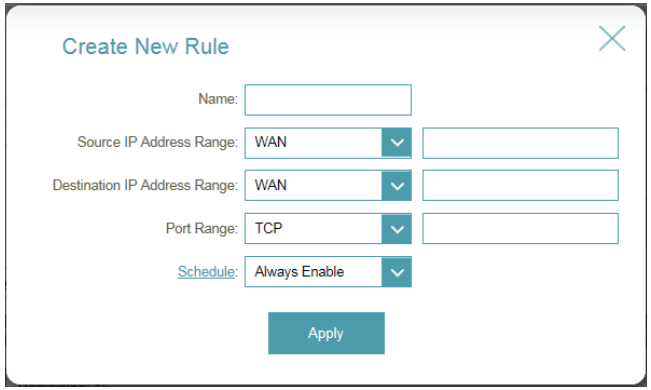
IPv4/IPv6 Rules

The IPv4/IPv6 Rules section is an advanced option that lets you configure what kind of traffic is allowed to pass through the network. To configure the IPv4 rules, from the Firewall Settings page click **IPv4 Rules**. To configure IPv6 rules, from the Firewall Settings page click **IPv6 Rules**. To return to the main Firewall Settings page, click **Security Check**.



To begin, use the drop-down menu to select whether you want to **ALLOW** or **DENY** the rules you create. You can also choose to turn filtering **OFF**.

If you wish to remove a rule, click on its trash can icon in the Delete column. If you wish to edit a rule, click on its pencil icon in the Edit column. If you wish to create a new rule, click the **Add Rules** button. Click **Save** when you are done. If you edit or create a rule, the following options will appear:



Name: Enter a name for the rule.

Source IP Address Range: Enter the source IP address range that the rule will apply to, and using the drop-down menu, specify whether it is a **WAN** or **LAN** IP address.

Destination IP Address Range: Enter the destination IP address range that the rule will apply to, and using the drop-down menu, specify whether it is a **WAN** or **LAN** IP address.

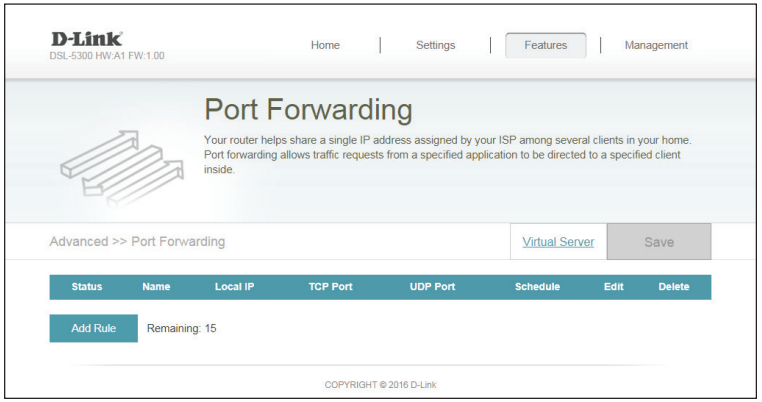
Port Range: Select the protocol of the traffic to allow or deny (**Any**, **TCP**, or **UDP**) and then enter the range of ports that the rule will apply to.

Schedule: Use the drop-down menu to select the time schedule that the rule will be enabled on. The schedule may be set to **Always Enable**, or you can create your own schedules in the **Schedules** section. Refer to page 83 for more information.

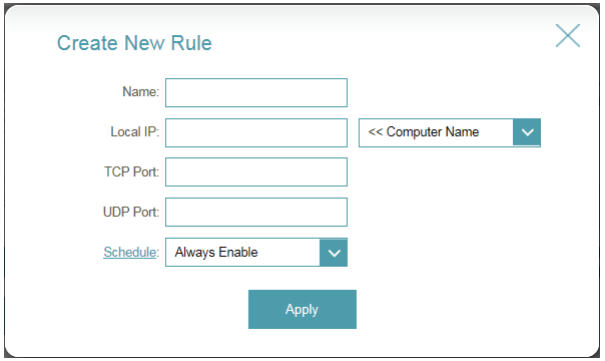
Click **Apply** when you are done.

Port Forwarding

Port forwarding allows you to specify a port or range of ports to open for specific devices on the network. This might be necessary for certain applications to connect through the router. In the Features menu on the bar on the top of the page, click **Port Forwarding**.



If you wish to remove a rule, click on its trash can icon in the Delete column. If you wish to edit a rule, click on its pencil icon in the Edit column. If you wish to create a new rule, click the **Add Rules** button. Click **Save** when you are done. If you edit or create a rule, the following options will appear:



Name: Enter a name for the rule.

Local IP: Enter the IP address of the computer on your local network that you want to allow the incoming service to. Alternatively, select the device from the drop-down menu.

TCP Port: Enter the TCP ports that you want to open. You can enter a single port or a range of ports. Separate ports with a comma (for example: 24,1009,3000-4000).

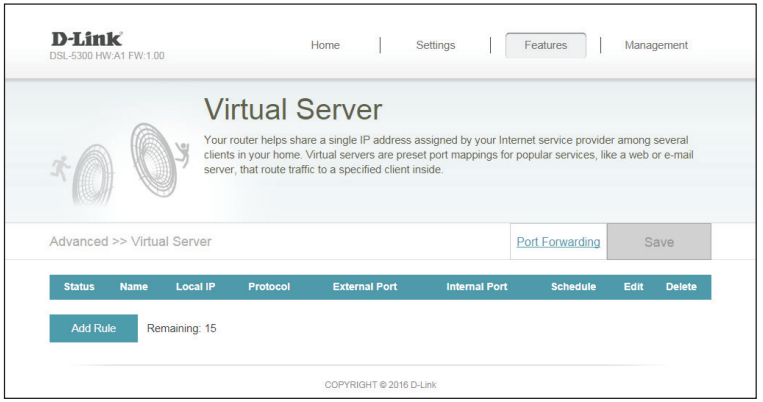
UDP Port: Enter the UDP ports that you want to open. You can enter a single port or a range of ports. Separate ports with a comma (for example: 24,1009,3000-4000).

Schedule: Use the drop-down menu to select the time schedule that the rule will be enabled on. The schedule may be set to **Always Enable**, or you can create your own schedules in the **Schedules** section. Refer to 83 for more information.

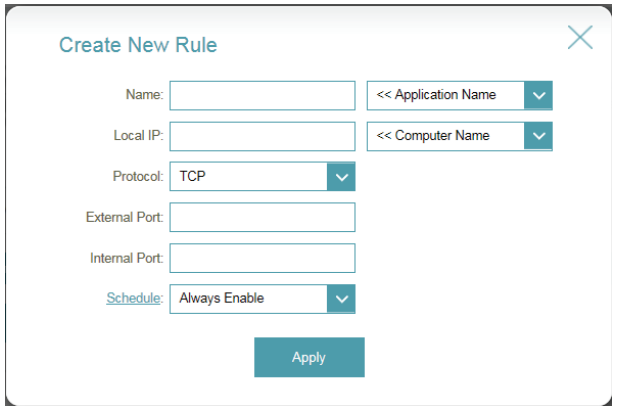
Click **Apply** when you are done.

Virtual Server

The virtual server allows you to specify a single public port on your router for redirection to an internal LAN IP Address and Private LAN port. To configure the virtual server, from the Port Forwarding page click **Virtual Server**. To return to the main Port Forwarding page, click **Port Forwarding**.



If you wish to remove a rule, click on its trash can icon in the Delete column. If you wish to edit a rule, click on its pencil icon in the Edit column. If you wish to create a new rule, click the **Add Rules** button. Click **Save** when you are done. If you edit or create a rule, the following options will appear:



Name: Enter a name for the rule.

Local IP: Enter the IP address of the computer on your local network that you want to allow the incoming service to. Alternatively, select the device from the drop-down menu.

Protocol: Select the protocol of the traffic to allow or deny (**TCP**, **UDP**, **Both**, or **Other**).

Protocol Number: If you entered **Other** above, enter the protocol number.

External Port: Enter the public port you want to open.

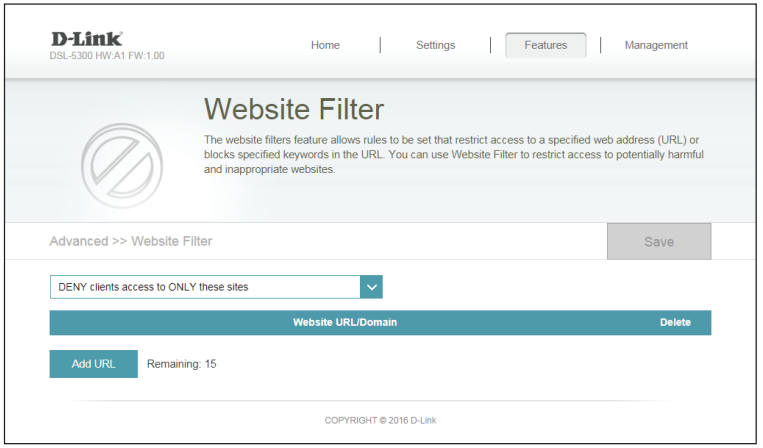
Internal Port: Enter the private port you want to open.

Schedule: Use the drop-down menu to select the time schedule that the rule will be enabled on. The schedule may be set to **Always Enable**, or you can create your own schedules in the **Schedules** section. Refer to page 83 for more information.

Click **Apply** when you are done.

Website Filter

The website filter settings allow you to block access to certain websites. You can either create a list of sites to block or create a list of sites to allow (with all other sites being blocked).



In the Features menu on the bar on the top of the page, click **Website Filter**.

