D-Link®

Version 1.00 | 05/15/2018

User Manual

Outdoor Internet Antenna

DWP-902

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 15, 2018	• 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.

Table of Contents

Product Overview 1
Package Contents 1
System Requirements 1
Introduction 2
Hardware Overview 3
Front View 3
Top Panel 4

Installation 5
Connecting to your Network 5

Configuration 6
Getting Started 6
Internet 7
WAN Service 7
SIM 7
Network Status 7
APN Settings 8
APN Configuration 9
Connection Settings 11
IPv4 and IPv6 info 12
Device Mode 13
Router Mode 14
LAN 15
IPv4 15
LAN Settings 15
DHCP 16
IPv6 17
IPv6 Config 17
Internet Connection Type 18
VPN 19
VPN Settings 19
Advanced 20
DNS 20
DNS 20
DNS Redirect 21
Firewall 22
Outbound Filter 22
Inbound Filter 23
URL Filter 24
MAC Address Filter 25
DMZ 26
QoS 27
SNMP 28
TR-069 30
Virtual Server 31
UPnP 32
Network Scan 33
Email Settings 34
System 35
Administration 35
Password Settings 35
Remote Login Settings 36

Configuration Backup 37
SMS 38
SMS Inbox 38
Compose SMS 39
Time Settings 40
Firmware Upgrade 41
Device Upgrade 41
System Log 42
Schedules 43
Schedule Rule Setting 43
Reboot and Reset 44
Reboot the Device 44
Connection Reset 45

Troubleshooting 46

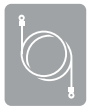
Networking Basics 50
Check your IP address 50
Statically Assign an IP address 51

Technical Specifications 52

Regulatory Information 53

Package Contents


DWP-902 Outdoor Internet Antenna


Grounding Wire

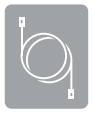

Grounding Screw


Quick Start Guide


Mounting kit (Pole Mount)


PoE Injector DPE-301GI


Power Adapter (54 V/0.6 A)


RJ-45 Ethernet Cable


Warranty Card


GPL Sheet

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

System Requirements

- Computer with Windows, macOS, or Linux-based operating system, and an Ethernet adapter installed
- Internet Explorer 7.0, Mozilla Firefox® version 12.0, Safari 4.0, or Chrome 20.0 or newer
- A U.S. Cellular®-provided home router, switch, or Wi-Fi access point is strongly recommended.

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

Introduction

The D-Link DWP-902 Outdoor Internet Antenna is an easy-to-deploy, high performance 4G LTE router. It features a dedicated Gigabit Ethernet port and 4G LTE mobile broadband for maximum redundancy and flexibility for intense Internet applications in remote areas. Rugged design and flexible deployment options combined with ease of use make the DWP-902 ideal for both large-scale and individual deployments.

Easily connect to your high-speed 4G LTE mobile service with the DWP-902 Outdoor Internet Antenna, and enjoy fast downlink speeds of up to 300 Mbps[1] and uplink speeds up to 50 Mbps[1], giving you the speed you need for fast, responsive Internet access. The blazing fast LTE connection allows multiple users to access e-mail and stream music and video on the go.

