Version 1.01 |11/21/2023

User Manual

AX1800 Wi-Fi 6 VDSL2/ADSL2+ Modem Router with VoIP

DSL-X1852E

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
1.01	11/13/2023	Removed Speed Test feature

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.

NBN™ is a trademark of NBN Co Limited.

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

Copyright © 2023 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.

ErP Power Usage

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

Network Standby: 9.61watts

Switched Off: 0.3 watts

Table of Contents

Preface ..... **i**

Product Overview **1**
- Package Contents 1
- System Requirements 2
- Introduction 3
- Hardware Overview 5
  - Back Panel 5
  - LEDs 7

Installation **9**
- Before you Begin 9
- Wireless Installation Considerations 10
- Manual Setup 11

Getting Started **14**
- Setup Wizard 15

Configuration **21**
- Home 21
  - Internet 22
    - IPv4/IPv6 23
    - DSL 24
    - 4G 25
    - VPN 26
  - DSL-X1852E 27
  - Connected Clients 28
  - USB Device 29
- Settings 30
  - Wizard 30
  - Internet 30
    - Internet - ADSL 31
    - Internet - VDSL 33
    - Internet - Ethernet 34
    - Connection Types 35
      - Connection Type: Dynamic IP (DHCP) 35
      - Connection Type: Static IP 37
      - Connection Type: PPPoE 39
      - Connection Type: Bridge Mode 41
  - VPN 42
    - IPSec 43
    - GRE 46
  - Wireless 47
    - Guest Zone 53
  - Network 54
    - Reserve IP 57
  - USB 58
    - USB Modem 59
  - Port Bind 60
  - QoS 61
- Features 63
  - Firewall 63
    - IPv4/IPv6 Filter 64
    - NAT 66

Application....68
ACL....69
Port Forwarding....70
Parental Control....71
Static Route....73
Dynamic DNS....74
IGMP....75
TR069....76
VoIP....78
VoIP Advanced....80
SIP Filter....82
Management....83
Time & Schedule....83
Time....83
Schedule....84
Log Info....85
System Log....86
System Settings....88
Admin....89
Firmware Upgrade....90
Statistics....91
Diagnostics....92

Connect and Share a USB Storage Device....93
Connecting from a Windows-Based PC....94
Connect and Share with DLNA Devices....97
Accessing from File Explorer on Windows....98

Connect a Wireless Client to Your Router....100
WPS Button....100
Windows® 11/10....101
WPA/WPA2/WPA3....101
Windows® 8....103
WPA/WPA2....103
Windows® 7....105
WPA/WPA2....105

Troubleshooting....107

Wireless Basics....111
What is Wireless?....112
Tips....114

Networking Basics....115
Check your IP address....115
Statically Assign an IP address....116
Wireless Security....117
What is WPA?....117

Technical Specifications....118

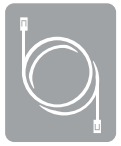
Regulatory Statements....119

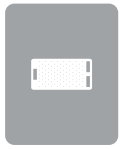
Package Contents

DSL-X1852E AX1800 Wi-Fi 6 VDSL2/ADSL2+ Modem Router with VoIP

Power Adapter

Ethernet Cable


Phone Cable


xDSL Microfilter/Splitter

Quick Install Guide

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

Note: Using a power supply other than the one included with the DSL-X1852E may cause damage and void the warranty for this product.

System Requirements

Network Requirements	• An active subscription with an Internet Service Provider using one of the following connection types: • A VDSL or an ADSL2+ connection to a telephone line using the DSL port Or • An activated existing broadband connection (e.g. NBN™ FTTP, NBN™ HFC) using the WAN port • A computer with 802.11ax/ac/n/g/b/a wireless or Ethernet adapter
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 7 or higher • Firefox 23 or higher • Safari 7 or higher • Chrome 28 or higher • Microsoft Edge

Introduction

The D-Link AX1800 Wi-Fi 6 VDSL2/ADSL2+ Modem Router with VoIP augments your smart home connectivity by leveraging the latest DSL technology. Not only can multiple devices share a single Internet connection, your phones can now use the same Internet access while these devices are transmitting data over the Internet, saving cost and offering convenience through Internet telephony.

The Wi-Fi 6 capability allows your Internet service to be shared wirelessly with a blazing speed of 1800 Mbps* plus the advantage of lower latency compared to previous generations of wireless networking protocols. Other major improvements that were brought with Wi-Fi 6 include Orthogonal Frequency Division Multiple Access (OFDMA), Overlapping Basic Service Sets (OBSS) and more robust security measures such as WPA3 encryption.

In addition to four gigabit Ethernet LAN ports, one Ethernet WAN port, the router also features one USB port for storing and sharing files in your local network. Without the need to configure file sharing on your system, just plug in a USB storage drive into the USB port on the back of your router and you can access files, stream videos, view photos, or listen to music on your laptop or mobile devices.

Some key features are described below:

- **Supporting both VDSL2 and ADSL2+** The built-in DSL modem connects to ADSL2+ or VDSL2 broadband while supporting Voice over IP technology with phone services so you can make and receive calls reliably.
- **Compatible with 802.11ax/ac/n/g/b/a Devices** - The DSL-X1852E is fully backwards compatible with the 802.11ac, 802.11n, 802.11g, 802.11b, and 802.11a* standards, so it can connect with wireless devices operating in this wireless standards.
- **Advanced Features** - The web-based user interface displays a number of advanced network management features including:
    - **QoS & VLAN-** Support traffic classification and prioritization with ATM QoS as well as VLAN tagging (802.1p).
    - **Filtering** - Easily apply content filtering based on IP address, MAC address, URL, or domain name.
    - **Scheduling** - The Internet accessibility and the wireless function can be scheduled.
    - **VPN** - Provides VPN connectivity using PPTP or L2TP, plus IPSec VPN and GRE Tunnel for creating

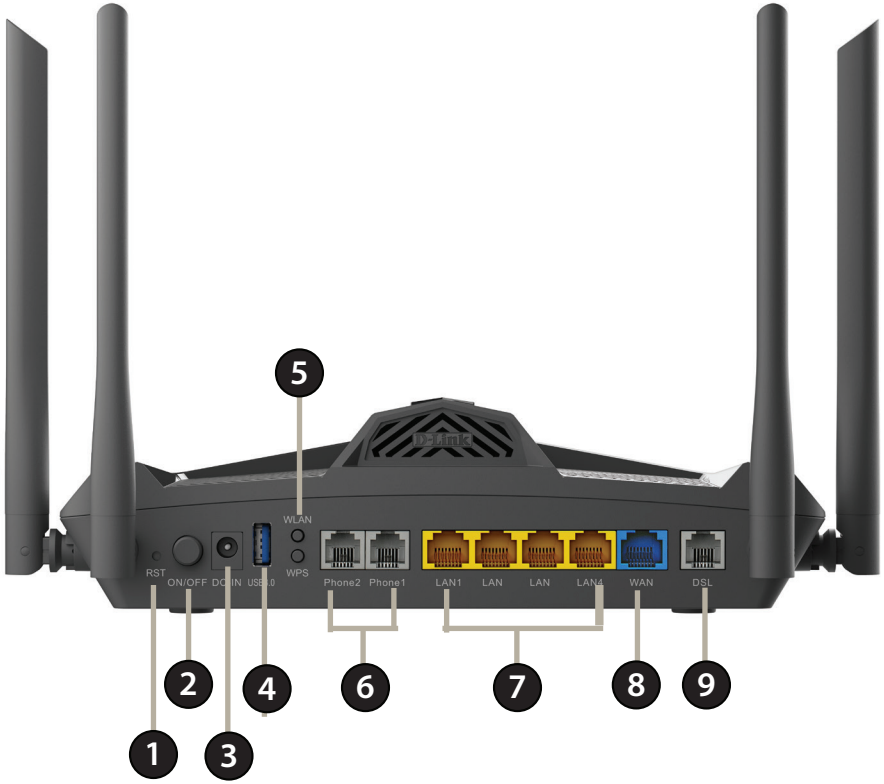
virtual links between two endpoints.

- **Remote Management -** The DSL-X1852E can be remotely provisioned with configuration profiles uploaded by service providers, eliminating on-site management and reducing time for large-scale deployment.

* Maximum wireless signal rate derived from IEEE Standard 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax 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.

Hardware Overview

Back Panel



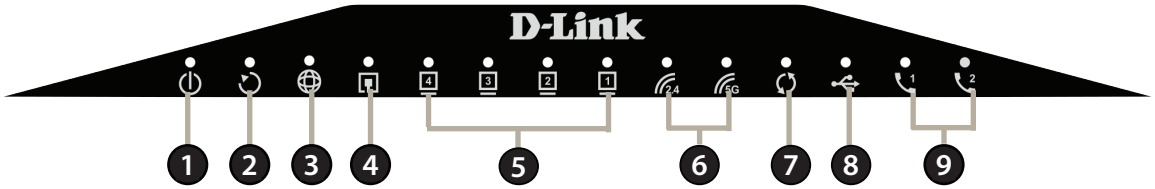
1	**Reset Button**	To reset the device to its factory default settings, use a paper clip to press and hold the reset button for 5 seconds. During the reset process, all lights will turn off and back on again.
2	**Power Button**	Power on/off switch.
3	**Power Connector**	Connector for the supplied power adapter.
4	**USB 3.0 Port**	Connects to USB flash drives to share content.

Back Panel- continued

5	**WLAN (upper)** **WPS Button (lower)**	Press to enable or disable the wireless function. Press to start the WPS process and automatically create an encrypted connection to a WPS client.
6	**Phone 1/2**	Connects to an analogue telephone for Internet telephony.
7	**Gigabit Ethernet Ports (1-4)**	Connects to Ethernet devices such as computers, switches, storage (NAS) devices and game consoles at speeds of up to 1000 Mbps..
8	**WAN Port**	Connects to a cable/DSL (or NBN™/UFB) modem or connection box.
9	**DSL Port**	Connects to a DSL-enabled telephone line.

Hardware Overview

LEDs



1	**Power**	Solid green Solid red Blinking red	Lights up green when the router is powered on and operating normally. When the router boots up or reboots, the LED lights up red. It also lights up red during the factory reset process. It flashes red when an error occurs or during firmware upgrade (when the Internet LED also flashes).
2	**DSL**	Solid green Blinking green Off	Lights up green when the DSL connection is established through the DSL port. Flashes green when the port is negotiating a connection. Off indicates these is no DSL connection.
3	**Internet**	Solid green Blinking green Solid red Blinking red Off	Lights up green when there is an Internet connection. Flashes green when there is Internet activity. It is red when an Internet connection failure occurs (due to authentication failure, IP assignment failure, etc.). It flashes red when firmware upgrade is in progress. Off indicates there is no broadband connection available.
4	**WAN**	Solid green Blinking green Off	Lights up green when the Ethernet WAN port has established a successful connection. It flashes green when there is activity on this port. It is off when a connection failure occurs or the port is not connected.
5	**Ethernet**	Solid green Blinking green Off	Lights up green when the respective LAN port is connected. It flashes green when there is activity on this LAN port. Off indicates the LAN port is not connected.
6	**Wireless 2.4G/5G**	Solid green Blinking green Off	Lights up green when the 2.4 or 5 GHz wireless network is enabled. Flashes green when there is wireless activity. Off indicates wireless function is disabled.

7	**WPS**	Solid green Blinking green Off	Lights up green when a Wi-Fi Protected Setup is established successfully. Flashes green when the WPS process is active. Off indicates that WPS is idle.
8	**USB**	Solid green Blinking green Off	Lights up green when a USB device is connected and detected. It flashes green when data is being transmitted through the USB port. Off indicates no USB device is connected.
9	**FXS 1/2**	Solid green Blinking green Off	Lights up green when the phone port has an active connection to an Internet phone service. It flashes green when the phone is in use. Off indicates that the port is not connected or the phone has no Internet phone 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-X1852E AX1800 Wi-Fi 6 VDSL2/ADSL2+ Modem Router with VoIP for the first time. If you are connecting to an existing cable/NBN™/UFB modem or connection box, you may need to modify these steps according to your broadband technology or plan .

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 which are necessary to establish a connection. This information may include the connection type (DHCP IP, Static IP, or PPPoE) and parameter settings such as VLAN ID.

- 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-X1852E 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-X1852E will be providing this 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 to 90 feet (1 to 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 (0.5 meters) thick, 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 to 6 feet or 1 to 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

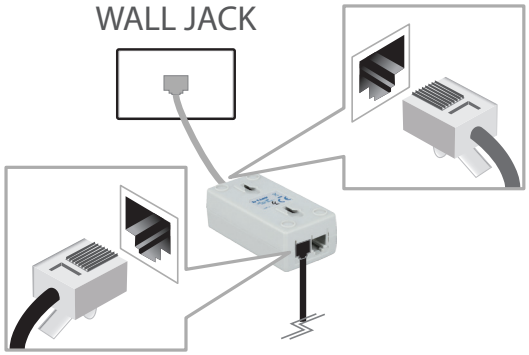
Note: Power off your network devices, including your existing connection box/modem and PC.

1 Position your DSL-X1852E near your PC and a telephone wall jack that provides DSL service. Keep the router in an open area for better wireless coverage.

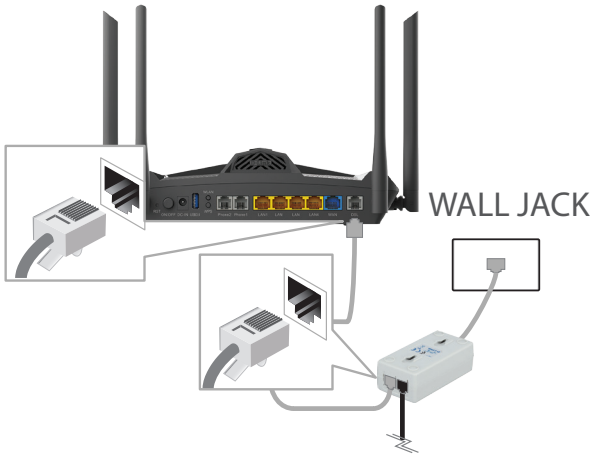
2 Connect the RJ-11 phone cable to the router's Phone 1 port. Connect the other end to your analog telephone. If you have a second Internet phone service account, connect a second telephone to the Phone 2 port.
Caution: Do not connect the Phone port to a telephone wall jack. This port can be only connected with an analog circuit telephone device.

3-1 **Use the DSL-X1852E as both a modem and router.** Plug one end of the supplied DSL phone cable into the DSL port on the back of the router and the other end into the telephone wall jack with the supplied microfilter installed in between.

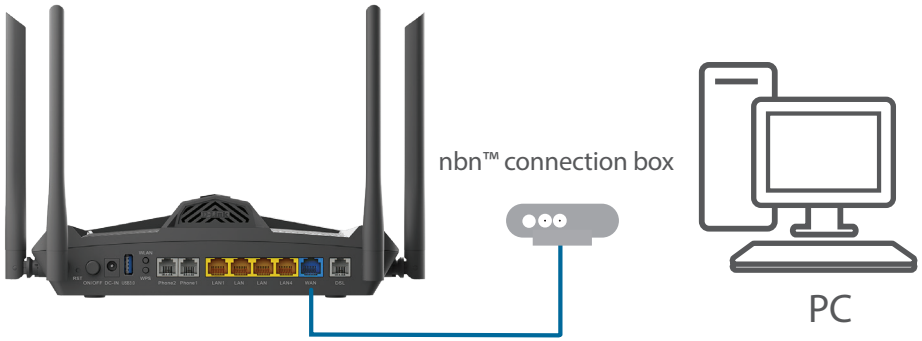
a. Connect the supplied microfilter to your telephone wall jack with the cable labelled WALL SOCKET.



b. Connect the supplied phone cable from the MODEM port on the microfilter to the DSL port of the router.

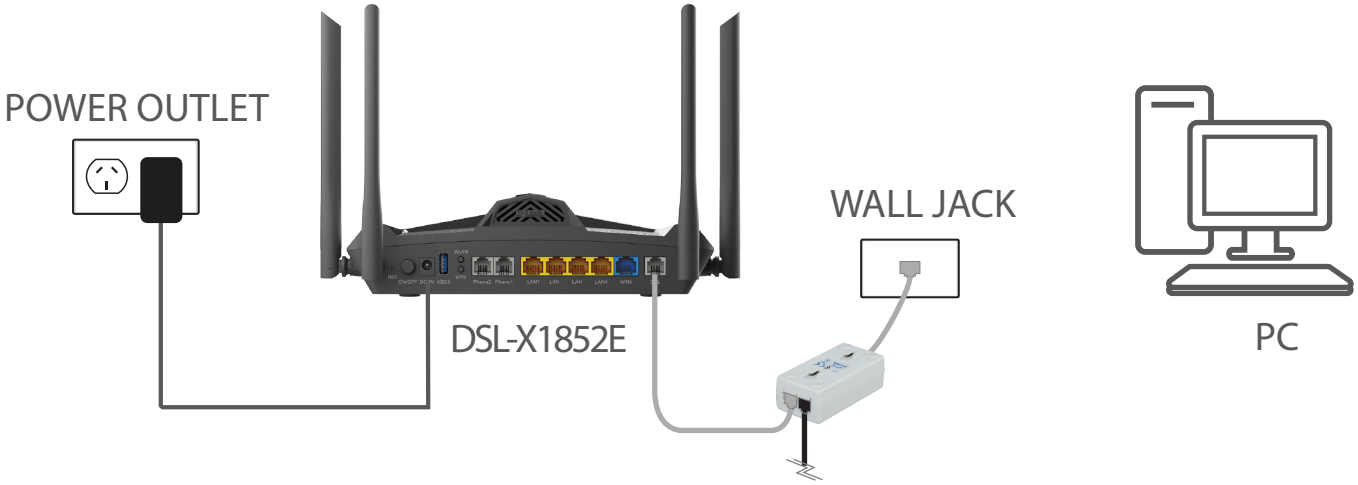


3-2 **Use the DSL-X1852E as a router only.** Plug one end of the supplied Ethernet cable into the WAN port on the back of the router and the other end to your existing cable/UFB/NBN™ connection box or modem. Then power on the connection box.



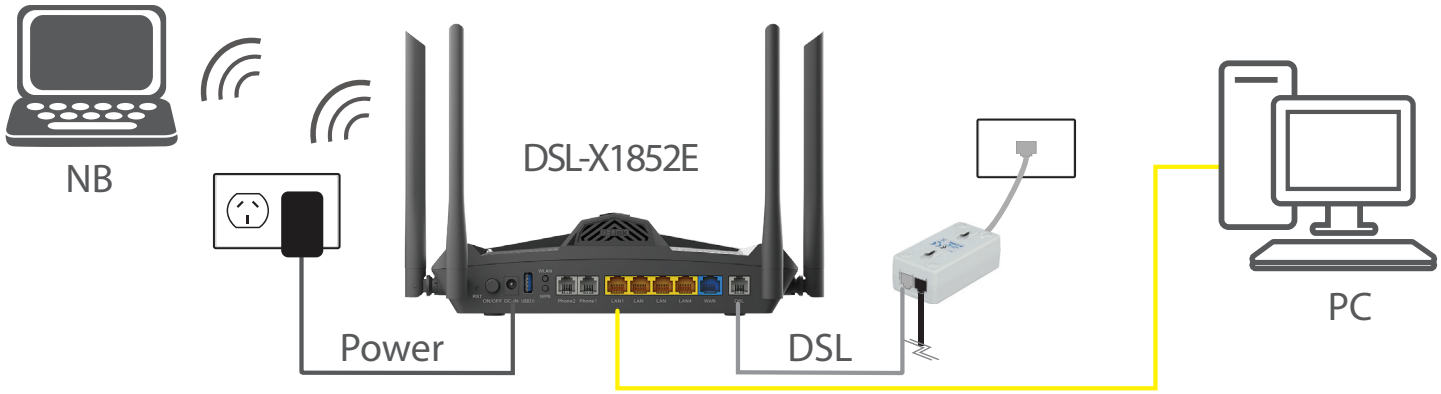
4 Connect the supplied power adapter to the router and a power outlet, and press the power button. The device LEDs will light up. Wait approximately three minutes before proceeding to the next step.

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



5 Plug one end of the supplied Ethernet cable into a yellow Ethernet port on the back of the router, and the other end into the Ethernet port on your computer.

If you are setting up the DSL-X1852E using a laptop or mobile device, connect to it using the Wi-Fi network name and password printed on the label attached to the bottom of your device.



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 **Setup Wizard** on page **15**.

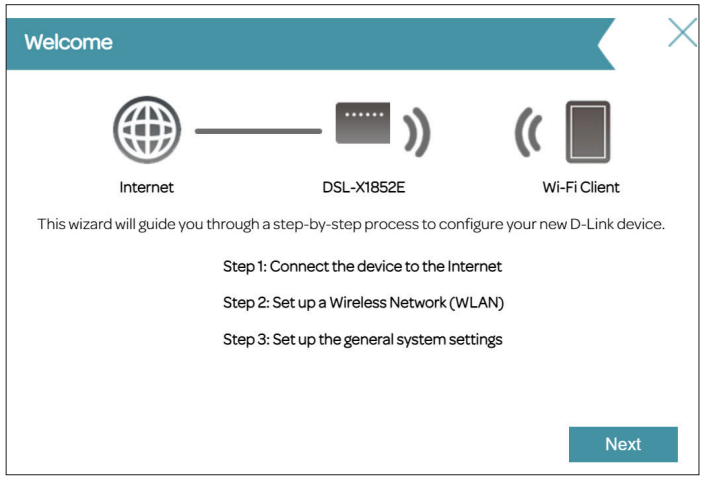
- **Manual Setup** - Log into the router and manually configure it. Refer to **Configuration** on page **21**.

Setup Wizard

If this is your first time using the router, open your web browser and enter the IP address of the router (default: **http://192.168.1.1**). The default password for admin is printed on the bottom of the device.

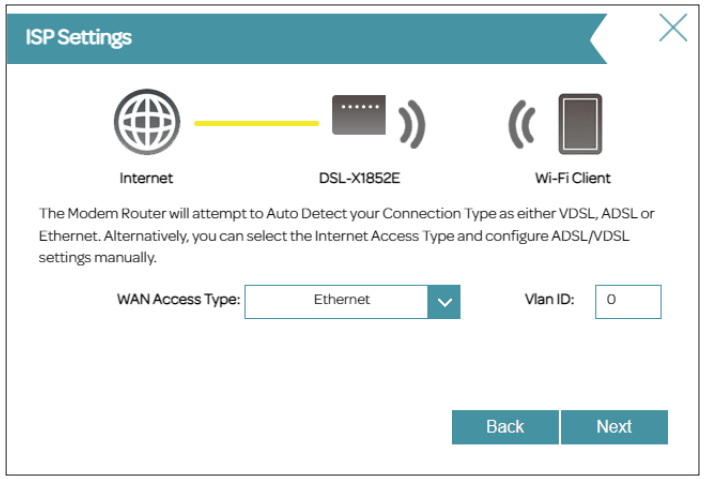
The wizard is designed to guide you through a step-by-step process to configure your new D-Link router and connect to the Internet. Depending on your Internet service and network environment, ensure that your DSL port is connected to the wall jack or an Ethernet WAN port is connected to an active Internet connection.

Click **Next** to continue.



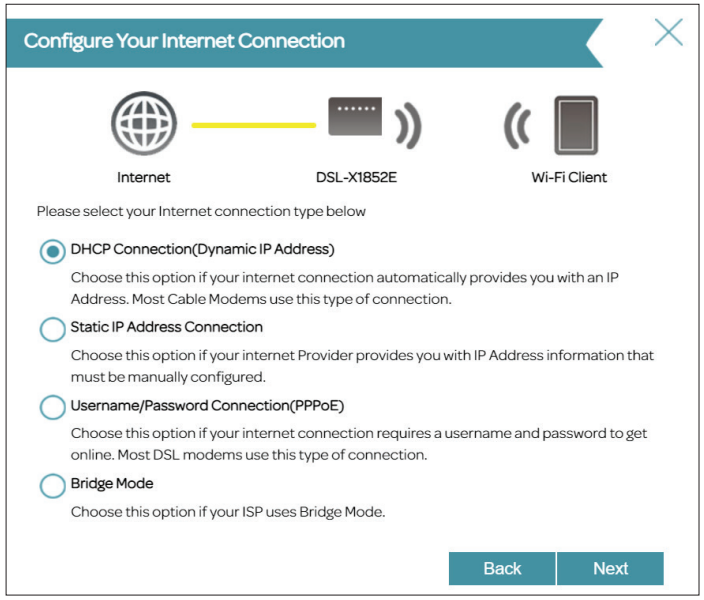
WAN Access Type would attempt to auto detect your connection type as either VDSL, ADSL or Ethernet.

Click **Next** to continue.



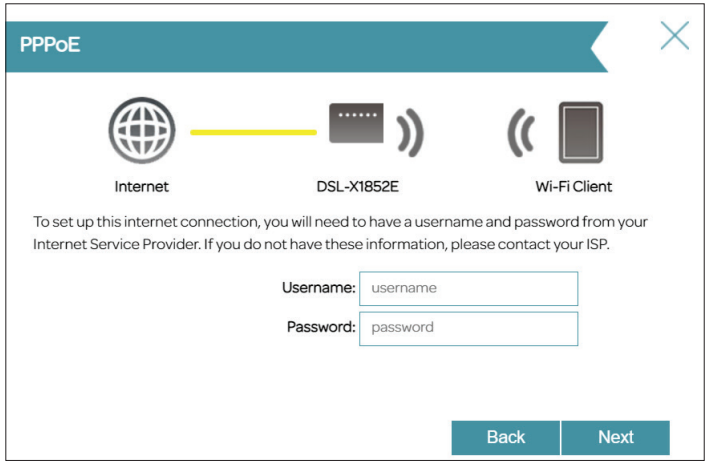
Setup Wizard (continued)

If the router cannot determine your connection type, 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.



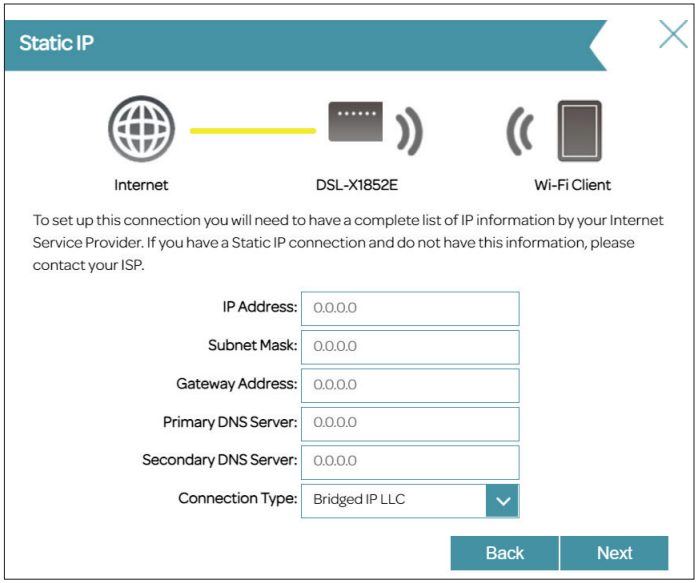
If the router detected or you selected **PPPoE**, enter your PPPoE username and password, choose the **Connection Type** if asked, and click **Next** to continue.