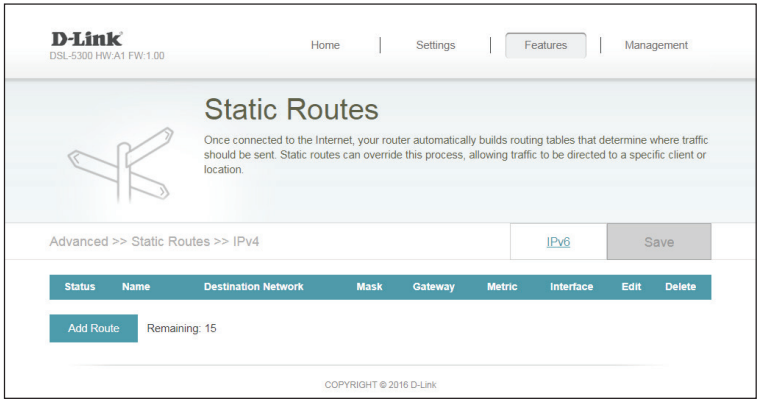
If you want to create a list of sites to block, select **DENY computers access to ONLY these sites** from the drop-down menu. All other sites will be accessible. If you want to specify a list of sites to allow, select **ALLOW computers access to ONLY these sites** from the drop-down menu. All other sites will be blocked.

You may specify a maximum of fifteen websites. To add a new site to the list, click **Create New Rule**. Next, under Website URL/Domain enter the URL or domain. If you wish to remove a rule, click on its trash can icon in the Delete column. If you wish to edit a rule, simply replace the URL or domain.

Click **Save** when you are done.

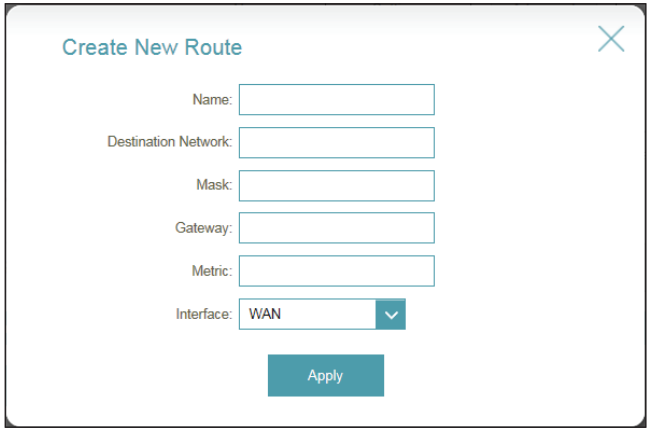
Static Routes

The Static Routes section allows you to define custom routes to control how data traffic is moved around your network.



In the Features menu on the bar on the top of the page, click **Static Routes**. To configure IPv6 rules, click **IPv6** and refer to page 77 for more information. To return to the main IPv4 static routes page, click **IPv4**.

If you wish to remove a rule, click on its trash can icon in the Delete column. If you wish to edit a rule, click on its pencil icon in the Edit column. If you wish to create a new rule, click the **Add Rules** button. Click **Save** when you are done. If you edit or create a rule, the following options will appear:



Name: Enter a name for the rule.

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

Netmask: Enter the netmask of the route.

Gateway: Enter your next hop gateway to be taken if this route is used.

Metric: The route metric is a value from 1 to 16 that indicates the cost of using this route. A value 1 is the lowest cost and 15 is the highest cost.

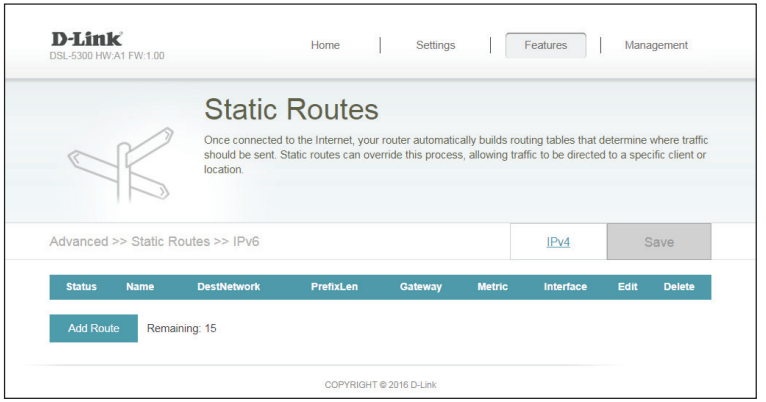
Interface: Select the interface that the IP packet must use to transit out of the router when this route is used.

Click **Apply** when you are done.

IPv6

To configure IPv6 rules, on the Static Routes page click **IPv6**. To return to the main IPv4 static routes page, click **IPv4**.

If you wish to remove a rule, click on its trash can icon in the Delete column. If you wish to edit a rule, click on its pencil icon in the Edit column. If you wish to create a new rule, click the **Add Rules** button. Click **Save** when you are done. If you edit or create a rule, the following options will appear:



Name: Enter a name for the rule.

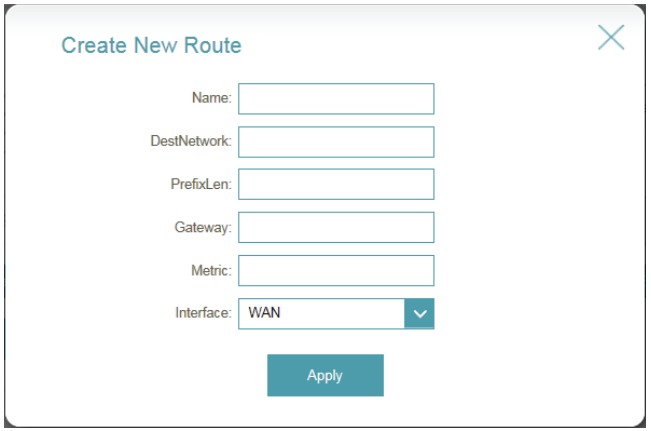
DestNetwork: This is the IP address of the router used to reach the specified destination.

PrefixLen: Enter the IPv6 address prefix length of the packets that will take this route.

Metric: Enter the metric value for this rule here.

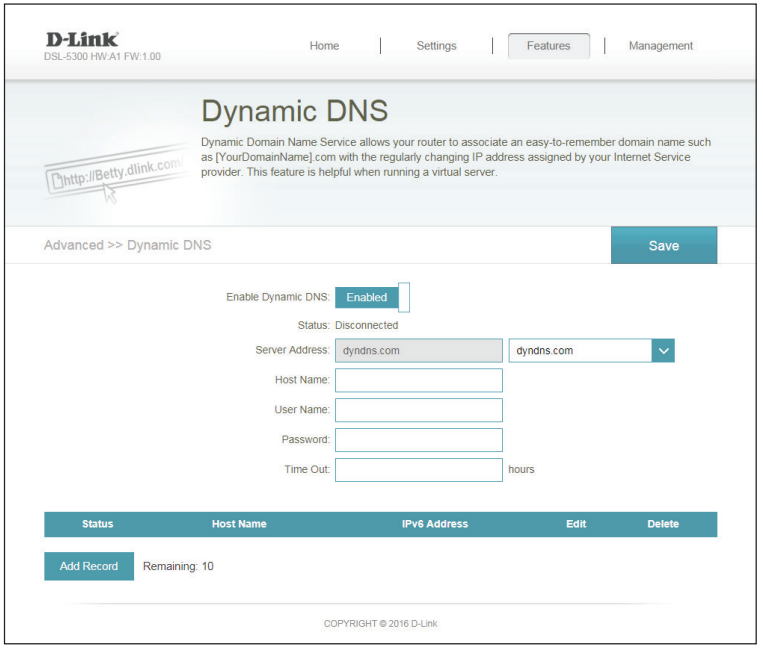
Interface: Select the interface that the IP packet must use to transit out of the router when this route is used.

Click **Apply** when you are done.



Dynamic DNS

Most Internet Service Providers (ISPs) assign dynamic (changing) IP addresses. Using a dynamic DNS service provider, people can enter your domain name in their web browser to connect to your server no matter what your IP address is.



In the Features menu on the bar on the top of the page, click **Dynamic DNS**.

Enable Dynamic DNS: Enabling dynamic DNS will reveal further configuration options.

Status: Displays the current dynamic DNS connection status.

Server Address: Enter the address of your dynamic DNS server, or select one from the drop-down menu.

Host Name: Enter the host name that you registered with your dynamic DNS service provider.

User Name: Enter your dynamic DNS username.

Password: Enter your dynamic DNS password.

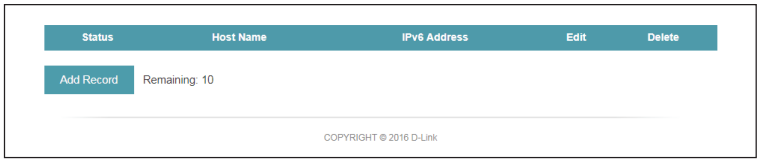
Time Out: Enter a timeout time (in hours).

Click **Save** when you are done.

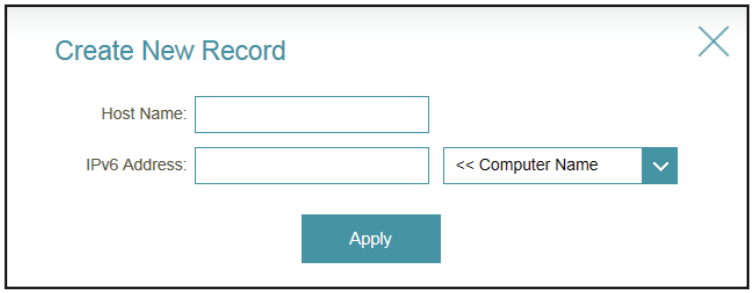
At the bottom of the page are the IPv6 host settings. To configure an IPv6 dynamic DNS host, refer to 79 for more information.

IPv6 Host

The IPv6 host settings are found at the bottom of the Dynamic DNS page.