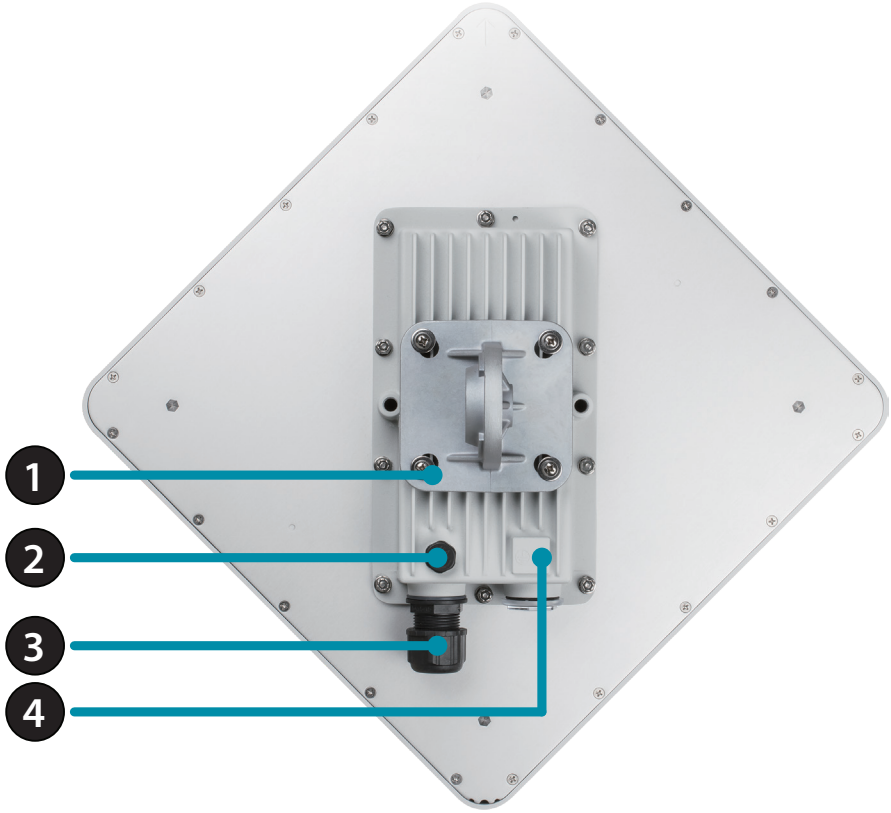
The industrial grade casing means that the DWP-902 provides reliable high-speed connectivity in extreme conditions. Specially built for outdoor use, the IP67 weather resistant housing helps protect it from dirt and rain. Pole mounting and sturdy brackets allow the device to be installed virtually anywhere for optimal connectivity, giving you the freedom to install it right where signal is strongest.

The DWP-902 Series features built-in 6 kV surge protection on its PoE Ethernet access port, and requires no external surge protection devices. The enclosure is also able to resist direct static discharges of up to 4 kV. This effectively protects the device against sudden electrical surges caused by events such as lightning strikes or unstable electrical current. This protection significantly reduces the chance of equipment being damaged by electrical surges, and effectively lowers maintenance costs by minimizing the need for expensive equipment repairs or replacement.