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



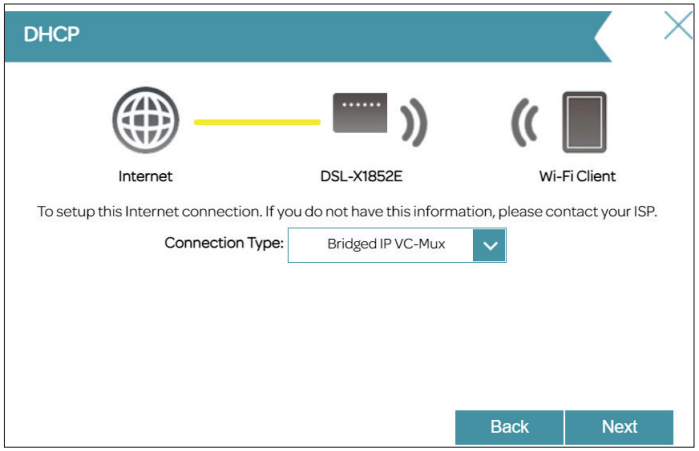
Setup Wizard (continued)

If you selected **Static IP Address**, enter the IP address, subnet mask, gateway address, and DNS servers provided by your ISP, then choose the **Connection Type** if asked. Click **Next** to continue.

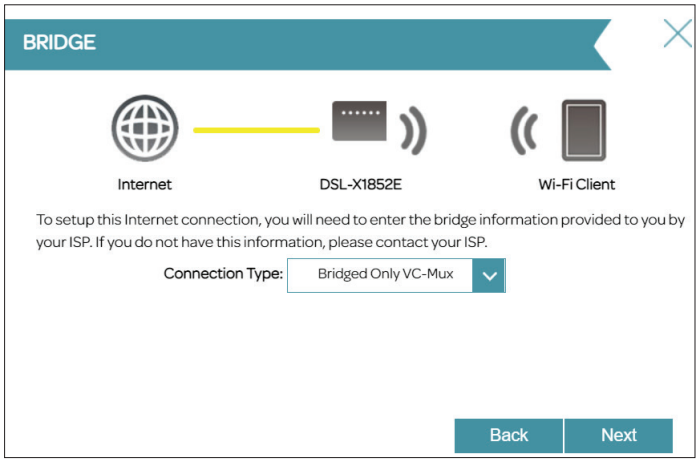


Setup Wizard (continued)

If the router detected or you selected **Dynamic IP Address (DHCP)**, choose the **Connection Type** if asked. Click **Next** to continue.



If you selected **Bridge Mode**, choose the **Connection Type** if asked. Click **Next** to continue.

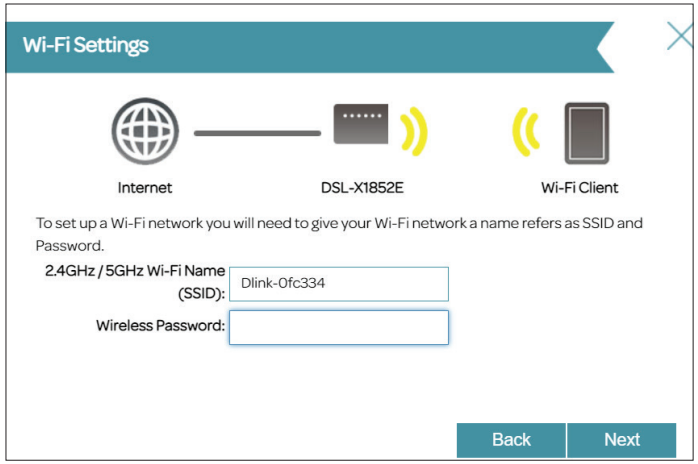


Setup Wizard (continued)

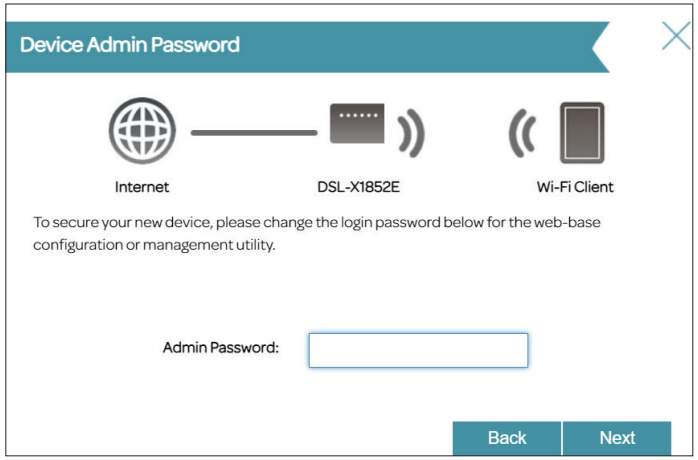
Create a Wi-Fi SSID and password for both the 2.4 GHz and 5 GHz wireless networks. The SSIDs must be between 3 and 32 alphanumeric characters in length and can include hyphens, underscores, periods, and the @ symbol. The password must contain 8 to 63 alphanumeric characters including a mix of uppercase and lowercase letters, numbers, and special characters with the exception of the following characters: '-;`=%+&|><"/.

Your wireless clients must use the correct SSID and password in order to connect to your wireless network.

Click **Next** to continue.

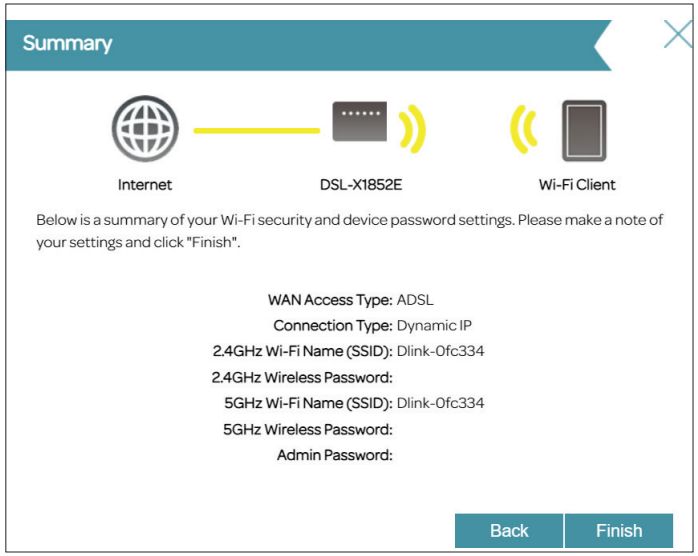


To help protect your router, please enter a new password. You will be prompted for this password every time you want to use the router's web configuration utility. Click **Next** to continue. Passwords must contain 6 to 32 alphanumeric characters including a mix of uppercase and lowercase letters, numbers, and special characters with the exception of the following characters: '-;`=%+&|><"/.



Setup Wizard (continued)

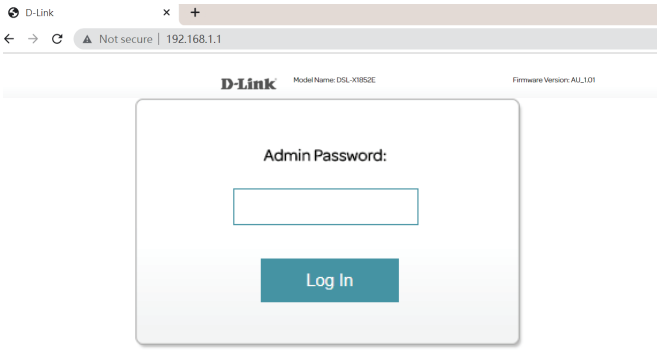
The **Summary** window will display your settings. Click **Next** if you are satisfied, or click **Back** to make changes to your configurations. The wizard will close and your settings will be saved.



Congratulations, setup is complete. You can access the Setup Wizard again from the web configuration utility: go to **Settings > Wizard**.

Configuration

To access the configuration utility, open a web browser such as Google Chrome and enter: **http://192.168.1.1**



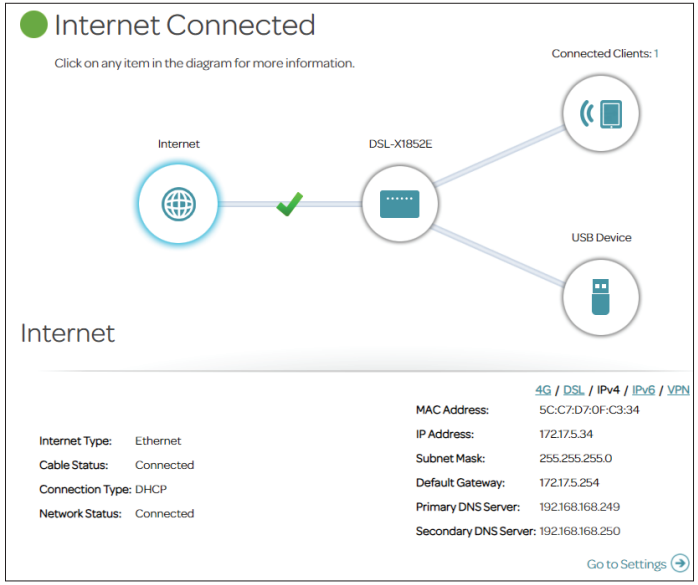
Input the default password as printed on the device label attached to the bottom of the device . If you previously followed the Setup Wizard (see page 15), please use the admin password you entered during the wizard. Click **Log In** to proceed.

Note: *If you cannot remember your password and cannot log in, press the reset button (see page 5) to restore the router to its default settings. However, all your configurations will be erased.*

Home

The **Home** page displays the current status of the router in the form of an interactive diagram. There are four main sections: Internet, the DSL-X1852E, 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, Features,** and **Management** functions. You may quickly jump back Home at any time.

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

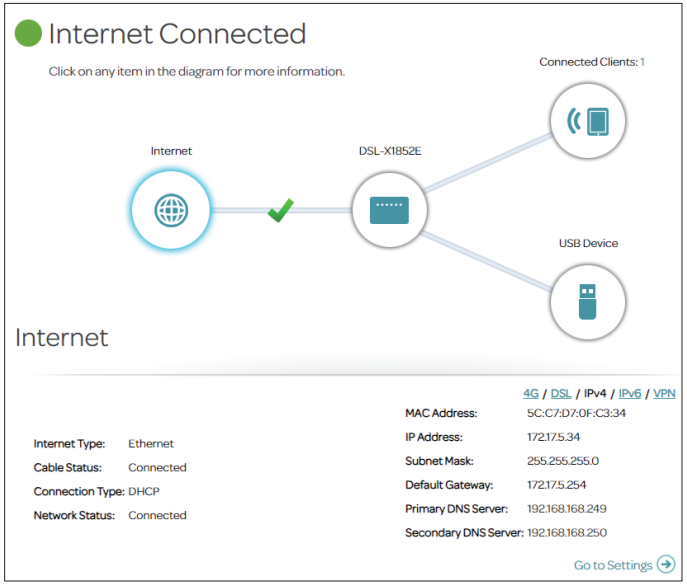


Internet

To bring up more details about your Internet connection, click on the **Internet** icon. The Internet Connection status being displayed will reflect the status of the currently selected WAN configuration: 4G, DSL, IPv4, IPv6, or VPN.

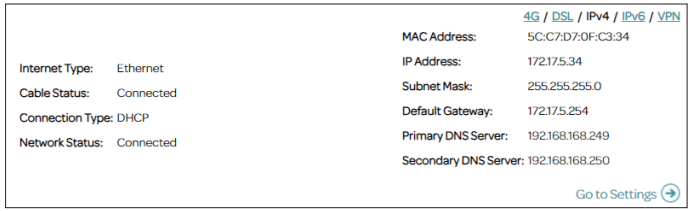
If your Internet is disconnected, indicated by a red X, you can launch the Setup Wizard to correct the issue by clicking **Wizard** from the **Settings** menu at the top of the page.

To reconfigure the Internet settings, refer to **Internet** on page **30**.



IPv4/IPv6

Click the **IPv4/IPv6** button to see the IPv4/IPv6 information for the DSL or WAN interface.



IPv4/IPv6

Internet Type: Displays the current connection type: Ethernet, ADSL or VDSL.

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.

MAC Address: Displays the MAC address of the WAN interface.

IP Address: Displays the current WAN IPv4 or IPv6 address.

Subnet Mask: Displays the current subnet mask of the IP address.

Default Gateway: Displays the current IPv4/IPv6 default gateway.

Prefix: Prefix identifies the subnet of a network in IPv6 addressing scheme.

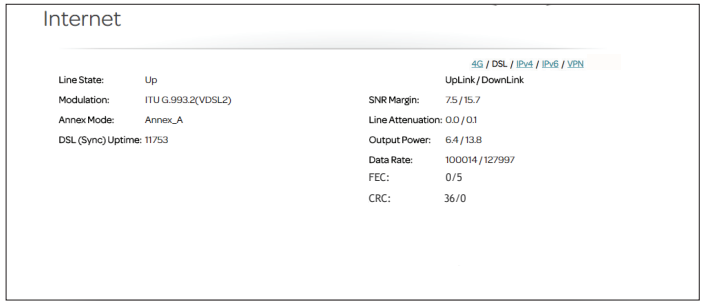
Primary DNS Server: Displays the current primary DNS server.

Secondary DNS Server: Displays the current secondary DNS server.

Click **Go to Settings** below to go to the Internet configuration page.

DSL

Click the **DSL** button to see the DSL port connection information. The DSL tab displays information regarding the DSL data connection.



DSL

Line State: Displays the current status of the data link connection to your ISP.

Modulation: Displays the current DSL standard in use.

Annex Mode: Displays the current Annex mode in use.

DSL (Sync) Uptime: Displays time duration of the DSL connection.

SNR Margin: Displays the Signal-to-Noise Ratio margin, which measures the connection quality by measuring the ratio of the signal power and the noise power.

Line Attenuation: Displays the current signal attenuation, which measures how much the signal's strength has been degraded.

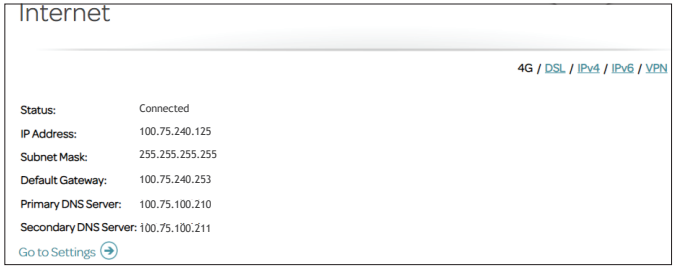
Data Rate: Displays the currently negotiated connection speed.

Output Power: Displays the output power of the DSL modem.

FEC, CRC: These error correction counts are used for diagnostic purposes. If you are having trouble with the connection to your ISP, these values may provide useful information for technicians.

4G

The onboard USB port supports 3G/4G mobile broadband adapters as a backup of your current DSL connection.



4G

Status: Displays the current status of the data link to your 4G service provider.

IP Address: Displays the IP address of the adapter's interface.

Subnet Mask: Displays the subnet mask of the IP address.

Default Gateway: Displays the current default gateway for the interface.

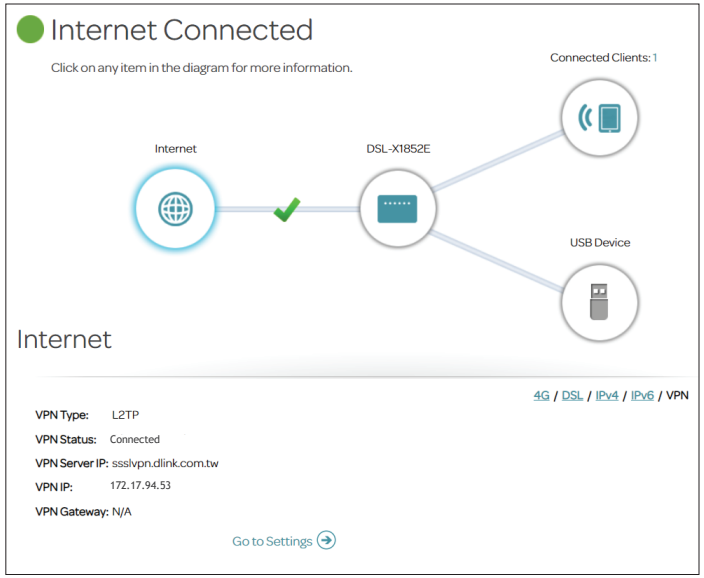
Primary DNS Server: Displays the current primary DNS server.

Secondary DNS Server: Displays the current secondary DNS server.

Click **Go to Settings** below to go to the USB Modem configuration page.

VPN

The VPN status displays the tunnel status of the VPN connection.



VPN

VPN Type: Displays the protocol used for VPN.

VPN Status: Displays the connection status.

VPN Server IP: Displays the IP address of the VPN server.

VPN IP: Displays the IP address used for VPN connection.

VPN Gateway: Displays the IP address used for VPN gateway.

Click **Go to Settings** below to go to the VPN configuration page.

DSL-X1852E

Click on the **DSL-X1852E** icon to view details about the router and its wireless settings.

Here you can see the router's current wireless networks settings such as SSID and password, as well as the local area network MAC and IPv4 addresses.

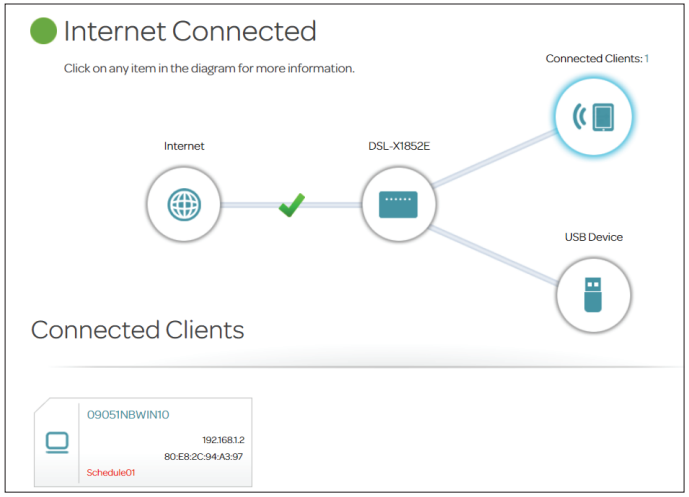
To reconfigure the network settings, click **Go to Settings** at the lower right. You can also click **Settings > Network** at the top to access the configuration page. Refer to **Network** on page **54** for more information.

To reconfigure the wireless settings, click **Go to Settings** at the lower right. You can also click **Settings > Wireless** at the top to access the configuration page. Refer to **Wireless** on page **47** for more information.

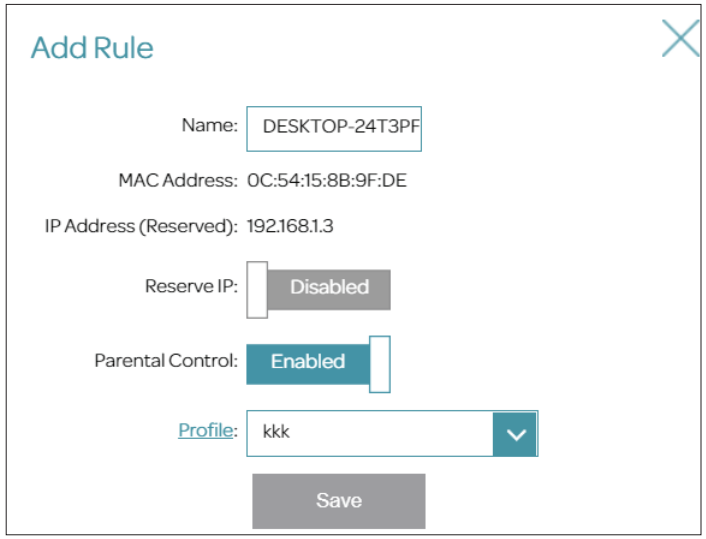
Connected Clients

Click on the **Connected Clients** icon to view details about the clients currently connected to the router and their IP and MAC addresses.

To edit a client's settings, click on the client you want to edit.



Edit Rule



Name: Enter a custom name for this client.

MAC Address: Displays the MAC address of the device.

IP Address: Displays the IP address for this client if **Reserve IP** is enabled. You can reserve this IP address for this client by enabling the below Reserve IP.

Reserve IP: Enable to reserve this IP address for this client. Go to **Settings > Network > Reserve IP** to obtain more information on DHCP reservation.

Parental Control: Enable Parental Control and select a profile to control the client's Internet access. Make sure that this device is also on the device list of the selected profile. Go to **Features > Parental Control** for more information on Parental Control.

Click **Save** when you are done.

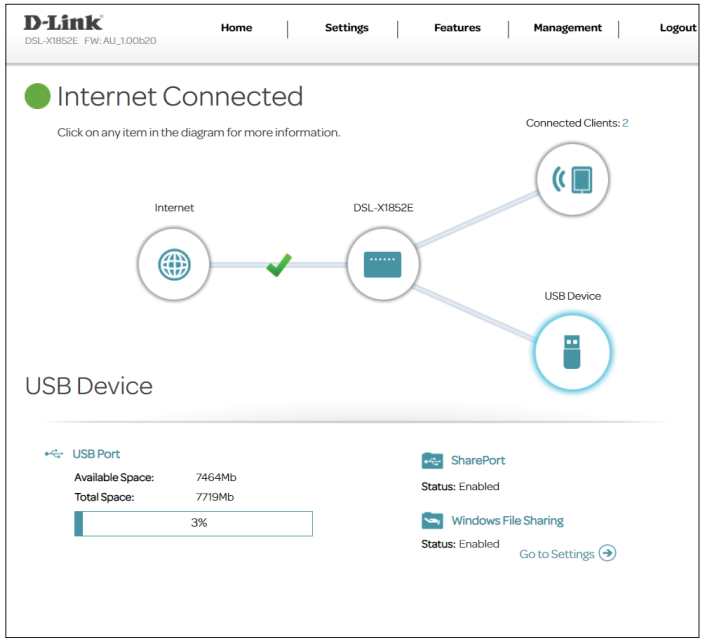
USB Device

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

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

To configure your USB settings, click **Go to Settings** or click **Settings > USB** to obtain more information on USB configuration.

For information on how to access your USB drive from a Windows-based PC refer to **Connect and Share a USB Storage Device** on page **93**.

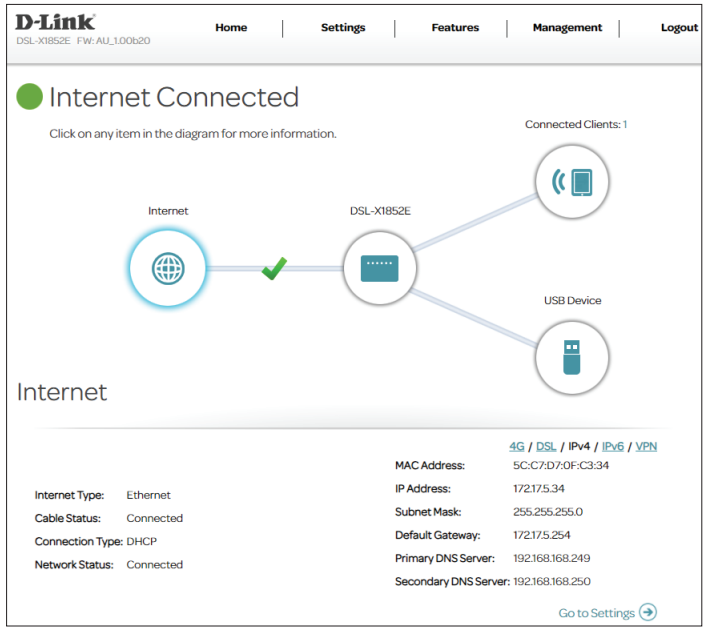


Settings

Wizard

To access the Setup Wizard page, go to **Settings > Wizard**. This is the same wizard that appears when you start the router for the first time. Refer to **Setup Wizard** on page **15** for more information.

Internet



The following pages will describe how to connect your DSL-X1852E to the Internet. To access this page, go to **Settings > Internet** at the top of the page. The DSL-X1852E supports multiple WAN connection types and WAN failover. We recommend that you set up Internet WAN connections one at a time, **save** the configuration, and confirm the connection works before returning to this section to add additional WAN connections.

Different WAN access types are described in the following sections.

WAN CONNECTION TYPE

Configure your WAN Connection: Select the WAN interface to configure. The options are **XDSL (**for **ADSL** or **VDSL)** or **Ethernet**.

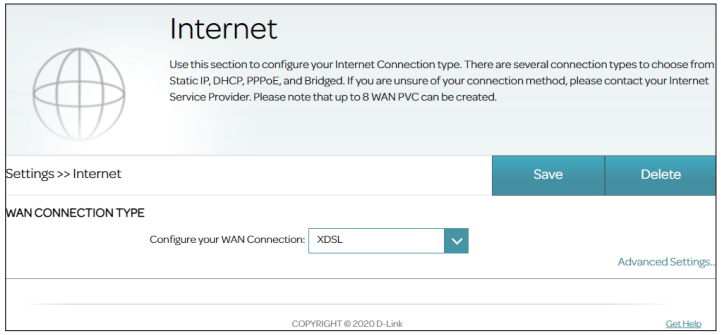
Select a WAN Connection and refer to its configuration page for setup information.

For ADSL, refer to **Internet - ADSL** on page **31**.

For VDSL, refer to **Internet - VDSL** on page **33**.

For Ethernet, refer to **Internet - Ethernet** on page **34.**

Internet - ADSL



ADSL is one of the first home broadband technologies introduced. ADSL uses the DSL port on your DSL-X1852E to connect to the Internet. In order for your DSL-X1852E to use ADSL, you must configure the **WAN Connection Type** and related WAN settings.

WAN Connection Type

Configure your WAN connection: Select **ADSL** to configure ADSL connection settings.

ADSL VC Settings

Interface: Select a configuration interface for this virtual circuit. If no service has previously been added, or you wish to add a new one, select **Add**.

DSL Type: Select DSL technology for this Virtual Circuit: ADSL or VDSL. Select ADSL in this case.

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

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

Service Category: Select the service category which defines the transmission parameters and performance: **UBR**, **CBR**, **NRT-VBR**, or **RT-VBR**.

