



User Manual

4G LTE M2M Router

Preface

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

Manual Revisions

Revision	Date	Description
1.00	May 16, 2017	• Initial release

Trademarks

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

Copyright © 2017 by D-Link Corporation.

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

Table of Contents

Product Overview	1	Router Mode.....	19
Package Contents.....	1	LAN	20
System Requirements	1	IPv4	20
Introduction	2	LAN Settings	20
Hardware Overview.....	3	Dynamic Route	21
Front View.....	3	DHCP	22
Top Panel	4	IPv6	23
Rear Panel.....	5	IPv6 Config	23
Installation	6	Internet Connection Type.....	24
Before You Begin.....	6	VPN	25
Attaching the External Antennas.....	7	IPSec	25
Installing the SIM card(s).....	8	VPN Settings	25
Configuration	9	XAUTH Account.....	28
Getting Started.....	9	PPTP.....	29
Internet.....	10	PPTP Server	29
WAN Service	10	PPTP Server	30
Preferred SIM Card.....	10	PPTP Client	31
SIMA/SIMB.....	11	L2TP	33
Network Status	11	L2TP Server	33
APN Settings.....	12	L2TP Client	35
APN Configuration	13	GRE.....	37
Connection Settings	15	Advanced	38
SIM Card Settings.....	16	DNS	38
IPv4 and IPv6 info	17	DNS	38
Device Mode.....	18	DNS Redirect.....	39
		Firewall	40

Outbound Filter	40	Reboot and Reset	64
Inbound Filter.....	41	Reboot the Device	64
URL Filter	42	Connection Reset	65
MAC Address Filter	43	Troubleshooting	66
DMZ	44	Networking Basics	70
QoS.....	45	Check your IP address.....	70
SNMP	46	Statically Assign an IP address	71
Virtual Server	48	Technical Specifications	72
UPnP.....	49	Regulatory Information	74
Network Scan	50		
System	52		
Administration.....	52		
Password Settings	52		
Remote Login Settings	53		
Configuration Backup	54		
SMS	55		
SMS Inbox.....	55		
Compose SMS	56		
Message Settings.....	57		
Time Settings	59		
Firmware Upgrade.....	60		
Device Upgrade.....	60		
Module Upgrade.....	61		
System Log.....	62		
Schedules	63		
Add New Rule.....	63		

Package Contents



DWM-312 4G LTE M2M Router



Power Adapter



2x 3G/4G Antennas



RJ-45 Cable

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

System Requirements

- A compatible micro-SIM/UICC card with service.*
- Computer with Windows, Mac OS, or Linux-based operating system with an installed Ethernet adapter.
- Java-enabled browser such as Internet Explorer 6, Safari 4.0, Chrome 20.0, or Firefox 7 or above (for configuration).

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

Introduction

The D-Link DWM-312 4G LTE M2M Router is an easy-to-deploy, high-performance 3G/4G router. It features a dedicated Fast Ethernet port and dual-SIM 4G LTE mobile broadband for maximum redundancy and flexibility for intense Machine-to-Machine (M2M) applications. Powerful VPN tools and advanced remote management combined with ease of use make the DWM-312 ideal for both large-scale and individual deployments.

Easily connect to your high-speed 3G/4G LTE mobile connection with the DWM-312 4G LTE M2M Router, and enjoy fast downlink speeds of up to 150 Mbps¹ and uplink speeds up to 50 Mbps¹, giving you the speed you need for fast, responsive Internet access. Deploy it in a remote location to access IP cameras and systems remotely. The blazing fast LTE connection allows multiple users to access e-mail and stream music and video on the go. Configurable dual-SIM fallback provides reliability and flexibility in mixed network environments.

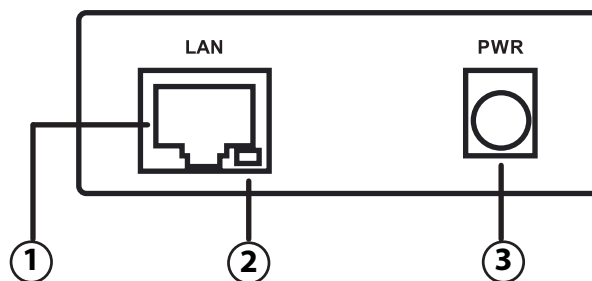
The DWM-312 4G LTE M2M Router's integrated VPN Client and Server support almost any VPN policy. The router's hardware engine can support and manage multiple VPN configurations. It supports IPSec, PPTP, L2TPv2, and GRE protocols in Server mode, and handles pass-through traffic as well. Advanced VPN configuration options include multiple encryption options, key management, negotiation modes, and VPN authentication using an internal user database.

The industrial-grade casing means the DWM-312 provides reliable high-speed connectivity in extreme conditions. The corrosion-resistant zinc-plated steel case and wide operating temperature and humidity tolerance mean that the DWM-312 is ready for the most demanding M2M applications in virtually any environment. Wall mounts allow the DWM-312 to be mounted virtually anywhere for optimal connectivity. Flexible power input allows the router to be powered by any convenient power source.

¹ Data rates are theoretical. Data transfer rate depends on network capacity, signal strength, and environmental factors.

Hardware Overview

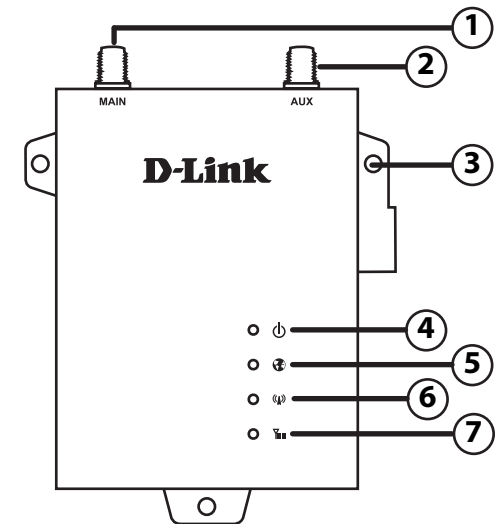
Front View



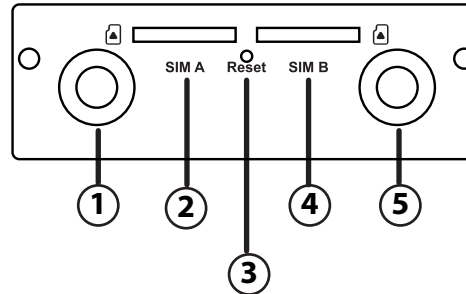
1	Ethernet Port	This is a standard 10/100 Mbps Ethernet port to connect any device via Cat 5/5e/6 RJ-45 cables.
2	Ethernet Activity	Flashes green when there is Ethernet traffic.
3	DC Power Input	5.5 mm barrel connector for power.

Top Panel

1	SMA Connector Main	SMA female connector - Primary antenna.	
2	SMA Connector AUX	SMA female connector - Auxiliary Antenna.	
3	Wall Mounts	Wall mounts for standard 8 gauge (4 mm) screws.	
4	Power	A green LED indicates the DWM-312 is receiving power.	
5	Internet	A green LED indicates Internet connectivity.	
6	Network	Solid Green	Connected to SIM A LTE Network.
		Flashing Green	Fallback to SIM A 3G/2G network.
		Solid Blue	Connected to SIM B LTE Network.
		Flashing Blue	Fallback to SIM B 3G/2G network.
		Off	No Service/SIM Error/APN Error.
7	Signal	Green	Indicates strong signal.
		Amber	Indicates fair signal.
		Red	Indicates weak signal.
		Off	Indicates no signal.



Rear Panel



1	SMA Connector AUX	SMA female connector - Auxiliary Antenna.
2	SIM A	Primary SIM card slot.
3	Reset	Press and hold for 3 seconds to reset.
4	SIM B	Secondary SIM card.
5	SMA Connector Main	SMA female connector - Primary antenna.

Installation

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

Before You Begin

Observe the following precautions to help prevent shutdowns, equipment failures, and personal injury:

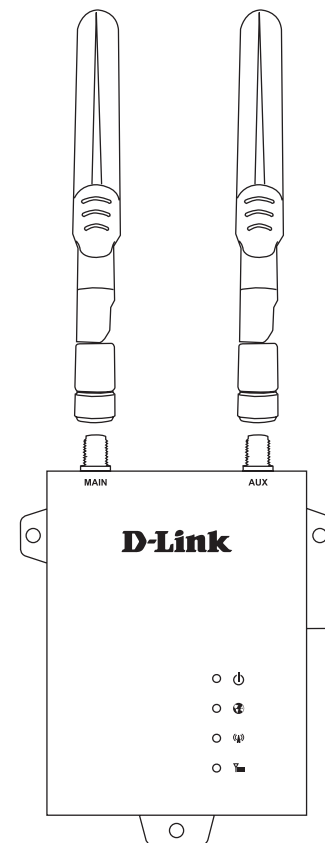
- Install the DWM-312 in a cool and dry place. Refer to the technical specifications in the user manual for the acceptable operating temperature and humidity ranges.
- Install the router in a site free from strong electromagnetic sources, vibration, dust, excessive moisture, and direct sunlight.
- Place antennas in an unobstructed area with clear mobile signal. Avoid metal boxes, brick walls, and other dense materials. It is recommended to use the web interface to confirm signal strength before permanent installation.
- Visually inspect the power connector and make sure that it is fully secure.
- Do not stack any devices on top of the router.

Attaching the External Antennas

The DWM-312 requires two external antennas to function correctly. The included antennas are interchangeable, but third party antennas may require connection to specific ports.

1. Attach the antennas to the SMA connectors labelled "Main" and "Aux" on the back of the router. Turn clockwise to fasten the antenna.
2. Position the router where it will receive optimal signal. Arrange them so they point upward.

Note: The included antennas are interchangeable. Third party antennas may require connection to specific ports.

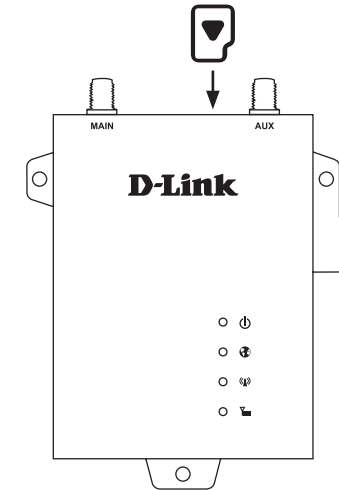


Installing the SIM card(s)

The DWM-312 is equipped with dual-SIM slots. At least one active SIM card with Internet access is required for proper operation.

1. Insert a micro-SIM card into the slot labelled **SIM A** with the contacts facing down. If you wish to install a second SIM card, insert it into the slot labelled **SIM B**.
2. Gently press the micro-SIM into the slot until it locks into place. To remove, press again and the SIM card will be ejected.

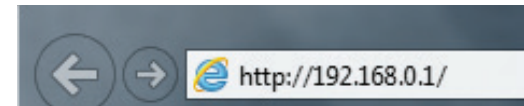
Note: SIM behavior must be configured from the web UI before an Internet connection can be established.



Configuration

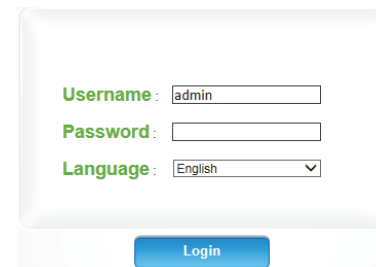
Getting Started

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

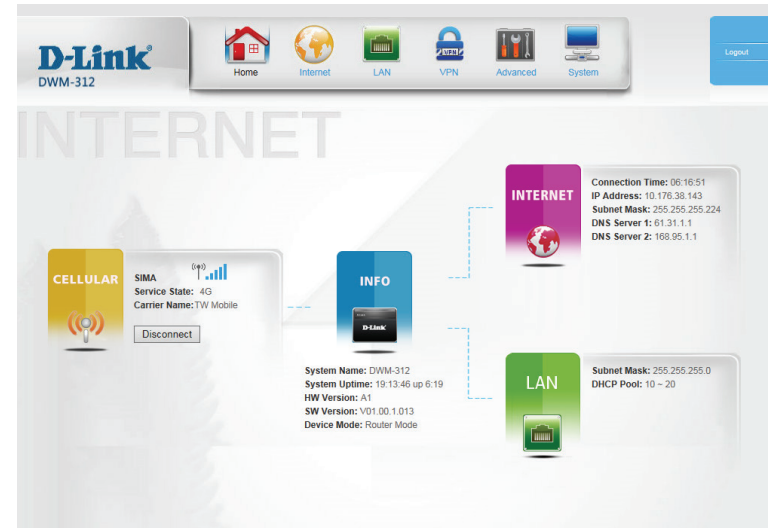


To log in to the configuration utility, enter the default username **admin** and the default password **admin**.

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



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



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

On each page, fill out the desired settings and click **Apply** when you are done or **Refresh** to revert to the old settings.

Internet WAN Service

On this page you can configure your Internet connection. If you are not sure which settings to use, please contact your Internet Service Provider (ISP). Note that the DWM-312 requires a SIM card and active cellular internet service to connect to the Internet.

Preferred SIM Card

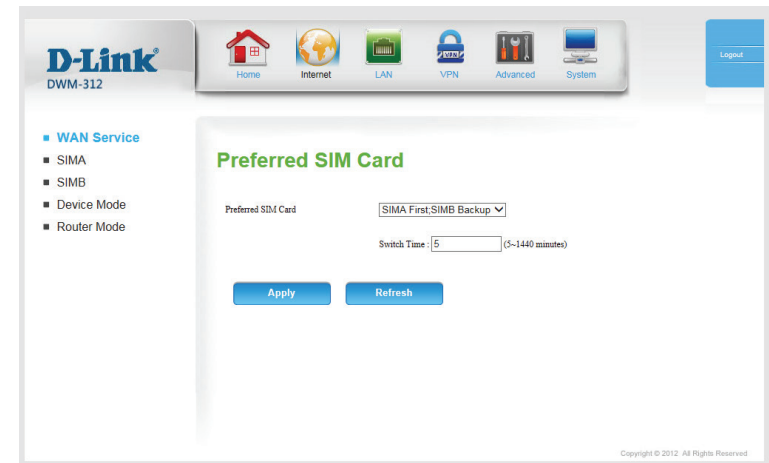
Preferred SIM Card: Select **SIMA**, **SIMB**, **SIMA First**, **SIMB Backup**, or **SIMB First**; **SIMA Card: Backup**.