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

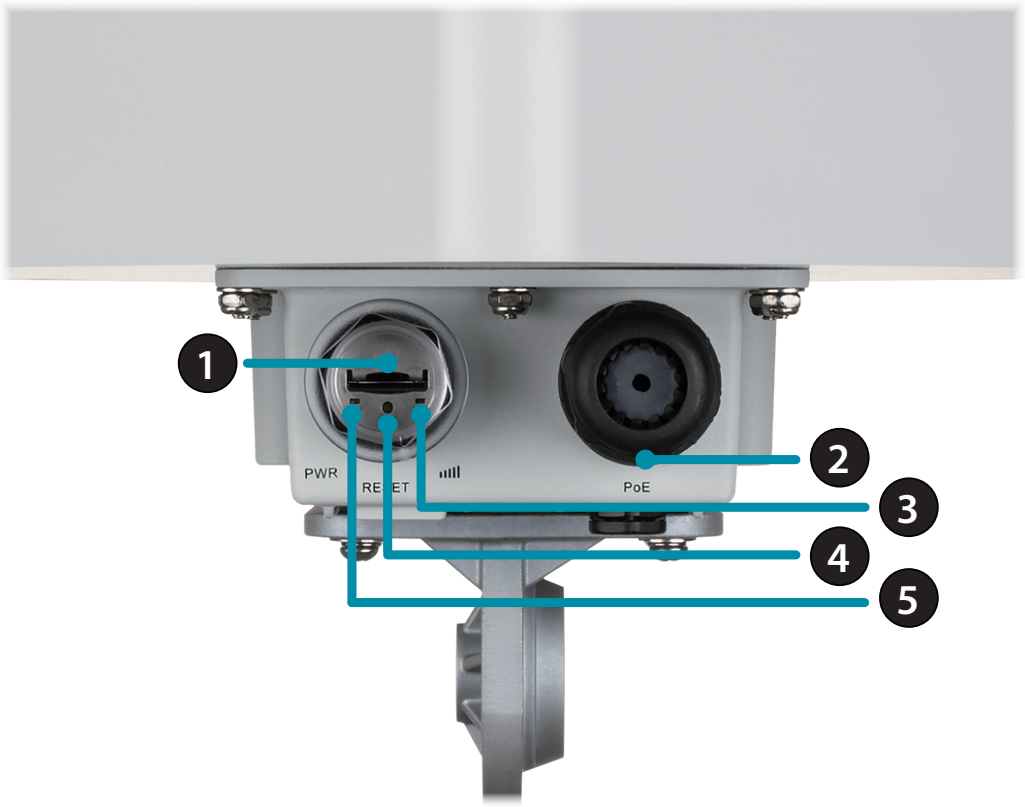
Hardware Overview

Front View



1	**Pole Mount**	Fastens the device to a pole for optimal signaling.
2	**Pressure Release**	Equalizes air pressure. Leave sealed for normal operation.
3	**Weather-resistant Cable Gland**	Connect a PoE Ethernet cable to power the device and connect to your network.
4	**Grounding Point**	Connect a grounding wire from this screw to ground to help the device resist electro-static discharge.

Top Panel



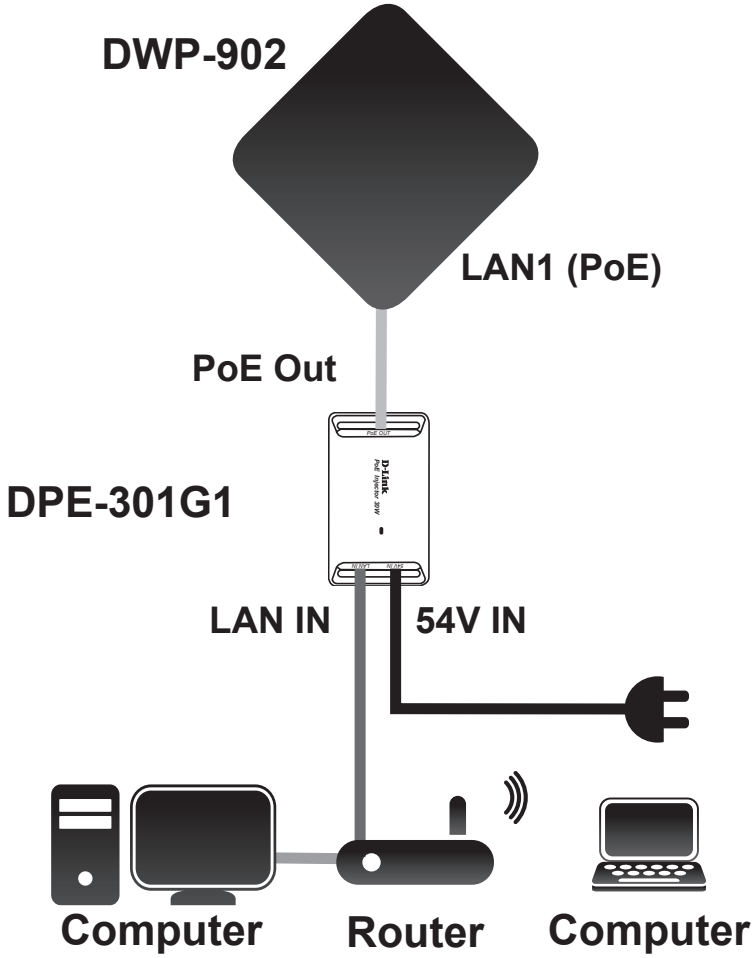
1	**Mini-SIM Card Slot**	Verify a Mini-SIM/UICC card is installed and activated by your carrier.
2	**Weather-resistant Cable Gland**	Connect a PoE Ethernet cable to power the device and connect to your network.
3	**LED Signal Indicator**	Illuminates green for good signal, orange for fair signal, or red for poor signal. Flashes to indicated data transfer.
4	**Reset Button**	Resets the device to factory defaults. Press and hold this button for 10 seconds to reset the device to defaults.
5	**LED Power Indicator**	Illuminates solid red when a power source is connected.