Internet - ADSL (continued)

If you selected **CBR**, **NRT-VBR**, or **RT-VBR**, configure the following additional options:

Peak Cell Rate (PCR): Enter the Peak Cell Rate in cells per second (0-5500).

If you selected **NRT-VBR** or **RT-VBR**, the additional following options are available:

Sustainable Cell Rate (SCR): Enter the Sustainable Cell Rate in cells per second (0~5500).

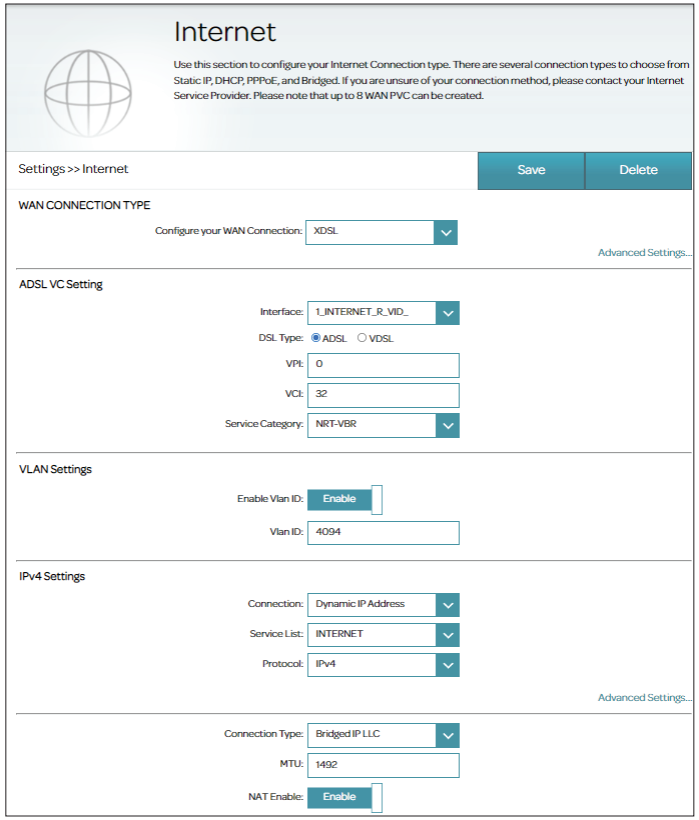
Maximum Burst Size (MBS): Enter the Maximum Burst Size in MB per second (0~5500).

VLAN Settings

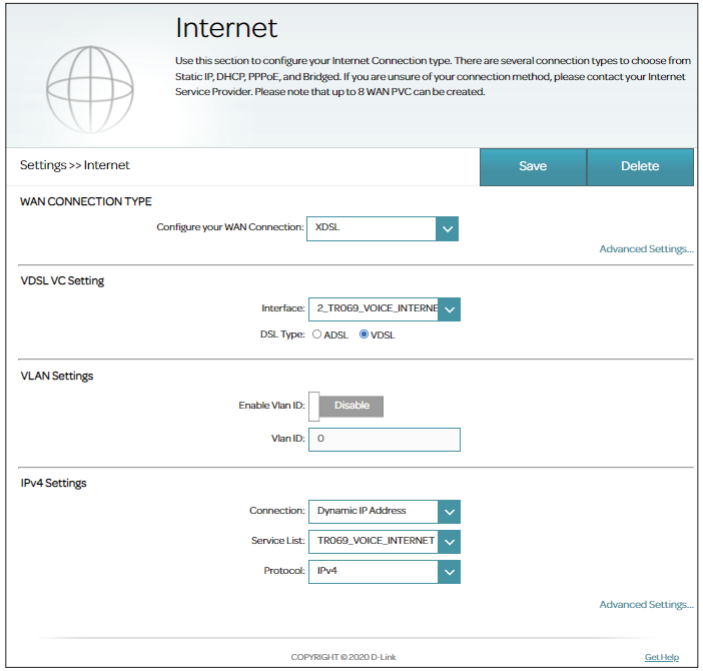
Enable Vlan ID Enable or disable VLAN settings.

Vlan ID Enter the VLAN ID. Enter a value from 1 - 4094.

To set your IPv4/IPv6 connection parameters of WAN connection, refer to **Connection Types** on page **35.**



Internet - VDSL



VDSL is one of the latest and fastest home broadband technologies. VDSL uses the DSL port on your DSL-X1852E to connect to the Internet. In order for your DSL-X1852E to use VDSL, you must configure the **WAN Connection Type** and related WAN settings.

Configure your WAN connection: Select **XDSL** to configure VDSL connection settings.

If you click on **Advanced Settings**, the following **WAN Settings** are available:

VDSL VC Settings

Interface: Select a configuration interface for this virtual circuit. If no service has previously been added, or you wish to add a new one, select **Add**.

DSL Type: Select DSL technology for this Virtual Circuit: ADSL or VDSL. Select VDSL in this case.

VLAN Settings

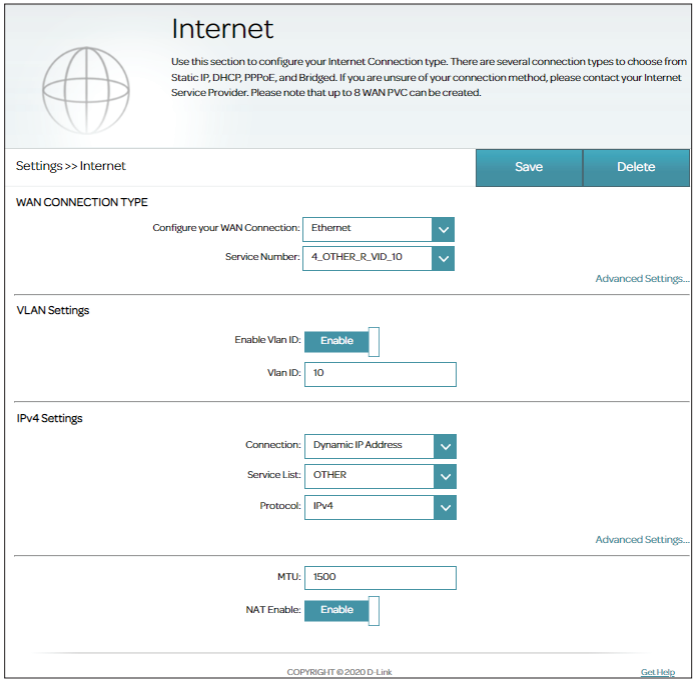
Enable VLAN ID: Enable or disable VLAN settings.

VLAN ID: Enter the VLAN ID. Enter a value from 1 - 4094.

To set your IPv4/IPv6 connection parameters of WAN connection, refer to **Connection Types** on page **35.**

Internet - Ethernet

Your DSL-X1852E is equipped with a multi-purpose Gigabit Ethernet LAN/WAN port which can be used to connect to the Internet. This port can also be used to connect to other Ethernet based networks. In order for your DSL-X1852E to use Ethernet, you must configure the WAN Connection Type and related WAN settings.



Configure your WAN connection: Select **Ethernet** to configure Ethernet connection settings.

Service Number: Select a service number from the drop-down menu, or to create a new service number for your Ethernet connection, click **Add**. The service number corresponds to the configured interface profile from your Ethernet **WAN Connection Type**.

VLAN Settings

Enable Vlan ID: Enable or disable VLAN settings.

Vlan ID: Enter the VLAN ID. Enter a value from 1 - 4094.

IPv4 Settings

Connection: Select the connection method for your Internet and refer to the respective configuration page for setup information.

For Dynamic IP (DHCP) Address, refer to **Connection Type: Dynamic IP (DHCP)** on page **35**.

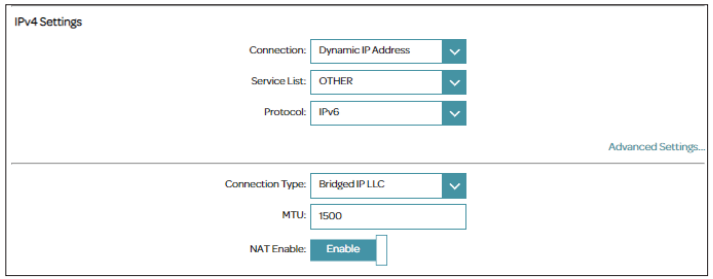
For Static IP Address, refer to **Connection Type: Static IP** on page **37**.

For PPPoE, refer to **Connection Type: PPPoE** on page **39.**

For Bridge Mode, refer to **Connection Type: Bridge Mode** on page **41.**

Connection Types

Connection Type: Dynamic IP (DHCP)



Select **Dynamic IP Address (DHCP)** to obtain an IP address automatically from your ISP. Select this option if your ISP does not provide you with a specific IP address.

IPv4 Settings

Connection: Select **Dynamic IP Address (DHCP)**.

Service List: Select a service type from the list. Choose from **INTERNET**, **TR069_INTERNET**, **VOICE, VOICE_INTERNET, TR069_VOICE, TR069_VOICE_INTERNET, TR069**, or **OTHER**. This information should be provided by your ISP. If you are configuring your connection manually and your ISP has not specified this setting, **INTERNET** is recommended.

Protocol: Select **IPv4, IPv6** or **IPv4/IPv6** for both IPv4 and IPv6 addressing mechanism. If you choose IPv6, refer to the below IPv6 Settings.

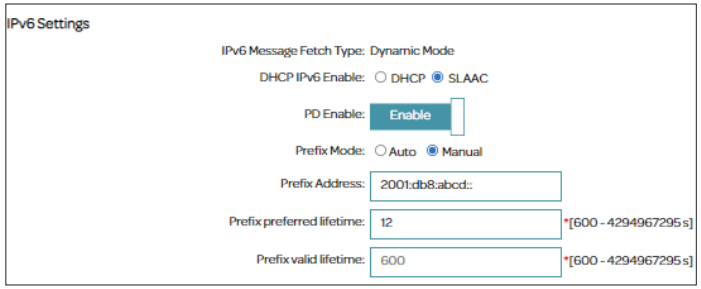
Advanced Settings

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

NAT Enable: Network address translation (NAT) translates private IP addresses to public IP addresses prior to allowing private IP networks to connect to the public network. This option is not available for related voice service types such as VOICE, VOICE_INTERNET, and TR069_VOICE and TR069.

Connection Type: Select **Bridged IP LLC** or **Bridged IP VC-Mux** as the encapsulation method. This is only available for ADSL.

IPv6 Settings



IPv6 Message Fetch Type: This displays the IP assignment method.

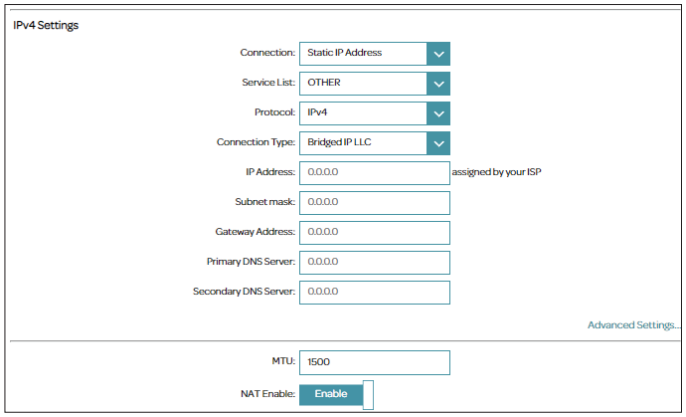
DHCP IPv6 Enable: Select the IPv6 auto-configuration type: **SLAAC** or **DHCP**. If DHCP is selected, enter the default gateway or leave it blank for automatic configuration.

PD Enable Enable or disable prefix delegation. Also select the prefix mode: **Auto** or **Manual**. For **Manual**, please enter the prefix address, for example 2001:b011:2000:0012::. Enter the prefix information option by specifying preferred lifetime and valid lifetime for the prefix (600-4294967295 seconds).

Click **Save** when you are done.

Connection Type: Static IP

Select **Static IP Address** if your ISP provides you with a specific IP address.



IPv4 Settings

Connection: Select **Static IP Address**.

Service List: Select a service type from the list. Choose from **INTERNET**, **TR069_INTERNET**, **VOICE, VOICE_INTERNET, TR069_VOICE, TR069_VOICE_INTERNET, TR069**, or **OTHER**. This information should be provided by your ISP. If you are configuring your connection manually and your ISP has not specified this setting, **INTERNET** is recommended.

Protocol Select **IPv4, IPv6** or **IPv4/IPv6** for both IPv4 and IPv6 addressing mechanism. If you choose IPv6, refer to the below IPv6 Settings.

Connection Type: Select **Bridged IP LLC** or **Bridged IP VC-Mux** as the encapsulation method. This is only available for ADSL.

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

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

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

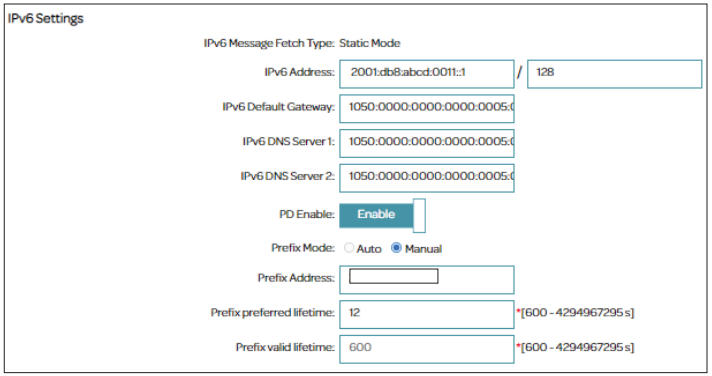
Primary DNS Server Enter the primary DNS server IP address assigned by your ISP. This address is usually obtained automatically from your ISP.

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

Advanced Settings

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

NAT Enable: Network address translation (NAT) translates private IP addresses to public IP addresses prior to allowing private IP networks to connect to the public network. This option is not available for related voice service types such as VOICE, VOICE_INTERNET, and TR069_VOICE and TR069.



IPv6 Settings

IPv6 Message Fetch Type: This displays the IP assignment method.

IPv6 Address Enter an IPv6 address in this format: x:x:x:x:x:x:x:x/y (where each x represents a hexadecimal digit, y is an integer from 1 to 128 as the prefix length), for example, 2001:b011:2000:0012::1/64.

IPv6 Default Gateway: Enter the IP address of the default gateway.

IPv6 DNS Server 1: Enter the DNS server address.

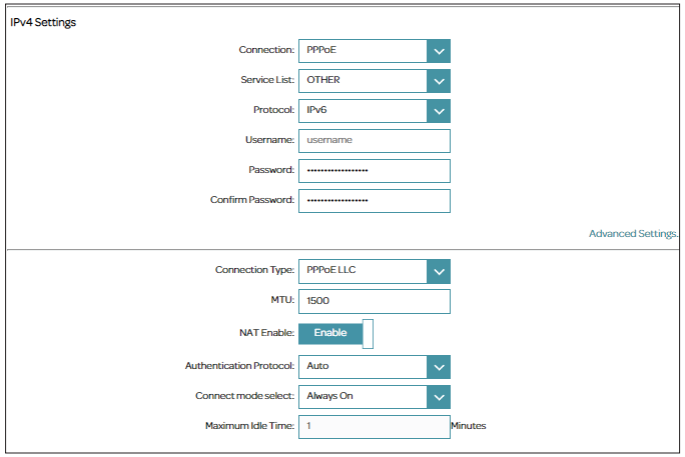
IPv6 DNS Server 2: Enter the secondary DNS server address as a backup.

PD Enable Enable or disable prefix delegation. Also select the prefix mode: **Auto** or **Manual**. For **Manual**, please enter the prefix address, for example, 2001:b011:2000:0012::. The prefix is used to determine the subnet prefix of an IPv6 address. Then enter the prefix information option by specifying preferred lifetime and valid lifetime for the prefix (600-4294967295 seconds).

Click **Save** when you are done.

Connection Type: PPPoE

Select **PPPoE** if your ISP provides and requires you to enter a PPPoE username and password in order to connect to the Internet.



WAN Settings

Connection: Select **PPPoE**.

Service List: Select a service type from the list. Choose from **INTERNET**, **TR069_INTERNET**, **VOICE**, **VOICE_INTERNET, TR069_VOICE, TR069_VOICE_INTERNET** or **TR069**, or **OTHER**. This information should be provided by your ISP. If you are configuring your connection manually and your ISP has not specified this setting, **INTERNET** is recommended.

Protocol Select **IPv4, IPv6** or **IPv4/IPv6** for both IPv4 and IPv6 addressing mechanism. If you choose IPv6, refer to the below IPv6 Settings.

Username: Enter the username provided by your ISP.

Password/Confirm Password: Enter the password provided by your ISP. Then enter it again to confirm your entry.

Connection Type: Select **PPPoE LLC** or **PPPoE VC-Mux**.

Advanced Settings

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

NAT Enable: Network address translation (NAT) translates private IP addresses to public IP addresses before allowing private IP networks to connect to the public network. This option is not available for related voice service types such as VOICE, VOICE_INTERNET, and TR069_VOICE and TR069.

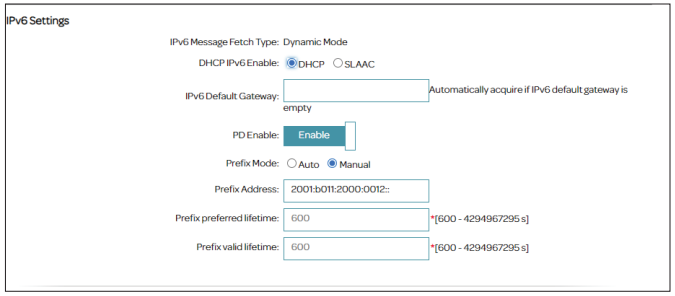
Authentication Protocol: Select the authentication protocol your ISP uses. The options are **Auto**, **PAP**, **MS-CHAP** or **CHAP.**

Connect Mode Select: Set the connection to be **Always-on** or **Connect-On-Demand**.

If you selected **Connect-On-Demand**, the following option is available:

Maximum Idle Time: Enter the amount of time in minutes the router will maintain the Internet connection before disconnecting it if there is no activity.

IPv6 Settings



IPv6 Message Fetch Type: This displays the IP assignment method.

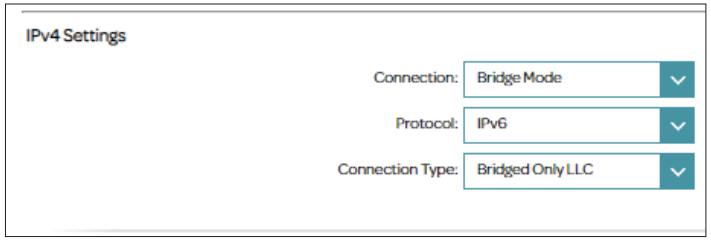
DHCP IPv6 Enable: Select the IPv6 auto-configuration type: **StateLess Address AutoConfiguration (SLAAC)** or **Dynamic Host Configuration Protocol (DHCP)**. If DHCP is selected, enter the default gateway or leave it blank for automatic configuration.

IPv6 Default Gateway: Enter the IP address of the default gateway if DHCP is selected or leave it blank for automatic configuration.

PD Enable Enable or disable prefix delegation. Also select the prefix mode: **Auto** or **Manual**. For **Manual**, please enter the prefix address, for example, 2001:b011:2000:0012::. Enter the prefix information option by specifying preferred lifetime and valid lifetime for the prefix (600-4294967295 seconds).

Click **Save** when you are done.

Connection Type: Bridge Mode



Select **Bridge Mode** to use the DSL-X1852E as a network bridge to extend an existing network.

IPv4 Settings

Connection: Select **Bridge Mode**.

Protocol Select **IPv4, IPv6** or **IPv4/IPv6** for both IPv4 and IPv6 addressing mechanism.

Connection Type: Select **Bridged Only LLC** or **Bridged Only VC-Mux** as the encapsulation method. This is only available for ADSL.

Click **Save** when you are done. Or click **Delete** to delete the configuration profile for the interface.

VPN

A Virtual Private Network (VPN) is used to establish a virtual, encrypted connection over an existing network utilizing tunneling protocol such as PPTP or L2TP. To access this page, go to **Settings > VPN**.

Configure the following to set up a VPN connection to a VPN server:

VPN Settings

VPN: Select **Point-to-Point Tunneling Protocol (PPTP)** or **Layer 2 Tunneling Protocol (L2TP)**.

Server Address: Enter the PPTP or L2TP server address.

Username: Enter the username for connection authentication.

Password: Enter the password for connection authentication.

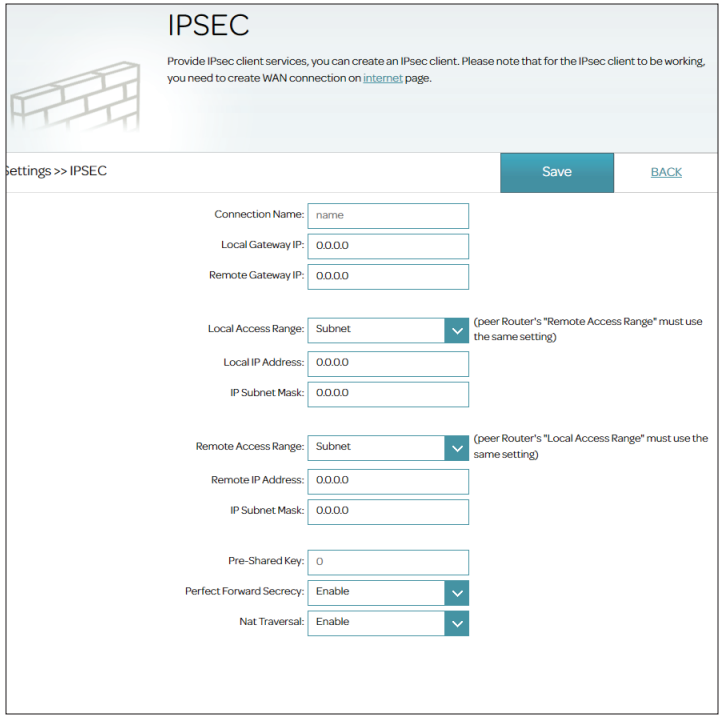
VPN is Used: Select **to the Internet** if the VPN is created for connecting to the Internet for all traffic through the WAN interface or **to the virtual private network** if the VPN is created to facilitate encapsulated and encrypted connections to another network across an existing Internet connection.

Click **Save** when you are done.

IPSec

IPSec facilitates VPN communications with security capabilities. This page allows you to create an IPSec tunnel between two sites and set parameters for authentication method and encryption algorithm.

Click **Add Rule** and configure the following to set up an IPSec profile for VPN connections:



IPSec Settings

Connection Name: Name this IPSec connection.

Local Gateway IP: Enter the IP address of the local gateway for this tunnel.

Remote Gateway IP: Enter the IP address of the remote gateway for this tunnel.

Local Access Range: Select either **Single IP** or **Subnet**. Note that the local and remote access range should use different subnetworks.

Local IP Address: Enter the IP address of the local device that can use this tunnel.

IP Subnet Mask: Enter the subnet mask if you choose **Subnet** for Local Access Range.

Remote Access Range: Select either **Single IP** or **Subnet**. Note that the local and remote access range should use different subnetworks.

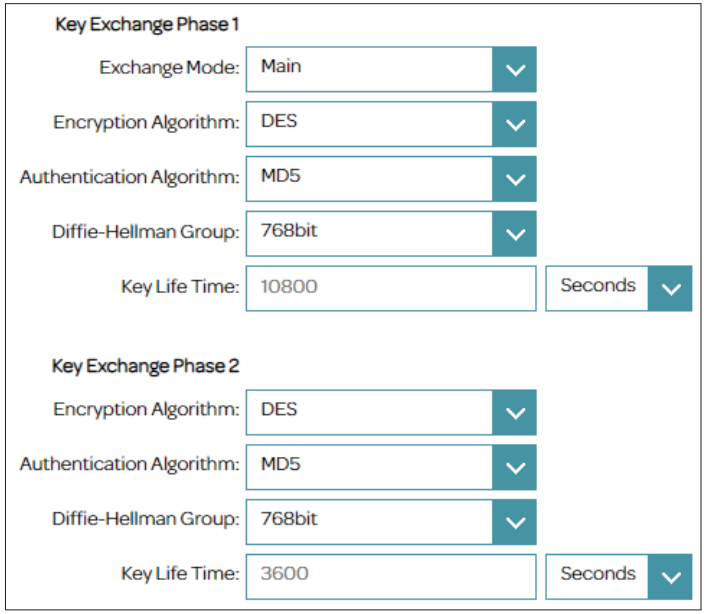
Remote IP Address: Enter the IP address of the remote device that can use this tunnel.

IP Subnet Mask: Enter the subnet mask if you choose **Subnet** for Remote Access Range.

Pre-Shared Key: Enter a pre-shared key to authenticate a remote peer. Up to 16 characters including symbols can be entered. Both local and remote device of the VPN tunnel must use the same pre-shared Key.

Perfect Forward Secrecy: Enable or disable Perfect Forward Secrecy. It uses public key cryptography to improve the security of IPSec data communication.

NAT Traversal: Enable or disable NAT traversal for the negotiation of an IPSec VPN connection. It allows IPsec VPN traffic to pass if NAT is used on the gateways.



Key Exchange Phase 1

Exchange Mode: Select **Main**, **Aggressive** or **Base**. In general, Aggressive mode is faster than the Main mode but offers less protection against authentication security. Unlike the Aggressive and Main Mode, the Base Mode can transmit the key exchange information and authentication data together .

Encryption Algorithm: Select encryption method as the algorithm for encrypting data packets. The options are **DES, 3DES, AES-128, AES-192** or **AES-256**.

Authentication Algorithm: The authentication algorithm validates data packets. Select **MD5, SHA1,** or **SHA256**. Both local and remote device of the VPN tunnel must use the same authentication algorithm. Both MD5 and SHA are one-way hashing algorithm but produce different number of digest bit.

Diffie-Hellman Group: The Diffie-Hellman key exchange protocol offers different prime key lengths. Select **768, 1024, 1536, 2048, 3072,** or **4096 bit**.

Key Life Time: Enter the amount of time that a key is active in Phase 1. Then select the unit: **Seconds, Minutes** or **Hours**.

Key Exchange Phase 2

Encryption Algorithm: Select encryption method as the algorithm for encrypting data packets. The options are **DES, 3DES, AES-128, AES-192** or **AES-256**.