Selecting a single SIM card, either **SIMA** or **SIMB** will connect over a single SIM only. Selecting a backup option will change cause the connection to switch to the specified backup if the primary SIM cannot connect after the specified time.

Selecting SIM cards will cause the menu options to display according to active SIM cards, either showing **SIMA**, **SIMB**, or **SIMA** and **SIMB**. The configuration options for each are the same.

Switch Time: Select the amount of time in minutes for the router to attempt to reconnect to the primary SIM. If this time elapses, it will automatically switch to the backup.

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



SIMA/SIMB Network Status

Network Provider: Shows the name of the current network provider.

Network Type: Specifies the current network type. Indicates **LTE**, **3G**, or **2G**.

Connection Time: Indicates the amount of time the network has been up.

Signal Strength: Shows cellular signal strength as a percentage.

IP Type: Shows whether the router is assigned an IPv4 or an IPv6 address.

Total DL: Shows total downloaded bytes since last reboot.

Total UL: Shows total uploaded bytes since last reboot.

Profile Name: Indicates the name of the APN profile.

Click **Refresh** to update the page.

The screenshot shows the D-Link DWM-312 web interface. The top navigation bar includes Home, Internet, LAN, VPN, Advanced, and System. The main content area is titled "Network Status" and displays the following information:

Network Provider	TW Mobile
Network Type	LTE
Connection Time	02:44:11
Signal Strength	100 %
IP Type	IPv4
Total DL	159495843 (Bytes)
Total UL	18730106 (Bytes)
Profile Name	internet

A "Refresh" button is located below the table. The left sidebar contains a menu with options: WAN Service, SIMA (selected), SIMB, Device Mode, and Router Mode. Under SIMA, there are sub-options: Network Status (selected), APN Settings, APN Configuration, Connection Settings, SIM Card Settings, and IPv4 and IPv6 info.

APN Settings

Dial Up Profile: Select **Auto-Detection** to have the router automatically detect the settings for your connection. Select **Manual** to enter the details of your connection manually. Select **Selection** to choose several pre-configured profiles, configurable in **APN Configuration** on page 12.

If you select **Manual**, the following options will appear:

Country/ Telecom: Select your country and service provider to automatically fill in some of the required settings.

Username: Fill in only if requested by ISP (optional).

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

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

Dialed Number: Enter the number to be dialed.

Authentication: Select **PAP**, **CHAP**, or **Auto** detection. The default authentication method is **Auto**.

APN: Enter the APN information (optional).

PIN Code: Enter the PIN associated with your SIM card.

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

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

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

The screenshot shows the D-Link DWM-312 web interface. The top navigation bar includes 'Home', 'Internet', 'LAN', 'VPN', 'Advanced', and 'System'. The left sidebar lists 'WAN Service', 'SIMA', 'Network Status', 'APN Settings', 'APN Configuration', 'Connection Settings', 'SIM Card Settings', 'IPv4 and IPv6 info', 'SIMB', 'Device Mode', and 'Router Mode'. The main content area is titled 'SIMA' and shows 'Setting completed'. Under 'APN Settings', the 'Dial-Up Profile' is set to 'Manual'. The 'Country' is 'Taiwan' and 'Telecom' is 'Taiwan Mobile'. There are input fields for 'Username', 'Password', 'Dialed Number', 'Authentication', 'APN', 'PIN Code', 'Primary DNS Server', and 'Secondary DNS Server'. 'Apply' and 'Refresh' buttons are at the bottom.

Copyright © 2012. All Rights Reserved

APN Configuration

Item: This check box allows you to select one or more APN profiles.

Profile Name: Indicates the name of the profile.

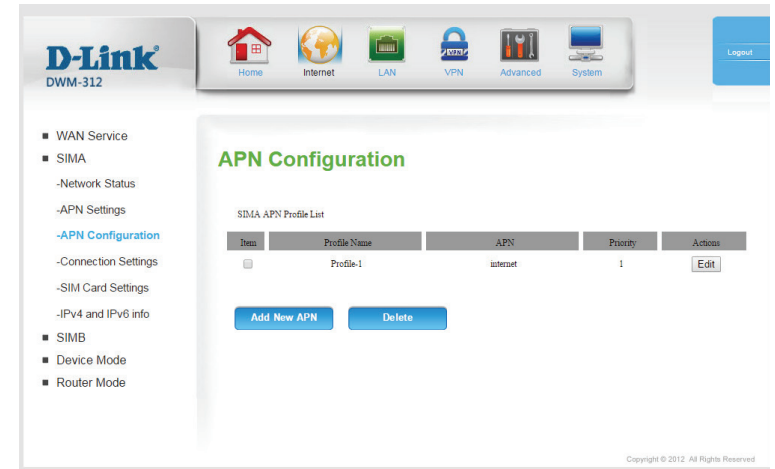
APN: Indicates the access point name (APN) in use by the selected profile.

Priority: APN profiles are prioritized by number. If one profile does not lead to an active internet connection, the router will automatically switch to the next profile in the queue.

Actions: Click **Edit** to edit the corresponding profile, described in **New/Edit APN Profile** on page 13.

Add New APN: Click **Add New APN** to create a new APN, described in **New/Edit APN Profile** on page 13.

Delete: Click **Delete** to all profiles selected in the **Item** column.



New/Edit APN Profile

Profile Name: Enter a name for the profile.

APN: Enter the APN to be used. This information should be provided by your ISP.

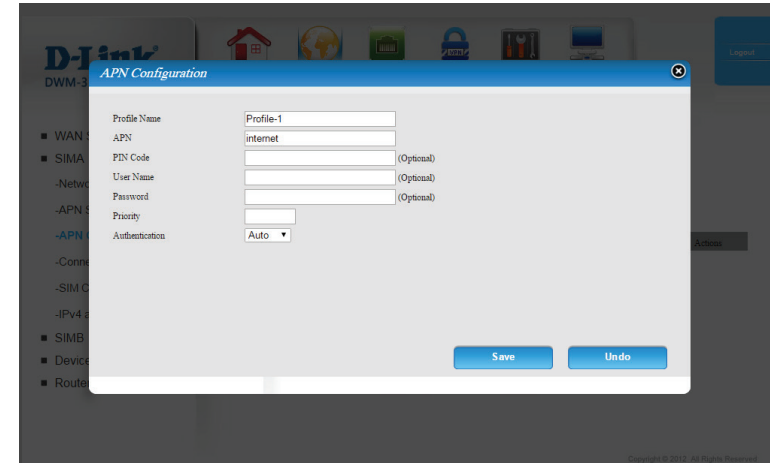
PIN Code: If your SIM uses a PIN, enter it here.

User Name: If your mobile connection requires a username, enter it here.

Password: If your mobile connection requires a password, enter it here.

Priority: Enter a priority between **1** and **4**, with **1** being highest priority and **4** being lowest.

Authentication: Select the authentication type used by your ISP.



Click **Save** to save your settings, or **Undo** to revert to your previous settings.

Connection Settings

Prefer Service Type: Choose whether the DWM-312 should only use 4G networks, 3G networks, 2G networks, or use **Auto Mode** to automatically select a network.

Allow Data Roaming: Enabling this option will allow you to connect when roaming outside your carrier's home coverage.

Note: Roaming connections may incur additional fees from your service provider.

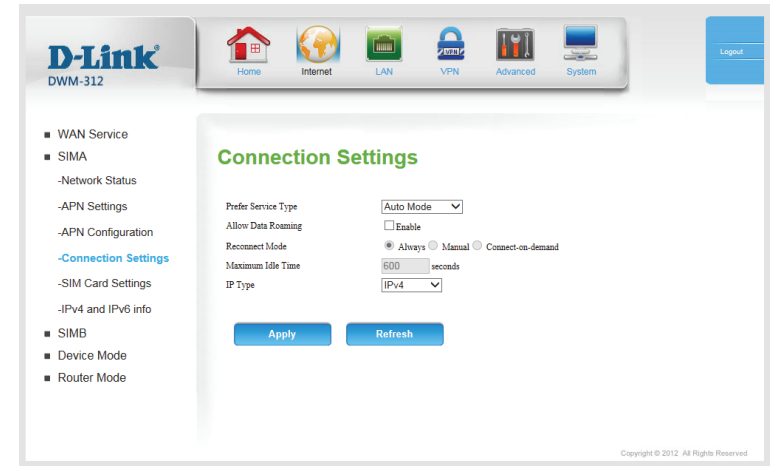
Reconnect Mode: Choose **Always** when you want to establish mobile connection all the time. Choose **Manual** to only connect when you click **Connect** on the home screen. If you choose **Connect-on-demand**, the device will establish a mobile connection when local users want to connect to the Internet, and disconnect if there is no traffic after the time period defined by the **Maximum Idle Time** setting.

Note: These options are only available if **SIMA Only** has been selected in **WAN Service** on page 15.

Maximum Idle Time: If you have chosen **Connect-on-demand**, enter the maximum idle time before disconnection in seconds.

IP Type: Specify **IPv4**, **IPv6**, or **IPv4/IPv6** to determine what type of IP address will be allocated by your ISP. This information should be provided by your ISP.

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



SIM Card Settings

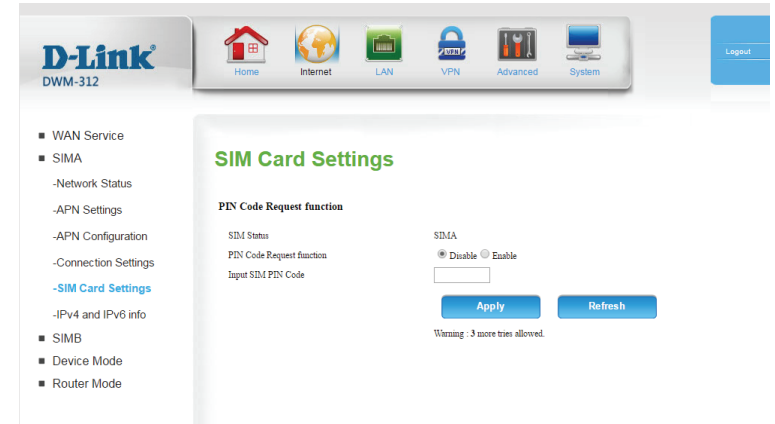
SIM Status: Indicates which SIM is currently active.

PIN Code Request function: Enable this if you wish to set a PIN for your SIM.

Input SIM PIN Code: If you have selected **Enable** for the above feature, enter your new PIN here.

PIN Attempts: Shows the number of attempts remaining before the SIM is locked. SIM cards generally allow three attempts, after which they can only be unlocked by a PUK code provided by the ISP. For information on the configuration of your SIM card, consult your ISP or carrier.

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



IPv4 and IPv6 info

IPv4

IP Address: Shows the IPv4 address of the current SIM card.

Subnet Mask Shows the subnet mark of the current SIM card.

Gateway: Shows the gateway used by the current SIM card.

DNS Server1: Indicates the IP address of the primary DNS server.

DNS Server2: Indicates the IP address of the primary DNS server.

IPv6

IP Address: Shows the IPv4 address of the current SIM card.

Gateway: Shows the gateway used by the current SIM card.

DNS Server1: Indicates the IP address of the primary DNS server.

DNS Server2: Indicates the IP address of the primary DNS server.

Click **Refresh** to update this page.

The screenshot displays the D-Link DWM-312 web interface. The top navigation bar includes icons for Home, Internet, LAN, VPN, Advanced, and System. The main content area is titled "WAN IPv4 And IPv6 Address Info". On the left, a sidebar menu lists various settings including WAN Service, SIMA, SIMB, Device Mode, and Router Mode. The main content area shows the following information:

IPv4	
IP Address	100.71.25.26
Subnet Mask	255.255.255.252
Gateway	100.71.25.25
DNS Server1	61.31.1.1
DNS Server2	168.95.1.1

IPv6	
IP Address	13
Gateway	0000:0000:0000:0000:0000:0000:0000:0000
DNS Server1	0000:0000:0000:0000:0000:0000:0000:0000
DNS Server2	0000:0000:0000:0000:0000:0000:0000:0000

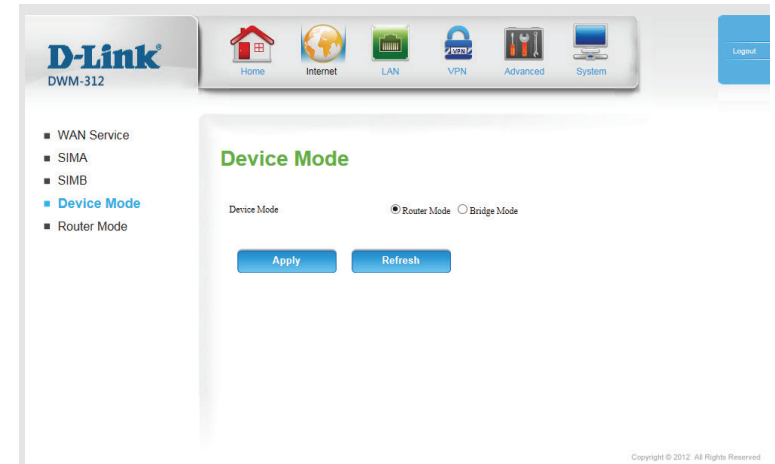
At the bottom of the main content area, there is a "Refresh" button. The footer of the page contains the text "Copyright © 2012. All Rights Reserved".

Device Mode

Device Mode: **Router Mode** is the default mode, which enables NAT and DHCP. In this configuration, the DWM-312 gets an IP from the ISP, and then creates its own subnet with a private IP range.

Bridge Mode disables all DHCP, NAT, and routing functions. In this mode, the DWM-312 acts as a simple modem, and IPs are assigned directly by the ISP.

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



Router Mode

NAT: Select **NAT** or **Classical**. The **Classical** option disables the NAT firewall.

Enable: Select **Enable** to enable WAN keep alive. This may be useful if your provider automatically disconnects you after an idle period.

DNS Query / ICMP Checking: Specify the method for keep-alive. Choose between **DNS Query** or **ICMP Checking**.