If you wish to remove a rule, click on its trash can icon in the Delete column. If you wish to edit a rule, click on its pencil icon in the Edit column. If you wish to create a new rule, click the **Add Rules** button. Click **Save** when you are done. If you edit or create a rule, the following options will appear:



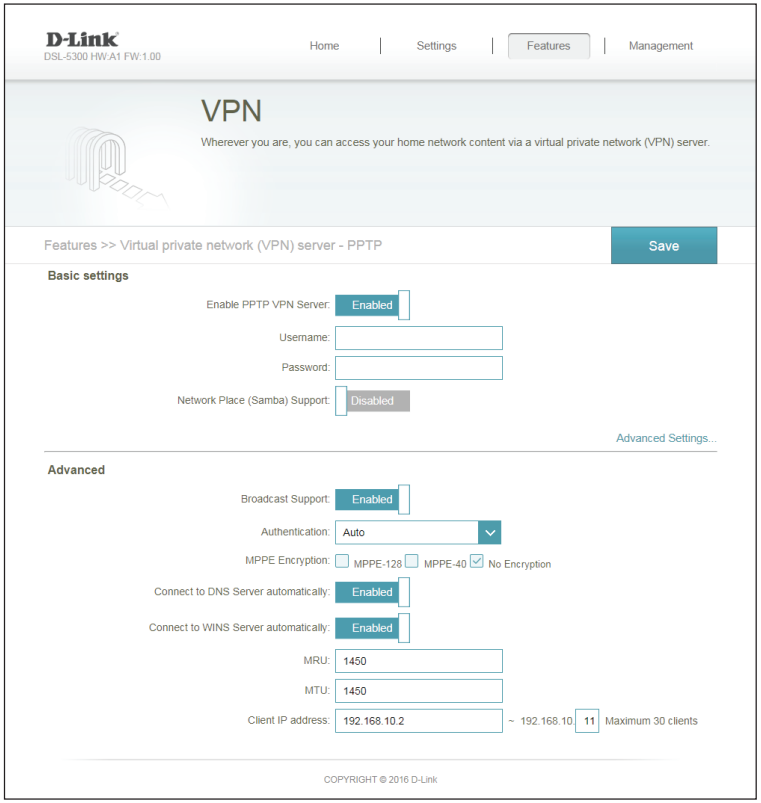
Host Name: Enter the host name that you registered with your dynamic DNS service provider.

IPv6 Address: Enter the IPv6 address of the dynamic DNS server. Alternatively, select the server device in the drop-down menu.

Click **Apply** when you are done.

VPN

This page allows you to configure the DSL-5300 as a VPN server. We recommend configuring Dynamic DNS before proceeding with VPN setup. If your router is assigned an IP address from your ISP using DHCP, it may frequently change, requiring clients credentials to be set up again and a simple DDNS address will be easier than an IP address.



Enable PPTP VPN Server: Select to enable the PPTP VPN server.

Username: Enter the Username that will be required to log into the server remotely.

Password: Enter the Password that will be required to log into the server remotely.

Network Place (Samba) Support: Select **Enable** to enable support for SAMBA and Windows networking over the PPTP connection.

Note that this will expose your network to anyone able to log in.
Select to Enable broadcast support over PPTP.

Broadcast Support: Select to enable broadcast support over VPN connections.

Authentication: Choose the authentication protocol type: **Auto**, **MSCHAPv1**, and **MSCHAPv2**. **Auto** is the default.

MPPE Encryption: Select encryption to be supported by the PPTP tunnel. Choose from **MPPE-128** or **MPPE-40** from Microsoft Point-to-Point Encryption (MPPE). Select **No Encryption** to disable encryption. Select multiple options to allow the client to choose between them.

Connect to DNS Server automatically: Select to automatically connect to the router's DNS server to resolve DNS queries.

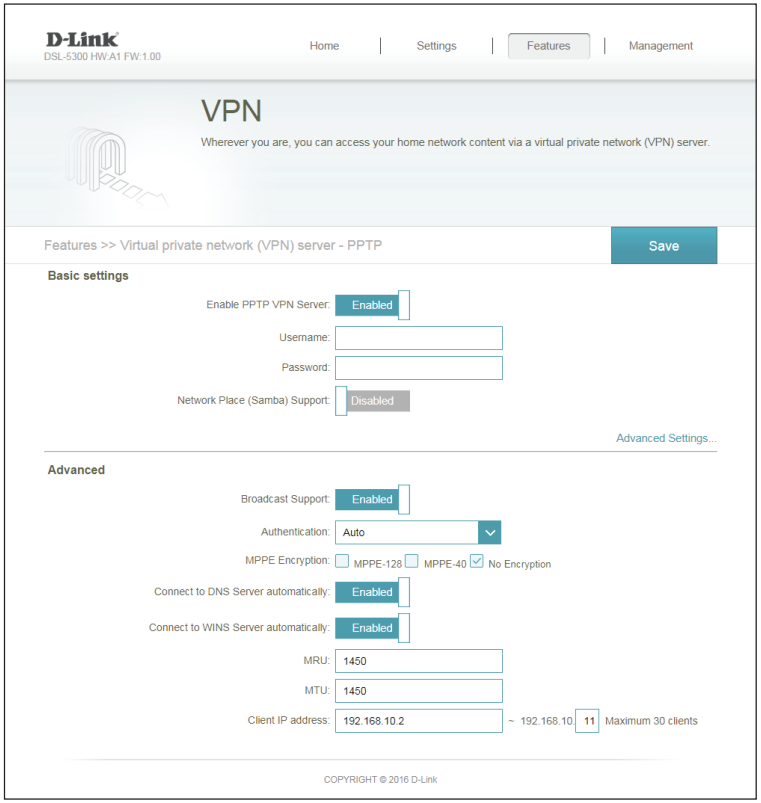
Connect to WINS Server automatically: Select to automatically connect to the router's WINS server to resolve net NetBIOS names.

MRU: Enter the maximum receive unit (MRU) packet size. The default is 1450 to allow additional overhead for the VPN protocol.

MTU: Enter the maximum transmission unit (MTU) packet size. The default is 1450 to allow additional overhead for the VPN protocol.

Client IP address: Enter a range of IPs to assign to VPN clients. Note that regardless of the range specified, the device cannot support more than 30 clients.

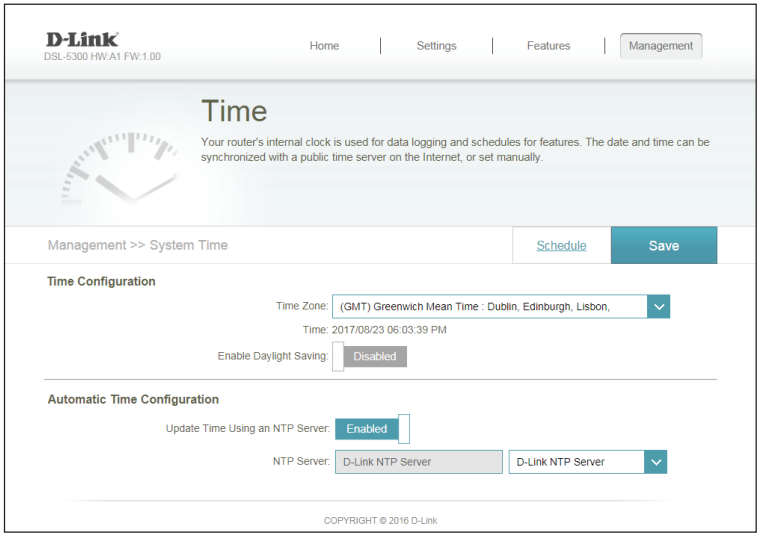
Click **Save** when you are done.



Management

Time & Schedule

Time



The Time page allows you to configure, update, and maintain the correct time on the internal system clock. From here you can set the time zone, the Network Time Protocol (NTP) server, and enable or disable daylight saving time.

In the Management menu on the bar on the top of the page, click **Time & Schedule**.

Time Zone: Select your time zone from the drop-down menu.

Time: Displays the current date and time of the router.

Daylight Saving: Enable or disable daylight saving time.

Update Time Using an NTP Server: Enable or disable to allow an NTP server on the Internet to synchronize the time and date with your router. If you enable this option, select an NTP server from the drop-down menu. To configure the router's time and date manually, disable this option and use the drop-down menus that appear to input the time and date.

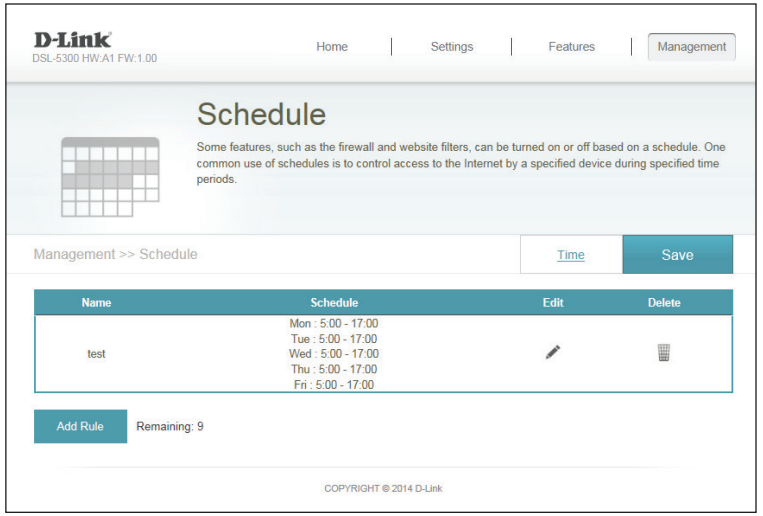
Click **Save** when you are done.

To configure and manage your schedules, click **Schedule** and refer to page 83 for more information.

Schedule

Some configuration rules can be set according to a pre-configured schedule. To create, edit, or delete schedules, from the Time page click **Schedule**. To return to the Time page, click **Time**.