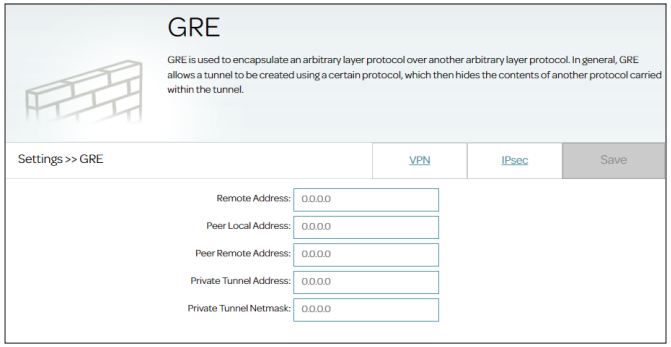
Authentication Algorithm: The authentication algorithm validates data packets. Select **MD5, SHA1,** or **SHA256**. Both local and remote device of the VPN tunnel must use the same authentication algorithm. Both MD5 and SHA1 are one-way hashing algorithm but they produce different length of digest bits.

Diffie-Hellman Group: The Diffie-Hellman key exchange protocol offers different prime key lengths. Select **768, 1024, 1536, 2048, 3072,** or **4096 bit**.

Key Life Time: Enter the amount of time that a key is active in Phase 2. Then select the unit: **Seconds, Minutes** or **Hours**.

Click **Save** when you are done. You can create up to 7 IPSec profiles.

GRE



Generic Routing Encapsulation (GRE) is a tunneling mechanism that creates virtual links for the two endpoints of the tunnel.

Configure the following to set up a GRE tunnel for VPN connections:

IPSec Settings

Remote Address: Enter the WAN IP address of the remote gateway.

Peer Local Address: Enter the IP address of the local tunnel network interface.

Peer Remote Address: Enter the IP address of the remote tunnel network interface.

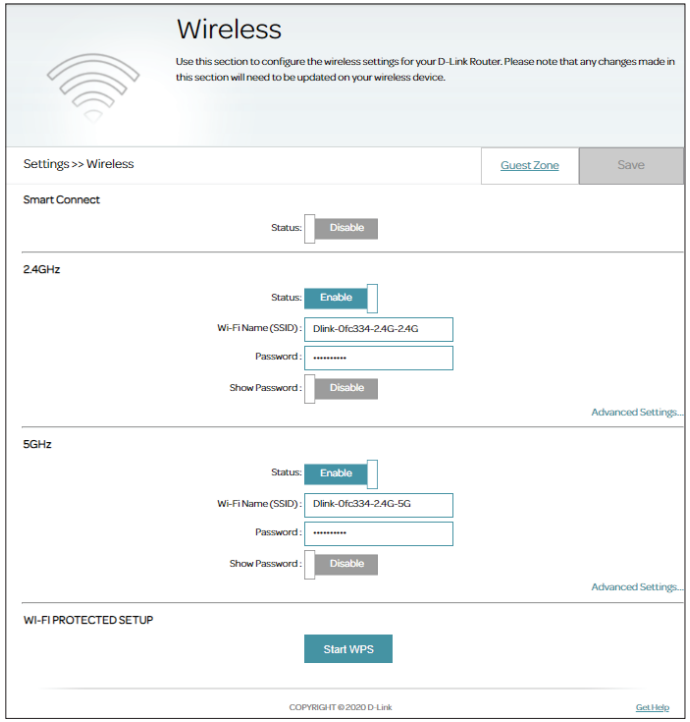
Private Tunnel Address: Enter the private IP address of the remote tunnel.

Private Tunnel Netmask: Enter the subnet mask of the private IP address of the remote tunnel.

Click **Save** when you are done.

Wireless

You can configure your wireless LAN (WLAN) on this page. To access this page, go to **Settings > Wireless**.



Smart Connect

The Smart Connect feature presents a single wireless network. When connecting clients to an extended network, they will be automatically added to the best band, either 2.4 GHz or 5 GHz. You can choose to disable the Smart Connect feature and individually configure 2.4 GHz and 5 GHz networks as below:

2.4 GHz

Status: Enable or disable the 2.4 GHz wireless network.

Wi-Fi Name (SSID): Create a name for your wireless network.

Password: Create a password to use for wireless security. The password must contain 8 to 63 alphanumeric characters including a mix of uppercase and lowercase letters, numbers and special characters with the exception of the following characters: '-;`=%+&|><"/ .

Show Password: Enable or disable display of the above password.

5 GHz

Status: Enable or disable the 5 GHz wireless network.

Wi-Fi Name (SSID): Create a name for your wireless network.

Password: Create a password to use for wireless security. The password must contain 8 to 63 alphanumeric characters including a mix of uppercase and lowercase letters, numbers and special characters with the exception of the following characters: '-;`=%+&|><"/ .

Show Password: Enable or disable display of the above password.

Wi-Fi Protected Setup

Start WPS: This triggers the WPS pairing process. The WPS LED on the front panel will start to flash. Refer to **WPS Button** on page **100** for more information about WPS. Note that WPS will be disabled for security methods other than WPA2.

Click **Save** when you are done. The following pages describe the **Advanced Settings** configuration options in detail.

Advanced Settings

Clicking **Advanced Settings** allows you to manually configure security, wireless radio operation, and schedule settings.

Security: Choose **None**, **WEP (WEP-128Bit, WEP-64Bit), WPA (WPA3, WPA2, WPA** or **WPA3/WPA2, WPA2/WPA)**. Select **None** for unsecured network if it is what you intend.

WPA

Wi-Fi Protected Access (WPA) offers stronger encryption capability than WEP. Using WPA3 with AES encryption is recommended. WPA3 provides the latest and most robust encryption among these security methods.

Security: **WPA3, WPA2, WPA** or mix of **WPA3/WPA2, WPA2/WPA**.

WPA Type

802.1x uses a RADIUS (Remote Authentication Dial-In User Service) server for user authentication. If you selected 802.1x, the following options are available:

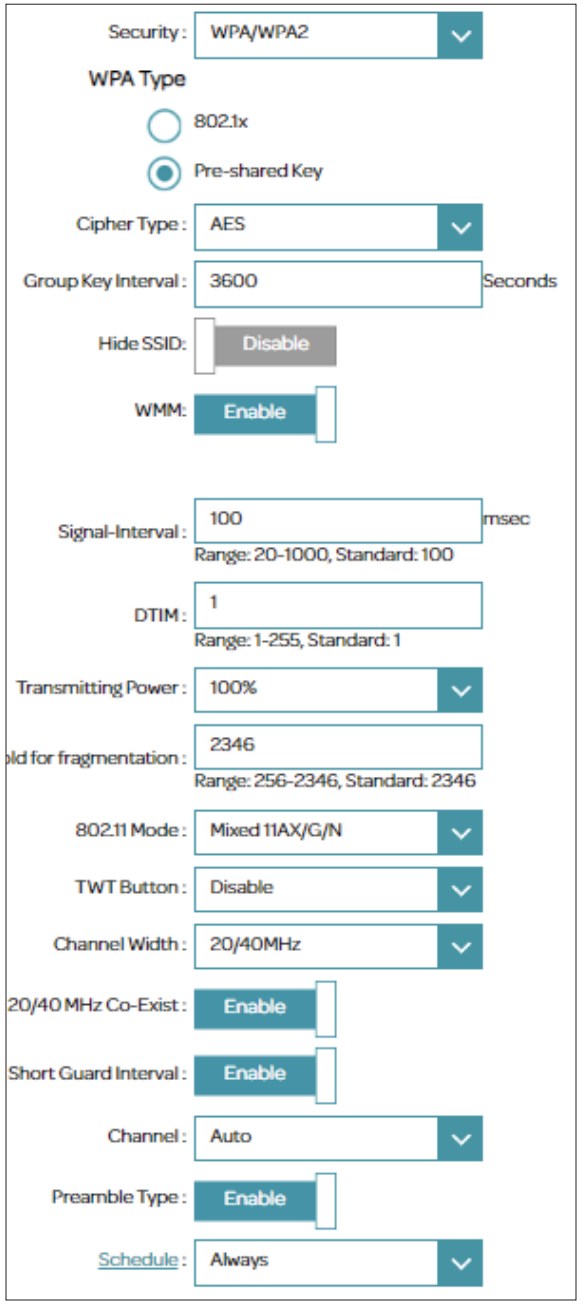
Server IP Address: Enter the IP address of the RADIUS Server.

Port: Enter the port used by the RADIUS Server.

Secret: Enter the secret used by the RADIUS Server.

Cipher Type: Select either **AES, TKIP** or **Both** (**AES/TKIP**). The options vary depending on the WPA type selected. **AES** is recommended if other types are presented.

Group Key Interval: Enter the Group Key Interval as the timing for rekeying the group temporal key. The default is **3600** seconds.



Advanced Settings (continued)

If you selected **Pre-shared key**, an alphanumeric passphrase will be required, enter it in the password field above. The following options are also available:

Cipher Type: Select either **AES, TKIP** or **Both** (**AES/TKIP**). The options vary depending on the WPA type selected. **AES** is recommended if other types are presented.

Group Key Interval: Enter the Group Key Interval as the timing for rekeying the group temporal key. The default is **3600** seconds.

WEP

Wireless Equivalent Privacy (WEP) offer only basic encryption capability and is less secure than WPA. Thus, WPA is the preferred method.

Security: **WEP-64Bit:** Enter 10 hexadecimal characters (0-9, a-f or A-F).
WEP-128Bit: Enter 26 hexadecimal characters (0-9, a-f or A-F).

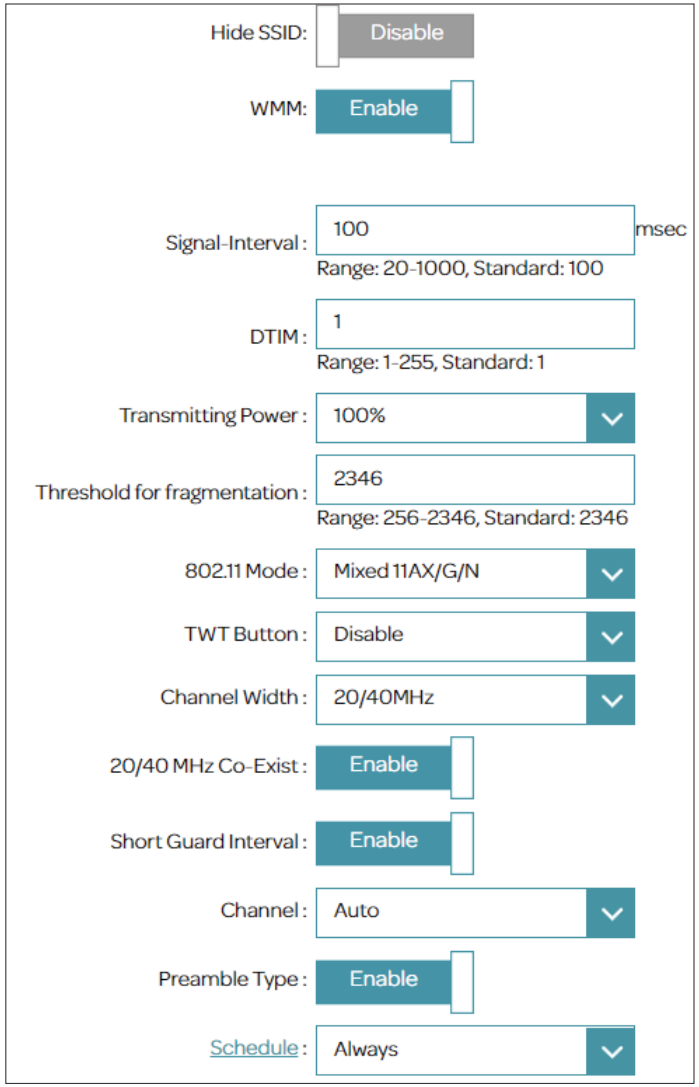
Authentication Type

Select either **Shared** or **Open**. These two types differ in the authentication process before association with an access point.

Click **Save** when you are done. The following pages describe more configuration options in **Advanced Settings** in detail.

Advanced Settings (continued)

2.4 GHz / 5 GHz Advanced Settings



Hide SSID: The default setting is **Disabled**. Select **Enabled** if you do not want to broadcast the Wi-Fi name or SSID of your wireless network.

WMM: Enable or disable Wi-Fi Multimedia Quality of Service (WMM QoS) for your wireless network. This can help to improve the quality of video and voice applications for your wireless clients.

Signal-Interval: Set the rate at which your wireless network is advertised. The range is 20-1000 and default is **100** milliseconds.

DTIM: Specify the Delivery Traffic Information Map (DTIM) message interval. Higher DTIM values can help conserve power at the cost of slight latency. The range is 1-255 and default is 1.

Transmitting Power: Select the desired wireless transmission power. The available options are **100%**, **75%**, **50%, 25%, 15%,** or **9%**. The default is **100%**.

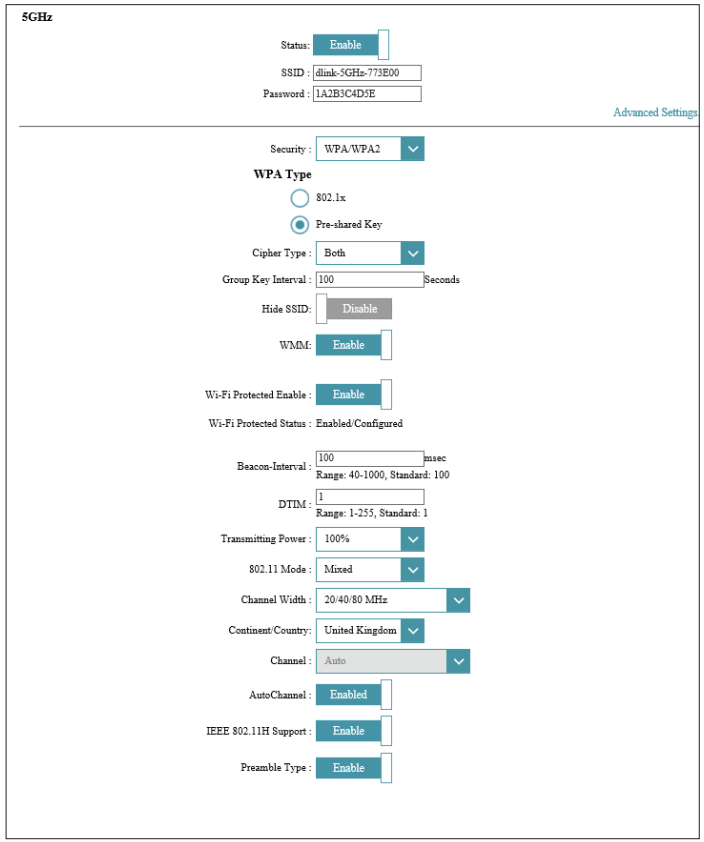
Threshold for fragmentation (2.4 GHz only): The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte threshold will be fragmented before transmission. The range is **256-2346** and **2346** is the default setting.

2.4 GHz 802.11 Mode: Select the desired wireless networking standard(s) to use. The available options are **11B only, 11G only, Mixed 11G/B, 11N only, Mixed 11G/N, Mixed 11N/G/B,** and **Mixed 11AX/G/N.**

TWT Button: Target Wake Time helps conserve battery life by negotiating sleep and wake-up time between the router and the wireless device. The options are **Disable, Enable,** and **Mandatory**.

2.4 GHz Channel Width: Channel Width is available if you selected **11N, Mixed 11G/N, Mixed 11N/G/B** or **Mixed 11AX/G/N** for **802.11 Mode**. Select **20/40** if you are using 802.11g/b devices or select **20 MHz** if you want to disable 40 MHz bandwidth communication. The recommended setting is **20/40**.

Advanced Settings (continued)



20/40 MHz Co-Exist (2.4GHz) : Enable or disable the existence of both 20 MHz and 40 MHz channel width. Keep it enabled to achieve the maximum operability of wireless products using different standards in your environment. However, it might prevent your 802.11ax or 802.11n devices from reaching the maximum performance.

5 GHz 802.11 Mode: Select the desired wireless networking standard(s) to use. The available options are **11A Only**, **Mixed 11A/N**, **Mixed 11AC/N/A, Mixed11AC/N, Mixed11AC/N/AX**.

5 GHz Channel Width: Channel Width is available if you selected **Mixed 11A/N, Mixed 11AC/N/A, Mixed 11AC/N,** and **Mixed 11AC/N/AX.** Select the desired channel width. The available options are **20 MHz**, **20/40 MHz**, or **20/40/80 MHz**. Using wider channel width can increase bandwidth, so if you have 802.11ax and 802.11ac devices, choose **20/40/80 MHz**. However, in a congested environment, the highest channel width is usually not recommended since it leads to higher probability of clashing channels. Depending on the selected 5 GHz 802.11 Mode, some options may be unavailable.

Short Guard Interval : This option is only available for 11N wireless standard. This increases data rate by lowering the guard interval to 400 ns.

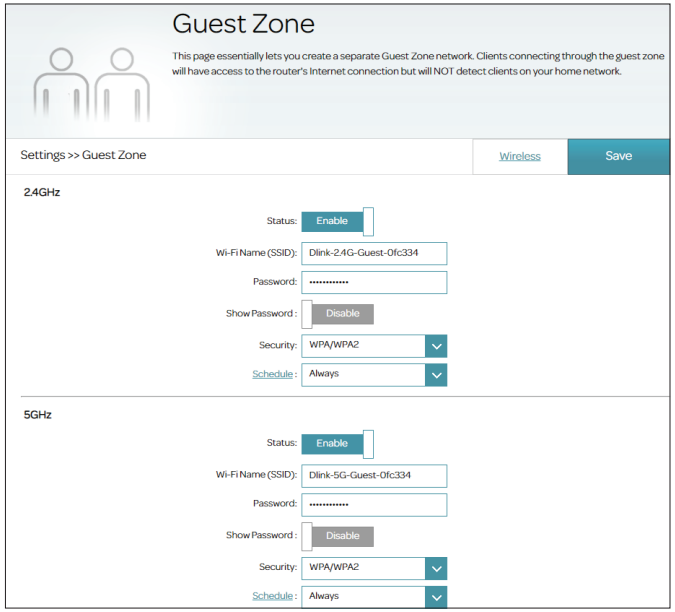
Channel: Select the desired channel for your wireless network to use. The default is **Auto** (recommended).

Preamble Type: This defines the length of the CRC block for communication between the wireless router and the devices. Ensure that all your wireless devices use the same type. Select **Enabled** to set it to short and **Disabled** to set it to long.

Schedule : Use the drop-down menu to select the time schedule for which the wireless network will be available. The schedule may be set to **Always**, or you can create your own schedules in the Schedule section. Refer to **Time & Schedule** on page **83** for more information.

Click **Save** when you are done.

Guest Zone



The Guest Access feature creates a separate network from your local network. It allows guest devices to access the Internet but not the servers and resources in your local network. This prevents guest users exposure of your local network. You may configure different zones for the 2.4 GHz and 5 GHz wireless bands.

Status Enable or disable the respective wireless band. The status is disabled by default.

Wi-Fi Name (SSID) Create a name for your wireless network.

Password Create a password to use for wireless security. The password must contain 8 to 63 alphanumeric characters including a mix of uppercase and lowercase letters, numbers and special characters with the exception of the following characters: '-;`=%+&|><"/ .

Show Password Enable or disable the display of the password.

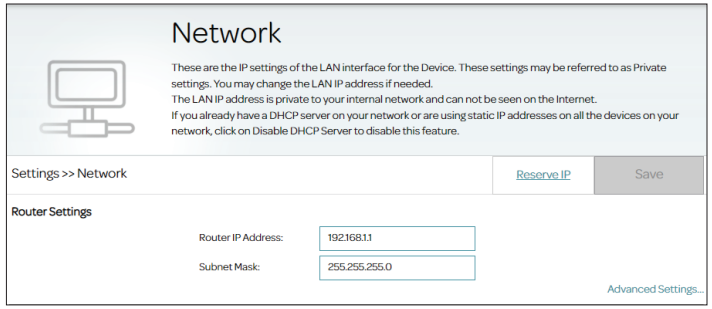
Security Choose **None**, **WEP (WEP-128Bit, WEP-64Bit), WPA (WPA3, WPA2, WPA** or **WPA3/WPA2, WPA2/WPA)**. Select **None** for unsecured network if it is what you intend. Refer to the above sections (**WEP** on page **50** and **WPA** on page **49)** for explanation of these security methods.

Schedule Use the drop-down menu to select the time schedule for which the wireless network will be available. The schedule may be set to **Always**, or you can create your own schedules in the Schedule section. Refer to **Time & Schedule** on page **83** for more information

Click **Save** when you are done.

Network

This section allows you to change the local network settings of the router and to configure the DHCP settings. Go to **Settings > Network** to access this page.



Router Settings

Router IP Address: Enter the IP address of the router to be identified in your local network. The default IP address is **192.168.1.1**.

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 this interface. The default subnet mask is **255.255.255.0**.

Click **Save** when you are done or click **Advanced Settings**.

Advanced Settings

DHCP Server Settings

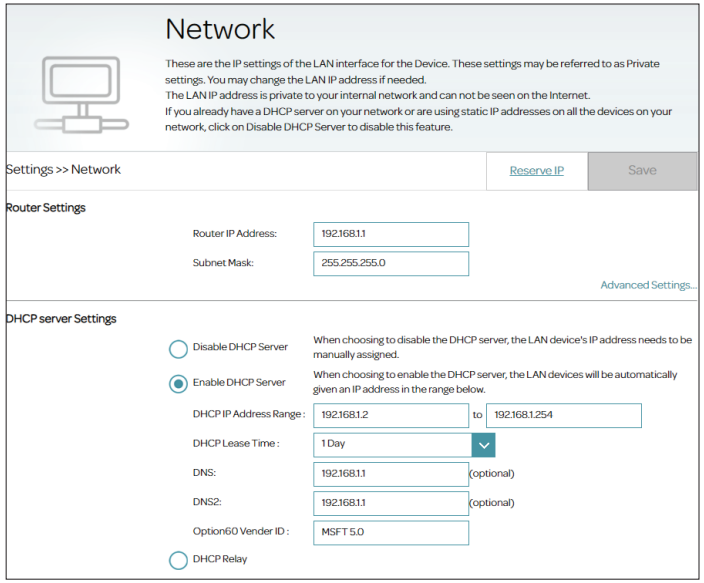
Disable DHCP Server: Select this option to disable the DHCP server. No further configuration is available. If you choose to disable the router's DHCP server, there should be other DHCP server on your network or you must configure the LAN devices' IP addresses manually.

Enable DHCP Server: Select this option to enable the DHCP server.

Enter the following settings to configure your DHCP server:

DHCP IP Address Range: Specify the start and end IP addresses for the range of addresses to be assigned by your router.

Network - Advanced Settings



DHCP Lease Time: Select the DHCP lease time from the drop down menu: **1 Hour, 2 Hours, 3 Hours, 1 Day, 2 Days, 3 Days,** or **1 Week**. The default is **1 Day**.

DNS: The Domain Name System (DNS) translates domain or website names into Internet addresses or URLs. Enter the DNS server's IP address.

DNS2: Enter the secondary DNS server's IP address.

Option60 Vendor ID: Enter Option 60 information here to be included in the DHCP request communication.

DHCP Relay: Select this option to enable DHCP Relay. Use this if you have a dedicated DHCP server on your network, then enter the server IP address.

Click **Save** when you are done.

LAN IPv6 Settings

IPv6 Enable: Enable or disable the IPv6 addressing scheme for the local network.

Config Mode: Select either SLAAC (stateless configuration) or DHCPv6 (stateful configuration).

Prefix Select: Select the prefix assignment method: **Auto**, **Manual**, or a **Service Number** of the WAN Interface if the IPv6 setting is configured for that service.

If you selected **Auto**, configure the following settings for DNS:

DNS Select: Configure the mode of DNS: **Auto**, a **Service Number** of the WAN Interface or **Manual** and enter the DNS server information manually below.

Primary DNS Server: Enter the DNS server's IP address.

Secondary DNS Server: Enter the secondary DNS server's IP address.

If you selected **Manual**, configure the following settings:

Address Format: Select the IPv6 addressing method: **EUI64 Address** or **Address Pool**.

Prefix: Enter the IPv6 prefix, for example, 2001:b011:2000:0012::.

Prefix Length : Enter the IPv6 prefix length (16-64).

Prefix Preferred Lifetime: Enter the preferred lifetime of the prefix (600-4294967295 seconds).. The default is 3600.

Prefix Valid Lifetime: Enter the valid lifetime of the prefix (600-4294967295 seconds). The default is 7200.

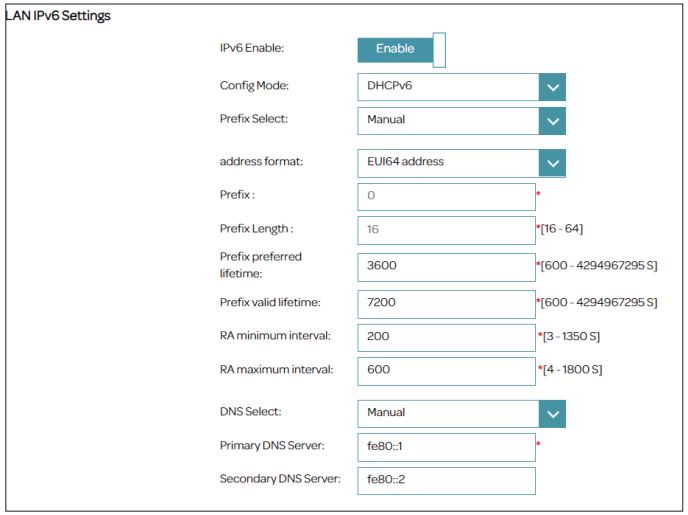
RA Minimum Interval: Enter the minimum time interval at which the router advertisement messages will be sent (3-1350 seconds). The default is 200 seconds.

RA Maximum Interval: Enter the maximum time interval at which the router advertisement messages will be sent (4-1800 seconds).The default is 600 seconds.

DNS Select: Select the DNS server assignment method: **Auto**, **Manual**, or a **Service Number** of the WAN Interface. If you selected Manual, enter the following DNS settings manually.

Primary DNS Server: Enter the DNS server's IP address.

Secondary DNS Server: Enter the secondary DNS server's IP address.

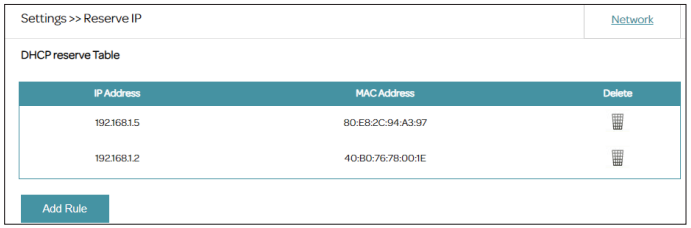


UPnP Settings

UPnP allows network devices to seamlessly discover each other on the local network for network services such as file sharing and advanced media functions. Select this option to allow UPnP (Universal Plug and Play) on the local network.