Check Incoming/Outgoing packet: This option cannot be changed.

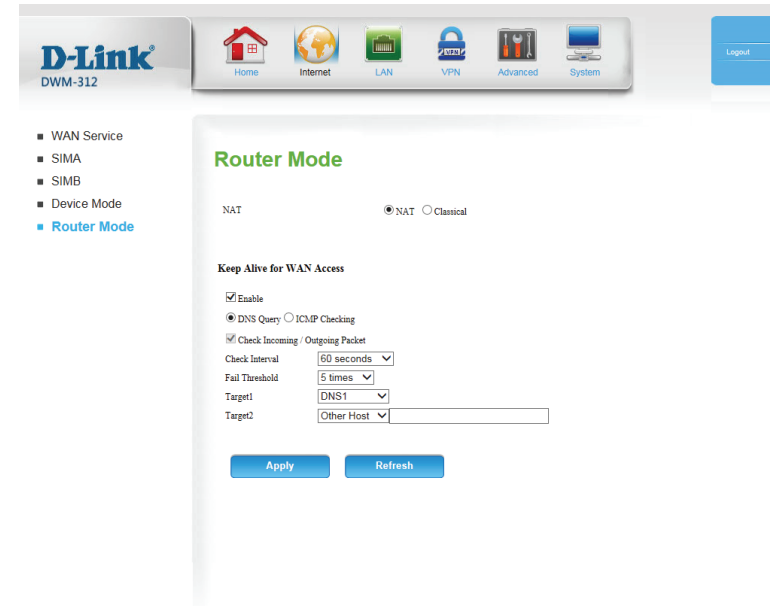
Check interval: Select either **60 seconds** or **120 seconds** to set the interval at which the router will check for a connection.

Fail Threshold: The **Failure Threshold** specifies the number of retries before the WAN is assumed to be down.

Target 1: Specify a target of the DNS queries or ICMP checks. Options include **DNS1**, **DNS2**, **Gateway**, **NTP Server** which automatically use this information from other settings, or you can manually specify an address after selecting **Other Host**. The default is **DNS1**.

Target 2: In addition to the options available for **Target1**, you can also select **None** to use only the host selected in **Target1**.

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



Copyright © 2012. All Rights Reserved.

LAN

This section allows you to change the local network settings of your router and to configure the DHCP Server settings. **IPv4** and **IPv6** are configured separately.

IPv4 LAN Settings

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

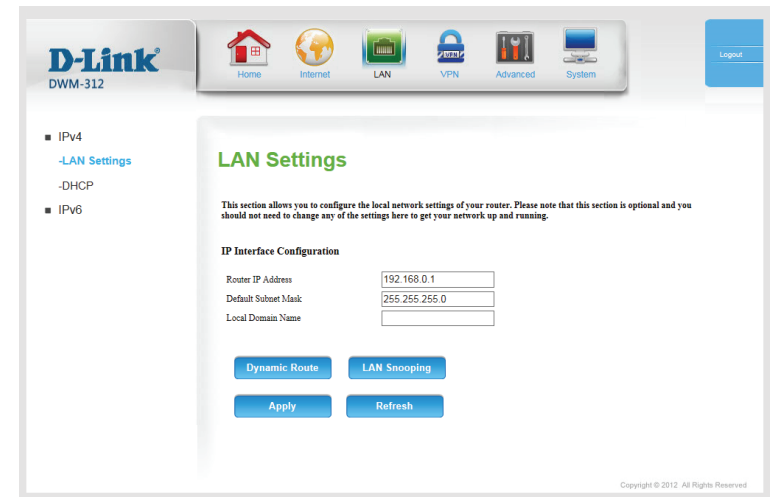
Default Subnet Mask: Enter the subnet mask of the router. The default subnet mask is **255.255.255.0**.

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

Dynamic Route: Click this to configure the Router Information Protocol (RIP), described on the following page.

LAN Snooping: Click this to toggle LAN snooping, described on the following page.

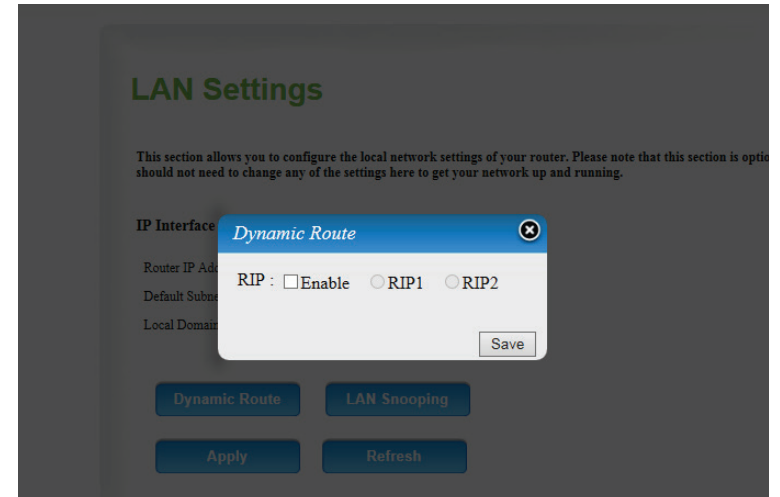
Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



Dynamic Route

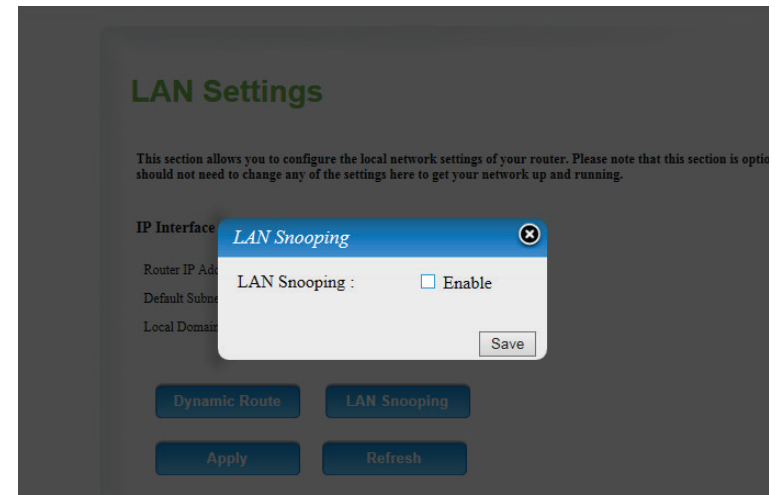
RIP: Click **Enable** to toggle the Router Identification Protocol (RIP). If enabled, choose **RIP1** or **RIP2**.

Click **Save** to save your settings, or the X button to revert to your previous settings.



LAN Snooping: Check **Enable** to enable LAN snooping.

Click **Save** to save your settings, or the X button to revert to your previous settings.



DHCP

The DWM-312 has a built-in DHCP (Dynamic Host Configuration Protocol) server. The DHCP server assigns IP addresses to devices on the network that request them. By default, the DHCP server is enabled on the device. The DHCP address pool contains a range of IP addresses, which are automatically assigned to the clients on the network.

Enable DHCP Server: Select this box to enable the DHCP server on your router.

DHCP IP Address Range: Enter the range of IPs for the DHCP server to use to assign IP addresses to devices on your network. These values will represent the last octet of the IP addresses in the pool.

DHCP Lease Time: Enter the lease time for IP address assignments.

Primary DNS IP Address: Enter the primary DNS IP address that will be assigned to DHCP clients.

Secondary DNS IP Address: Enter the secondary DNS IP address that will be assigned to DHCP clients.

Static IP Setting: Click **Static IP Setting** to assign a dedicated IP to a specified MAC address to be saved by the DHCP server.

Select a DHCP client and click **Copy to**, or enter the MAC address and IP address manually, to assign the IP address to the MAC address. Click **Enable** to enable the rule.

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

D-Link DWM-312

Home Internet LAN VPN Advanced System Logout

- IPv4
 - LAN Settings
 - DHCP
 - IPv6

DHCP

DHCP Server Configuration

Enable DHCP Server:

DHCP IP Address Range: 10 to 20 (addresses within the LAN subnet)

DHCP Lease Time: 604800 (seconds)

Primary DNS IP Address:

Secondary DNS IP Address:

Static IP setting

Apply Refresh

D-Link DWM-312

Home Internet LAN VPN Advanced System Logout

- IPv4
 - LAN Settings
 - DHCP
 - IPv6

Static IP Setting

DHCP clients: -- Select one -- ID: -- --

ID	MAC Address	IP Address	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Previous page

Apply Refresh

IPv6 IPv6 Config

IPv6: Select **Enable** to enable IPv6, otherwise select **Disable**.

IPv6 settings are configured on the next page.

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



Internet Connection Type

The DWM-312 supports both SLAAC and DHCP IPv6 configuration options. Which one is used will depend on your service provider and network configuration.

LAN Assigned Type: Select **DHCPv6**, **SLAAC+Stateless DHCP** or **SLAAC+RDNSS**.

If you selected **DHCPv6**, the following options will appear:

IPv6 Address Range(Start): Enter the starting IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Range (End): Enter the ending IPv6 address for the DHCP server's IPv6 assignment.

IPv6 Address Lifetime: Enter the IPv6 address lifetime (in seconds).

The screenshot shows the D-Link DWM-312 web interface. The main navigation bar includes Home, Internet, LAN, VPN, Advanced, and System. The left sidebar shows a tree view with IPv4, IPv6, and IPv6 Config. The 'IPv6 Config' section is expanded to show 'Internet Connection type'. The main content area is titled 'Internet Connection Type' and contains the following fields:

- LAN Assigned Type:
- IPv6 Address Range(Start):
- IPv6 Address Range(End):
- IPv6 Address Lifetime: seconds

At the bottom of the form are two buttons: 'Apply' and 'Refresh'.

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

VPN

The DWM-312 supports a number of virtual private network (VPN) protocols. VPNs are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin authentication, and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms. Supported protocols as a client include: IPSec, PPTP, L2TP, and GRE. Supported protocols as a server include PPTP and L2TP.

IPSec VPN Settings

VPN-IPSEC: Tick this box to enable the IPSec VPN function.

Netbios over IPSEC: Tick this box to receive Netbios from Network Neighborhood.

NAT Traversal: Some NAT routers and ISPs will block IPSec packets if they don't support IPSec passthrough. If you connect to another NAT router which doesn't support IPSec passthrough on the WAN side, you need to activate this option.

Dyanmic VPN: Tick this box to enable this feature and click **More** to configure VPN Dynamic IP on a separate page. Please see the next page for more details.

Tunnel Settings: Tunnel details are displayed here. Click **More** to configure a new tunnel or click **Disconnect** to disconnect from an existing tunnel. Select the **Enable** checkbox to activate this rule. In tunnel settings page, you can click **More** under **Action** for detailed tunnel settings.

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

The screenshot shows the D-Link DWM-312 VPN Settings page. The navigation menu includes Home, Internet, LAN, VPN, Advanced, and System. The main content area is titled "VPN Settings" and includes the following sections:

- VPN Settings:**
 - VPN-IPSEC: Enabled
 - Netbios over IPSEC: Enabled
 - NAT Traversal: Enabled
- Dynamic VPN Setting:**
 - VPN Dynamic IP Setting: Enable [More](#)
- Tunnel Settings:**

ID	Tunnel Name	Remote Addr	Gateway	Status	Action	Enable
1					More	<input type="checkbox"/>
2					More	<input type="checkbox"/>
3					More	<input type="checkbox"/>
4					More	<input type="checkbox"/>
5					More	<input type="checkbox"/>

At the bottom of the page, there are "Apply" and "Refresh" buttons. The footer of the page reads "Copyright © 2012 All Rights Reserved".

Dynamic VPN Settings

Enabled: Tick this box to enable this feature and click **More** to configure VPN Dynamic IP on a separate page. Please see the next page for more details.

Tunnel Name: Enter a name for your VPN.

Local Subnet: Enter the local (LAN) subnet. (ex. 192.168.0.0)

Local Netmask: Enter the local (LAN) subnet mask. (ex. 255.255.255.0)

Phase1 Key Life Time: Enter the amount of time in seconds that the Phase 1 key should last.

Phase2 Key Life Time: Enter the amount of time in seconds that the Phase 2 key should last.

Encapsulation protocol: Choose either **ESP**, **AH** or **ESP+AH** from the drop-down menu.

PFS Group: **Enable** or **Disable** the PFS Group option using the drop-down menu. PFS is an additional security protocol.

Aggressive Mode: Check this box to enable aggressive mode.

Preshare Key: Enter an ASCII passphrase in the box.

Local ID: Choose from **Username**, **FQDN**, **User@FQDN**, or **Key ID** using the drop-down menu and then enter an ID in the box.

The screenshot shows the 'VPN Dynamic IP Setting' page in the D-Link DWM-312 web interface. The page is divided into several sections:

- General Settings:** Includes checkboxes for 'Enabled', 'Tunnel Name', 'Local Subnet', 'Local Netmask', 'Phase1 Key Life Time', 'Phase2 Key Life Time', 'Encapsulation Protocol' (ESP), 'PFS Group' (Disable), 'Aggressive Mode' (Enable), 'Preshare Key', 'Local ID' (Type: Username), 'Dead Peer Detection (DPD)' (Enable), and 'XAUTH' (None).
- IKE Proposal Settings:** A table with columns for ID, Encryption, Authentication, DH Group, and Enable.

ID	Encryption	Authentication	DH Group	Enable
1	DES	SHA1	Group1	<input type="checkbox"/>
2	DES	SHA1	Group1	<input type="checkbox"/>
- IPSEC Proposal Settings:** A table with columns for ID, Encryption, Authentication, and Enable.

ID	Encryption	Authentication	Enable
1	DES	SHA1	<input type="checkbox"/>
2	DES	SHA1	<input type="checkbox"/>

At the bottom of the page, there are 'Apply', 'Refresh', and 'Back' buttons. A copyright notice 'Copyright © 2012. All Rights Reserved' is visible at the bottom right.

Dynamic VPN Settings (Cont)

Dead Peer Detection (DPD): Tick this box to enable Dead Peer Detection, then enter the time in seconds after which a peer is determined to be no longer active. You may also enter a delay period in seconds.