If you wish to remove a rule, click on its trash can icon in the Delete column. If you wish to edit a rule, click on its pencil icon in the Edit column. If you wish to create a new rule, click the **Add Rules** button. Click **Save** when you are done. If you edit or create a rule, the following screen will appear:

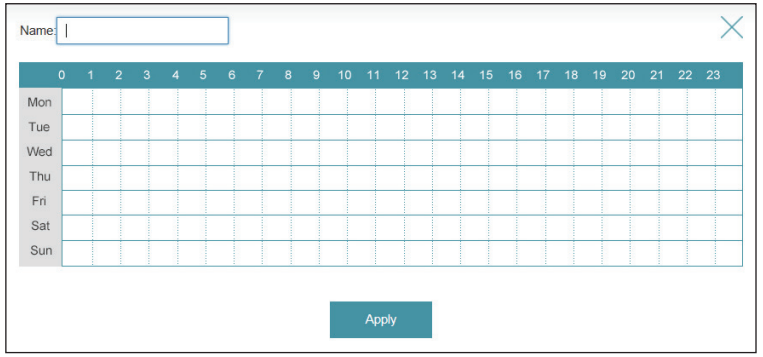


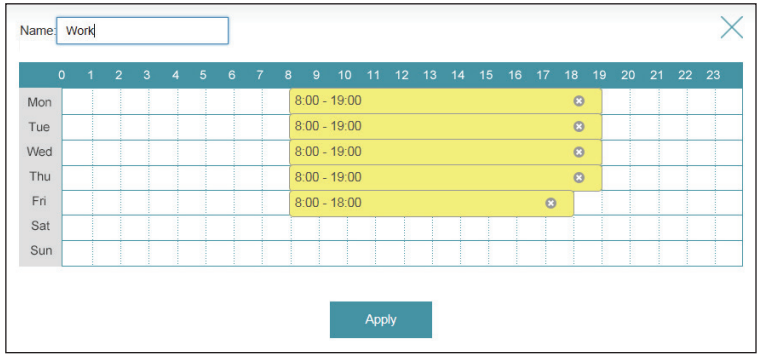
First, enter the name of your schedule in the **Name** field.

Each box represents one hour, with the time at the top of each column. To add a time period to the schedule, simply click on the start hour and drag to the end hour. You can add multiple days to the schedule, but only one period per day.

To remove a time period from the schedule, click on the cross icon.

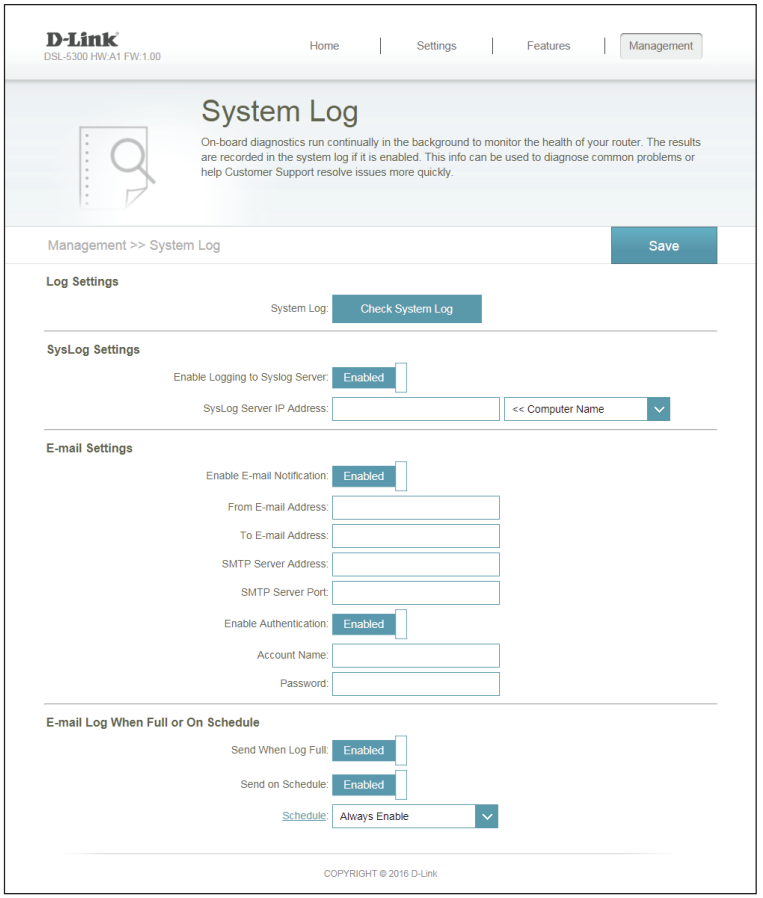
Click **Apply** when you are done.





System Log

The router keeps a running log of events. This log can be sent to a Syslog server or sent to your email address. In the Management menu on the bar on the top of the page, click **System Log**.



System Log: Click **Check System Log** to view the full log in-browser.

Enable Logging to Syslog Server: Check this box to send the router logs to a SysLog Server. If this is disabled, there will be no other options on this page.

Syslog Server IP Address: Enter the IP address for the Syslog server. If the Syslog server is connected to the router, select it from the drop-down menu to automatically populate the field.

Enable Email Notification: If you want the logs to be automatically sent to an email address, enable this option.

Enter the settings for your email account. These are obtained from your email service provider.

On Log Full: If email notification is enabled, this option will set the router to send the log by email when the log is fully.

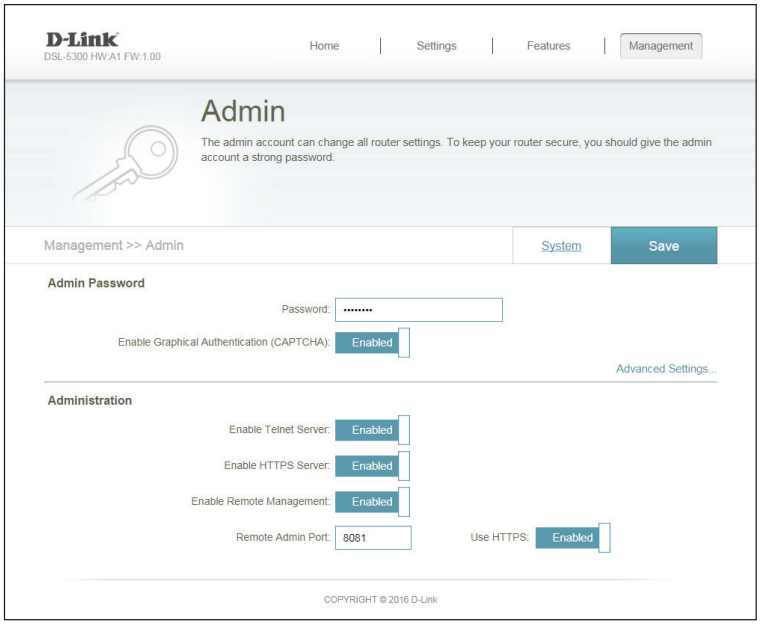
On Schedule: This option can be enabled to send an email according to a pre-configured schedule. See below.

Schedule: If you enable **On Schedule** is enabled, use the drop-down menu to select the time schedule that the rule will be enabled on. The schedule may be set to **Always Enable**, or you can create your own schedules in the **Schedules** section. Refer to page 83 for more information.

Click **Save** when you are done.

Admin

This page will allow you to change the administrator (Admin) password and enable remote management.



In the Management menu on the bar on the top of the page, click **Admin**.

Password: Enter a new password for the administrator account. You will need to enter this password whenever you configure the router using a web browser.

Enable Graphical Authentication (CAPTCHA): Enables a challenge-response test to require users to type letters or numbers from a distorted image displayed on the screen to prevent online hackers and unauthorized users from gaining access to your router's network settings.

Enable Telnet Server: If you want to allow router setup via the protocols, you can configure it here. For Telnet, click **Enable Remote Management** to allow administrators to configure the network from outside. If you enabled remote management, enter the remote port number that the router will use for that protocol.

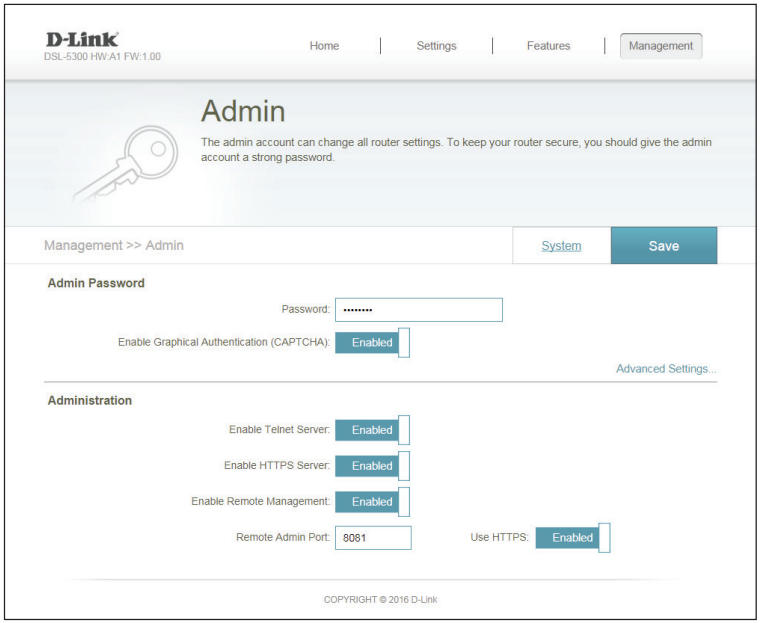
Enable HTTPS Server: Check to enable HTTPS to connect to the router securely. This means to connect to the router, you must enter **https://dlinkrouter.local./** instead of **http://dlinkrouter.local./**

Enable Remote Management: Remote management allows the DIR-860L to be configured from the Internet by a web browser. A password is still required to access the web management interface.