Installation
Connecting to your Network

A. Connect an Ethernet cable from the Outdoor Internet Antenna to the "PoE OUT" port on the PoE Injector.

B. Connect an Ethernet cable from a router/switch or PC to the "LAN IN" port on the PoE Injector.

C. Attach the power adapter to the connector labeled "54V IN" on the PoE Injector, then connect it into an electrical outlet.



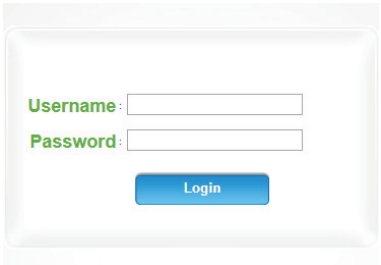
Configuration

Getting Started

To access the configuration utility, open a web browser such as Internet Explorer and enter the address of the router (**192.168.17.1** by default).

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

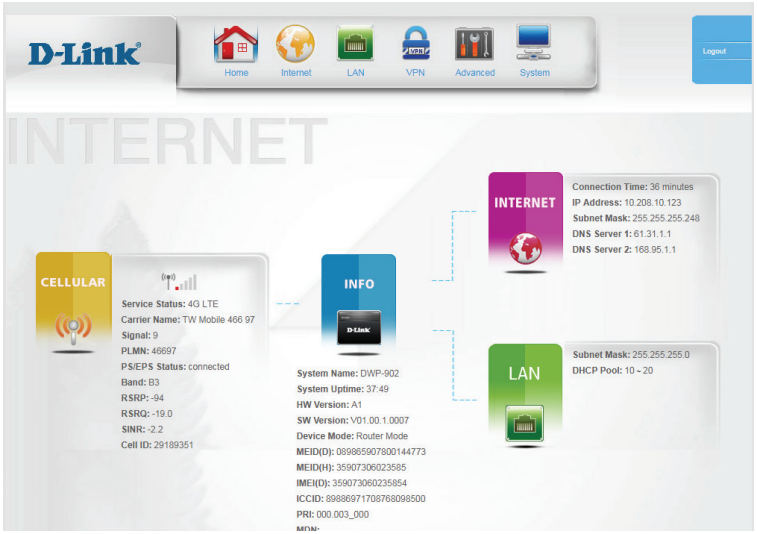
Note: *If you get a* ***Page Cannot be Displayed*** *error, please refer to the* ***Troubleshooting*** *section for assistance.*



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.



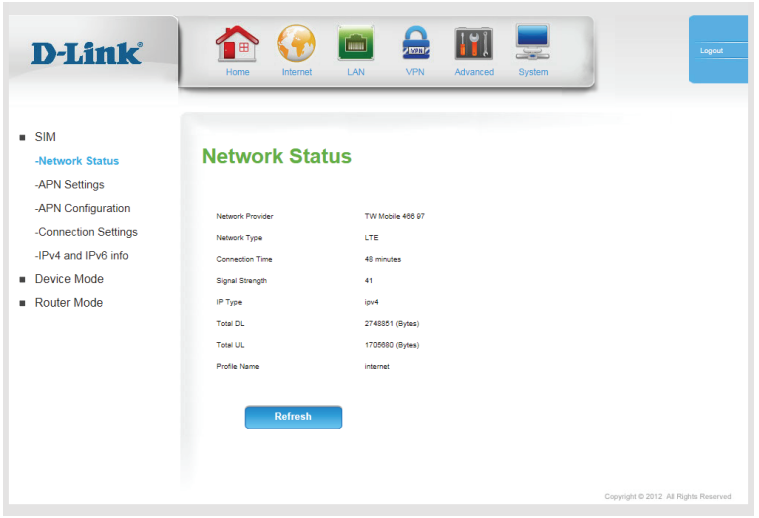
Internet

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 DWP-902 requires a SIM card and active cellular internet service to connect to the Internet.