XAUTH: Select **Server** or **None**. If **Server** has been selected, set up XAUTH user accounts in **XAUTH Account** on page 27.

Set IKE Proposal: Check this box to enable IKE Proposal.

Set IPSEC Proposal: Check this box to enable IPSEC Proposal.

IKE Proposal Settings: Use this area to **Enable** IKE Proposals. Then choose the **Encryption** and **Authentication** types, as well as the **DH Group** from the drop-down menus

IPSEC Proposal Settings: Use this area to **Enable** IPSEC Proposals. Then choose the **Encryption** and **Authentication** types from the drop-down menus.

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

VPN Dynamic IP Setting

Enabled
 Tunnel Name:
 Local Subnet:
 Local Netmask:
 Phase1 Key Life Time: seconds
 Phase2 Key Life Time: seconds
 Encapsulation Protocol:
 PFS Group:
 Aggressive Mode: Enable
 Preshare Key:
 Local ID: Type:
 ID:
 Dead Peer Detection (DPD): Enable
 ▶ Timeout: Second(s)
 ▶ Delay: Second(s)
 XAUTH: None
 Server
 Set IKE Proposal: Enable
 Set IPSEC Proposal: Enable

IKE Proposal Settings

ID	Encryption	Authentication	DH Group	Enable
1	<input type="text" value="DES"/>	<input type="text" value="SHA1"/>	<input type="text" value="Group1"/>	<input type="checkbox"/>
2	<input type="text" value="DES"/>	<input type="text" value="SHA1"/>	<input type="text" value="Group1"/>	<input type="checkbox"/>

IPSEC Proposal Settings

ID	Encryption	Authentication	Enable
1	<input type="text" value="DES"/>	<input type="text" value="SHA1"/>	<input type="checkbox"/>
2	<input type="text" value="DES"/>	<input type="text" value="SHA1"/>	<input type="checkbox"/>

Copyright © 2012. All Rights Reserved

XAUTH Account

If you have configured an IPSec server on the previous page, enter XAUTH account information for clients here.

Username: Enter an XAUTH username for users to connect to your IPSec server.

Password: Enter a password corresponding to the username for users to connect to your IPSec server.

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



The screenshot shows the D-Link DWM-312 web interface. The top navigation bar includes icons for Home, Internet, LAN, VPN, Advanced, and System, along with a Logout button. The left sidebar shows a tree view with the following items: IPSec, -VPN Settings, -XAUTH Account (selected), PPTP, L2TP, and GRE. The main content area is titled "XAUTH Account" and contains a table with 10 rows for adding accounts. Each row has columns for "No.", "Username", and "Password". Below the table are "Apply" and "Refresh" buttons. A copyright notice "Copyright © 2012 All Rights Reserved" is visible in the bottom right corner.

No.	Username	Password
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

PPTP

PPTP Server

Server Setup: Check this box to enable the DWM-312's internal PPTP server. If enabled, the following options will appear:

Authentication Type: Select one or more authentication types for the server, either **PAP**, **CHAP**, **MS_CHAP**, or **MS_CHAP2**. Note that **PAP** and **CHAP** are not compatible with encryption.

Server Virtual IP: Enter the address assigned to the server within the VPN. This will dictate the IP pool for clients.

IP Pool Start Address: Input the starting address for the server's IP pool, from 1 to 254.

IP Pool End Address: Input the end address for the server's IP pool from 1 to 254. Note that this number must be higher than the start address.

Encryption: Check this box to enable PPTP encryption.

Encryption Length: Specify the length of the encryption key.

User Account Setting: Up to 5 user accounts can be created for VPN access. Specify the user names and passwords that will be used to connect to the VPN server. Note that user names and passwords are visible to any administrator.

D-Link DWM-312

Home Internet LAN VPN Advanced System

- IPSec
- PPTP
 - PPTP Server
 - PPTP Client
- L2TP
- GRE

PPTP Server

Server Setup

Server Setup: Enable

Server Configuration

Authentication Type: PAP CHAP MS_CHAP MS_CHAP2

Server virtual IP:

IP Pool Start Address:

IP Pool End Address:

Encryption: Enable

Encryption Length: 40 bits 56 bits 128 bits

User Account Setting

ID	User Name	Password
1	<input type="text" value="test"/>	<input type="text" value="test"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>

Connection Status

User Name	Peer IP	Virtual IP	Peer Call ID	Operation
test	192.168.0.10	192.168.15.10	149569	<input type="button" value="Disconnect"/>

Copyright © 2012. All Rights Reserved

PPTP Server

Connection Status: This table describes the connection status of each client, displayed in detail below.

User Name: The user name that the client has used to connect to the VPN network.

Peer IP: The “real” IP of the client.

Virtual IP: The client’s IP address within the virtual network.

Peer Call ID: Used to identify and associate a tunnel with a packet.

Operation: Click **Disconnect** to disconnect a specific client.

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

The screenshot shows the PPTP Server configuration interface for a D-Link DWM-312 device. The interface includes a navigation menu on the left with options like IPsec, PPTP, PPTP Server, PPTP Client, L2TP, and GRE. The main content area is titled 'PPTP Server' and contains the following sections:

- Server Setup:** A checkbox for 'Server Setup' is checked and labeled 'Enable'.
- Server Configuration:**
 - Authentication Type: Checkboxes for PAP, CHAP, MS_CHAP, and MS_CHAPv2 are all checked.
 - Server virtual IP: A text input field containing '192.168.15.1'.
 - IP Pool Start Address: A text input field containing '10'.
 - IP Pool End Address: A text input field containing '100'.
 - Encryption: A checkbox labeled 'Enable' is unchecked.
 - Encryption Length: Radio buttons for 40 bits, 56 bits, and 128 bits are present, with 56 bits selected.
- User Account Setting:** A table with columns for ID, User Name, and Password.

ID	User Name	Password
1	test	test
2		
3		
4		
5		
- Connection Status:** A table showing active connections.

User Name	Peer IP	Virtual IP	Peer Call ID	Operation
test	192.168.0.10	192.168.15.10	149569	Disconnect

At the bottom of the configuration area, there are 'Apply' and 'Refresh' buttons.

PPTP Client

VPN-PPTP Client: Check **Enable** to enable the router to act as a PPTP client. If enabled, the following options will appear:

ID: Indicates the internal ID of the PPTP account for reference in the **Connection Status** table.

Name: Specify a name for the PPTP account for reference in the **Connection Status** table. This name is for reference only and does not affect functionality.

Peer IP/Domain: Enter the IP address or domain of your VPN server.

User Name: Enter the user name provided to you by your VPN operator.

Password: Enter the password provided to you by your VPN operator.

Route: Enter the route to which to bind the VPN tunnel.

Connect: Select **On Demand**, **Auto**, or **Manual**.

Option: Check the appropriate boxes to support Microsoft Point-to-Point Encryption (**MPPE**) and Network Address Translation (**NAT**).

Enable: Check this box to enable the VPN client.

D-Link DWM-312

Home Internet LAN VPN Advanced System

Log out

- IPSec
- PPTP
 - PPTP Server
 - PPTP Client
- L2TP
- GRE

PPTP Client

Setting completed

Client Setup

VPN-PPTP Client: Enable

User Account Setting

ID	Name	Peer IP/Domain	User Name	Password	Route	Connect	Option	Enable
1	test	test	test	*****		<input type="radio"/> On demand <input checked="" type="radio"/> Auto <input type="radio"/> Manual	<input checked="" type="checkbox"/> MPPE <input checked="" type="checkbox"/> NAT	<input checked="" type="checkbox"/>
2						<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
3						<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
4						<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
5						<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>

Connection Status

ID	Tunnel Name	Virtual IP	Remote IP	Status
1	test	0.0.0.0	0.0.0.0	Connecting...

Apply Refresh

Copyright © 2012. All Rights Reserved.

PPTP Client (Cont)

Connection Status This table displays information about currently active tunnels.

ID: Displays the numeric ID of the tunnel.

Tunnel Name: Displays the name of the tunnel.

Virtual IP: Lists the IP assigned by the tunnel.

Remote IP: Lists the IP of the VPN server.

Status: Displays the current connection status of the VPN tunnel.

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

D-Link
DWM-312

Home Internet LAN VPN Advanced System

■ IPsec
■ PPTP
-PPTP Server
-PPTP Client
■ L2TP
■ GRE

PPTP Client

Setting completed

Client Setup

VPN PPTP Client: Enable

User Account Setting

ID	Name	Peer IP/Domain	User Name	Password	Route	Connect	Option	Enable
1	test	test	test	*****		<input type="radio"/> On demand <input checked="" type="radio"/> Auto <input type="radio"/> Manual	<input checked="" type="checkbox"/> MPPE <input checked="" type="checkbox"/> NAT	<input checked="" type="checkbox"/>
2						<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
3						<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
4						<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
5						<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>

Connection Status

ID	Tunnel Name	Virtual IP	Remote IP	Status
1	test	0.0.0.0	0.0.0.0	Connecting...

Apply Refresh

Copyright © 2012. All Rights Reserved.

L2TP

L2TP Server

Server Setup: Check this box to enable the DWM-312's internal L2TP server. If enabled, the following options will appear:

Authentication Type: Select one or more authentication types for the server, either **PAP**, **CHAP**, **MS_CHAP**, or **MS_CHAP2**. Note that **PAP** and **CHAP** are not compatible with encryption.

Server Virtual IP: Enter the address assigned to the server within the VPN. This will dictate the IP pool for clients.

IP Pool Start Address: Input the starting address for the server's IP pool, from 1 to 254.

IP Pool End Address: Input the end address for the server's IP pool from 1 to 254. Note that this number must be higher than the start address.

Encryption: Check this box to enable L2TP encryption.

Encryption Length: Specify the length of the encryption key.

User Account Setting: Up to 5 user accounts can be created for VPN access. Specify the user names and passwords that will be used to connect to the VPN server. Note that user names and passwords are visible to any administrator.

The screenshot shows the D-Link DWM-312 web interface. The top navigation bar includes Home, Internet, LAN, VPN, Advanced, and System. The main content area is titled "L2TP Server" and contains the following configuration options:

- Server Setup:**
 - VPN-L2TP Server: Enable
- Server Configuration:**
 - Authentication Type: PAP CHAP MS_CHAP MS_CHAPv2
 - Server virtual IP:
 - IP Pool Start Address:
 - IP Pool End Address:
 - Encryption: Enable
 - Encryption Length: 40 bits 56 bits 128 bits
- User Account Setting:**

ID	User Name	Password
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
- Connection Status:**

User Name	Peer IP	Virtual IP	Peer Call ID	Operation
No connection from remote				

At the bottom of the page, there are "Apply" and "Refresh" buttons.

L2TP Server (Cont)

Connection Status: This table describes the connection status of each client, displayed in detail below.

User Name: The user name that the client has used to connect to the VPN network.

Peer IP: The “real” IP of the client.

Virtual IP: The client’s IP address within the virtual network.

Peer Call ID: Used to identify and associate a tunnel with a packet.

Operation: Click **Disconnect** to disconnect a specific client.

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

The screenshot shows the D-Link DWM-312 web interface. The main navigation bar includes Home, Internet, LAN, VPN, Advanced, and System. The left sidebar lists configuration options: IPsec, PPTP, L2TP (selected), L2TP Server (selected), L2TP Client, and GRE. The main content area is titled 'L2TP Server' and contains the following sections:

- Server Setup:** VPN-L2TP Server: Enable
- Server Configuration:**
 - Authentication Type: PAP CHAP MS_CHAP MS_CHAPv2
 - Server virtual IP:
 - IP Pool Start Address:
 - IP Pool End Address:
 - Encryption: Enable
 - Encryption Length: 40 bits 56 bits 128 bits
- User Account Setting:** A table with 3 columns: ID, User Name, and Password. It contains 5 rows of input fields.
- Connection Status:** A table with 5 columns: User Name, Peer IP, Virtual IP, Peer Call ID, and Operation. Below the table, it displays 'No connection from remote' and two buttons: 'Apply' and 'Refresh'.

L2TP Client

VPN-PPTP Client: Check **Enable** to enable the router to act as a L2TP client. If enabled, the following options will appear:

ID: Indicates the internal ID of the L2TP account for reference in the **Connection Status** table.

Name: Specify a name for the L2TP account for reference in the **Connection Status** table. This name is for reference only and does not affect functionality.

Peer IP/Domain: Enter the IP address or domain of your VPN server.

User Name: Enter the user name provided to you by your VPN operator.

Password: Enter the password provided to you by your VPN operator.

Route: Enter the route to which to bind the the VPN tunnel.

Connect: Select **On Demand**, **Auto**, or **Manual**.

Option: Check the appropriate boxes to support Microsoft Point-to-Point Encryption (**MPPE**) and Network Address Translation (**NAT**)

Enable: Check this box to enable the VPN client.

D-Link DWM-312

Home Internet LAN VPN Advanced System Logout

- IPSec
- PPTP
- L2TP
 - L2TP Server
 - L2TP Client
- GRE

L2TP Client

Client Setup

VPN-L2TP Client: Enable

User Account Setting

ID	Name	Peer IP/Domain	User Name	Password	Route	Connect	Option	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>

Connection Status

ID	Tunnel Name	Virtual IP	Remote IP	Status

Apply Refresh

Copyright © 2012. All Rights Reserved.

L2TP Client (cont)

Connection Status This table displays information about currently active tunnels.

ID: Displays the numeric ID of the tunnel.

Tunnel Name: Displays the name of the tunnel.

Virtual IP: Lists the IP assigned by the tunnel.

Remote IP: Lists the IP of the VPN server.

Status: Displays the current connection status of the VPN tunnel.

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

D-Link DWM-312

Home Internet LAN VPN Advanced System Logout

- IPSec
- PPTP
- L2TP
 - L2TP Server
 - L2TP Client**
 - GRE

L2TP Client

Client Setup

VPN-L2TP Client: Enable

User Account Setting

ID	Name	Peer IP Domain	User Name	Password	Route	Connect	Option	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> On demand <input type="radio"/> Auto <input type="radio"/> Manual	<input type="checkbox"/> MPPE <input type="checkbox"/> NAT	<input type="checkbox"/>

Connection Status

ID	Tunnel Name	Virtual IP	Remote IP	Status

Apply Refresh

Copyright © 2012. All Rights Reserved.