Reserve IP

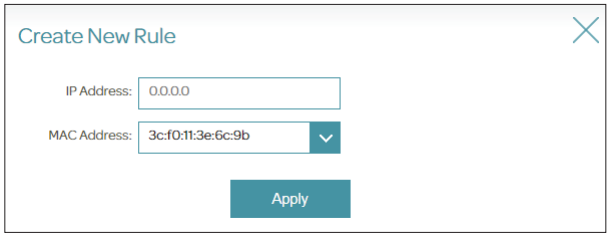
This section allows you to assign a static IP address to a specific computer on your LAN. Go to **Settings > Network** and click the **Reserve IP** tab to access this page.



Click **Add Rule** to add a new entry to reserve an IP address to a client device:

IP Address: Enter an IPv4 address to be assigned.

MAC Address: Select a device from the available clients' MAC addresses.

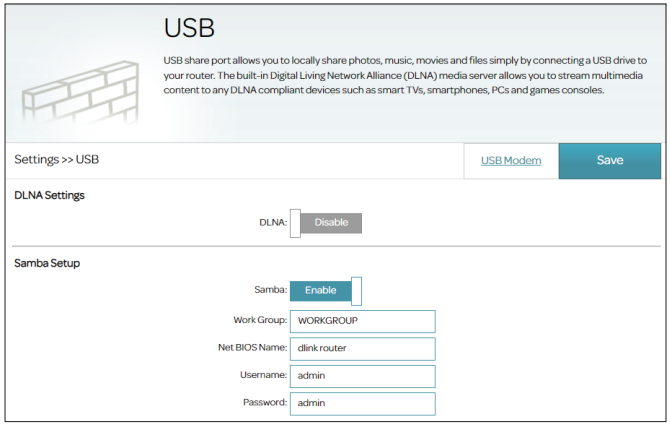


Click **Apply** when you are done to close the screen.

Click **Save** when you are done adding the rules.

USB

This page allows you to set up access to files on an external USB device plugged into the router. Then you can perform file sharing through local network. To access this page, go to **Settings > USB**.



DLNA Settings

DLNA: Enable or disable the DLNA media server functions, allowing connected DLNA clients access to media files over the network.

Samba Setup

Samba: Enable or disable Windows File Sharing or Samba. Computers and devices which support Samba will be able to access the files on the USB device connected to this router.

Work Group: Enter the Windows workgroup name.

Net BIOS Name: Enter the name for this device as you wish it to appear on your network.

Username: Enter a username for authentication for access.

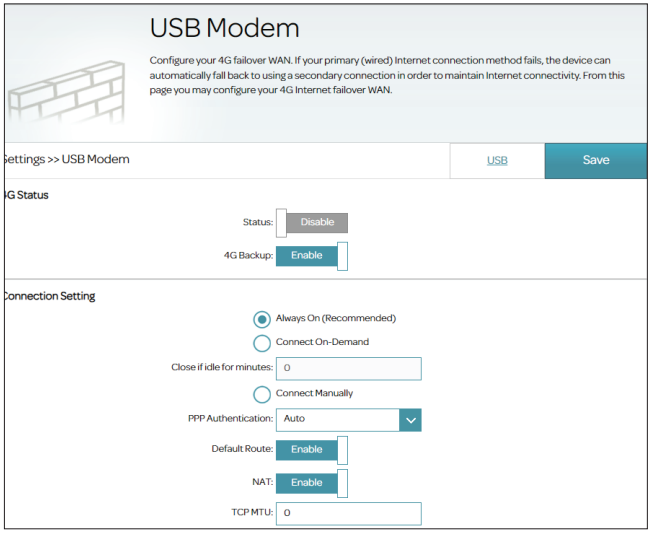
Password: Enter a password for authentication for access.

Click **Save** when you are done.

For information on how to access your USB drive from a Windows-based PC refer to **Connect and Share a USB Storage Device** on page **93**.

USB Modem

The USB port can be inserted with a 3G/4G mobile broadband adapters to be a backup of your primary Internet connection. On this page, you can check and edit the router's configuration for the USB modem (if one is inserted). To access this page, go to **Settings > USB and** select the **USB Modem** tab.



4G Status

Status: Enable or disable the USB modem. If it is enabled, the router will use the USB modem to connect to the Internet instead of the DSL or Ethernet WAN port.

4G Backup: Enable the USB modem to be a backup of the primary Internet connection. When the primary Internet connection fails, it will be active and resume the connection.

Connection Settings

Select the connection method: **Always On**, **Connect On-Demand**, or **Connect Manually**.

If you selected Connect On-Demand, enter the following option:

Close if Idle for Minutes: Enter a maximum idle time in minutes to wait before closing the connection due to inactivity.

f you selected Connect Manually, enter the following option:

PPP Authentication: Select the authentication method for Point-to-Point Protocol (PPP) connections: PAP, Auto, or CHAP.

Default Route: Enable or disable default route established through your USB modem for Internet connection.

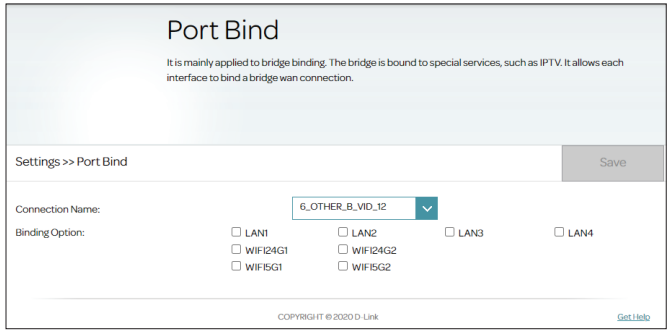
NAT: Enable or disable Network Address Translation (NAT).

TCP MTU: Enter the Maximum Transfer Unit (100-1492). The default is 0.

Click **Save** when you are done.

Port Bind

With Port Bind, you can designate devices attached to a LAN port running application services to go through a specifically pre-defined WAN interface for external connections. To access this page, go to **Settings > Port Bind**.



Port Bind

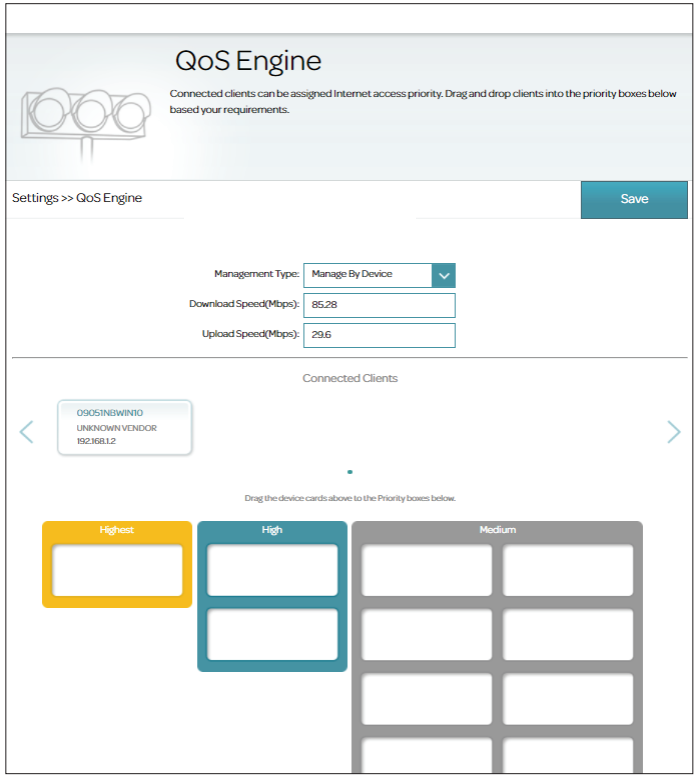
Connection Name: Select a Service Number of the WAN interface for external connections. The available Service Numbers of the WAN interface are those with a configured VLAN ID.

Binding Option: Select the binding port to be bridged to the WAN interface: LAN1-LAN4, WiFi2.4G 1/2, WiFi5G 1/2.

Click **Save** when you are done.

QoS

The QoS Engine allows you to assign priorities to designated clients. Go to **Settings > QoS** to configure clients' Internet access priorities. It aims to optimize Internet traffic to enhance the overall user experience.



Management Type Select **Off** to disable this feature or **Manage By Device** to enable this feature.

Upload Speed (Mbps) The rate at which the content is being transferred to the Internet.

Download Speed (Mbps) The rate at which the content is being transferred to the router.

Upload/download speeds can be obtained from your Internet Service Provider.

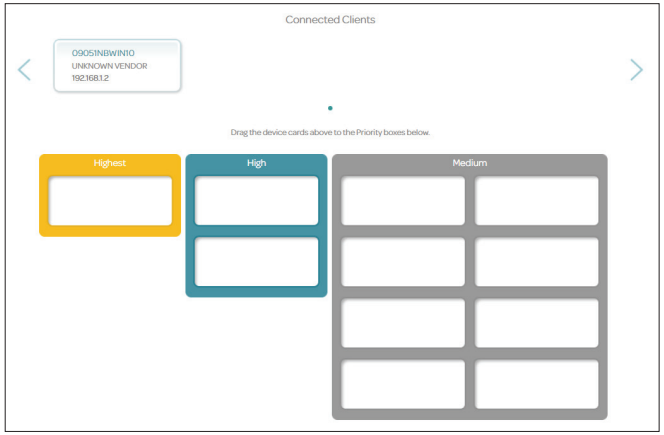
Click **Save** after filling in the above information.

This **Quality of Service (QoS) Engine** allows you to prioritize particular clients over others, so that these clients receive higher bandwidth. For example, if one client is streaming a movie and another is downloading a bulk of files, you might want to assign the former device a higher priority than the latter so that the movie streaming is not disrupted.

Under **Connected Clients**, you will see device cards representing each connected client.

To assign a priority level to a device, click the client and drag and drop to one of the priority categories: **Highest, High,** or **Medium**.

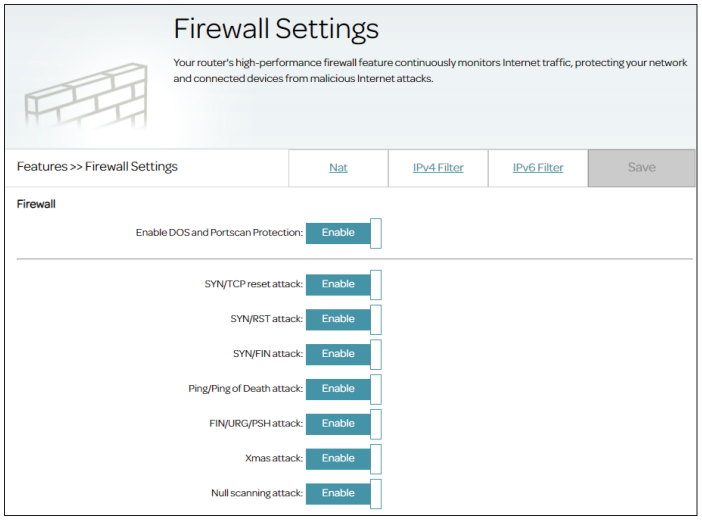
To change the client's priority, click **x** on its card to place it back to the **Connected Clients**.



Features

Firewall

The router's firewall protects your network from malicious attacks over the Internet. To access this page, go to **Features > Firewall**. It is recommended to leave all values at their default **Enable** setting.



Firewall

Enable DOS and Portscan Protection: Denial of Service (DoS) protection prevents attacks such as **Ping of Death** and others as the following described.

SYN/TCP reset attack: TCP reset breaks the three-way TCP connection between two parties by sending a spoofed RST packet.

SYN/RST attack: SYN/RST attack sends continuous SYN packets to a targeted network device, causing the device to spawn a half-open connection by sending back a TCP SYN-ACK packet (Acknowledge) and waiting for a packet in response from the sender address (response to the ACK packet).

SYN/FIN attack: This type of Denial of Service attacks a targeted device by continuously sending illegitimate SYN-FIN packets.

Ping/Ping of Death attack: The Ping of Death attack aims to disrupt a targeted network device by sending abnormally large packets.

FIN/URG/PSH attack: A URG-ACK-PSH-FIN flood attack brings down a device by sending illegitimate URG-ACK-PSH-FIN packets.

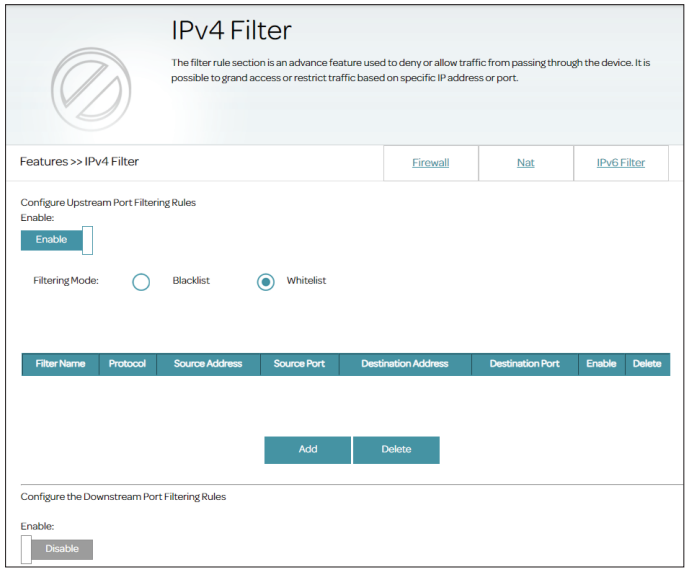
Xmas attack: Christmas tree attack sends crafted TCP packet to obtain information about the target system.

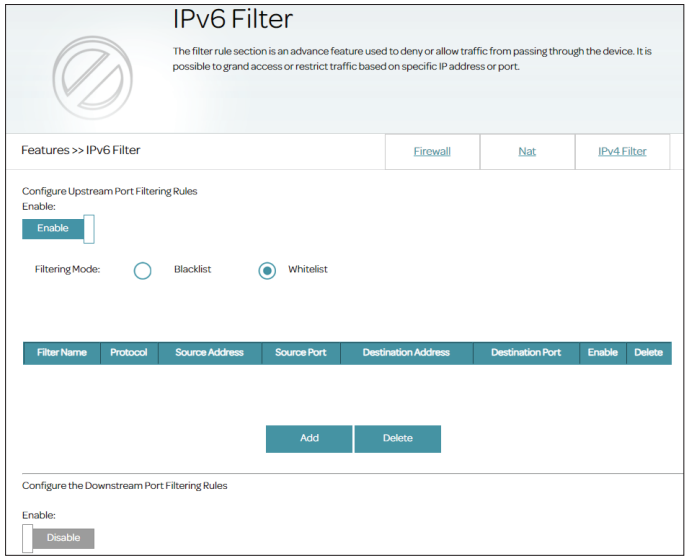
Null scanning attack: In Null Scanning attack, a packet without any flags of the TCP header tries to exploit a system.

Click **Save** when you are done.

IPv4/IPv6 Filter

The Firewall contains filtering functions to filter traffic based on the network protocols and source and destination IP addresses.
Go to **Features > Firewall**, then click the **IPv4 Filter** tab or the **IPv6 Filter** tab to configure rules for traffic filtering. To configure a rule to filter unwanted traffic, first enable this feature by clicking **Enable** for either **Upstream Port Filtering Rules** for traffic that is sent out of the router (LAN to WAN) or **Downstream Port Filtering Rules** for traffic that is received by the router from an external network (WAN to LAN).





Configure the following settings:

Filtering Mode: Select either **Blacklist** or **Whitelist** to deny or permit the following filtering list.

Filter Name: Enter a name for the filtering rule.

Protocol: Select the network protocol for the traffic: **TCP/UDP, TCP, UDP,** or **ICMP** (or **ICMPv6** for IPv6).

Source IP Address/Port: Enter the starting source IP address (e.g. 1.1.1.1 for IPv4 or 2001::1 for IPv6) and starting port that the rule will apply to. Depending on whether it is a upstream or downstream traffic, this can be either a WAN or LAN IP address. Both a single IP address and a range of IP addresses can be used.

End Source IP Address/Port: Enter the ending source IP address (e.g. 1.1.1.5 for IPv4 or 2001::5 for IPv6) and ending port that the rule will apply to. For a single IP address assignment, enter the same address as the starting IP address. Depending on whether it is a upstream or downstream traffic, this can be either a WAN or LAN IP address.

Source Subnet Mask/Prefix Length: Enter the subnet mask of the source IP address for IPv4 addressing scheme (four 8-bit octets). Or enter the prefix length for IPv6 addressing scheme (1-128).

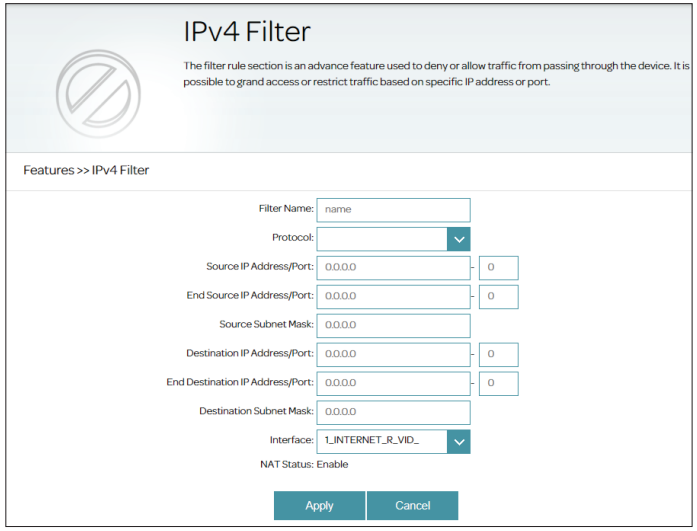
Destination IP Address/Port: Enter the starting destination IP address (e.g. 1.1.1.1 for IPv4 or 2001::1 for IPv6) and starting port that the rule will apply to. Depending on whether it is a upstream or downstream traffic, this can be either a WAN or LAN IP address. Both a single IP address and a range of IP addresses can be used.

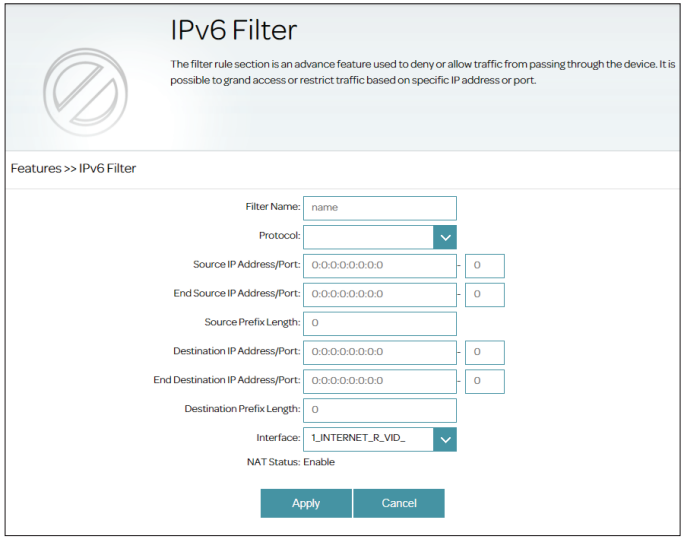
End Destination IP Address/Port: Enter the ending destination IP address (e.g. 1.1.1.5 for IPv4 or 2001::5 for IPv6) and ending port that the rule will apply to. For a single IP address assignment, enter the same address as the starting IP address. Depending on whether it is a upstream or downstream traffic, this can be either a WAN or LAN IP address.

Destination Subnet Mask/ Prefix Length: Enter the subnet mask of the destination IP address (four 8-bit octets). Or enter the prefix length for IPv6 addressing scheme (1-128).

Interface: Select a **Service Number** of the WAN Interface for which the traffic will pass through.

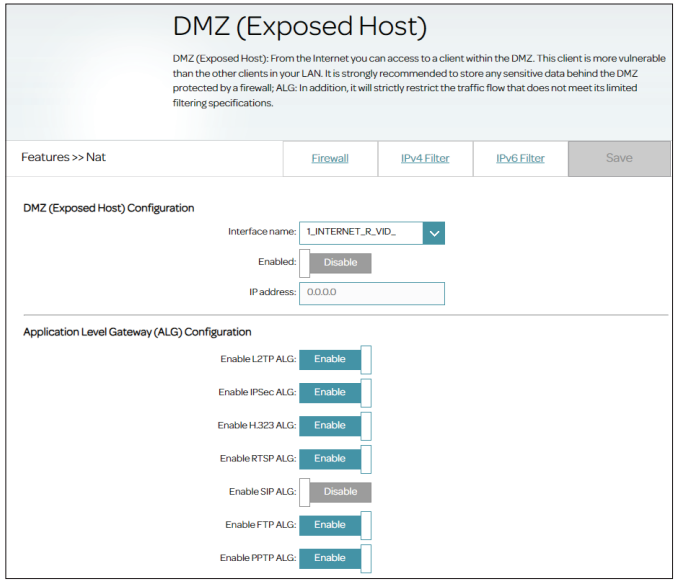
Click **Apply** to save your settings. A maximum of 20 rules can be defined.





NAT

Go to **Features > Firewall** and click the **NAT** tab to configure the router's advanced firewall settings such as DMZ and Application Level Gateway (ALG).



Interface Name: Select the interface for which the packets coming into the WAN port will be redirected to a specific IP address in DMZ.

Enable DMZ Enable or disable Demilitarized Zone (DMZ). Devices in this zone are completely exposed to threats over the Internet. This is not recommended unless they are servers that must be exposed to the public network.

DMZ IP Address If you enable DMZ, enter the IP address of the client to be placed in this zone.

Application Level Gateway (ALG) Configuration

Different ALGs provide special handling for specific protocols or applications to allow data of these applications to pass through an NAT-enabled router. For each protocol type, click **Enable** to activate the ALG. A number of ALGs for common applications are enabled by default.

Enable L2TP ALG: Allows multiple machines on the LAN to connect to their corporate network using the Layer 2 Tunneling Protocol (L2TP).

Enable IPSec ALG: Allows 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 with 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.

Enable H.323 ALG: H.323 standard provides VoIP telephony and video conferencing. Enable ALG for H.323 if such applications will be used in your network.

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

Enable SIP ALG: 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. This is disabled by default.

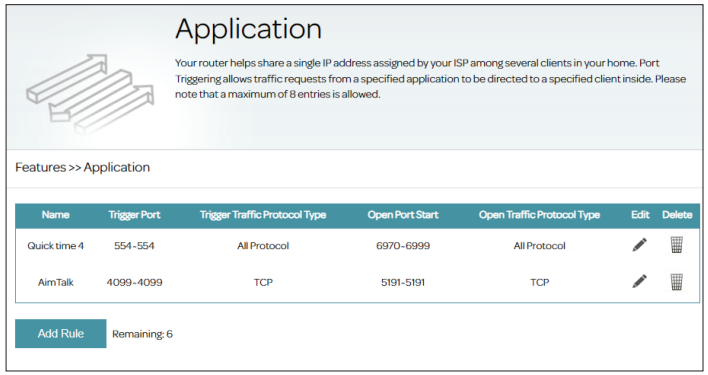
Enable FTP ALG: Allows devices running FTP (File Transfer Protocol) to provide such service successfully through the NAT router.

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

Click **Save** when you are done.

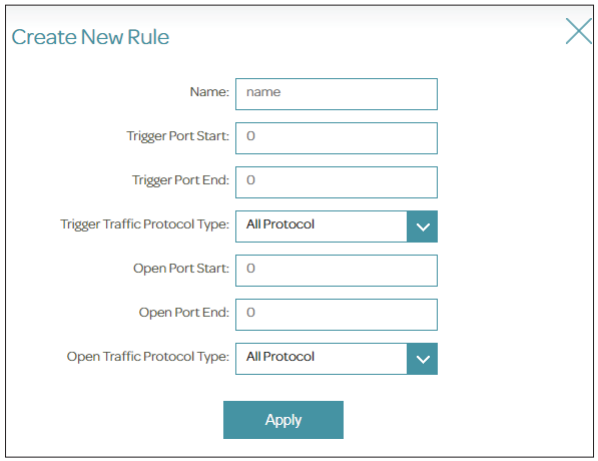
Application

Port triggering allows ports to be opened for inbound traffic when outbound traffic is detected on specified ports . This is used for facilitating communication between applications and servers behind a NAT firewall. To access this page, go to **Features > Application**.



The currently defined Application rules are displayed in the table. Some commonly used Applications are pre-configured by default. You may create up to 8 application rules. If you wish to remove an application rule, click . If you wish to edit an application rule, click in the **Edit** column. If you wish to create a new application rule, click the **Add Rule** button.

Create New Rule



Name: Enter a name for this application.

Trigger Port Start: Enter the starting port range for the traffic that will be forwarded.

Trigger Port End: Enter the ending port range for the traffic that will be forwarded.

Trigger Traffic Protocol Type: Select the protocol to trigger this rule: **TCP**, **UDP,** or **All Protocol**.

Open Port Start: Enter the starting port to open once triggered.

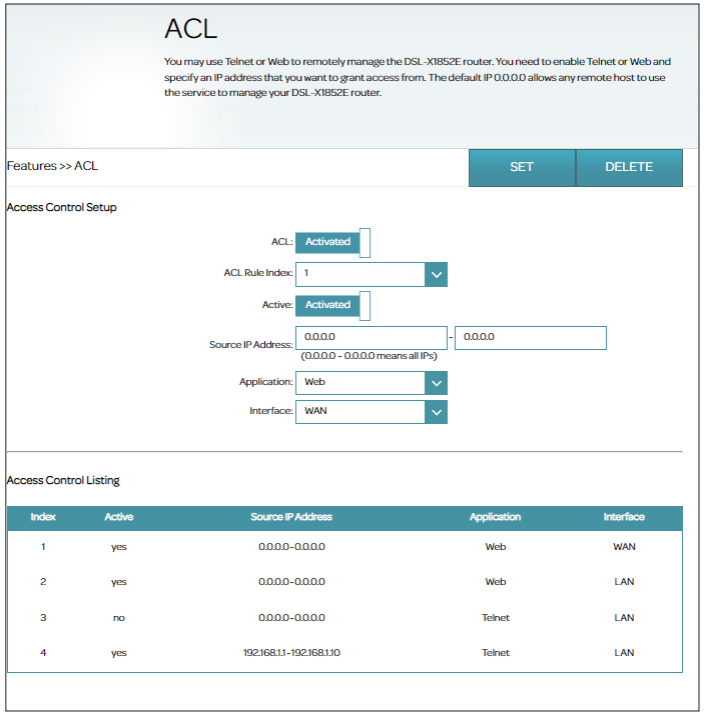
Open Port End: Enter the ending port to open once triggered.

Open Traffic Protocol Type: Select the protocol to trigger this rule: **TCP**, **UDP,** or **All Protocol**.

Click **Apply** when you are done. A maximum of 8 rules can be defined.