SIM

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.

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 9.

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**.

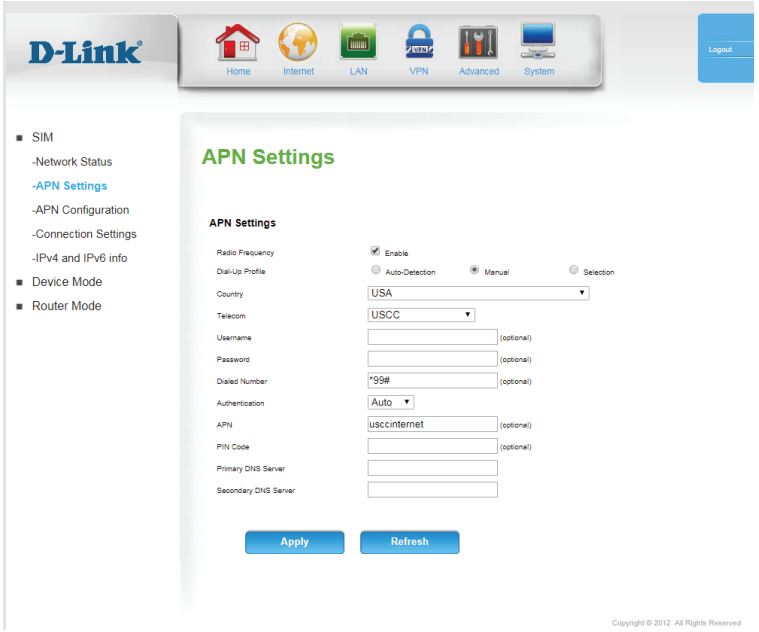
APN: Enter the APN information (optional).

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.



APN Configuration

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

Profile Name: Indicates the name of the profile.

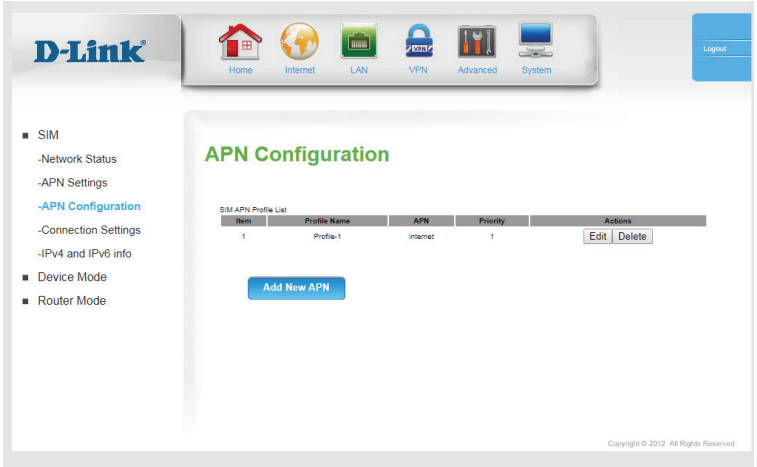
APN: Indicates the access point name (APN) in use by the selected profile.

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.

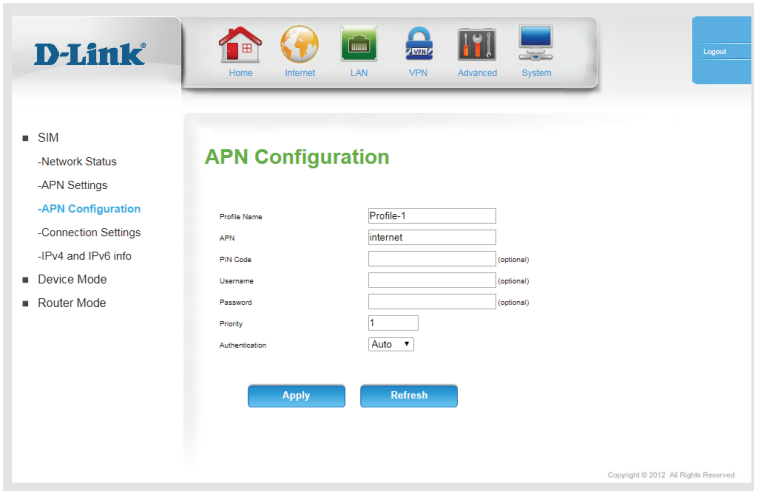
Actions: Click **Edit** to edit the corresponding profile, described in **New/Edit APN Profile** on page 10. Click **Delete** to delete the profile.