GRE

The Generic Routing Encapsulation protocol (GRE) can be used to create tunnels to compatible servers similar to IPSec.

ID: Displays the numeric ID of the tunnel.

Name: Enter the name of the IP tunnel for reference.

Tunnel IP: Enter the IP used to connect to the tunnel (optional).

Peer IP: Enter the remote IP of the GRE gateway. This is normally a public IP address.

Key: Enter a key for the GRE connection.

TTL: Specifies the time to live in number of hops, up to 255.

Subnet: Specify a gateway to reach the GRE server. Specify a subnet (e.g. 10.0.0.2/24).

Enable: Check this box to enable the GRE tunnel.

Default Gateway: Select a default gateway from the drop down list.

Tunnels Information: This table displays information about currently active tunnels.

ID: Displays the numeric ID of the tunnel

Transmitted Packets: Displays the number of packets sent.

Transmitted Bytes: Displays the number of bytes sent.

Received Packets: Displays the number of packets received.

Received Bytes: Displays the number of bytes received.

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

D-Link DWM-312

Home Internet LAN VPN Advanced System

Logout

- IPSec
- PPTP
- L2TP
- GRE**

GRE Tunnel

ID	Name	Tunnel IP	Peer IP	Key	TTL	Subnet	Enable
1							<input type="checkbox"/>
2							<input type="checkbox"/>
3							<input type="checkbox"/>
4							<input type="checkbox"/>
5							<input type="checkbox"/>
6							<input type="checkbox"/>
7							<input type="checkbox"/>
8							<input type="checkbox"/>

Default Gateway: None

Tunnels information

ID	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0

Apply Refresh

Copyright © 2012. All Rights Reserved.

Advanced DNS

On this page you can configure the Domain Name System (DNS) server, which manages the resolution of host/domain names to IP addresses.

DNS

This page allows you to configure Dynamic DNS (DDNS) services to more easily gain remote access to your router.

DDNS: Tick this check box to enable the DDNS feature.

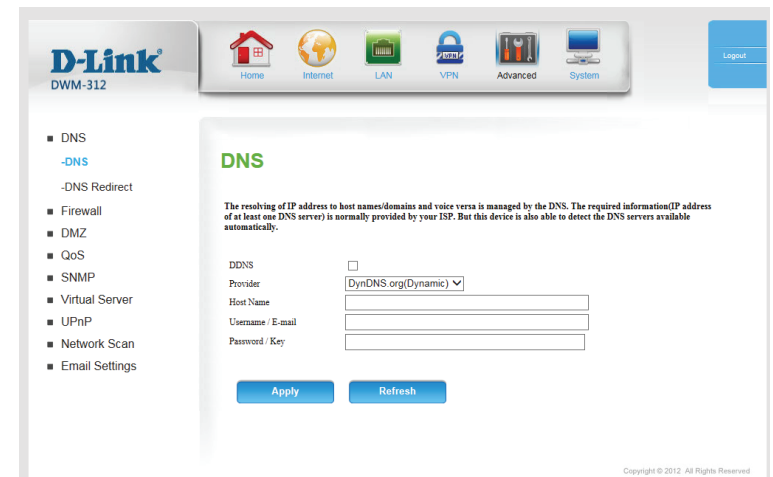
Provider: Select a DDNS service provider to use.

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

Username / E-mail: Enter the **Username** for your DDNS account.

Password / Key: Enter the **Password** for your DDNS account.

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



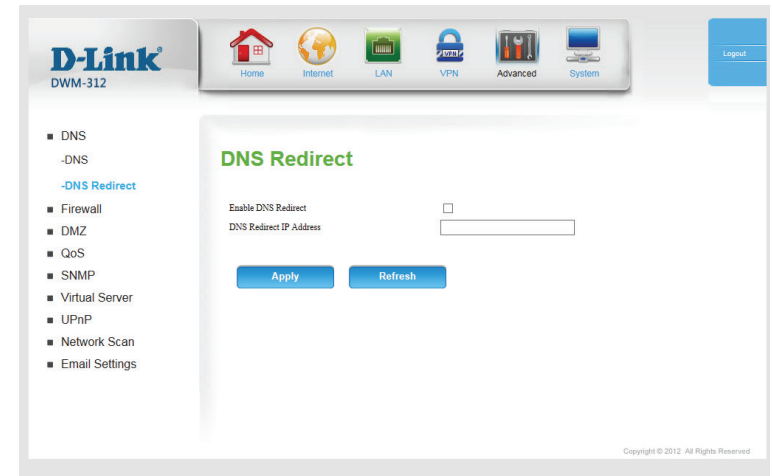
DNS Redirect

DNS Redirect causes all DNS requests to reply with a single address, resulting in all traffic using the local DNS resolver to be redirected to a single location.

Enable DNS Redirect: Select **Enable** to enable DNS redirect.

DNS Redirect IP Address: Enter the IP that should be returned whenever a DNS request is sent to the router. All URLs queried through the router's DNS will redirect to the same location.

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



Firewall

Outbound Filter

Outbound Filter enables you to control what packets are allowed to be sent out to the Internet. The outbound filter applies to all outbound packets.

Outbound Filter: Select this box to enable outbound filtering.

Use Schedule Rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to **Schedules** on page 40.

OUTBOUND FILTER RULES LIST

Here, you can select whether to **Allow** or **Deny** all outgoing traffic except for traffic that matches the listed rules.

ID: This identifies the rule.

Source IP : Ports: Specify the local IP address and then specify the port after the colon.

Destination IP : Ports: Specify the remote IP address and then the port after the colon.

Enable: Check the box to enable the specified rule.

Schedule Rule #: Specify the schedule rule number. Click on the **Add New Rule** button to create a new schedule rule.

Previous Page: Click to go back to the previous filter page.

Next Page: Click to advance to the next filter page.

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

The screenshot shows the D-Link DWM-312 Firewall configuration interface. The 'Outbound Filter' section is active, showing the 'Outbound Filter Setting' where the 'Outbound Filter' checkbox is checked. Below this, there is a 'Use schedule rule' dropdown set to 'ALWAYS ON' and a 'Copy to' button. The 'Outbound Filter Rules List' section shows a table with 8 rows, each with an 'ID', 'Source IP:Ports', 'Destination IP:Ports', 'Enable' checkbox, and 'Schedule Rule#'. Each row has an 'Add New Rule...' button. At the bottom, there are 'Apply' and 'Refresh' buttons.

ID	Source IP:Ports	Destination IP:Ports	Enable	Schedule Rule#
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> Add New Rule...
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> Add New Rule...
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> Add New Rule...
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> Add New Rule...
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> Add New Rule...
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> Add New Rule...
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> Add New Rule...
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> Add New Rule...

Inbound Filter

Inbound Filter enables you to control what packets are allowed to come in to your network from the Internet. The inbound filter only applies to packets that are destined for Virtual Servers or DMZ hosts.

Inbound Filter: Select this box to enable the filter.

Use Schedule Rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to **Schedules** on page 41.

INBOUND FILTER RULES LIST

Here, you can select whether to **Allow** or **Deny** all incoming traffic except for traffic that matches the listed rules.

ID: This identifies the rule.

Source IP : Ports: Specify the local IP address and then specify the port after the colon.

Destination IP : Ports: Specify the remote IP address and then the port after the colon.

Enable: Check the box to enable the specified rule.

Schedule Rule #: Specify the schedule rule number. Click on the **Add New Rule** button to create a new schedule rule.

Previous Page: Go back to the previous filter page.

Next Page: Advance to the next filter page.

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

D-Link DWM-312

Home Internet LAN VPN Advanced System

Inbound Filter

Inbound Filter Setting

Inbound Filter Enable

Use schedule rule [ALWAYS ON] ID [v]

Inbound Filter Rules List

Allow all to pass except those match the following rules.
 Deny all to pass except those match the following rules.

ID	Source IP:Ports	Destination IP:Ports	Enable	Schedule Rule#
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/> <input type="button" value="Add New Rule..."/>

Copyright © 2012. All Rights Reserved

URL Filter

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

URL Filtering: Check the box to enable URL Filtering.

URL FILTERING RULES

ID: This identifies the rule.

URL: Enter a URL that you would like to block. All URLs that begin with this string will be blocked.

Enable: Check the box to enable the specified rule.

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

The screenshot shows the D-Link DWM-312 web interface. The top navigation bar includes icons for Home, Internet, LAN, VPN, Advanced, and System, along with a Logout button. The left sidebar lists various settings: DNS, Firewall (with sub-items Outbound Filter, Inbound Filter, URL Filter, and MAC Address Filter), DMZ, QoS, SNMP, Virtual Server, UPnP, Network Scan, and Email Settings. The main content area is titled "URL Filter" and contains the following sections:

- URL Filter**: A heading for the configuration page.
- URL Filter provides the useful tools for restricting Internet access. Website URL Blocking allows you to quickly create a list of all web sites that you wish to allow or deny users from accessing.**
- URL Filtering Setting**: A section with a "URL Filtering" label and an "Enable" checkbox.
- URL Filtering Rules**: A table with columns for ID, URL, and Enable.

ID	URL	Enable
1		<input type="checkbox"/>
2		<input type="checkbox"/>
3		<input type="checkbox"/>
4		<input type="checkbox"/>
5		<input type="checkbox"/>

At the bottom of the main content area, there are "Apply" and "Refresh" buttons. The footer of the page reads "Copyright © 2012. All Rights Reserved."

MAC Address Filter

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

MAC Address Control: Tick this box to enable MAC Filtering.

Connection Control: Check the box to allow wireless and wired clients with **C** selected to connect to this device. You can also select to **allow** or **deny** connections from unspecified MAC addresses.

MAC FILTERING RULES

ID: This identifies the rule.

MAC Address: Specify the MAC address of the computer to be filtered.

C: If this box is ticked, the rule will follow the connection control setting specified in MAC filtering settings specified above.

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

The screenshot shows the D-Link DWM-312 web interface. The main content area is titled "MAC Address Filter". Under "MAC Filtering Settings", there is a checkbox for "MAC Address Control" (unchecked) and a checkbox for "Connection control" (unchecked). Below these, there is a dropdown menu for "DHCP clients" (set to "Select one"), a "Copy to" button, and an "ID" dropdown. A note states: "Wired clients with C checked can connect to this device; and [allow] unspecified MAC addresses to connect." Under "MAC Filtering Rules", there is a table with columns "ID", "MAC Address", and "C".

ID	MAC Address	C
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>

Buttons at the bottom include "Previous page", "Next page", "Apply", and "Refresh".

DMZ

A Demilitarized Zone (DMZ) directly exposes a single client device to the outside world for certain types of applications. If you choose to expose a computer, you can enable a DMZ.

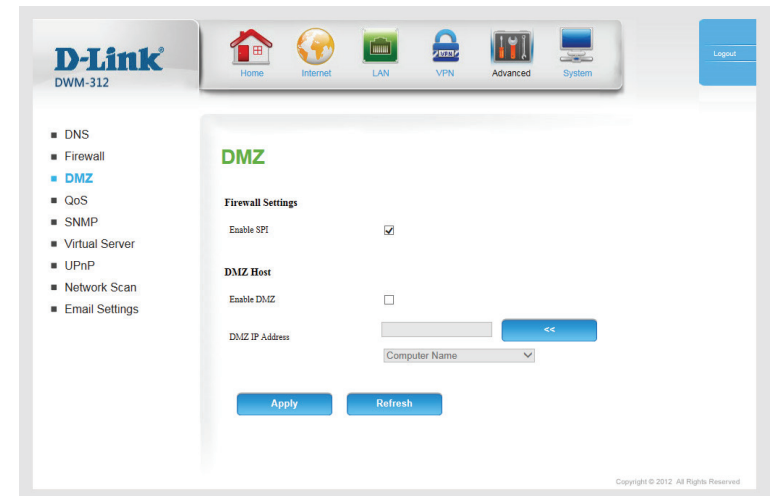
Enable SPI: Enabling Stateful Packet Inspection (SPI) helps to prevent cyber attacks by validating that the traffic passing through the session conforms to the protocol.

Enable DMZ: If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

Note: Placing a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is recommended for advanced users only.

DMZ IP Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its IP address automatically using DHCP, be sure to make a static reservation on the **Setup > Network** Settings page so that the IP address of the DMZ machine does not change.

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



QoS

The **QoS Engine** improve the performance of certain bandwidth or latency-sensitive applications by ensuring that your such traffic is prioritized over other network traffic, such as FTP or web. For best performance, use the Automatic Classification option to automatically set the priority for your applications.

Enable QoS Select this box to enable the QoS feature.

Packet Filter:

Upstream Bandwidth: Specify the maximum upstream bandwidth here (e.g. 400 Kbps).

Use Schedule Rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to **Schedules** on page 45.

QOS RULES

ID: This identifies the rule.

Local IP : Ports: Specify the local IP address(es) and port(s) for the rule to affect.

Remote IP : Ports: Specify the remote IP address(es) and port(s) for the rule to affect.

QoS Priority: Select what priority level to use for traffic affected by the rule: **Low, Normal, or High.**

Enable: Check the box to enable the specified rule.

Use Rule #: Specify the schedule rule number. To create a new schedule, click on the **Add New Rule** button. For more information about schedules, please refer to **Schedules** on page 45.

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

D-Link DWM-312

Home Internet LAN VPN Advanced System

QoS

QoS Engine Setup

Enable QoS Packet Filter:

Upstream bandwidth: Kbps

Use schedule rule: **Copy to** ID:

QoS Rules

ID	Local IP: Ports	Remote IP: Ports	QoS Priority	Enable	Use Rule#
1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
3	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
4	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
5	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
6	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
7	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...
8	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	High	<input type="checkbox"/>	<input type="text"/> Add New Rule...

Apply **Refresh**

Copyright © 2012. All Rights Reserved.

SNMP

SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol that reports activity on each network device to the administrator of the network. SNMP can be used to monitor traffic and statistics of the DWM-312. The DWM-312 supports SNMP v1, v2c, and v3. D-View software uses the SNMP protocol. For details on managing your device with D-View, see the D-View Manual.

SNMP Local: Select whether to **Enable** or **Disable** local SNMP administration.