ACL

The Access Control List (ACL) page allows you to enable or disable various services of the router to be used within the LAN or from the WAN side. To access this page, go to **Features > ACL**. To start enforcing the ACL, click **Activated**.



Access Control Setup

ACL Rule Index: Select the rule index from the drop-down menu.

Active Enable or disable this particular access rule. Enable means the particular service can be accessed by the specified IP address range. Disable means the particular service cannot be accessed by the specified IP address range.

Source IP Address: Enter the IP address range to apply the rule to. Only addresses in the specified range have the permission to access this router with the below application. Enter 0.0.0.0 to allow any IP address to access the router.

Application: Select a pre-defined service: Web, Telnet, Ping or All for all of the above services.

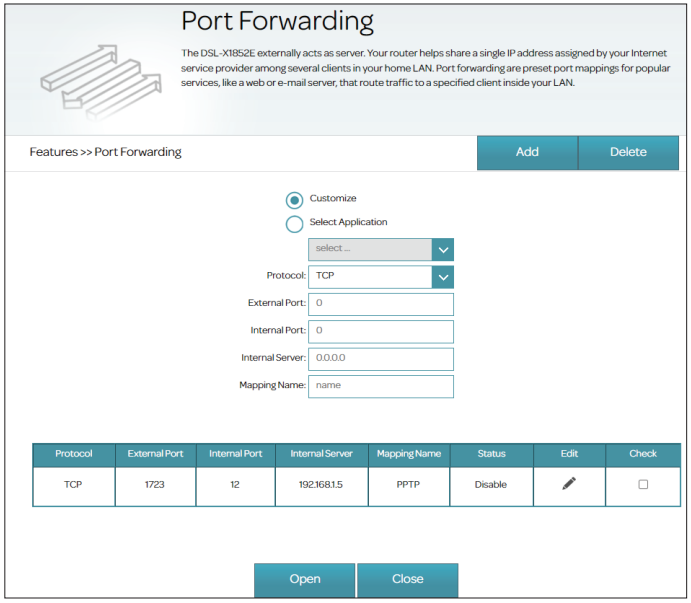
Interface: Select the interface from the drop-down menu to apply this access rule: Both, WAN, or LAN. For Telnet, only LAN is available.

Note: The default ACL for web access IP range - 0.0.0.0~0.0.0.0 (any IP address) on the LAN interface cannot be deleted or modified.

Click **Add** when you are done or **Delete** to remove the selected rule. Up to 4 rules can be created.

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. To access this page, go to **Features > Port Forwarding**.



If you wish to remove a rule, select it in the **Check** column, then click **Delete** in the upper right corner. If you wish to edit a rule, click in the **Edit** column. If you wish to create a new rule, click the **Add** button. Click **Save** when you are done. If you edit or create a rule, the following options will appear:

To begin, select either **Customize** to customize your service and ports or **Select Application** to use a pre-defined service with the associated port.

Protocol: Select **TCP**, **UDP** or both **TCP/UDP**. Refer to the documentation for this service hosting on your internal computer.

External Port: Enter the external port for this type of service.

Internal Port: Enter the internal port for this type of service.

Internal Server: Enter the IP address of the computer on your local network that should receive the service requests.

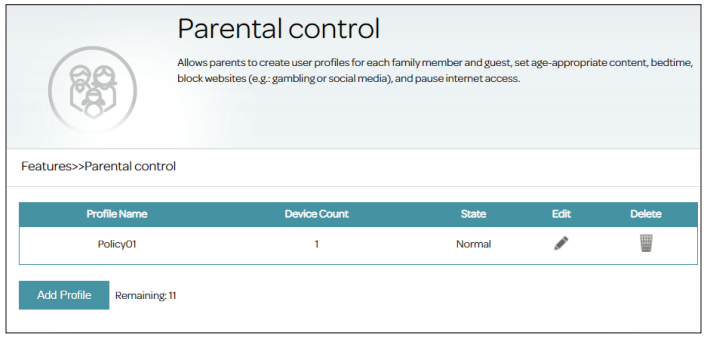
Mapping Name: Enter a name for this service or application. Do not include space in the name.

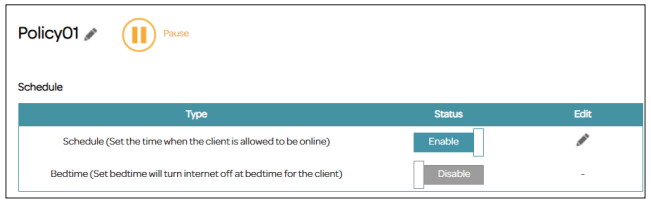
Click **Add** when you are done or **Delete** to remove the selected rule. After creating a port forwarding rule, you can select it and click **Open** to enable it or **Close** to disable it. The Status column will reflect its current enable/disable status. Up to 10 rules can be created.

Parental Control

With Parental Control, you can configure schedules that set time limits for Internet access and prevent access to certain websites. Go to **Features > Parental Control** to configure parental control policies.

Click **Save** at any time to save the changes you have made on this page.





To add a profile, configure the following:

Schedule

Profile Name: Enter a name for this profile. Note that special characters such as space, ?, <, >, +, and - are not allowed.

Schedule (Set the time when the client is allowed to be online) Click **Enabled** and define the schedule to allow Internet access. Select the time during which the Internet will be available.

To add a schedule:
Each box represents one hour, with the clock time (0~23) at the top of each column. To add a time period to the schedule, simply click on the start time and drag to the end time. You can add multiple days and multiple periods per day to the schedule. If no time periods are selected, all devices in this profile will be granted Internet access. If you do not set any schedule, you will be prompted to set one when saving the policy.

Bedtime (Set bedtime will turn Internet off at bedtime for the client)

Click **Enabled** and define the schedule to block Internet access during bedtime.
To add a bedtime schedule:
Select the time during which bedtime schedule will be active. Select the days of the week, then select the **Start** time and the **End** time for the period during which Internet access will be blocked. If you do not set any schedule, you will be prompted to set one when saving the policy.

Website Filter

Click **Add Rule** to add a new website to be blocked:

Website Name

Enter the name for the website. This blocks access to websites based on a website's address. For example, enter "ABC.com" or "www.ABC.com."

URL Keyword

This blocks access to websites based on the keywords with matching URLs. For example, use "ABC" to block "www.ABC.com" and "xxx.ABC.com" and other URLs containing ABC. Enter the same website name as the above in this field to block only the specific URL.

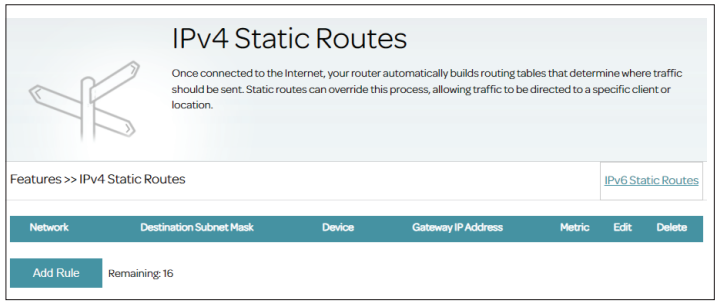
Device

Click **Add Device** to add devices to be in the defined profile. Select the devices from the list of connected devices to which the access policy should be applied, then click **Apply** to close the screen. Click **Save** to save your profile settings and the new profile will be added to the profile list. You can also modify or delete an existing profile by clicking or respectively.On the Edit page for a selected profile, you can click to pause Internet access to specified devices of the profile immediately.

You can also modify or delete an existing rule by clicking **Edit** or **Delete** respectively. Up to 12 rules can be created.

Static Route

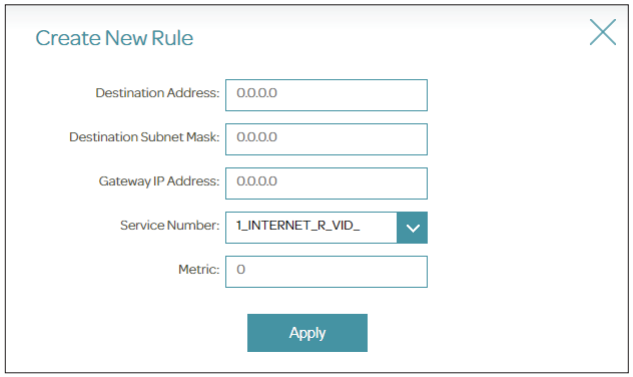
The Static Routes page allows you to define custom routes to control how data traffic is moved around your network. To access this page, go to **Features > Static Route.** Select **IPv4 Static Routes** or **IPv6 Static Routes**.



If you wish to remove a rule, click in the **Delete** column. If you wish to edit a rule, click in the **Edit** column. If you wish to create a new rule, click the **Add Rule** button. Click **Save** when you are done.

Complete the following to create or edit a rule:

Create New Rule



Destination Address: Enter the destination subnetwork IP address.

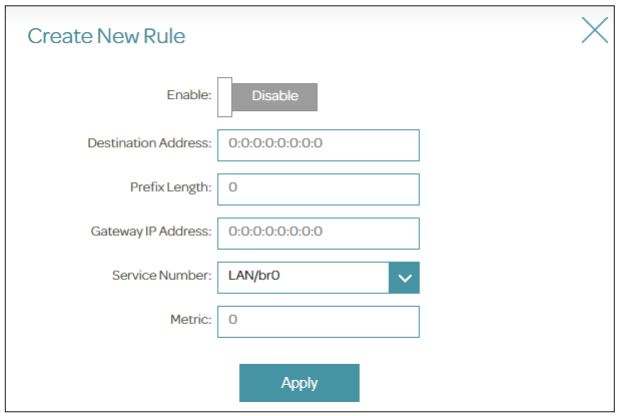
Destination Subnet Mask (IPv4): Enter the subnet mask of the destination address. The subnet mask determines an IPv4 subnetwork.

Prefix Length (IPv6): Enter the IPv6 prefix length (0~128), which is the number of prefix bits of an IPv6 address. The prefix determines an IPv6 subnetwork.

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

Service Number: Specify the interface to transit the packets of this static route.

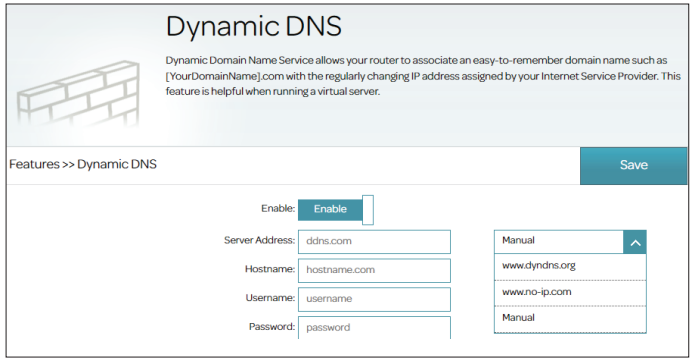
Metric: The route metric is a value from 0 to 15 that indicates the cost of using this route.



Click **Apply** when you are done. A maximum of 16 rules can be defined.

Dynamic DNS

The Dynamic Domain Name System (DDNS) assigns an easy-to-remember domain name such as [YourDomainName].com to a dynamic IP address assigned by your Internet Service Provider. Through the DDNS service provider, people can enter your domain name in their web browser to connect to your server (e.g. FTP or web), no matter what your IP address is. To access this page, go to **Features > Dynamic DNS**.



Complete the following to configure the DDNS:

Enable: Enable or disable Dynamic DNS.

Server Address: Select your DDNS service provider: www.dyndns.org or www.no-ip.com. Select **Manual** to enter your DDNS service address manually.

Hostname: Enter the host name that you registered with your DDNS service provider.

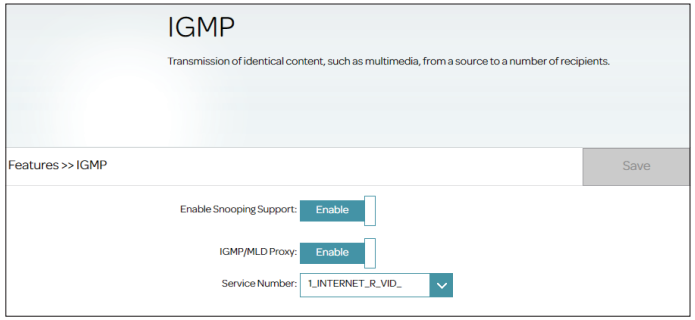
Username: Enter the username for your DDNS account.

Password: Enter the Password for your DDNS account.

Click **Save** when you are done.

IGMP

The Internet Group Management Protocol (IGMP) allows for the transmission of identical content, such as multimedia, from a source to a number of destination recipients.



Enable Snooping Support: Enable and disable Internet Group Management Protocol (IGMP) snooping to build multicast tables.

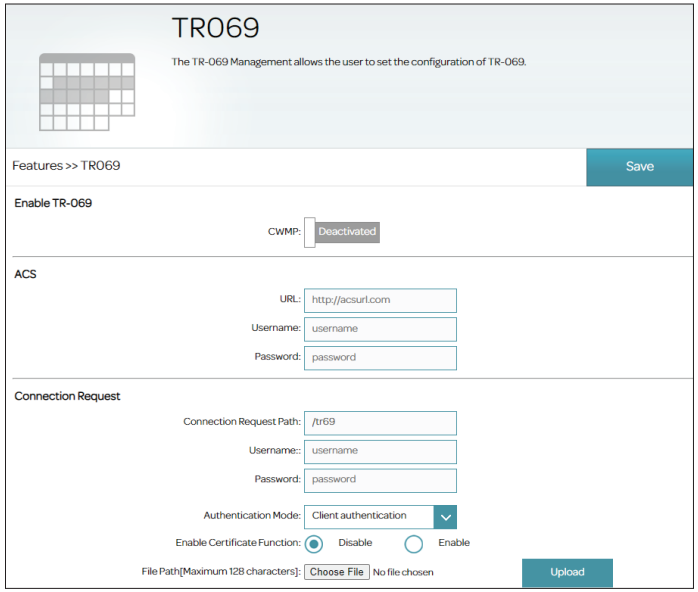
IGMP/MLD Proxy: Check the box to enable the router to operate as an Internet Group Management Protocol (IGMP) for IPv4 and Multicast Listener Discovery (MLD) proxy for IPv6.

Service Number: Select the interface to apply the IGMP proxy for IGMP communication.

Click **Save** when you are done.

TR069

TR069 allows for automatic configuration between an auto-configuration server (ACS) and your router. To access this page, go to **Features > TR069**. Please check with your service provider, or leave the settings at their defaults if you are not sure.



TR-069

CWMP: Activate or deactivate CPE WAN Management Protocol (CWMP)

ACS

URL: Specify the URL of the auto-configuration server (ACS), starting with http://.

Username: Enter the username to log in to the ACS remote server.

Password: Enter the password to log in to the ACS remote server.

Connection Request

Connection Request Path: Specify the request path here.

Username: Enter the username for connection request sent from the ACS remote server to the router.

Password: Enter the password for connection request sent from the ACS remote server to the router.

Periodic Inform: Activate or deactivate the periodic inform function.

Interval: Specify the interval in seconds for each inform packet (1-999999). The default is 43200.

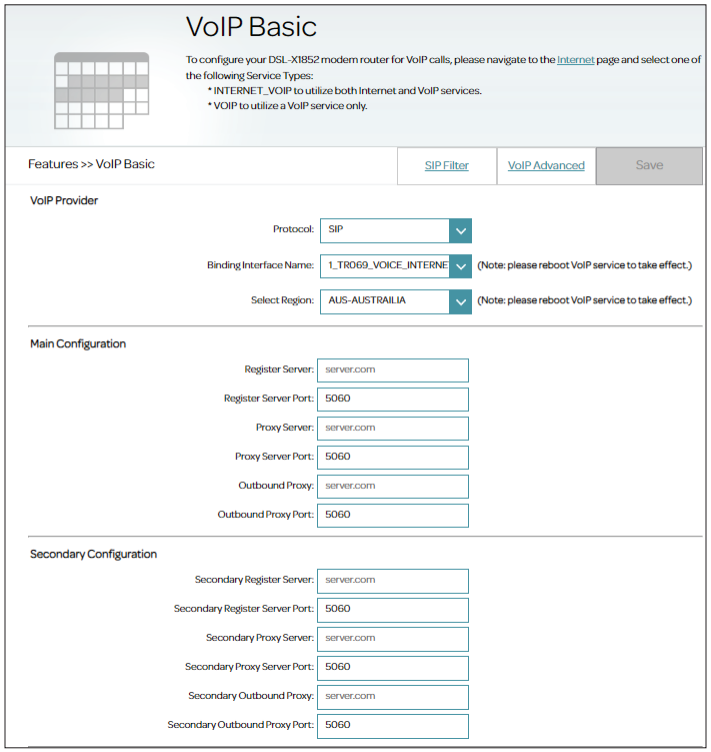
Authentication Mode: Select either **Server** or **Client** authentication method.

Enable Certificate Function: Enable or disable certification for authentication.

File Path: Click **Choose File** to locate the certificate file. Then click **Upload** to upload the certificate file.

Click **Save** when you are done.

VoIP



The VoIP page allows you to configure all of the parameters essential for Voice over Internet Protocol(VoIP) and specify all required settings for the phone connected to the router. Go to **Features> VoIP** and select **VoIP Basic, SIP Filter,** or **VoIP Advanced**. Please check with your Internet phone service provider or leave the settings at their defaults if you are not sure.

Configure the following basic VoIP settings:

VoIP Provider

Protocol: Select the protocol used for VoIP. The default is Session Initiation Protocol (SIP). It is a networking protocol which allows your VoIP devices and servers to communicate with one another.

Binding Interface Name: Specify the WAN interface for VoIP. Please select the Service Number of WAN interface with VoIP service.

Select Region: Select the region for your IP telephony service.

Main Configuration

Enter the information of the primary VoIP registrar in this section.

Register Server: Enter the IP or URL address of the registrar.

Register Server Port: Specify the port number used for VoIP registration.

Proxy Server: Enter the IP or URL address of the SIP proxy server.

Proxy Server Port: Enter the port used for SIP proxy.

Outbound Proxy: Enter the IP or URL address of the SIP outbound proxy server.

Outbound Proxy Port: Enter the port used for SIP outbound proxy.

Secondary Configuration

Enter the information of the secondary VoIP registrar in this section.

Secondary Register Server	Enter the IP or URL address of the registrar.
Secondary Register Server Port:	Specify the port used for VoIP registration.
Secondary Proxy Server:	Enter the IP or URL address of the SIP proxy server.
Secondary Proxy Server Port:	Enter the port used for SIP proxy.
Secondary Outbound Proxy:	Enter the IP or URL address of the SIP outbound proxy server.
Secondary Outbound Proxy Port:	Enter the port for the SIP outbound proxy server.

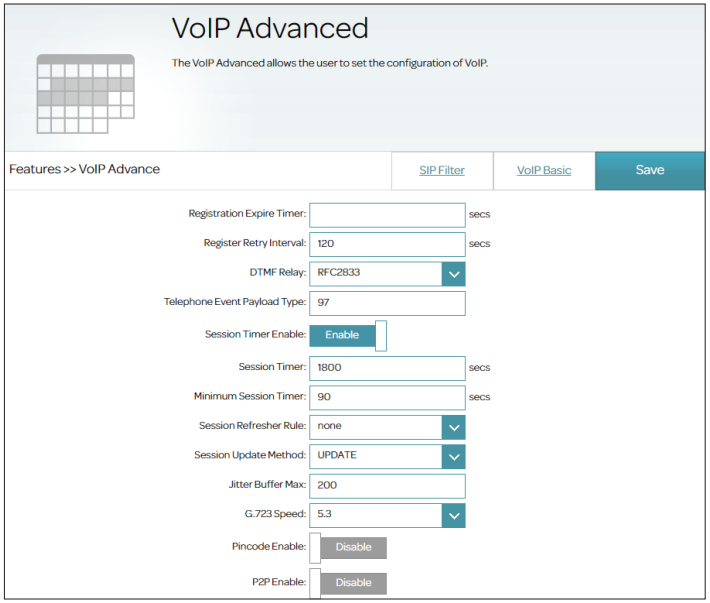
Line Configuration

The router features two phone ports, each of which can be configured independently to convert voice traffic into data packets for transmission over an IP network. Configure the following for both VoIP1 and VoIP2 lines.

Line	Indicates the respective VoIP line for configuration.
Port Enable Setting:	Enable or disable the respective phone port.
Registration Status:	Displays whether the line is registered successfully.
Account:	Enter the name for your VoIP account.
Password:	Enter the password for your VoIP account.

VoIP Advanced

With this menu, you can configure advanced settings for Voice over Internet Protocol(VoIP). Go to **Features> VoIP** and select **VoIP Advanced**. Please check with your Internet phone service provider, or leave the settings at their defaults if you are not sure.



Enter the information for VoIP registration in this section.

Registration Expire Timer: Enter the expiration time after which the router will change the VoIP registration status in case of no response from the SIP proxy server. The default is 3600 seconds.

Register Retry Interval: Specify the interval after which the VoIP registration will repeat. The default is 120 seconds.

DTMF Relay: Select the DTMF relay mode: SIP Info, RFC2833, or InBand.
- InBand: Transmission with voice data.
- RFC2833: Transmission in accordance with RFC2833.
- SIPInfo: Transmission in the relevant SIP messages.

For RFC2833, enter the below **Telephone Event Payload Type**.

Telephone Event Payload Type: Enter the **Telephone Event Payload Type**. The default is 97.

Session Timer Enable: Enable or disable the voice session timer.

Session Timer: Enter the VoIP session timer value. The default is 1800 seconds.

Minimum Session Timer: Enter the minimum voice session timer value. The default is 90 seconds.

Session Refresher Rule: Select the voice session refresher rule: none, uac, or uas.

Session Update Method: Select the method for updating a voice session: Update or Invite.

Jitter Buffer Max: Enter the maximum value for jitter buffer size. The default is 200 bytes

G.723 Speed: Select the speed for the G.723 audio codec: 5.3 or 6.3 kbit/s.

Pincode Enable: Enable or disable the use of pin code before making calls. If Enabled, enter the pin code below.

P2P Enable: Enable or disable Peer-to-Peer (P2P) communication.

Line Configuration

The router features two phone ports, each of which can be configured independently to convert voice traffic into data packets for transmission over an IP network. Configure the following audio codecs for both VoIP1 and VoIP2 lines. Select the encoding mode which defines the encoding rate control parameters for each of the following audio codec for both VoIP1 and VoIP2 lines.

G.722: Select the mode for the codec (0~7). The default is 1.

G.711 a-law: Select the mode for the codec(0~7). The default is 2.

G.711 u-law:: Select the mode for the codec (0~7). The default is 3.

G.729: Select the mode for the codec (0~7). The default is 4.

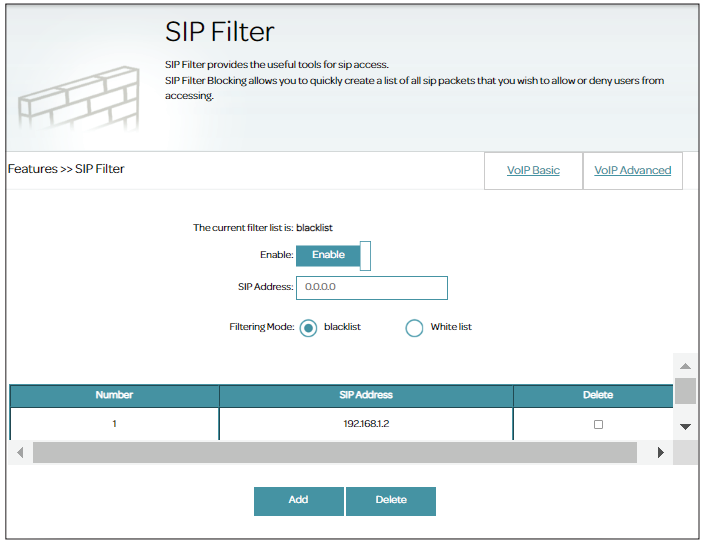
G.723: Select the mode for the codec (0~7). The default is 0.

ptime setup Select the packetization time (ptime): 10, 20, or 30.

Digit Map Enable: Enable or disable the digital map. If enabled, input the digit map in the text box below.

SIP Filter

SIP Filter allows you to configure filtering rules for incoming calls of the phone connected to the phone ports of the router. Go to **Features > VoIP** and select **SIP Filter**. Please check with your Internet phone provider, or leave the settings at their defaults if you are not sure. To start configuring filter rules, click **Enable**.



Enter the following information for filtering SIP messages:

SIP Address: SIP server uses Session Initiation Protocol to communicate with VoIP devices to control communication sessions for voice and multimedia content delivery.

Filtering Mode: Specify the filtering mode: blacklist or whitelist:
Blacklist: With this policy, the router accepts incoming calls (INVITE packets) from any IP addresses or domains except for those specified in a blacklist.
Whitelist: With this policy, the router accepts incoming calls (INVITE packets) only from IP addresses or domains specified in a whitelist.

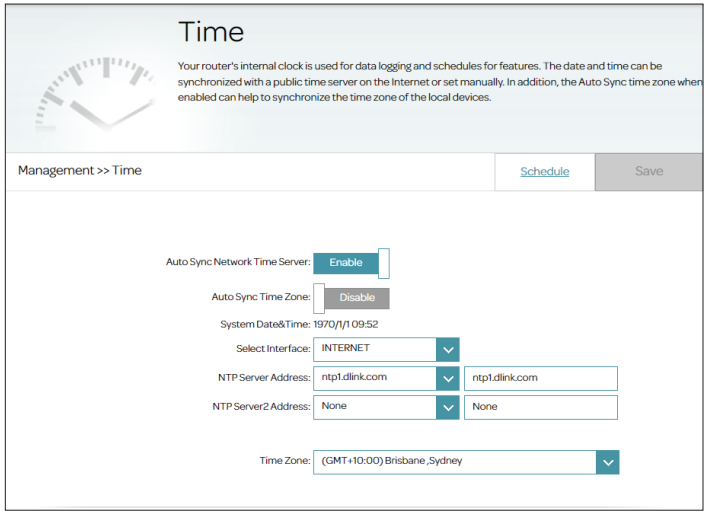
Click **Add** to add your filtering rule. After adding the rules, you can select a rule and click **Delete** to delete it. A maximum of 16 rules can be created.

Management

Time & Schedule

Time

The Time page allows you to configure, update, and maintain the correct time for the internal system clock. From here you can set the time zone and the Network Time Protocol (NTP). To access this page, go to **Management > Time & Schedule**.



Auto Sync Network Time Server: Enable or disable automatic synchronization of the date and time with a Network Time Protocol (NTP) server.