Remote Admin Port: The port number used to access the DIR-860L is used in the URL. Example: **http://x.x.x.x:8080** where x.x.x.x is the Internet IP address of the DIR-860L and 8080 is the port used for the web management interface.

Note: *If you enabled* ***HTTPS Server*** *and wish to access the router remotely and securely, you must enter* ***https://*** *at the beginning of the address.*

Click **Save** when you are done.

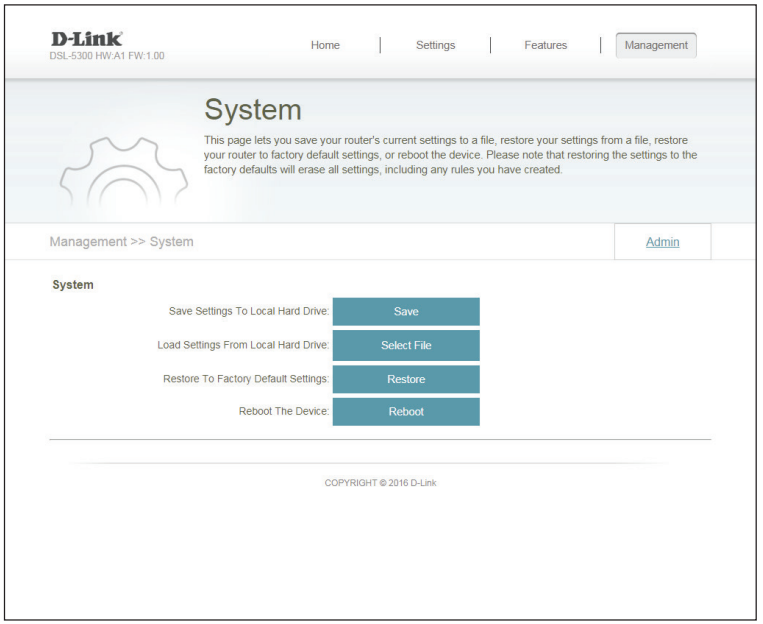


To load, save, or reset settings, or reboot the router, click **Save.**

System

This page allows you to save the router's current configuration, load a previously saved configuration, reset the router to its factory default settings, or reboot the router.

From the Admin page, click **System**. To return to the Admin page, click **Admin**.



Save Settings To Local Hard Drive: This option will save the current router configuration settings to a file on your computer.

Load Settings From Local Hard Drive: This option will load a previously saved router configuration file. This will overwrite the router's current configuration.

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

Auto Reboot Configuration You may configure the router to automatically reboot at a set time. Please note, the router will be temporarily unavailable while rebooting.

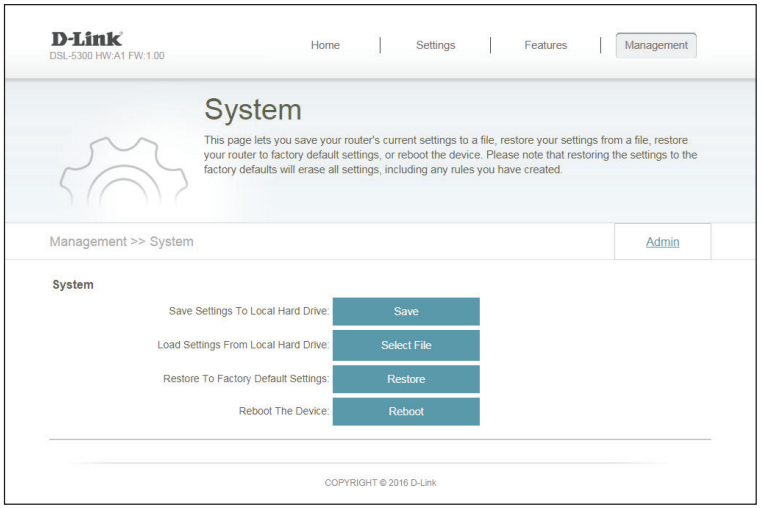
Reboot The Device: Click to reboot the router immediately.

Click **Save** when you are done.

Upgrade

This page will allow you to upgrade the router's firmware or language pack, either automatically or manually. To manually upgrade the firmware or language pack, you must first download the relevant file from **http://support.dlink.com**.

In the Management menu on the bar on the top of the page, click **Upgrade**.



Firmware Information: The current firmware's version and date will be displayed.

Check for New Firmware: Click this button to prompt the router to automatically check for a new firmware version. If a newer version is found, it will prompt you to install it.

Upgrade Firmware: If you wish to upgrade manually, first download the firmware file you wish to upgrade to. Next, click the **Upgrade Firmware** button and browse to the file to install the new firmware. You can also browse to a language pack file to install a new language pack.

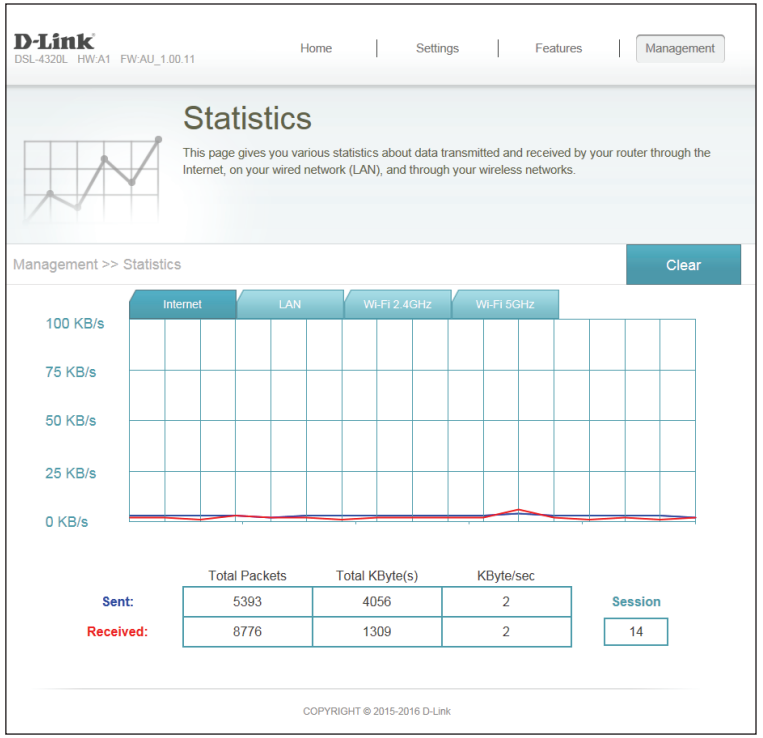
Statistics

On the Statistics page, you can view the amount of packets that pass through the router on the WAN, LAN, and wireless segments.

In the Management menu on the bar on the top of the page, click **Statistics**.

You can view the **Internet**, **LAN**, **Wi-Fi 2.4 GHz**, **Wi-Fi 5 GHz**, or **Wi-Fi 5 GHz** by clicking on the respective tabs at the top. The graph will update in real time. To clear the information on the graph, click **Clear**.

The traffic counter will reset if the device is rebooted.



Connect a Wireless Client to your Router

WPS Button

The easiest and most secure 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 DSL-5300 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 DSL-5300 for about 1 second. The Internet LED on the front will start to blink.

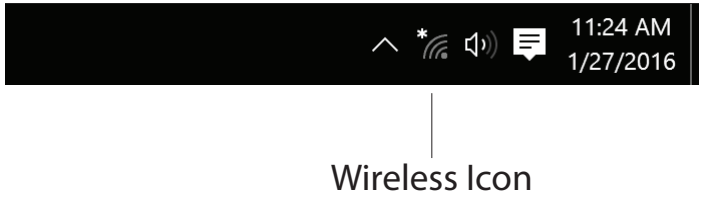
Step 2 - Within 2 minutes, press the WPS button on your wireless device (or launch the software utility and start the WPS process).

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.

Windows® 10

When connecting to the DSL-5300 wirelessly for the first time, you will need to input the wireless network name (SSID) and Wi-Fi password (security key) of the device you are connecting to. If your product has a Wi-Fi configuration card, you can find the default network name and Wi-Fi password here. Otherwise, refer to the product label for the default Wi-Fi network SSID and password, or enter the Wi-Fi credentials set during the product configuration.

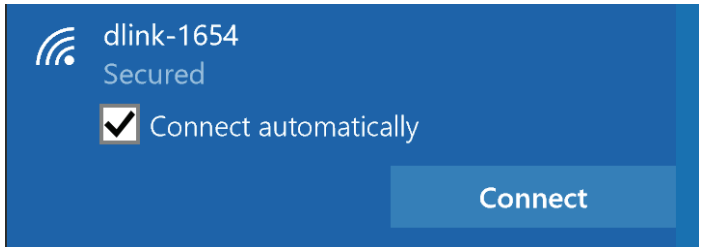
To join an existing network, locate the wireless network icon in the taskbar, next to the time display, and click on it.



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

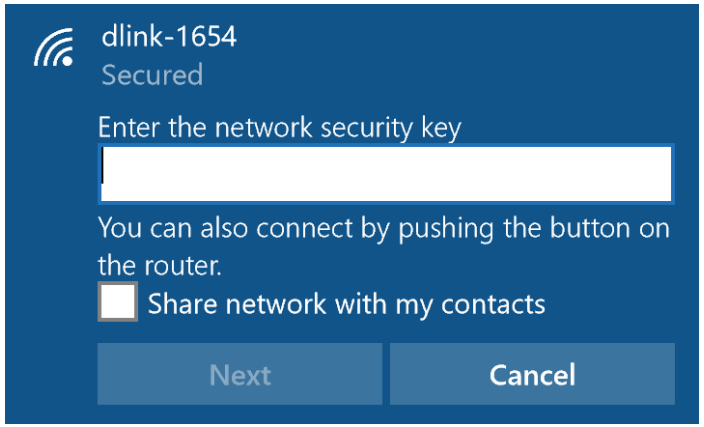
To connect to the SSID, click **Connect.**

To automatically connect to the router when your device detects the SSID, click the **Connect Automatically** check box**.**



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. Your computer will now automatically connect to this wireless network when it is detected.