SNMP Remote: Select whether to **Enable** or **Disable** remote SNMP administration.

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

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

IP 1/IP 2/IP 3/IP 4: Enter up to 4 IP addresses to use as trap targets for your network.

SNMP Version: Select the SNMP version of your system.

WAN Access IP Address: If you want to limit remote access SNMP access, enter the IP address of the remote computer you will use to access this device; all other IP addresses will be denied remote SNMP access.

System Contact: Enter a contact point for the system for reference.

System Name: Enter the system name for reference.

System Location: Enter the system location for reference.

User Privacy Definition

User accounts can be defined for SNMP remote access. Click **Edit** to change settings. Up to five users can be added.

The screenshot shows the D-Link DWM-312 web interface. The left sidebar contains a navigation menu with the following items: DNS, Firewall, DMZ, QoS, **SNMP** (highlighted), Virtual Server, UPnP, Network Scan, and Email Settings. The main content area is titled 'SNMP' and contains the following configuration options:

- SNMP Local: Enable Disable
- SNMP Remote: Enable Disable
- Get Community:
- Set Community:
- IP 1:
- IP 2:
- IP 3:
- IP 4:
- SNMP Version: v1 v2c v3
- WAN Access IP Address:
- System Contact:
- System Name:
- System Location:

Below the configuration options is a 'User Privacy Definition' table:

ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	Enable	Action
1			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit
2			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit
3			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit
4			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit
5			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit

At the bottom of the page are 'Apply' and 'Refresh' buttons.

SNMP (Cont)

ID: Indicates the ID of the user account.

User Name: Enter the user name of the account.

Password: Enter the password of the account.

Note: Passwords are stored in plaintext and are visible to anyone with access to the web UI.

Authentication: If **authNoPriv** or **authPriv** is selected under **Privacy Mode**, choose **SHA1** or **MD5** authentication.

Encryption: If **authPriv** is selected under **Privacy Mode**, **DES** encryption is available.

Privacy Mode: Select **NoauthNoPriv** for no authentication and no encryption, **authNoPriv** for authentication only, and **authPriv** to use both authentication and encryption.

Privacy Key: If encryption is enabled, enter a key between 8 and 27 ASCII characters in length.

Authority: Select **Read** to allow this user read-only access to configuration, or **Read/Write** to enable full read-write access.

Enable: Check **Enable** to activate the user account. Uncheck to disable the user account.

Actions: Click **Edit** to make changes to the corresponding account.

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

The screenshot shows the D-Link DWM-312 web interface. The top navigation bar includes Home, Internet, LAN, VPN, Advanced, and System. The left sidebar lists various settings: DNS, Firewall, DMZ, QoS, **SNMP** (selected), Virtual Server, UPnP, Network Scan, and Email Settings. The main content area is titled "SNMP" and contains the following settings:

- SNMP Local: Enable Disable
- SNMP Remote: Enable Disable
- Get Community:
- Set Community:
- IP 1:
- IP 2:
- IP 3:
- IP 4:
- SNMP Version: V1 V2c v3
- WAN Access IP Address:
- System Contact:
- System Name:
- System Location:

Below the settings is a "User Privacy Definition" table:

ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	Enable	Action
1			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit
2			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit
3			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit
4			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit
5			MD5	Disable	authNoPriv	Disable	Read	<input type="checkbox"/>	Edit

At the bottom of the page, there are "Apply" and "Refresh" buttons. A small copyright notice "Copyright © 2012. All Rights Reserved" is visible in the bottom right corner.

Virtual Server

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

Well-known Services: This contains a list of pre-defined services. You can select a service, select a rule ID, then click the **Copy to** button to copy the default settings for that service to the specified rule ID.

ID: Specifies which rule to copy the selected **Well known service** settings to when you click the **Copy to** button.

Use schedule rule: Select a schedule to use and copy to the specified rule ID when you click the **Copy to** button. You may select **Always On** or use a specific schedule that you have defined. To create and edit schedules, please refer to **Schedules** on page 48.

VIRTUAL SERVERS LIST

ID: This identifies the rule.

Service Ports Enter the public port(s) you want to open.

Server IP: Port: Enter the IP address and port of the computer on your local network that you want to forward the Service Ports to.

Enable: Check the box to enable the specified rule.

Schedule Rule #: Specify the schedule rule number. To create schedules, click on the **Add New Rule** button. For further information on schedules, please refer to **Schedules** on page 48.

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

D-Link
DWM-312

Home Internet LAN VPN Advanced System Logout

- DNS
- Firewall
- DMZ
- QoS
- SNMP
- **Virtual Server**
- UPnP
- Network Scan
- Email Settings

Virtual Server

The Externally acts as server. It receives the requests of remote users under its public IP address and forwards them automatically to the Virtual Server. So a client in your network behind NAT or firewall can provide services as a Virtual Server. You just have to enable specific ports or port ranges and protocols (UDP/TCP). File sharing or web services for e.g. HTTP, FTP or POP3 are possible. The private IP addresses of the servers in the local network remains safe. If you have a dynamic IP address, you may want to enable DynDNS additionally.

Well known services: Select one Copy to ID

Use schedule rule: ALWAYS ON

ID	Service Ports	Server IP: Port	Enable	Schedule Rule#
1			<input type="checkbox"/>	<input type="text"/> Add New Rule...
2			<input type="checkbox"/>	<input type="text"/> Add New Rule...
3			<input type="checkbox"/>	<input type="text"/> Add New Rule...
4			<input type="checkbox"/>	<input type="text"/> Add New Rule...
5			<input type="checkbox"/>	<input type="text"/> Add New Rule...
6			<input type="checkbox"/>	<input type="text"/> Add New Rule...

Apply Refresh

Copyright © 2012. All Rights Reserved

UPnP

Enable UPnP: Check the box to enable the Universal Plug and Play (UPnP™) feature. UPnP provides compatibility with various networking equipment, software, and peripherals.

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



Network Scan

This page lets you set whether to allow the DWM-312 to automatically select a 3G/4G network based on the inserted SIM card, or allows you to manually scan for networks and select one to connect to.

Scan Approach: Leave this setting on **Auto** to allow the DWM-312 to automatically select a cellular network to connect to. If you need to select a network manually, select **Manual**, and the following options will appear:

Network Provider List

Scan: Click **Scan** to load the list of network providers.

Register: Allows you to register on the selected network.

Provider Name: The name of the detected cellular carrier.

Mobile System: Indicates whether the network is using 2G, 3G, or 4G technology.

Network Status: Indicates the status of the network.

Action: Check the box corresponding to the network you wish to register on, and then click **Register**.

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

Note: You will only be able to scan for networks if the device is set to single SIM mode in **WAN Service** on page 50, as well as having Reconnect Mode set to **Manual** in **Connection Settings** on page 50.

Network Scan

Physical Interface: SIMA
Scan Approach: Manually

Network Provider List

Provider Name	Mobile System	Network Status	Action
TWM	4G	Current	<input type="checkbox"/> Select
TWM	3G	Available	<input type="checkbox"/> Select
T Star	4G	Forbidden	<input type="checkbox"/> Select
FET	4G	Forbidden	<input type="checkbox"/> Select
466 05	4G	Forbidden	<input type="checkbox"/> Select
Chungghwa	2G	Forbidden	<input type="checkbox"/> Select
Chungghwa	3G	Forbidden	<input type="checkbox"/> Select
FET	3G	Forbidden	<input type="checkbox"/> Select
Chungghwa	4G	Forbidden	<input type="checkbox"/> Select
T Star	3G	Forbidden	<input type="checkbox"/> Select
466 05	2G	Forbidden	<input type="checkbox"/> Select
FET	2G	Forbidden	<input type="checkbox"/> Select

Apply Refresh

Copyright © 2012. All Rights Reserved

Email Settings

Email Settings allow you to send the system log files, router alert messages, and firmware update notifications to an e-mail address.

Enable Email Notification: When this option is enabled, router activity logs will be e-mailed to the specified e-mail address.

SMTP Sever IP and Port: Enter the SMTP server IP address the router will use to send e-mails. Enter the complete IP address followed by a colon(:) and the port number. (e.g. 123.123.123.1:25).

SMTP Username: Enter the username for the SMTP account.

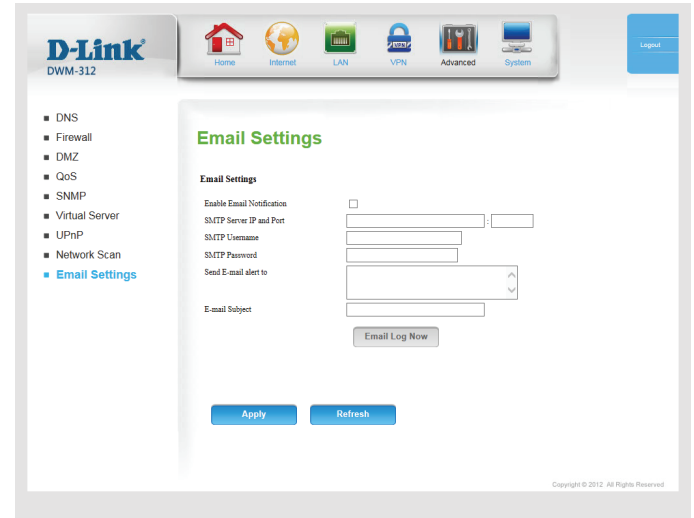
SMTP Password: Enter the password for the SMTP account.

Send Email alert to: Enter the email address where you would like the router to send e-mails to.

Email Subject: Enter a subject for the e-mail.

Email Log Now: Click this button to send the current logs to the specified e-mail address.

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



System Administration Password Settings

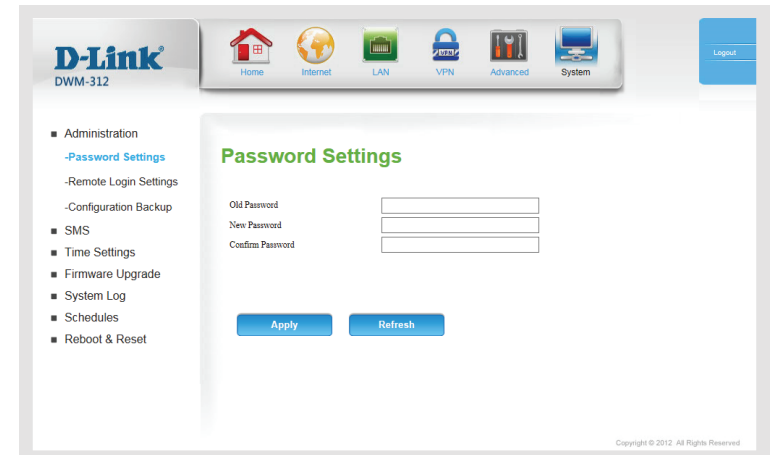
The **Admin** page allows you to change the Administrator password and enable Remote Management. The admin has read/write access while users only have read-only access. Only the admin has the ability to change both admin and user account passwords.

Old Password: Enter the current admin password.

New Password: Enter the new admin password.

Confirm Password: Reenter the new password to confirm.

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



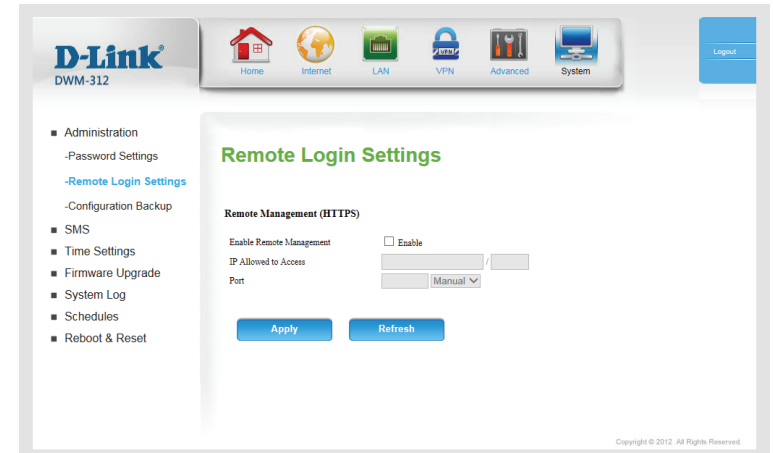
Remote Login Settings

Enable Remote Management: Tick this check box to enable remote management. Remote management allows the DWM-312 to be configured over the Internet through a web browser. A username and password will still be required to access the web-management interface.

IP Allowed to Access: Enter the Internet IP address of the PC that has access to the broadband router. If you enter an asterisk (*) in this field, then anyone will be able to access the router. Adding an asterisk (*) into this field could present a security risk and is not recommended.

Port: This is the port number used to access the router. 443 is the port usually used for the HTTPS web-management interface. Select **443**, **88**, **1080**, or **Manual** to enter one manually.

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



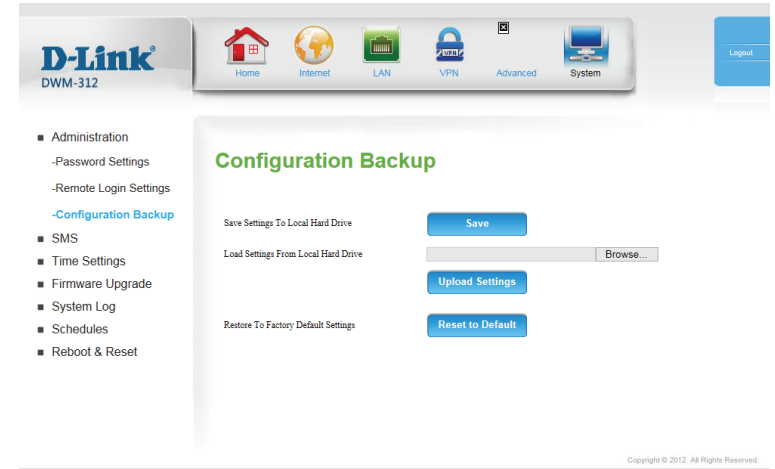
Configuration Backup

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

Save Settings To Local Hard Drive: Use this option to save your current router configuration settings to a file. Click **Save** to open a file dialog, and then select a location and file name for the settings.

Load Settings From Local Hard Drive: Use this option to load previously saved router configuration settings. Click **Browse...** and select the saved file and then click the **Upload Settings** button to upload the settings to the router.