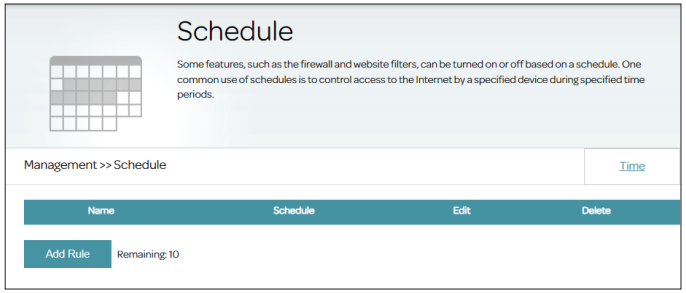
Auto Sync Time Zone: Enable or disable automatic time zone selection. If this is disabled, select your time zone in the following **Time Zone** drop-down list.

System Date&Time: Displays the current system date and time.

NTP Server/2 Address: Select the NTP server address from a list of available NTP servers. If you selected **Other**, enter the NTP server in the field**.** Adding a second server is optional. Select **None** if you don't want to specify a backup NTP server.

Click **Save** when you are done. To configure and manage the schedule, click the **Schedule** tab and refer to **Schedule** on page **84**.

Schedule



Some configuration rules can be set according to a pre-configured schedule. For example, Wi-Fi schedules for wireless network availability (refer to **Settings > Wireless**). To access this page, go to **Management >Time & Schedule** and click the **Schedule** tab.

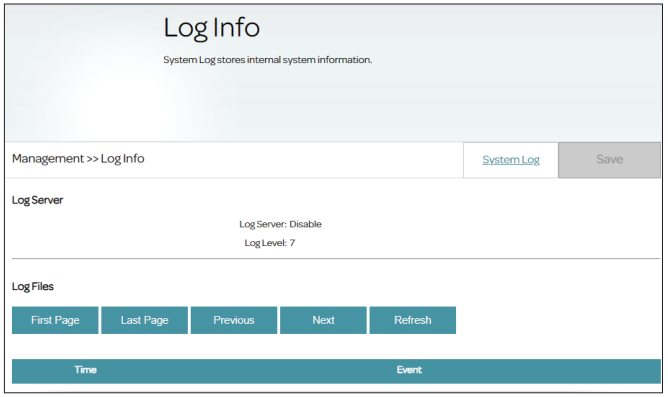
To edit or create a rule, use the following procedure:
First, enter the name of your schedule in the **Name** field. Please do not enter special characters such as space or !~<>+-. Note that name cannot be modified once a rule created.

Each box represents one hour, with the time for a 24-hour clock 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 periods per day and multiple days to the schedule.
To remove a time period from the schedule, click on the x icon. Click **Apply** when you are done to close the screen.

If you wish to remove a schedule, click in the **Delete** column. If you wish to edit a rule, click in the **Edit** column. If you wish to create a new schedule, click the **Add Rule** button. A maximum of 10 schedules can be created.

Log Info

The router keeps a running log of events. To access this page, go to **Management > Log Info**. System logging must be enabled in order for this feature to work.

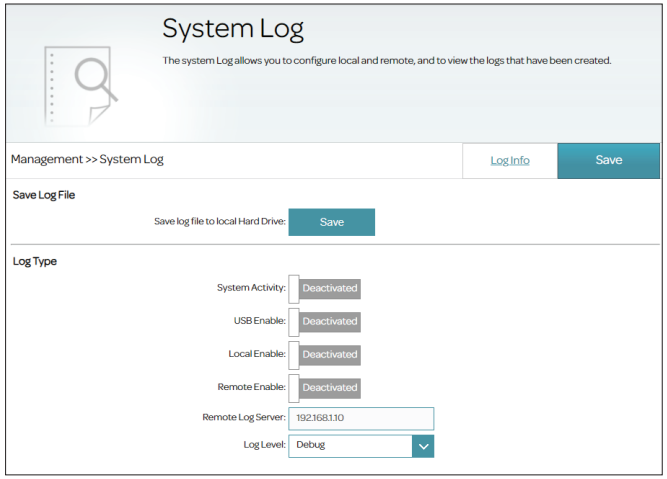


Refer to **System Log** on page **86** for information on how to enable the system logging.

Note that the type of log events is determined by the log level settings in **System Log**.

System Log

This page controls how the System Log operates. System Log can be used to analyze connectivity problems and troubleshoot a network. This log can be sent to a syslog server or saved to your local hard drive. To access this page, go to **Management > Log Info** and click the **System Log** tab.



Save Log File

Save Log File to Local Hard Drive: Click this button to save a copy of the log file to your local hard drive. It will be saved according to your browser's default download directory. You can view the log entries by opening with any text editing applications such as WordPad on Windows.

Log Type

System Activity: Activate or deactivate logging for system activities. Enable this to start the system log server.

USB Enable: Activate or deactivate logging on the USB storage.

Local Enable: Activate or deactivate logging on the system's flash of the router.

Remote Enable: Activate or deactivate remote logging. If enabled, enter the remote log server below.

Remote Log Server: Enter the IP address or URL address for the Syslog server.

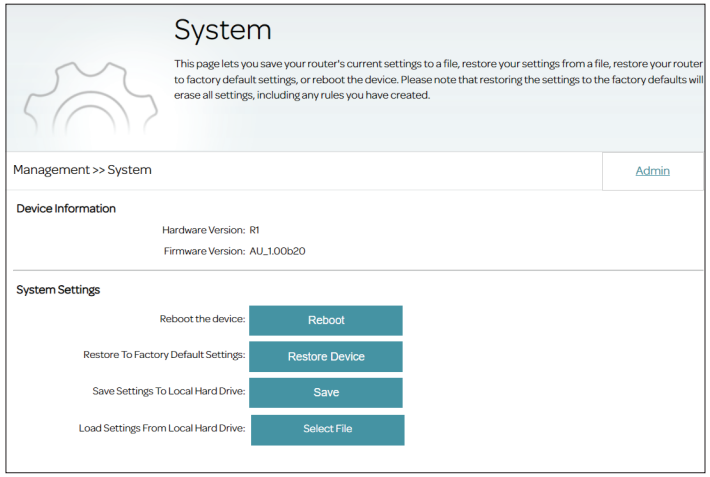
Log Level: Select the level of severity as listed from the highest to the lowest to be logged:

Emergency: Indicates that the system is almost unusable.
Alarm: Indicates that immediate action is needed.
Important: Indicates that the system is in a condition that requires urgent attention.
Error: Indicates that there is an error in the device.
Warning: Indicates that a warning message of an operational problem .
Note: Indicates a normal but not stable condition.
Notice: Indicates a condition that is not erroneous but requires some attention.
Debug: Contains debugging messages for debugging purposes.

Click **Save** when you are done.

System Settings

This page allows you to save the router's current configuration, load a previously saved configuration, reset the router to its factory defaults or reboot the router. To access this page, go to **Management > System Settings**.



Device Information

Hardware Version: Displays the hardware version of the router.

Firmware Version: Displays the current firmware version.

System Settings

Reboot the Device: Click **Reboot** to reboot the router.

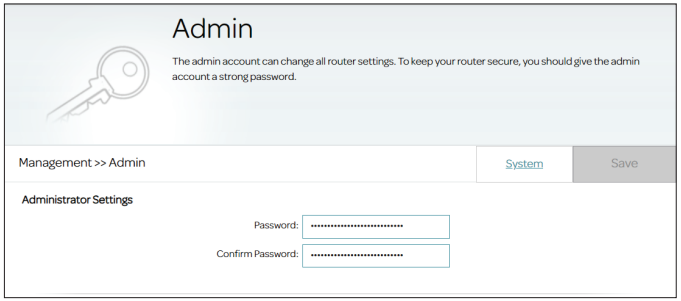
Restore to Factory Default Settings: This option will restore all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings after that time will be lost, including any rules that you have created. You can save the current router configuration settings before performing factory restoration with the **Save Settings to Local Hard Drive** function below.

Save Settings to Local Hard Drive: This option will save the current router configuration settings to a file (.cfg) on your computer. Click **Save** to save the configuration file to your browser's default download directory. This configuration file can be used to restore your router to a previous state with the **Load Settings From Local Hard Drive** below.

Load Settings From Local Hard Drive: This option will load a previously saved router configuration file. This will overwrite the router's current configuration. Click **Select File** to locate the configuration file from your local directory, then click **Upload Settings** to start uploading the configurations.
Note: The router will reboot during the restoration process. Do not turn the power on or off.

Admin

This page allows you to change the administrator (admin) password and enable remote management of the router. To access this page, go to **Management > System Settings**, and click the **Admin** tab.



Administrator Settings

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

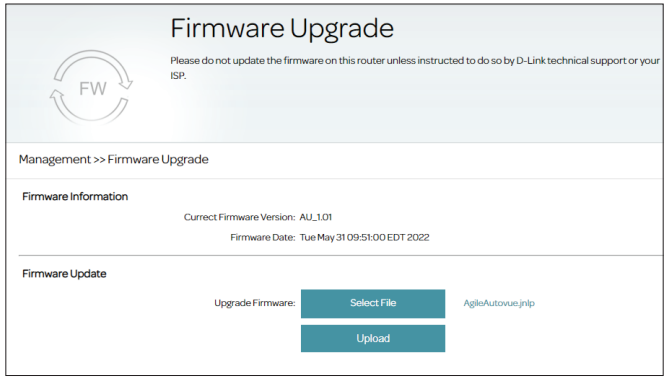
Confirm Password: Confirm the administrator account password.

Click **Save** when you are done.

Firmware Upgrade

This page allows you to upgrade the router's firmware. To access this page, go to **Management > Firmware Upgrade**.

To upgrade the firmware, you must first download the relevant file from **http://support.dlink.com**.



Firmware Information

Current Firmware Version: Displays the current firmware's version.

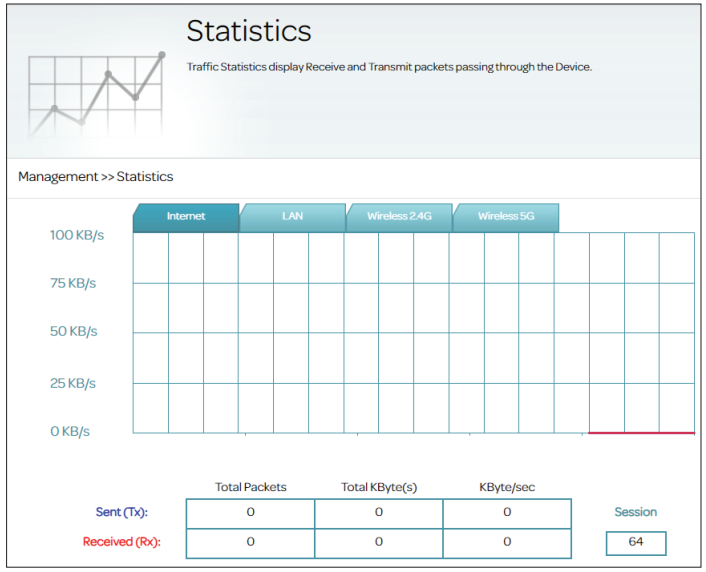
Firmware Date: Displays the current firmware's timestamp.

Firmware Update

Upgrade Firmware: If you wish to upgrade manually, first download the firmware file you wish to upgrade to. Next, click the **Select File** button and locate the firmware file. Then click **Upload** to begin the upgrade process. Do not power off the router while the firmware is being uploaded; otherwise, errors will occur that may result in malfunction of the router and further RMA services may be required.

Statistics

This page gives you various statistics about data transmitted and received by your router through the Internet and on your wired network (LAN) and your wireless networks. To access this page, go to **Management > Statistics**.



You can view the statistics of the **Internet**, **LAN**, **Wireless 2.4 GHz**, or **Wireless 5 GHz** interface by clicking on the respective tab at the top of the graph. The current amount of traffic being sent and received, measured in kilobyte per second is displayed, along with the current number of sessions. The graph will update every few seconds.

The table at the bottom of the page displays the total number of packets and the amount of data sent and received since the DSL-X1852E started.

Note: The traffic counter will reset if the device restarts.

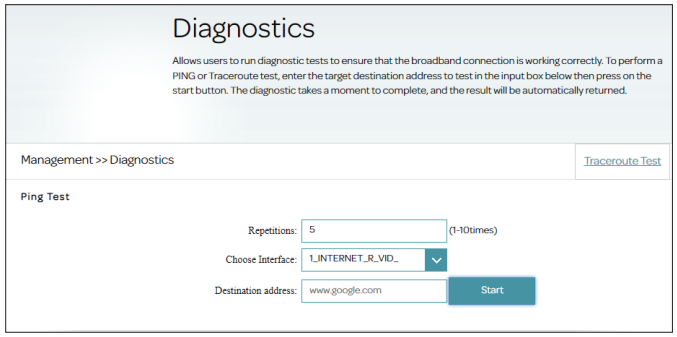
Diagnostics

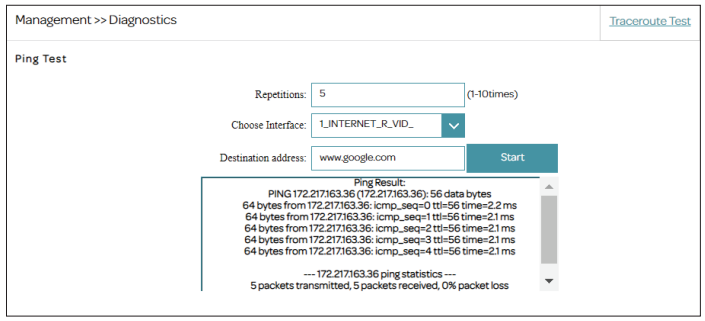
This page provides functions to test the router's connection to another device in the Internet. To access this page, go to **Management > Diagnostics**. Select the **Ping Test** or **Traceroute Test** tab. The ping test verifies the availability of a destination host while traceroute shows the route of data transferred to a destination host.

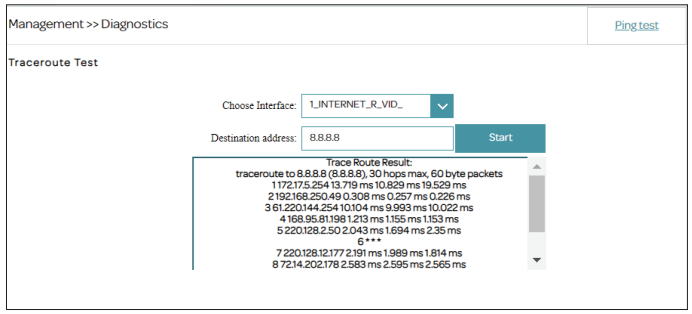
For Ping Test, enter the IP address or web address in the **Destination Address** field, choose the WAN **Interface** through which the packets will be transferred, enter the number of ICMP packets (1-10) to be sent, then click **Start**.

For Traceroute Test, choose the WAN **Interface** through which the packets will be transferred, enter the IP address or web address in the **Destination Address** field, then click **Start**.

The results of the test will be displayed in the text box below.







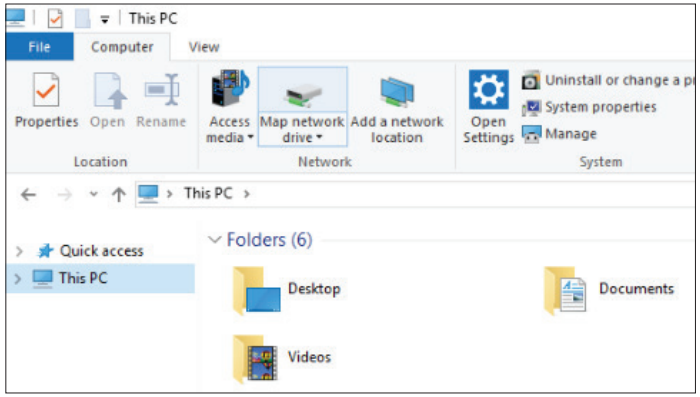
Connect and Share a USB Storage Device

After you have successfully installed and configured your D-Link Router, you are ready to enjoy the benefits of D-Link's USB sharing technology. This allows you to quickly and easily share a USB storage device with multiple computers on your network.

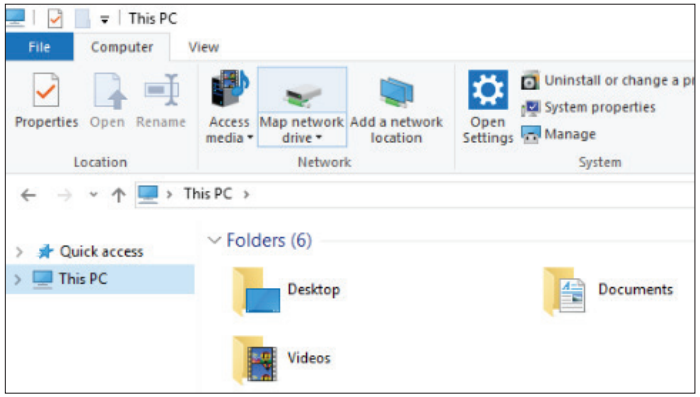
The DSL-X1852E will share a FAT32 or NTFS-formatted USB storage device using the Samba file sharing protocol. Once connected, you can copy, move, delete, and edit files over the network like you would with any ordinary drive attached to your computer. First, connect a USB storage device to the USB Port on the DSL-X1852E.

Connecting from a Windows-Based PC

It is required that all of your devices are connected to the same wireless network as the DSL-X1852E.



Step 1 - Press the Windows logo key ⊞ + E to open **File Explorer**.

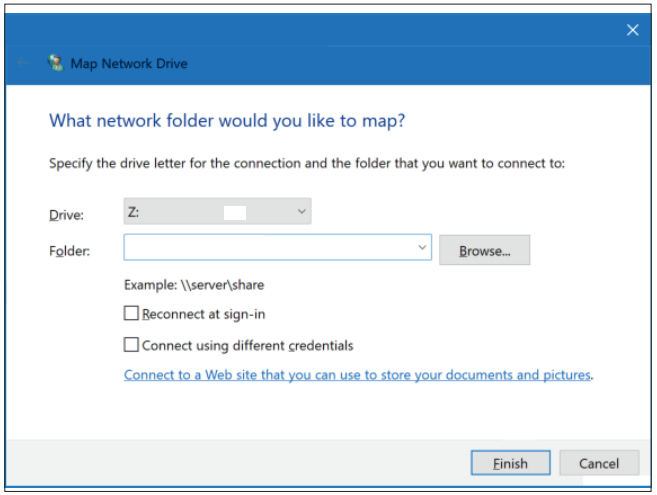


Step 2 - Select **This PC** from the left pane. Then, on the **Computer** tab, select **Map network drive**. On Windows 11, select **More ....** and select **Map network drive** at the top.

Step 3 - Select the drive letter you wish to map your network drive to. In the **Folder** box, enter the DSL-X1852E's IP address (or the NetBIOS name) and the name of the USB volume, for example, **\\192.168.1.1\usb1_1**. You may also click **Browse...** to locate the networked device and mapped drive.

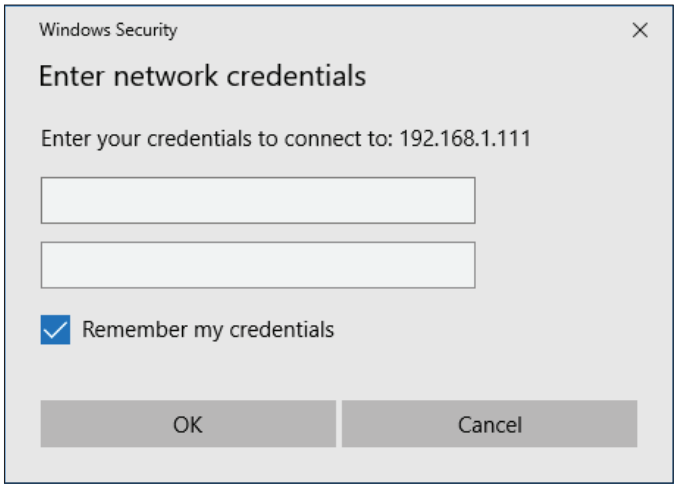
Check the boxes **Reconnect at Sing-in (**if you want to connect every time you sign in to your PC) and **Connect using different credentials.**

Click **Finish**.

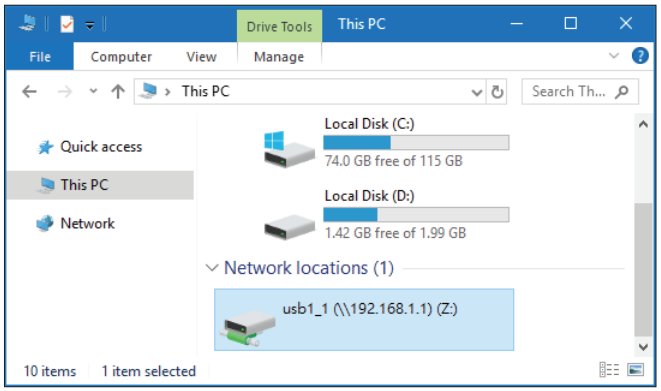


If you have multiple USB storage devices attached via a **USB hub**, click **USB Device** from the **Home** page of the DSL-X1852E's Web Configuration utility for a list of available volume names.

Step 4 - Enter the username and the password to connect to the router and click **OK**. Also check the **Remember my credentials** box. The credentials can be found on the USB settings page (refer to **Settings > USB**).



Congratulations! Your files are now shared. The new network drive can be found in your File Explorer. You can access it without having to type its network name each time. Repeat this process from each Windows PC you wish to share your USB drive with.



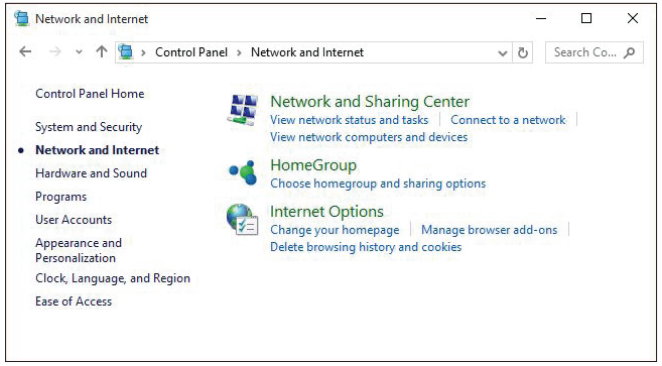
Connect and Share with DLNA Devices

The DSL-X1852E can also stream media files using Digital Living Network Alliance (DLNA). With other DLNA-enabled devices, you can share photos, music, and videos stored in the USB drive with other computers and devices on your network . Connect a USB storage device to the USB Port on the DSL-X1852E first.

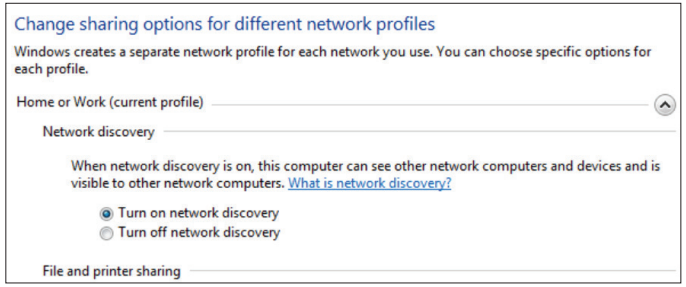
Accessing from File Explorer on Windows

Note: It is required that all of your devices are connected to the same wireless network as the DSL-X1852E.

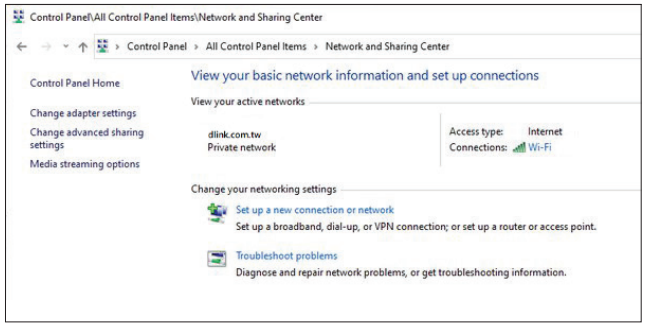
Step 1 - Enable network discovery on Windows:
Go to **Control Panel > Network and Internet > Network and Sharing Center** and select **Change advanced sharing settings** on the left.



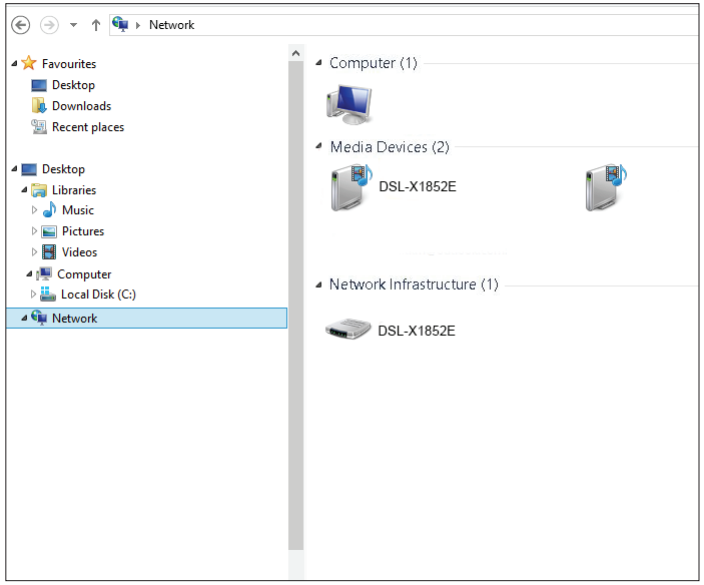
Step 2 - Network sharing settings can be configured differently for different network profiles. Select **Turn on network discovery** for your **private network** or choose the desired network. Also select **Turn on automatic setup of network connected devices**.



Step 3 - Enable media streaming:
Go back to the previous menu and select **Media streaming options**. Click **Turn on media streaming** if it says that Media streaming is not turned on.



Step 4- Click **Network** to list connected network devices on your network in your File Explorer.



Step 5 - Double-click your **DSL-X1852E** listed under **Media Devices.** The Windows Media Player will start automatically. You can then browse your shared media under Other Libraries and play them directly.

Connect a Wireless Client to Your Router

WPS Button

The easiest way to connect your wireless devices to the router is with WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras have a WPS button (or a software utility with WPS) that you can press to connect to the DSL-X1852E. 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-X1852E for about 5 seconds. The WPS LED on the front panel 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 WPS LED stops blinking, you will be connected using WPA2 encryption.

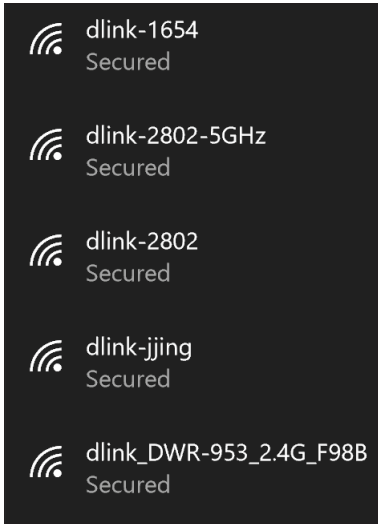
Windows® 11/10
WPA/WPA2/WPA3

When connecting to the DSL-X1852E 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 on the bottom of the device for the default Wi-Fi network SSID and password or enter the Wi-Fi credentials set during the product configuration.