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

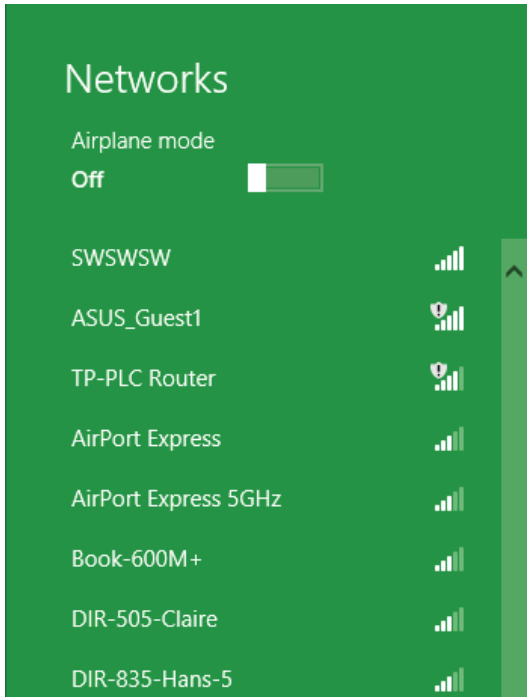


Windows® 8
WPA/WPA2

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.

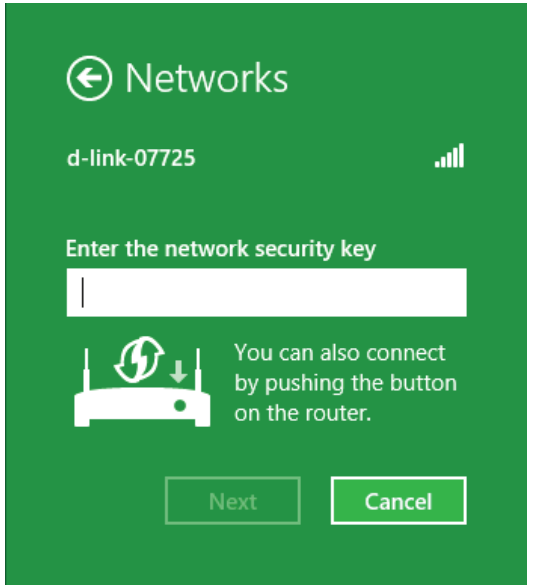
To join an existing network, locate the wireless network icon in the taskbar next to the time display.

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.

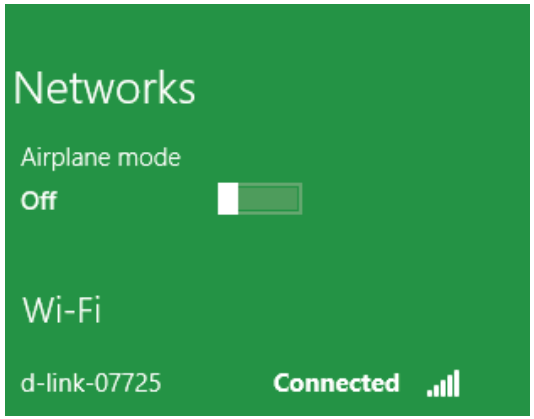


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

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.

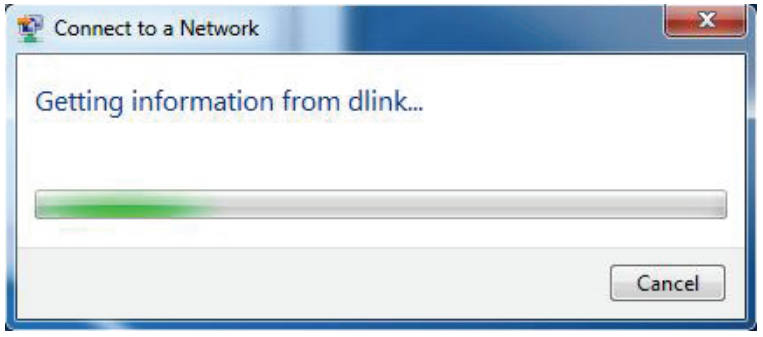
1. Click on the wireless icon in your system tray (lower-right corner).

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

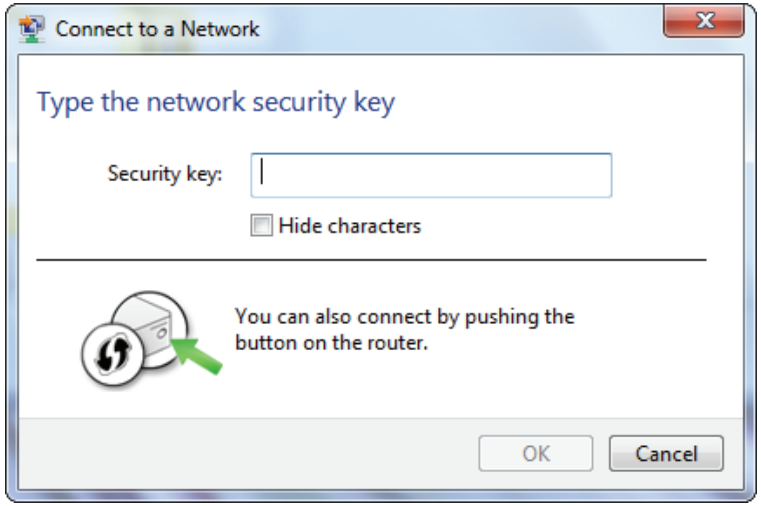
3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

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

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



5. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.

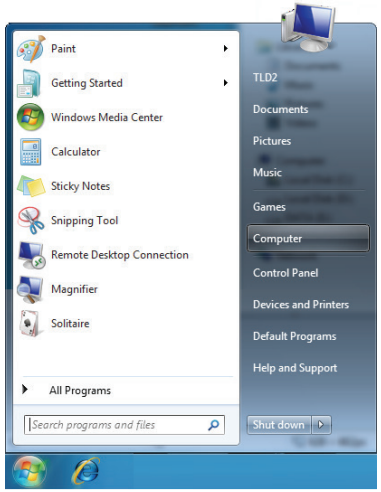


It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as the one on the wireless router.

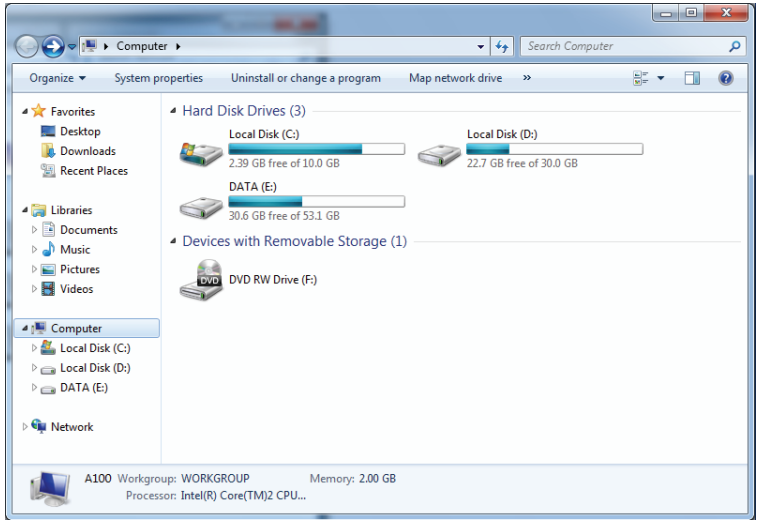
WPS

The WPS feature of the DSL-5300 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

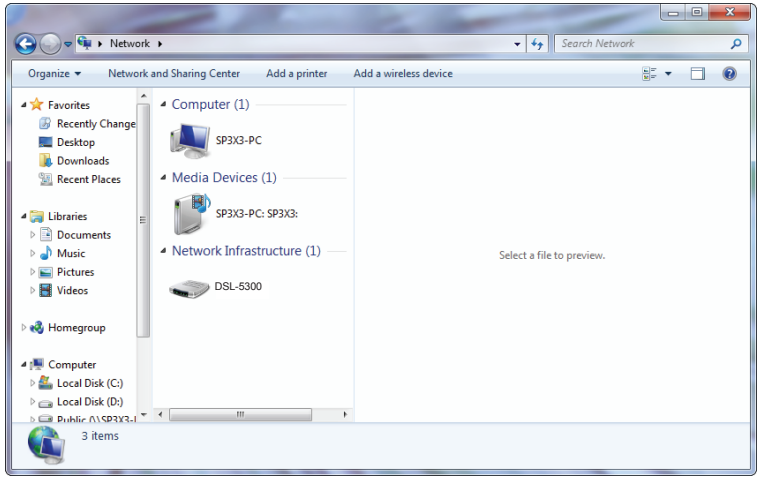
1. Click the **Start** button and select **Computer** from the Start menu.