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



SMS

SMS Inbox

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

Delete: Deletes the selected SMS message(s).

Reply: Opens a Create Message window to reply to the selected SMS message.

Forward: Opens a Create Message windows to forward the selected SMS message to another recipient.

Refresh: Click this button to check for new messages.

The screenshot shows the D-Link DWM-312 web interface. The top navigation bar includes Home, Internet, LAN, VPN, Advanced, System, and Logout. The left sidebar contains a menu with options like Administration, SMS, -SMS Inbox, -Compose SMS, -Message Settings, Time Settings, Firmware Upgrade, System Log, Schedules, and Reboot & Reset. The main content area is titled "SMS Inbox" and displays the following information:

SMS Status

SIM Status	SIM4
Received SMS	14
New SMS	0
Total Capacity	40

Inbox

From	Timestamp	Text
<input type="checkbox"/> 0935120188	2016/09/10,08:55:31	親愛的用戶，本公司已...
<input type="checkbox"/> 0935120188	2016/09/10,09:04:40	感謝您使用300型以...
<input type="checkbox"/> 0935120188	2016/09/10,09:44:00	感謝您使用300型以...
<input type="checkbox"/> 0935120188	2016/09/10,10:40:28	4G用戶權益通知：攝...
<input type="checkbox"/> 8311	2016/09/10,11:00:15	您已成功申請推來電腦...
<input type="checkbox"/> 803	2016/09/10,11:20:46	行動連絡服務已開通...
<input type="checkbox"/> 838032	2016/10/04,09:36:49	您的行動連絡服務即將...

SMS

親愛的用戶，本公司已為您開辦3G「行動上網789型」上網服務，若有疑問請洽客服Line!

Buttons: Delete, Reply, Forward, Refresh

Compose SMS

This page allows you to send an SMS message. Enter the phone number of the recipient, and type the content of message. Then click the **Send Message** button to send this message. To add more than one recipient, put a semicolon (;) between each of the phone numbers.

Receiver: Type the phone number of the recipient.

Text Message: Type the message that you would like to send.

Click **Send** to send your message, or **Refresh** to clear the message.

The screenshot displays the D-Link DWM-312 web management interface. At the top, there is a navigation bar with icons for Home, Internet, LAN, VPN, Advanced, and System, along with a Logout button. A left sidebar contains a menu with the following items: Administration, SMS, -SMS Inbox, -Compose SMS (highlighted in blue), -Message Settings, Time Settings, Firmware Upgrade, System Log, Schedules, and Reboot & Reset. The main content area is titled "Compose SMS" and features a "Receiver:" label followed by a text input field with a placeholder "Add * for international format of the phone number". Below this is a "Text message:" label followed by a larger text area. At the bottom of the form, there are two buttons: "Send" and "Refresh". A small note at the bottom of the form states: "Current input text length: 0. The max. length of a message is 160 characters for pure alphabetical or numeric."

Message Settings

The DWM-312 can be managed remotely over SMS. Get status updates, manage connections, and reboot remotely with a single text. Receive continuous updates about connectivity status. Access control lists and security keys can help protect your router from unwanted remote management. Once remote management is configured, you can send SMS messages to the router's phone number in the following format: <security Key> <command>. For example, if your security key were "12345" and you wanted to reboot the router, you would send an SMS to the router's phone number with the contents **12345 reboot**. Note that commands must be either lower case, upper case, or with only the first letter capitalized.

Note: SMS messages may incur fees from your operator.

Remote Management via SMS: Select **Enable** to enable SMS remote management. The default is **Disable**.

Delete SMS for Remote management: Select **Enable** to delete SMS messages related to remote management from the inbox once they are processed. The default is **Disable**.

Security Key: If you have enabled Remote Management via SMS, you will have the option to add a security key, which is sent at the beginning of the message. The key is case-sensitive.

Note: The security key is not encrypted, and all messages to and from the router are sent in plaintext.

Command Settings

Status: Select **Enable** and send the **Status** command over SMS to receive a message with the WAN IP, current networks, and connection time.

Connect: Select **Enable** to use the **Connect** command to have the router connect to the mobile network.

The screenshot shows the D-Link DWM-312 web interface. The top navigation bar includes icons for Home, Internet, LAN, VPN, Advanced, and System, along with a Logout button. The left sidebar lists menu items: Administration, SMS, SMS Inbox, Compose SMS, Message Settings (highlighted), Time Settings, Firmware Upgrade, System Log, Schedules, and Reboot & Reset. The main content area is titled "Message Settings" and contains the following sections:

- Management Settings:**
 - Remote Management via SMS: Enable Disable
 - Delete SMS for Remote Management: Enable Disable
 - Security Key:
- Command Settings:**
 - Status: Enable Disable
 - Connect: Enable Disable
 - Disconnect: Enable Disable
 - Reconnect: Enable Disable
 - Reboot: Enable Disable
- Notification Settings:**
 - WAN Link Up: Enable Disable
 - WAN Link Down: Enable Disable
- Access Control List:**
 - Access Control: Enable Disable
 - Phone 1: Management Notification
 - Phone 2: Management Notification
 - Phone 3: Management Notification
 - Phone 4: Management Notification
 - Phone 5: Management Notification

At the bottom of the page, there are "Apply" and "Refresh" buttons. A small copyright notice "Copyright © 2012. All Rights Reserved." is visible in the bottom right corner.

Message Settings (Cont)

Disconnect: Select **Enable** to use the **Disconnect** command to have the router disconnect from the mobile network.

Reconnect: Select **Enable** to use the **Reconnect** command to have the router cycle the mobile connection off and then back on again.

Reboot: Select **Enable** to use the **Reboot** command to have the router initiate a reboot.

Notification Settings

WAN Link Up: Select **Enable** to receive SMS notifications when the WAN Link is up. These notifications will be sent to numbers specified in the access control list.

WAN Link Down: Select **Enable** to receive SMS notifications when the WAN Link is down.

Access Control Settings

Access Control: Select **Enable** to input phone numbers. When enabled, the router will accept SMS commands only from those phone numbers which have the **Management** option selected. Additionally, the router will send any notification messages to any numbers with the **Notification** option selected.

Note: The access control settings rely on caller-ID information provided by the phone system, and contain no additional authentication or encryption tools.

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

The screenshot shows the D-Link DWM-312 web interface. The top navigation bar includes Home, Internet, LAN, VPN, Advanced, and System. The left sidebar lists various settings categories, with Message Settings highlighted. The main content area is titled 'Message Settings' and contains the following sections:

- Management Settings:**
 - Remote Management via SMS: Enable Disable
 - Delete SMS for Remote Management: Enable Disable
 - Security Key:
- Command Settings:**
 - Status: Enable Disable
 - Connect: Enable Disable
 - Disconnect: Enable Disable
 - Reconnect: Enable Disable
 - Reboot: Enable Disable
- Notification Settings:**
 - WAN Link Up: Enable Disable
 - WAN Link Down: Enable Disable
- Access Control List:**
 - Access Control: Enable Disable
 - Phone 1: Management Notification
 - Phone 2: Management Notification
 - Phone 3: Management Notification
 - Phone 4: Management Notification
 - Phone 5: Management Notification

At the bottom of the page, there are 'Apply' and 'Refresh' buttons. The footer indicates 'Copyright © 2012. All Rights Reserved'.

Time Settings

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

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

Enable Daylight Saving: Check the box to allow for daylight saving adjustments. Use the drop-down boxes to specify a start date and end date for daylight saving time adjustments.

Automatically synchronize with Internet time server: Check the box to allow the router to use an NTP server to update the router's internal clock.

NTP Server Used: Enter an NTP server to use for time synchronization, or use the drop-down box to select one. Click the **Update Now** button to synchronize the time with the NTP server.

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

D-Link
DWM-312

Home Internet LAN VPN Advanced System

- Administration
- SMS
- Time Settings**
- Firmware Upgrade
- System Log
- Schedules
- Reboot & Reset

Time Settings

The time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

Time: Tue May 02, 2017 18:33:27

Time Zone: (GMT -12:00) Eniwetok, Kwajalein

Enable Daylight Saving:

Automatically synchronize with Internet time server

NTP Server Used: time.nist.gov

Sync. RESULT

Copyright © 2012. All Rights Reserved

Firmware Upgrade

Device Upgrade

Here, you can upgrade the firmware of your router. The DWM-312 provides support for both Firmware Over the Air and for manual upgrades. For a manual upgrade, make sure the firmware you want to use is on the local hard drive of the computer and then click **Browse** to upload the file. You can check for and download firmware updates at the D-Link support site at <http://support.dlink.com>.

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

Check File: Queries the remote server to check for a firmware update over the Internet. If one is available, it will be displayed below.

Update: This button will appear if **Check File** finds new firmware. Click this button to begin the update process.

Warning: Do not unplug or power off the device while the update is in progress.

Current Firmware Date: Displays your current firmware's release date.

Upgrade: Use this option if you wish to manually install firmware. After you have downloaded a new firmware file, click **Browse** to locate the firmware on your computer, then click **Upgrade** to start the firmware upgrade.

Accept unofficial Firmware: If the firmware you want to install is not an official D-Link release, you will need to check this box.

Warning: Unofficial firmware is not supported, and may cause damage to your device. Use of unofficial firmware is at your own risk.

The screenshot shows the D-Link DWM-312 web interface. The top navigation bar includes Home, Internet, LAN, VPN, Advanced, System, and Logout. The left sidebar lists menu items: Administration, SMS, Time Settings, Firmware Upgrade (selected), -Device Upgrade, -Module Upgrade, System Log, Schedules, and Reboot & Reset. The main content area is titled 'Device Upgrade' and contains the following information:

Please use the "Upgrade" button to update firmware version for your device.

Firmware Information

Current Firmware Version	V01.00.1.014	Check File
Current Firmware Date	2017/03/28	

New Firmware Information

new FW image in remote server

Return Code : 0x0000

New Firmware Version	V01.00.1.015	Update
New Firmware Date	2017/04/14	
MD5	23c9846887ecc193b3d3cd63dd4ef6f5	

Firmware Update

Select Firmware Browse...

Accept unofficial firmware.

Copyright © 2012. All Rights Reserved

Module Upgrade

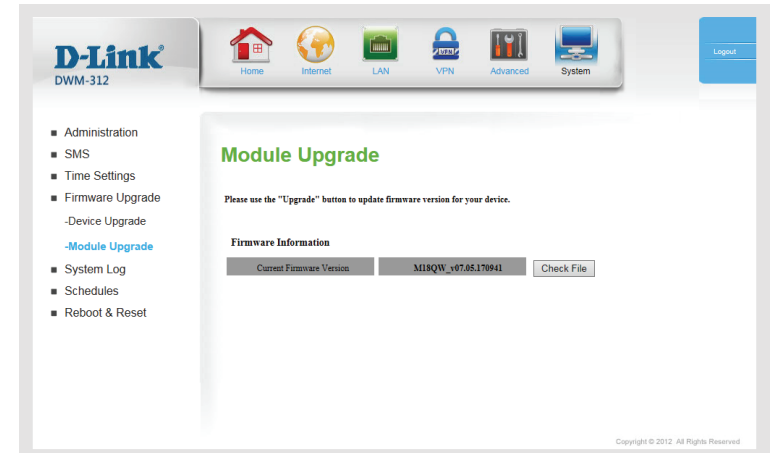
This section allows you to perform an upgrade of the cellular module's firmware, separate from the router firmware. For this option, only Firmware Over the Air (FOTA) is supported.

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

Check File: Queries the remote server to check for a firmware update over the Internet. If one is available, it will be displayed below.

Update: This button will appear if **Check File** finds new firmware. Click this button to begin the update process.

Warning: Do not unplug or power off the device while the update is in progress.



System Log

The DWM-312 keeps a running log of events and activities occurring on the router. You may send these logs to a Syslog server on your network.

Enable Logging to Syslog Server: Check the box to send the router logs to a Syslog server.

Syslog Server IP Address: Enter the IP address of the Syslog server that the router will send the logs to.

View Logs

Previous Page: Click to go to the previous page of logs.

Next Page: Click to go to the next page of logs.

First Page: Click to go to the first page of logs.

Last Page: Click to go to the last page of logs.

Download: Click to download a text file with all log entries.

Clear logs: Click this button to clear all logs.

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

D-Link
DWM-312

Home Internet LAN VPN Advanced System Logout

- Administration
- SMS
- Time Settings
- Firmware Upgrade
- System Log**
- Schedules
- Reboot & Reset

System Log

The System Log allows you to configure local, remote and email logging, and to view the logs that have been created.

Enable Logging To Syslog Server

Syslog Server IP Address

Apply Refresh

View Logs

Time	Message
May 1 13:34:41	kernel: klogd started: BusyBox v1.3.2 (2017-02-03 11:16:31 CST)
May 1 13:34:43	cmdrun: Original sess.handle: 30
May 1 13:34:44	BEID: No WAN = 00:50:18:01:40:01
May 1 13:34:44	BEID: No LAN = 00:50:18:01:40:01
May 1 13:34:44	BEID: WLAN0 = 00:50:18:01:40:01
May 1 13:34:44	BEID: BEID STATUS : 0 , STATUS OK!
May 1 13:34:44	syslog: WAN 0 Get available PVID 2
May 1 13:34:44	syslog: ID : id=2, nr=1, Using VLAN Count 0
May 1 13:34:44	syslog: Set NAT (request vid: 1) Lan 0 id 1 tagged: 0, member : 2 3 4 5 0
May 1 13:34:44	syslog: ID : id=1, nr=2, Using VLAN Count 1
May 1 13:34:44	syslog: i: 0,B0 using MAC: 00:50:18:01:40:01
May 1 13:34:44	syslog: br0 added
May 1 13:34:44	syslog: ifconfig eth2.1 hw ether 005018014001
May 1 13:34:45	syslog: Get Wan 0, wantype: 10
May 1 13:34:45	syslog: Start set virtual wan

Page: 1/18 (Log Number : 264)

Previous page Next page First Page Last Page

Refresh Download Clear logs

Copyright © 2012. All Rights Reserved

Schedules

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

Enable Schedule: Check this box to enable schedules.