Note: To enjoy the benefits offered by Wi-Fi 6 and WPA3, please make sure that your operating system and wireless network adapter support Wi-Fi 6.

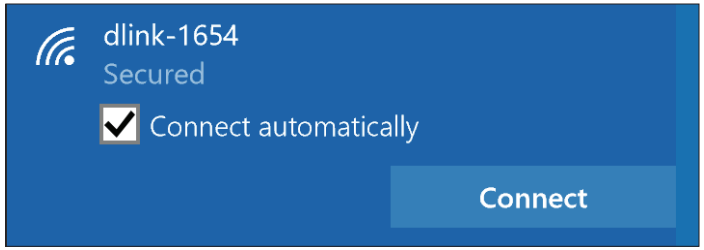
To join an existing network, locate the wireless network icon in the taskbar, next to the time display and click on it.

Clicking on the Network icon , , or to enable Wi-Fi to display a list of wireless networks which are within the range of your computer. Select the desired network by clicking on the SSID.



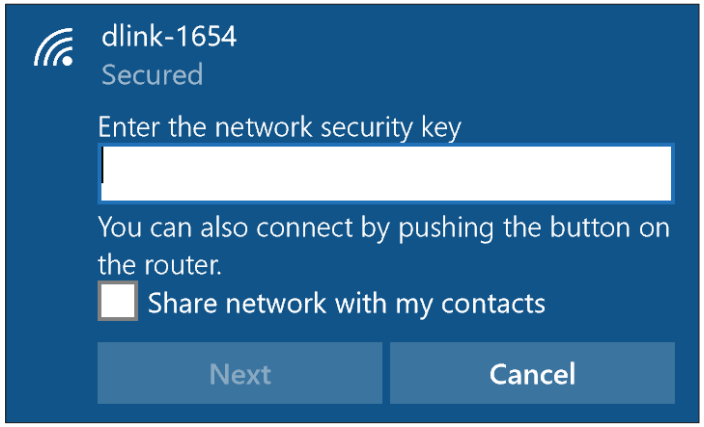
To connect to the SSID, click **Connect.**

To automatically connect with the router when your device next 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 router and you will be automatically connected.

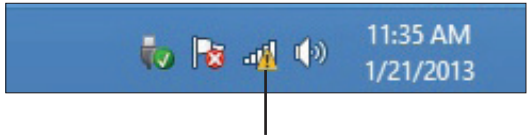


Windows® 8

WPA/WPA2

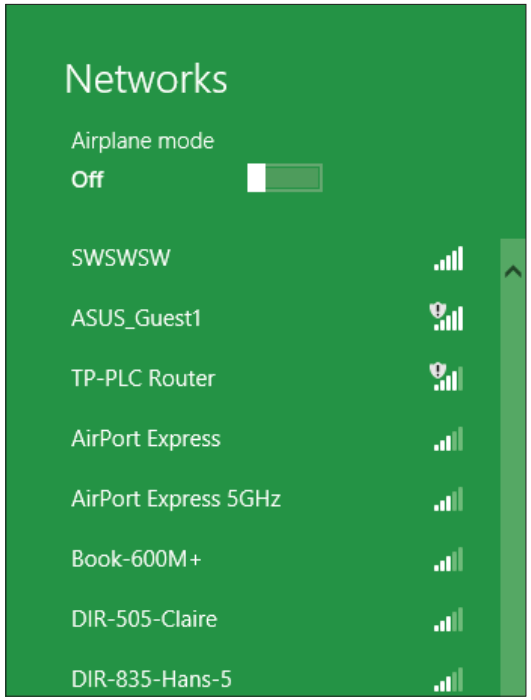
Please configure the wireless security (WPA/WPA2) method on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password).

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



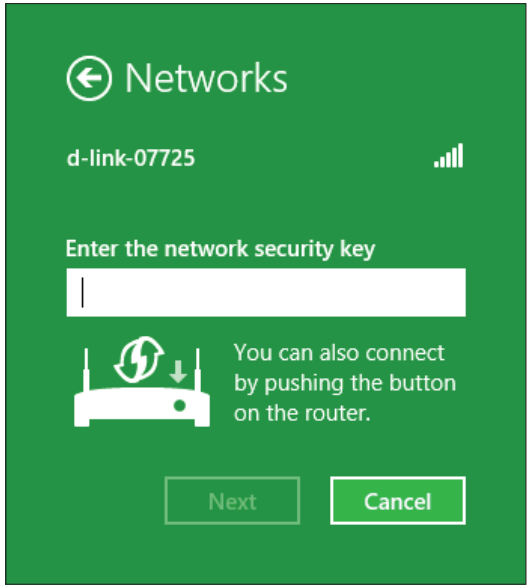
Wireless Icon

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.

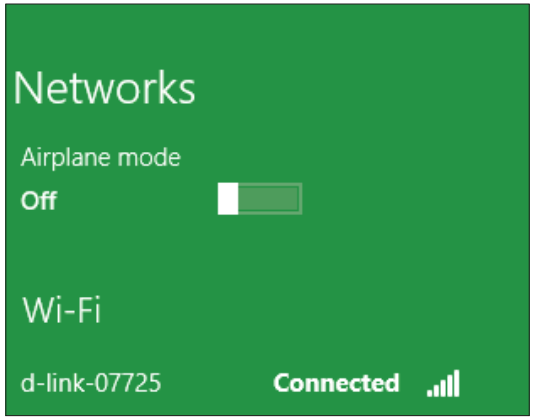


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

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

Please configure the wireless security (WPA/WPA2) method 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.

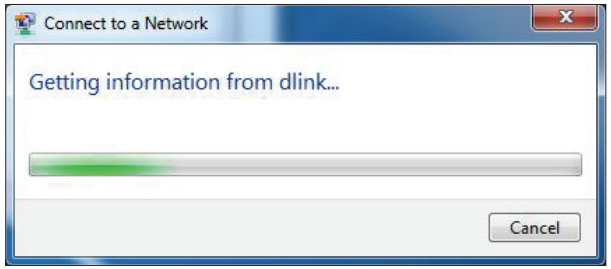
1. Click on the wireless icon in your system tray (lower-right corner).

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

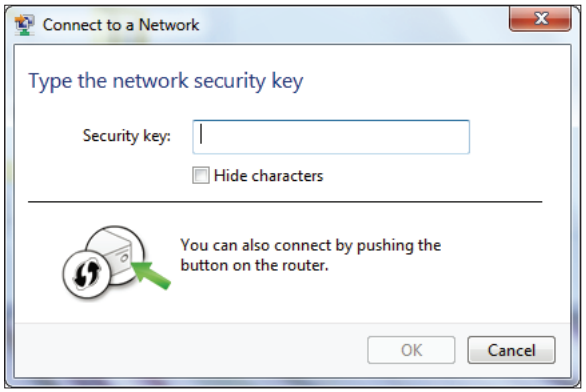
3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

   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 **OK**. 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.



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DSL-X1852E. 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/Edge
  - Mozilla® Firefox 23 or higher
  - Google™ Chrome 28 or higher
  - Apple® Safari 7 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 and Norton Personal 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.

- Access the web configuration. 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 configuration.

- 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 5 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, enter the admin password shown on device label attached to the bottom of the device.

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 encrypted 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**.

or

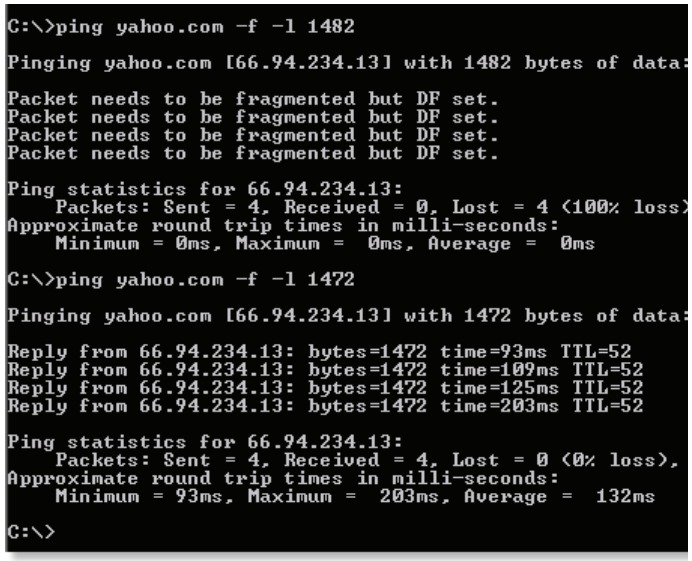
- Click on **Start** and type *cmd* in the **Search** box.

- Once Command Prompt opens, you'll need type the ping command with parameters. Use the following syntax:

ping [url] [-f] [-l] [MTU value]

Example: **ping yahoo.com -f -l 1472**

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



```
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:\>
```

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 the admin password (default device password is on the device label). Click **OK** to enter the web configuration page for the device.
- Go to **Settings > Internet.** Then select the **Service Number** of your WAN connection. Choose the **Advanced Settings**.
- To change the **MTU**, enter the number in the MTU field and click **Save** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

4. The phone cannot make external calls using VoIP.

Check to see if the phone's line is registered. Follow follow the steps below:

- Open your web browser and log in to the web configuration page.
- Go to **Features>VoIP** and scroll down to the **Line Configuration** section.
- Verify if the line (VoIP1/2)'s Registration Status displays "registered" which indicates successful registration. If the Registration Status displays "Disable", "Fault", or "Unreached Network", make sure VoIP Basic settings are correctly entered and also check your internet connectivity. The VoIP settings should be supplied by your Internet telephony service provider.

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

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

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

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

What is Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

Who uses wireless?

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

Home Uses/Benefits

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

Small Office and Home Office Uses/Benefits

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

Where is wireless used?

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

Using a D-Link USB 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.

Encryption

Don't let your next-door neighbors or intruders connect to your wireless network. Encrypt your wireless network by turning on the latest WPA3 encryption on the router. Refer to the previous sections for detail information on how to set it up.

Networking Basics

Check your IP address

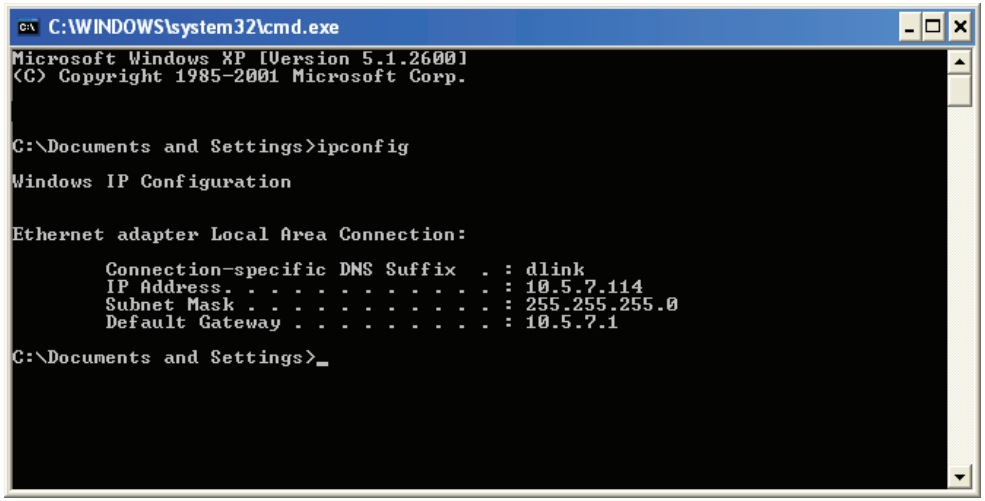
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start** and type *cmd* in the **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

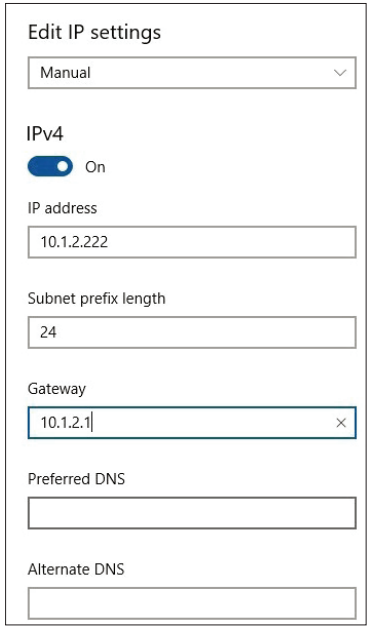
1. If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Windows® 11/10	Start> Settings > Network & Internet.
Windows® 7 /8	Start > Control Panel > Network and Internet > Network and Sharing Center
Windows® XP	Start > Control Panel > Network Connections

2. Select **Wi-Fi > Manage known networks**. For Windows 7/8/XP, click **Change adapter settings.** Choose the network you want to modify, right-click on it, then select **Properties.**

3. Under **IP assignment**, select **Edit**. For Windows 7/8/XP, Select the **Networking** tab. Under **This connection uses the following items**, select **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**. Then select **Use the Following IP Address**.

4. Under **Edit network IP settings** or **Edit IP settings**, select **Manual**. If IPv4 is selected, type the IP address settings in **IP address, Subnet prefix length** (subnet mask), and **Gateway** fields. If IPv6 is selected, type the IP address settings in **IP address, Subnet prefix length,** and **Gateway** fields. The prefix-length in IPv6 has the same function as the subnet mask in IPv4: determine the subnetwork. However, it is expressed as an integer between 1 through 128 as opposed to four octets in IPv4.



Example: Enter x.x.x.x for IPv4 addressing scheme (where x is between 0 and 255) and xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx for IPv6 addressing scheme (where x is a hexadecimal digit).

Set Preferred DNS the same as the LAN IP address of your router.
The Alternate DNS is only optional or you may enter a DNS server from your ISP.

5. When you're done, click **Save**.

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DSL-X1852E offers the following types of security:

- WPA2/WPA with 802.1x (Wi-Fi Protected Access 2)
- WEP (Wired Equivalent Privacy)
- WPA3-SAE/WPA2-PSK/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). WPA has 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/WPA3-SAE uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. This key must be the exact same key entered on your wireless router or access point. Further, the Simultaneous Authentication of Equals (SAE) of WPA3 enhances the protection against dictionary attacks. WPA3-SAE has the strongest encryption among these with the increased cryptographic capability and the requirements of the Protected Management Frames (PMFs) to help prevent snooping attacks.

The WPA2/WPA with 802.1x option features WPA2/WPA used in coordination with a RADIUS server for user authentication in an organization or enterprise environment. The exchange of authentication information between wireless clients and a RADIUS server employs Extensible Authentication Protocol (EAP).

Technical Specifications

Device Interfaces
- One RJ-11 DSL port
- 802.11ax[1]/ac/n/g/b/a[2] Wireless LAN
- One Gigabit Ethernet WAN port
- Four Gigabit Ethernet LAN ports
- One USB 3.0 port
- Two FXS VoIP ports

Standards
- IEEE 802.11ax[1]/ac/n/g/b/k/v/a
- IEEE 802.3/u/az/x

ADSL Standards
- G.dmt/G.lite/G.hs/VBR, CBR, UBR
- ITU-T G.992.5/ G.992.3/ G.992.2/ G992.1

VDSL Standards
- ITU-T G.993.5
- Profile 8a/8b/12a/12b/17a/30a/35b

VoIP Functions
- Call rules, speed dial, call blocking, country code selection, logs
- G.711u law, G.711a law, G.722, G.723, G.729

Antenna Types
- Four external dual-band antennas

Wireless Signal Rate[3]
- 2.4 GHz up to 600 Mbps[2]
- 5 GHz up to 1200 Mbps[2]

Security
- WEP-128Bit/64Bit
- WPA3™-Personal
- WPA™ - Personal/Enterprise
- WPA2™ - Personal/Enterprise
- Wi-Fi Protected Setup (WPS)

Power
- Input: 100 to 240 V AC, 50/60 Hz
- Output: 12 V DC, 2 A

Operating Temperature
- 5 to 40 °C (41 to 104 °F)

Storage Temperature
- -20 to 70 °C (-4 to 158 °F)

Operating Humidity
- 10% to 90% maximum (non-condensing)

Storage Humidity
- 5% to 95% maximum (non-condensing)

Certifications
- CE
- RCM
- Telepermit

Dimensions
- 251.64 mm (9.90 inches)
- 166.47 mm (6.55 inches)
- 194.18 mm (7.64 inches)

Weight
- 485.6 grams (1.073 pounds)

Notes:
1. The DSL-X1852E may not support all of the mandatory features, established in Wave 1 of the IEEE 802.11ax specifications.
2. Maximum wireless signal rate derived from IEEE Standard 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax 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.
3. Frequency Range varies depending on country's regulation.

Regulatory Statements

CE

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

European Community Declaration of Conformity:

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

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

Íslenska [Icelandic]	Hér með lýsir D-Link Corporation því yfir að þessi vara, fylgihlutir og hugbúnaður eru í samræmi við tilskipun 2014/53/EB. Sækja má ESB-samræmisyfirlýsinguna í heild sinni og fastbúnað vörunnar af vefsíðu vörunnar á www.dlink.com.
Norsk [Norwegian]	Herved erklærer D-Link Corporation at dette produktet, tilbehøret og programvaren er i samsvar med direktivet 2014/53/EU. Den fullstendige teksten i EU-erklæring om samsvar og produktets fastvare er tilgjengelig for nedlasting fra produktsiden på www.dlink.com.

Warning Statement:

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

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

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

Usage Notes:

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

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

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

Gebrauchshinweise:

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

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

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

Notes d'utilisation:

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

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

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

Notas de uso:

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

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

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

Note per l'uso

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

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

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

Gebruiksaanwijzingen:

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

SAFETY INSTRUCTIONS

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

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

SICHERHEITSVORSCHRIFTEN

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

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

CONSIGNES DE SÉCURITÉ

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

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

INSTRUCCIONES DE SEGURIDAD

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

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

ISTRUZIONI PER LA SICUREZZA

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

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

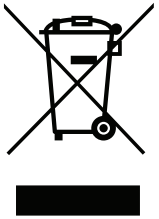
VEILIGHEIDSINFORMATIE

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

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

Disposing and Recycling Your Product

ENGLISH EN



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

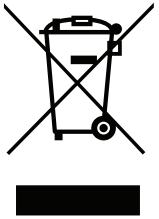
D-Link and the Environment

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

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

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

DEUTSCH DE



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

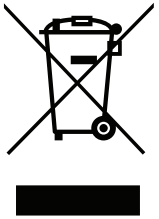
D-Link und die Umwelt

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

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

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

FRANÇAIS FR



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

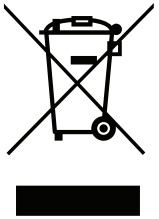
D-Link et l'environnement

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

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

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

ESPAÑOL ES



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

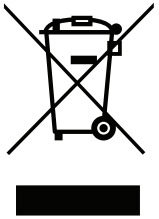
D-Link y el medio ambiente

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

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

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

ITALIANO IT



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

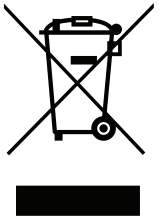
D-Link e l'ambiente

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

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

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

NEDERLANDS NL



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

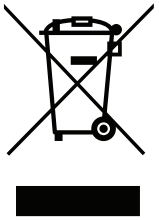
D-Link en het milieu

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

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

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

POLSKI PL



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

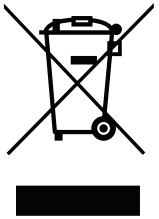
D-Link i środowisko

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

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

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

ČESKY CZ



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

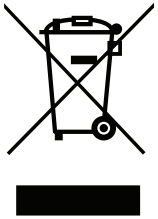
D-Link a životní prostředí

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

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

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

MAGYAR HU



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

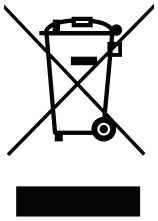
A D-Link és a környezet

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

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

Környezetbarát termékeinkről és csomagolásainkról további információkat a **www.dlinkgreen.com** weboldalon tudhat meg.

NORSK NO



Dette symbolet på produktet eller forpakningen betyr at dette produktet ifølge lokale lover og forskrifter ikke skal kastes sammen med husholdningsavfall, men leveres inn til gjenvinning. Vennligst ta det til et innsamlingssted anvist av lokale myndigheter når det er kommet til slutten av levetiden. Noen steder aksepteres produkter uten avgift. Ved på denne måten å gjenvinne produktet og forpakningen hjelper du å verne miljøet og beskytte folks helse.

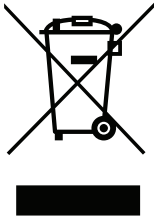
D-Link og miljøet

Hos D-Link forstår vi oss på og er forpliktet til å minske innvirkningen som vår drift og våre produkter kan ha på miljøet. For å minimalisere denne innvirkningen designer og lager D-Link produkter som er så miljøvennlig som mulig, ved å bruke resirkulerbare, lav-toksiske materialer både i produktene og forpakningen.

D-Link anbefaler at du alltid slår av eller frakobler D-Link-produkter når de ikke er i bruk. Ved å gjøre dette hjelper du å spare energi og å redusere CO2-utslipp.

For mer informasjon angående våre miljøansvarlige produkter og forpakninger kan du gå til **www.dlinkgreen.com**.

DANSK DK



Dette symbol på produktet eller emballagen betyder, at dette produkt i henhold til lokale love og regler ikke må bortskaffes som husholdningsaffald, mens skal sendes til genbrug. Indlever produktet til et indsamlingssted som angivet af de lokale myndigheder, når det er nået til slutningen af dets levetid. I nogle tilfælde vil produktet blive modtaget gratis. Ved at indlevere produktet og dets emballage til genbrug på denne måde bidrager du til at beskytte miljøet og den menneskelige sundhed.

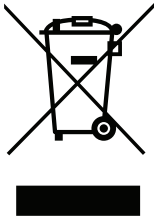
D-Link og miljøet

Hos D-Link forstår vi og bestræber os på at reducere enhver indvirkning, som vores aktiviteter og produkter kan have på miljøet. For at minimere denne indvirkning designer og producerer D-Link sine produkter, så de er så miljøvenlige som muligt, ved at bruge genanvendelige materialer med lavt giftighedsniveau i både produkter og emballage.

D-Link anbefaler, at du altid slukker eller frakobler dine D-Link-produkter, når de ikke er i brug. Ved at gøre det bidrager du til at spare energi og reducere CO2-udledningerne.

Du kan finde flere oplysninger om vores miljømæssigt ansvarlige produkter og emballage på **www.dlinkgreen.com**.

SUOMI FI



Tämä symboli tuotteen pakkauksessa tarkoittaa, että paikallisten lakien ja säännösten mukaisesti tätä tuotetta ei pidä hävittää yleisen kotitalousjätteen seassa vaan se tulee toimittaa kierrätettäväksi. Kun tuote on elinkaarensa päässä, toimita se lähimpään viranomaisten hyväksymään kierrätyspisteeseen. Kierrättämällä käytetyn tuotteen ja sen pakkauksen autat tukemaan sekä ympäristön että ihmisten terveyttä ja hyvinvointia.

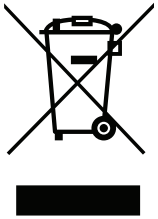
D-Link ja ympäristö

D-Link ymmärtää ympäristönsuojelun tärkeyden ja on sitoutunut vähentämään tuotteistaan ja niiden valmistuksesta ympäristölle mahdollisesti aiheutuvia haittavaikutuksia. Nämä negatiiviset vaikutukset minimoidakseen D-Link suunnittelee ja valmistaa tuotteensa mahdollisimman ympäristöystävällisiksi käyttämällä kierrätettäviä, alhaisia pitoisuuksia haitallisia aineita sisältäviä materiaaleja sekä tuotteissaan että niiden pakkauksissa.

Suosittelemme, että irrotat D-Link-tuotteesi virtalähteestä tai sammutat ne aina, kun ne eivät ole käytössä. Toimimalla näin autat säästämään energiaa ja vähentämään hiilidioksiidipäästöjä.

Lue lisää ympäristöystävällisistä D-Link-tuotteista ja pakkauksistamme osoitteesta **www.dlinkgreen.com**.

SVENSKA SE



Den här symbolen på produkten eller förpackningen betyder att produkten enligt lokala lagar och föreskrifter inte skall kastas i hushållssoporna utan i stället återvinnas. Ta den vid slutet av dess livslängd till en av din lokala myndighet utsedd uppsamlingsplats, vissa accepterar produkter utan kostnad. Genom att på detta sätt återvinna produkten och förpackningen hjälper du till att bevara miljön och skydda människors hälsa.

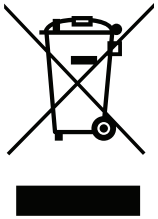
D-Link och miljön

På D-Link förstår vi och är fast beslutna att minska den påverkan våra verksamheter och produkter kan ha på miljön. För att minska denna påverkan utformar och bygger D-Link sina produkter för att de ska vara så miljövänliga som möjligt, genom att använda återvinningsbara material med låg gifthalt i både produkter och förpackningar.

D-Link rekommenderar att du alltid stänger av eller kopplar ur dina D-Link produkter när du inte använder dem. Genom att göra detta hjälper du till att spara energi och minska utsläpp av koldioxid.

För mer information om våra miljöansvariga produkter och förpackningar **www.dlinkgreen.com**.

PORTUGUÊS PT



Este símbolo no produto ou embalagem significa que, de acordo com as leis e regulamentações locais, este produto não deverá ser eliminado juntamente com o lixo doméstico mas enviado para a reciclagem. Transporte-o para um ponto de recolha designado pelas suas autoridades locais quando este tiver atingido o fim da sua vida útil, alguns destes pontos aceitam produtos gratuitamente. Ao reciclar o produto e respectiva embalagem desta forma, ajuda a preservar o ambiente e protege a saúde humana.

A D-Link e o ambiente

Na D-Link compreendemos e comprometemo-nos com a redução do impacto que as nossas operações e produtos possam ter no ambiente. Para minimizar este impacto a D-Link concebe e constrói os seus produtos para que estes sejam o mais inofensivos para o ambiente possível, utilizando meteriais recicláveis e não tóxicos tanto nos produtos como nas embalagens.

A D-Link recomenda que desligue os seus produtos D-Link quando estes não se encontrarem em utilização. Com esta acção ajudará a poupar energia e reduzir as emissões de CO2.

Para saber mais sobre os nossos produtos e embalagens responsáveis a nível ambiental visite **www.dlinkgreen.com**.