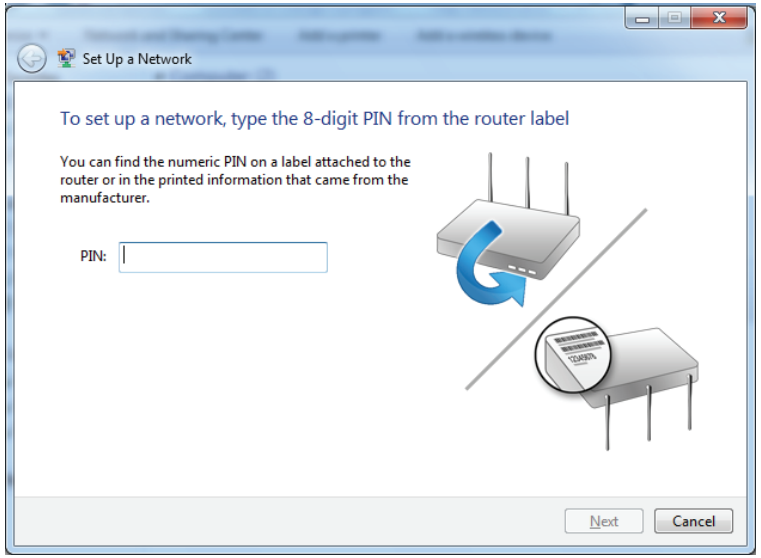
2. Click **Network** on the left side.



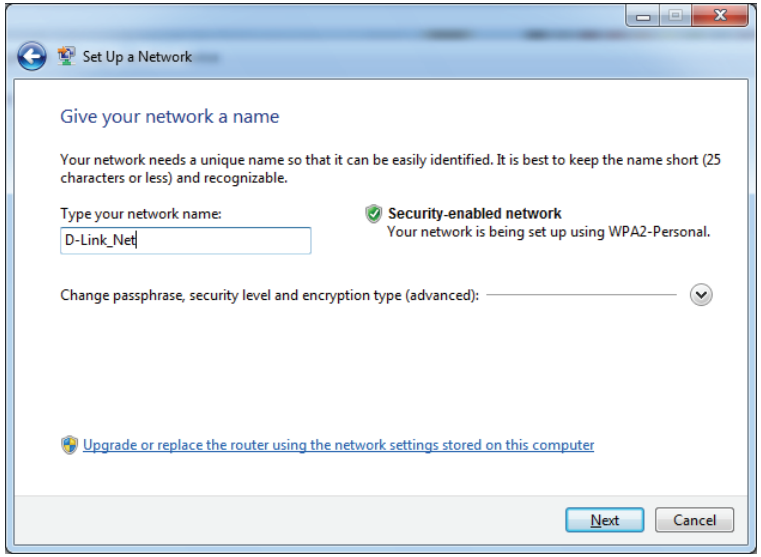
3. Double-click the DSL-5300.



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**.

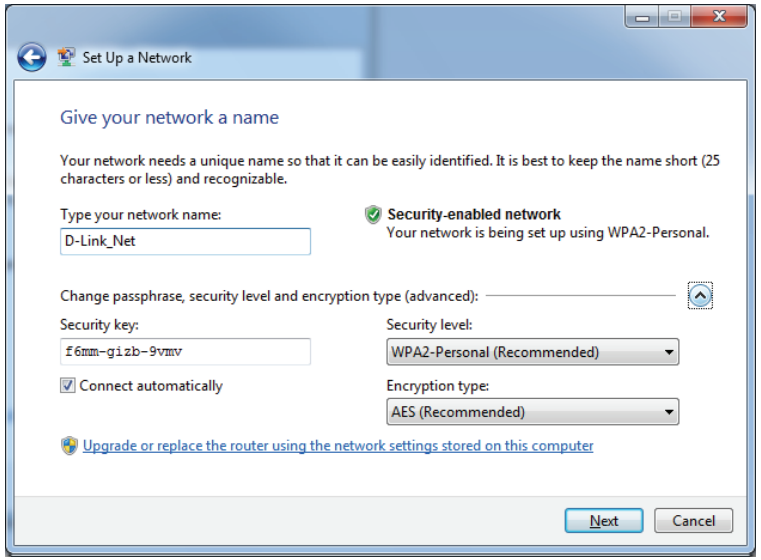


5. Type a name to identify the network.



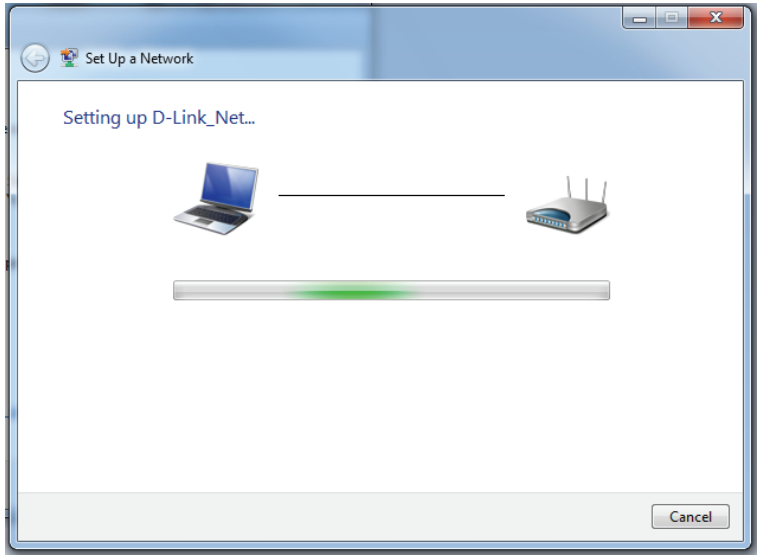
6. To configure advanced settings, click the icon.

Click **Next** to continue.



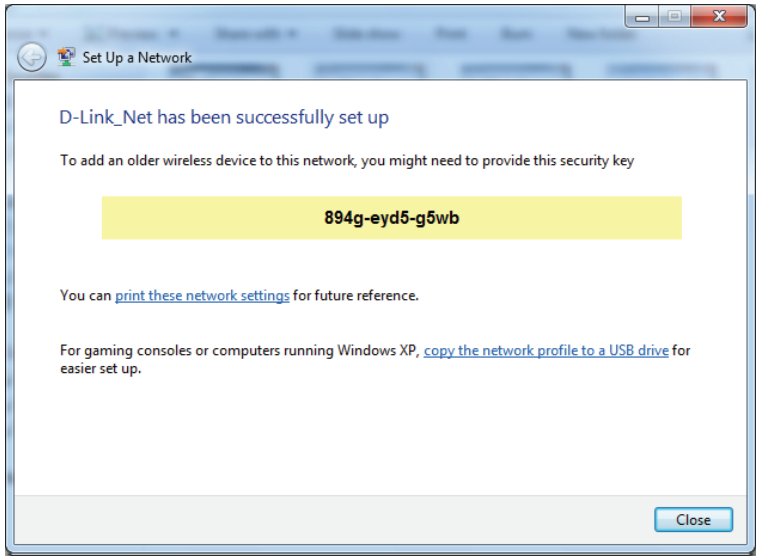
7. The following window appears while the Router is being configured.

   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.

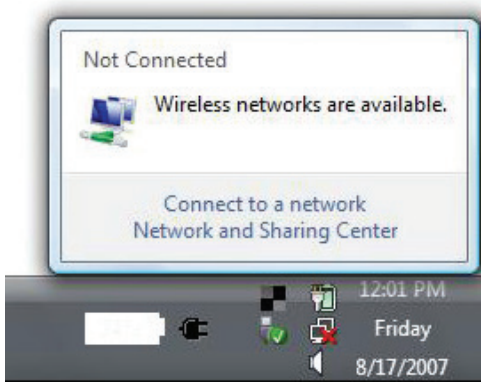
Windows Vista®

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.

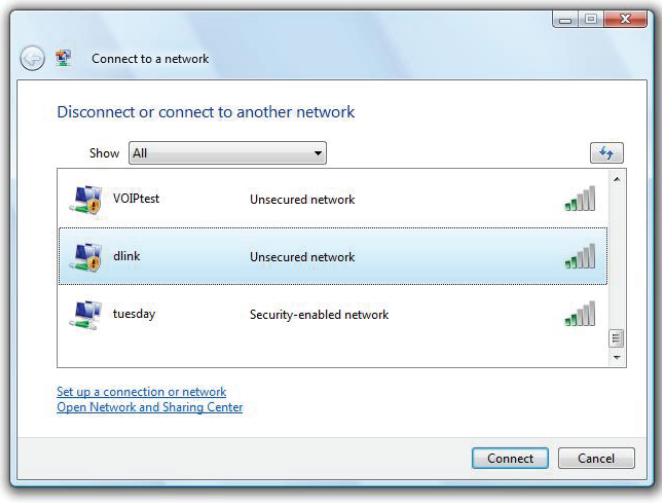
or

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.

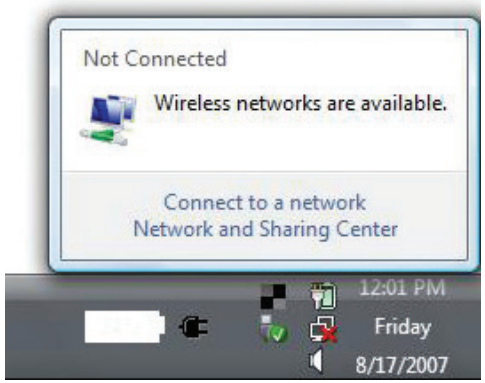
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



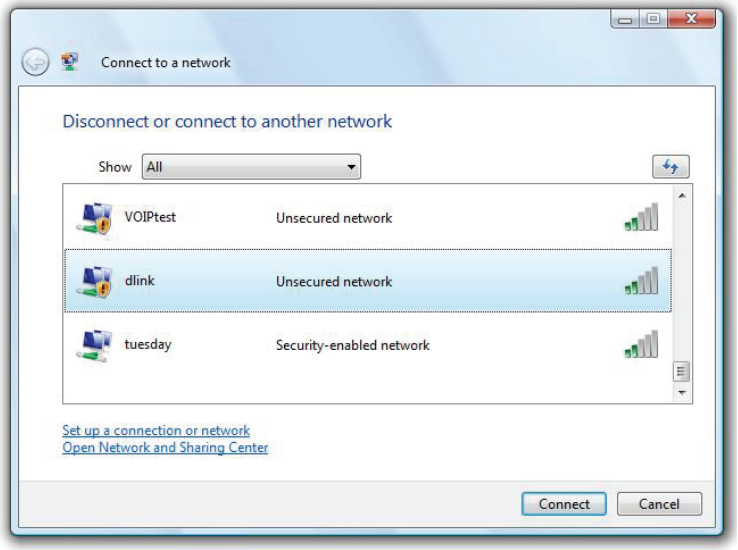
WPA/WPA2

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**.