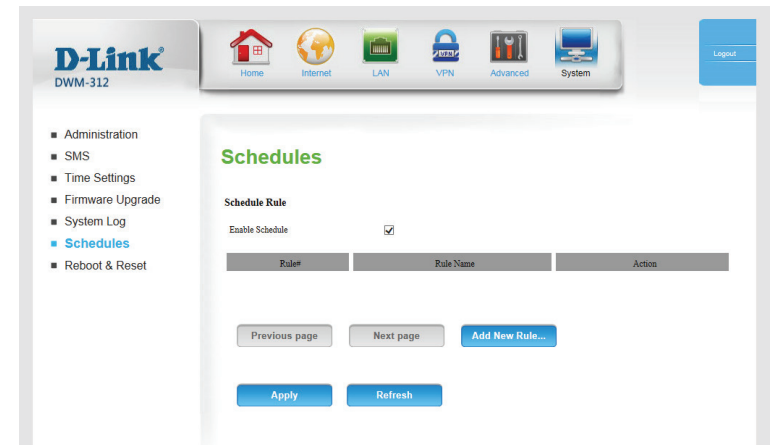
Edit: Click this icon to edit the selected rule. (see below)

Delete: Click this icon to delete the selected rule.

Previous Page: Click this button to go to the previous page of rules.

Next Page: Click this button to go to the next page of rules.
Click this button to specify the start time, end time, and name of the rule.

Add New Rule...: Click this button to create a new rule. (see below)



Add New Rule

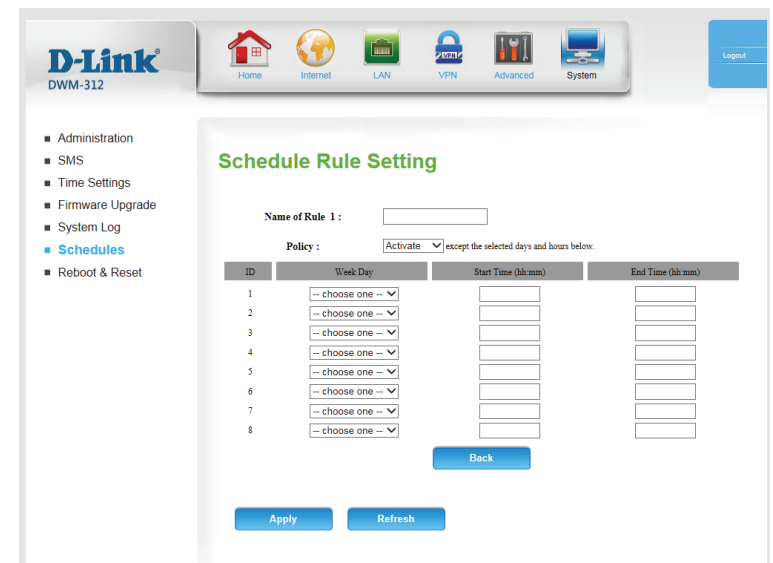
Name of Rule #: Enter a name for your new schedule.

Policy: Select **Activate** or **Inactivate** to decide whether features that use the schedule should be active or inactive except during the times specified.

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

Start Time (hh:mm): Enter the time at which you would like the schedule to become active.

End Time (hh:mm): Select the time at which you would like the schedule to become inactive.



Reboot and Reset

Reboot the Device

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



Connection Reset

This feature allows you to reset the Internet connection on your router by periodically resetting the connection. You can choose to have this happen on a predetermined schedule by configuring the options on this page.

Auto-Reboot: Select whether the connection reset feature should be enabled or disabled.

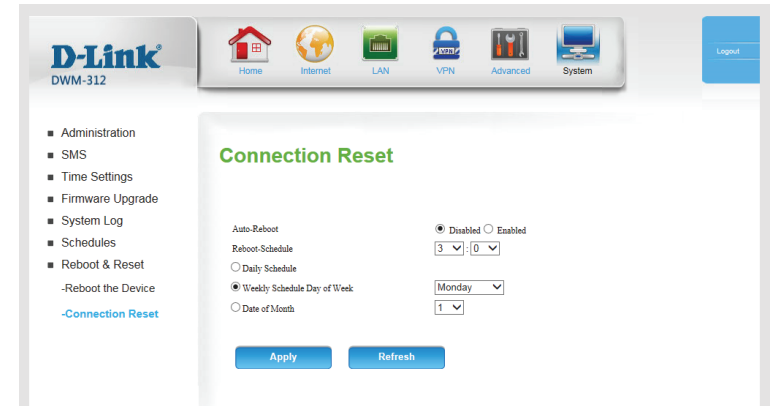
Reboot-Schedule: If the connection reset feature is enabled, select the hour and minute it should be triggered using the dropdown boxes.

Daily Schedule: Select this option if you want the connection reset feature to activate on a daily schedule.

Weekly Schedule Select this option if you want the connection reset feature to activate only on a certain day of the week.
Day of Week:

Date of Month: Select this option if you want the connection reset feature to activate only on a certain day of the month.

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



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DWM-312. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to these examples.

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

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

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Microsoft Internet Explorer® 7 or higher
 - Mozilla Firefox 3.5 or higher
 - Google™ Chrome 8 or higher
 - Apple Safari 4 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable, or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any Internet security software running on the computer. Software firewalls such as ZoneAlarm, BlackICE, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:
 - Go to **Start > Settings > Control Panel**. Double-click the **Internet Options** icon. From the **Security** tab, click the button to restore the settings to their defaults.
 - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
 - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
 - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

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

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

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

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

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

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, XP, Vista®, and 7 users type in **cmd**) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

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

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

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52
Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 203ms, Average = 132ms
C:\>
```


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

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

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

- Navigate to the Internet configuration page (see **Internet** on page 69 for details).
- To change the MTU, enter the number in the MTU field and click **Apply** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Networking Basics

Check your IP address

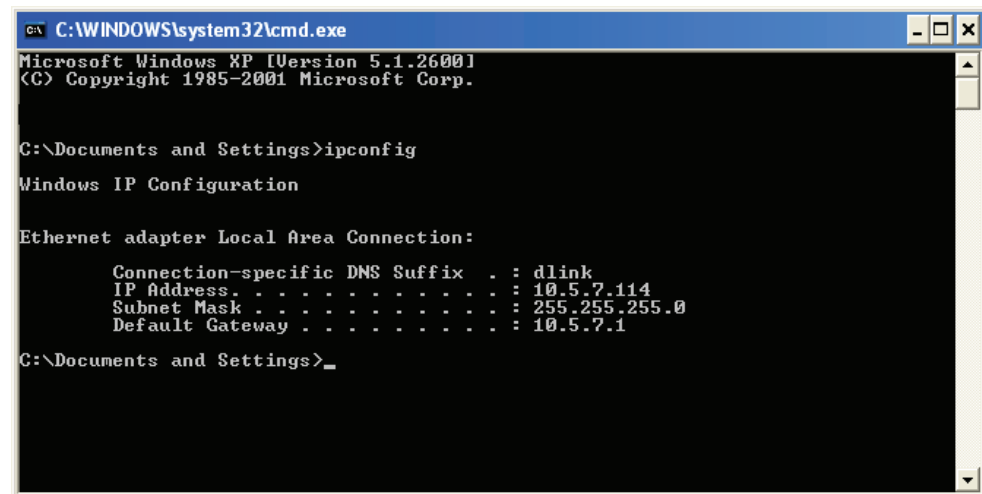
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start > Run**. In the run box type **cmd** and click **OK**. (Windows® 7/Vista® users type **cmd** in the **Start Search** box.)

At the prompt, type **ipconfig** and press **Enter**.

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

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



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : dlink
    IP Address . . . . . : 10.5.7.114
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.5.7.1

C:\Documents and Settings>_
```

Statically Assign an IP address

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

- Step 1**
- Windows® 7 - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center.**
 - Windows Vista® - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.**
 - Windows® XP - Click on **Start > Control Panel > Network Connections.**
 - Windows® 2000 - From the desktop, right-click **My Network Places > Properties.**

Step 2
Right-click on the **Local Area Connection** which represents your network adapter and select **Properties.**

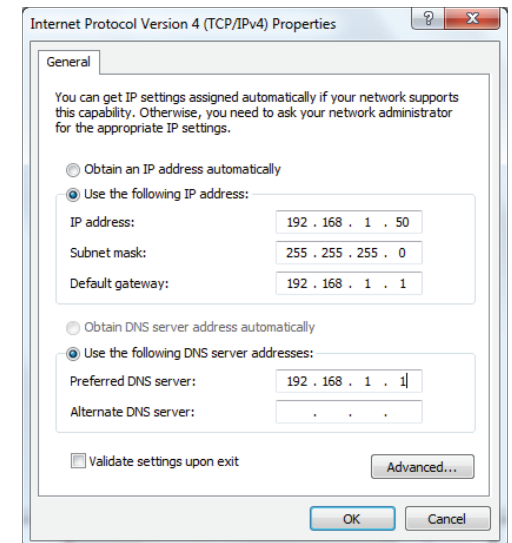
Step 3
Highlight **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties.**

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

Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.1.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set the Default Gateway the same as the LAN IP address of your router (I.E. 192.168.0.1).

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

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



Technical Specifications

Technical Specifications		
General		
Mobile Network Support ²	<ul style="list-style-type: none"> North America <ul style="list-style-type: none"> LTE Cat. 4 Bands 2/4/5/12/13/17 UMTS/HSPA 2/5, 850/1900 Mhz World Wide <ul style="list-style-type: none"> LTE Cat. 4 Bands 1/2/3/5/7/8/20/28/38/40 UMTS/HSPA 1/2/5/8, 850/900/1900/2100 Mhz 	<ul style="list-style-type: none"> Japan <ul style="list-style-type: none"> LTE Cat. 3 Bands 1/3/5/8/9/18/19/21 UMTS 1/6/8/19, 800(19)/800(6)/900/2100 Mhz All regions <ul style="list-style-type: none"> Quadband GSM
Data Throughput ¹	<ul style="list-style-type: none"> LTE Throughput <ul style="list-style-type: none"> NA and WW: Up to 150 Mbps down/50 Mbps Up JP: Up to 100 Mbps down/50 Mbps Up 	<ul style="list-style-type: none"> All Regions <ul style="list-style-type: none"> HSPDA-DC up to 42 Mbps down/5.76 Mbps up Quadband EDGE up to 236.8 kbps
Device Interfaces	<ul style="list-style-type: none"> 1 x 10/100 Fast Ethernet WAN port 1 x 5.5 mm DC input 	<ul style="list-style-type: none"> 2 x SMA (antenna connectors) Dual Micro-SIM slots
Standards	<ul style="list-style-type: none"> IEEE 802.3i 	<ul style="list-style-type: none"> IEEE 802.3u
Advanced Features	<ul style="list-style-type: none"> QoS engine (Quality of Service) L2TP/PPTP/IPSec VPN Client/Server modes SNMP and D-View 7 Support 	<ul style="list-style-type: none"> Firmware over the air (FOTA) upgrades Web-based UI TR-069 CPE WAN Management Protocol
Physical		
LED Status Indicators	<ul style="list-style-type: none"> Power Internet Connectivity Network Status 	<ul style="list-style-type: none"> Signal Strength Ethernet
Power	<ul style="list-style-type: none"> 5V/2A adapter 	<ul style="list-style-type: none"> Flexible input: DC 5V/2A ~ 18V/0.7A
Enclosure	<ul style="list-style-type: none"> Corrosion-resistant zinc-plated steel 	
Dimensions	<ul style="list-style-type: none"> 93 x 70 x 23.6 mm (3.66 x 2.76 x 0.92 in) 	
Weight	<ul style="list-style-type: none"> 210 g (7.41 oz) 	
Temperature	<ul style="list-style-type: none"> Operating: -20 to 60 °C (-4 to 140 °F)³ 	<ul style="list-style-type: none"> Storage : -40 to 85 °C (-40 to 185 °F)³
Humidity	<ul style="list-style-type: none"> Operating: 5% to 85% non-condensing 	<ul style="list-style-type: none"> Storage: 0% to 95% non-condensing
Certifications	<ul style="list-style-type: none"> RoHS CE FCC 	<ul style="list-style-type: none"> TELEC (optional) JATE (optional)

Order Information	
<i>Part Number</i>	<i>Description</i>
DWM-312	4G LTE M2M Router

¹ Data rates are theoretical. Data transfer rate depends on network capacity, signal strength, and environmental factors.

² Available frequencies and speeds vary and may not be available in all regions.

³ Default power adaptor operating temperature range limited to 0 to 40 °C (32 to 104 °F). An optional power adaptor supports 20 to 60 °C (-4 to 140 °F).

Updated 2017/05/16

Regulatory Information

Federal Communication Commission Interference Statement

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

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

Non-modifications Statement:

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

Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Note

The country code selection is for non-USA models only and is not available to all USA models. Per FCC regulations, all WiFi product marketed in the USA must be fixed to USA operational channels only.

IMPORTANT NOTICE:

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

NCC 警語：

以下警語適用台灣地區

依據 低功率電波輻射性電機管理辦法

第十二條: 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條: 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

電磁波曝露量MPE標準值(MPE) 0.9 mW/cm^2 ，送測產品實值為 0.0738 mW/cm^2

減少電磁波影響，請妥適使用。

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. rendeletnek. 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 2014/53/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-samræmisýfirlýsinguna 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 ohne einen 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, 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 u het product aanraakt.
- U mag nooit proberen het product te onderhouden en u mag het product nooit demonteren. Voor sommige producten met door de gebruiker te vervangen batterij, dient u de instructies in de gebruikershandleiding te lezen en te volgen.
- Mors geen voedsel of vloeistof op uw product en u mag nooit voorwerpen in de openingen van uw product duwen.
- Gebruik dit product niet in de buurt van water, gebieden met hoge vochtigheid of condensatie, tenzij het product specifiek geclassificeerd is voor gebruik buitenshuis.
- Houd het product uit de buurt van radiators en andere warmtebronnen.
- U dient het product steeds los te koppelen van de stroom voordat u het reinigt en gebruik uitsluitend een droge pluisvrije doek.

Disposing of and Recycling Your Product

ENGLISH

EN



This symbol on the product or packaging means that according to local laws and regulations this product should 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 réglementations 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. Někteří 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.

Suosittellemme, 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 materiais 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.