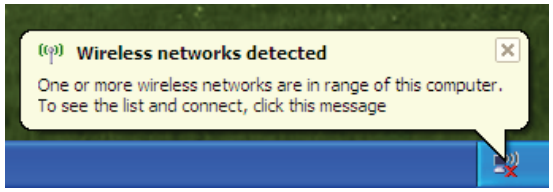
3. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**.

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

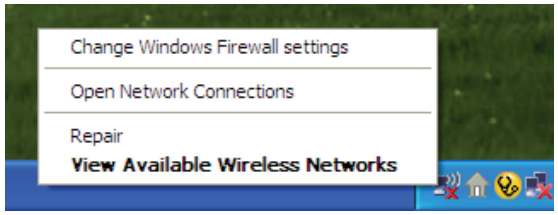
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities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



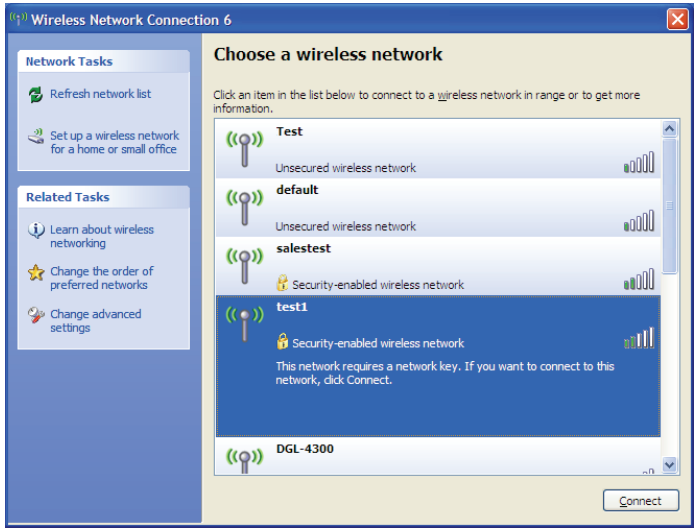
or

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.

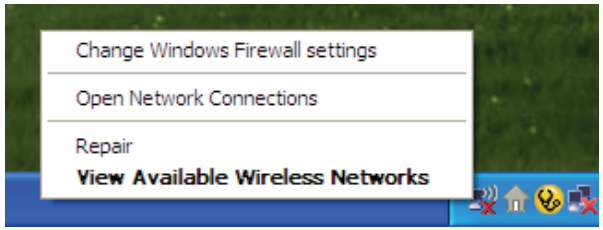
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



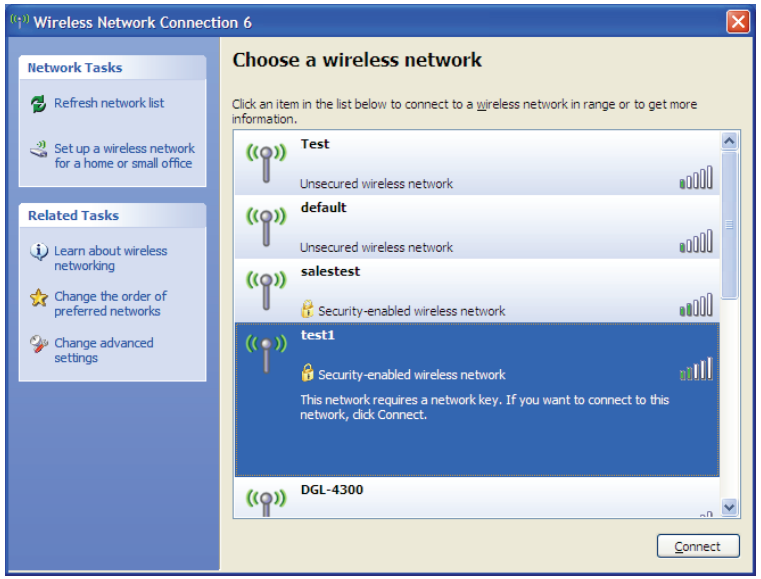
WPA/WPA2

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.

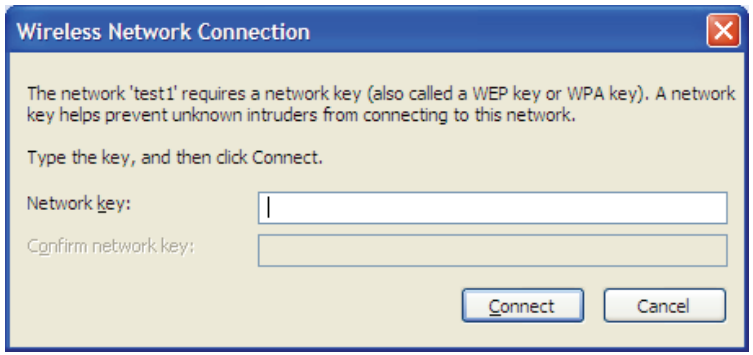
1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.



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 DSL-5300. 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 (**192.168.1.1** 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 **192.168.1.1**. 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:

- Open your browser, enter the IP address of your router (192.168.1.1) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.
- To change the MTU, enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

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 securely access the data you want, when, and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people 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 networksl: 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

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

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.

- **Ad-hoc** – Directly connecting to another computer for peer-to-peer communication using wireless network adapters on each computer, such as two or more DSL-5300 wireless network CardBus adapters.

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

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

Networking Basics

Check your IP address

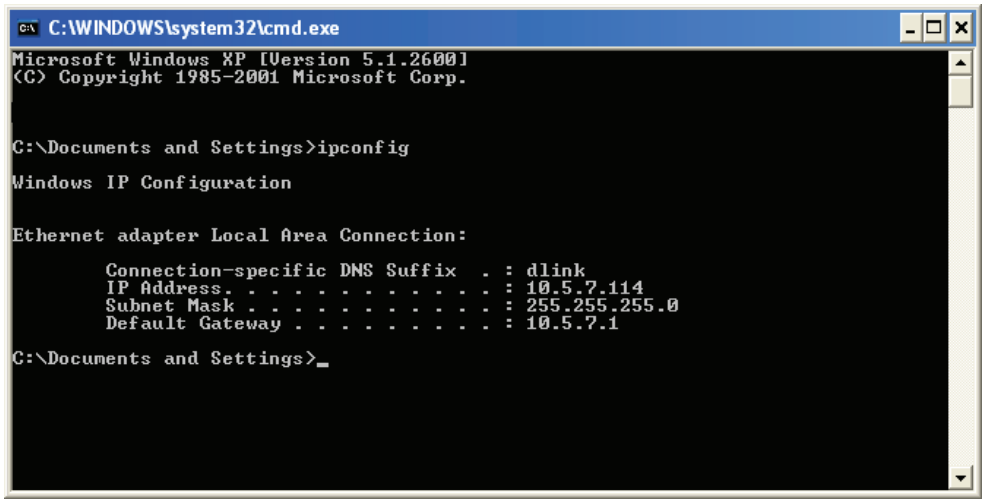
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

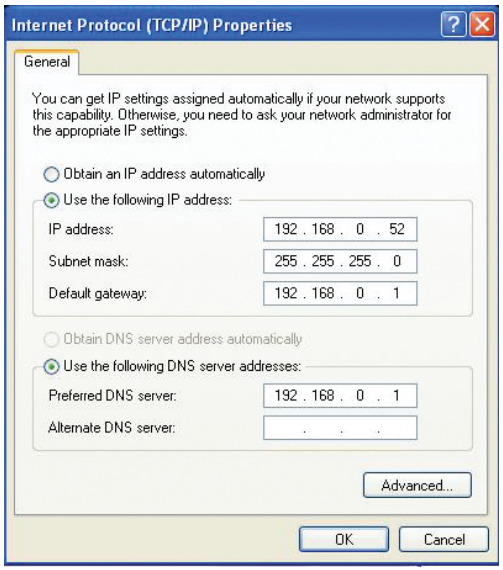
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4

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

Example: If the router´s LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set 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 Secondary 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 protect your data from intruders. The DSL-5300 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, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.

- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

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

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

Technical Specifications

Device Interfaces
- 802.11 ac/n/g/b/a wireless LAN
- DSL Port
- Four 10/100/1000 Gigabit LAN ports
- Two USB ports (one USB 3.0, one USB 2.0)

Antenna Types
- Six external antennas

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

Security
- WPA™ - Personal/Enterprise
- WPA2™ - Personal/Enterprise
- Wi-Fi Protected Setup (WPS) PIN/PBC

Power
- Input: 100 to 240 V AC, 50/60 Hz
- Output: 12 V DC, 5 A

USB Port Power
- 5 V / 0.9 A

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

Operating Humidity
- 10% to 95% maximum (non-condensing)

Certifications
- CSA/LVD
- CE Class B
- RCM
- Wi-Fi Protected Setup (WPS)
- Wi-Fi Multimedia (WMM)

Dimensions
- 225.20 mm (8.87 inches)
- 342.70 mm (13.49 inches)
- 100.88 mm (3.97 inches)

Weight
- 970 g (2.13 lbs)

Note:

- Maximum wireless signal rate derived from IEEE Standard 802.11a, 802.11g, 802.11n, and 802.11ac 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.
- Frequency Range varies depending on country's regulation.
- The DSL-5300 does not include 5.25-5.35 GHz & 5.47-5.725 GHz in some regions.