Add New APN: Click **Add New APN** to create a new APN, described in **New/Edit APN Profile** on page 10.

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

Connection Settings

Prefer Service Type: Choose whether the DWP-902 should only use 4G networks, 3G networks, 2G networks, or use **Auto Mode** to automatically select a network. As of this writing, the device supports **LTE Only Mode**.

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

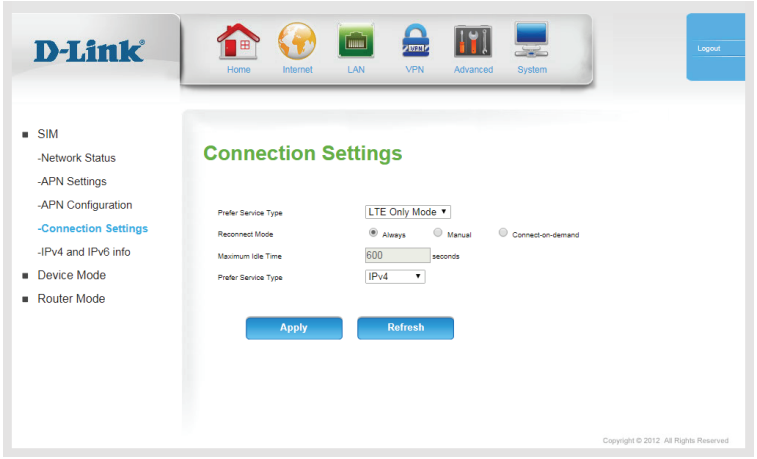
Note: Roaming connections may incur additional fees from your service provider.

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.

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.



IPv4 and IPv6 info

IPv4

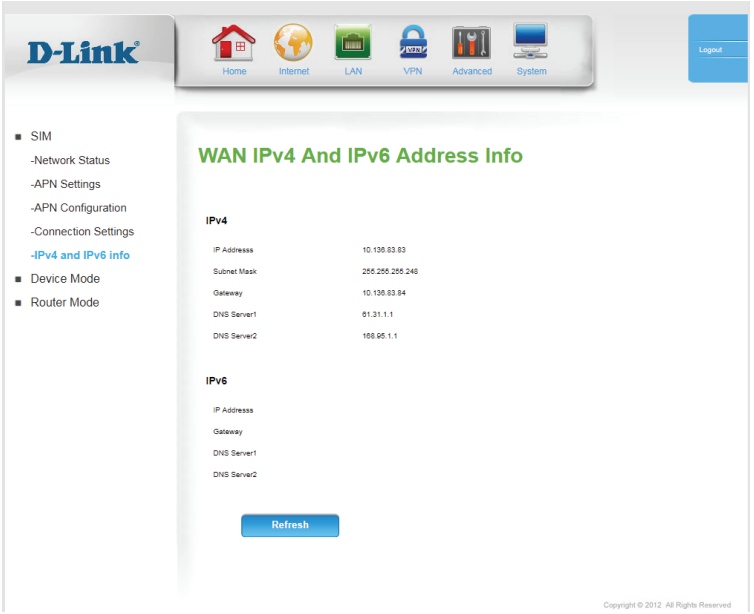
IP Address: Shows the IPv4 address of the current connection.

Subnet Mask Shows the subnet mark of the current connection.

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 connection.

Gateway: Shows the gateway used by the current connection.

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

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

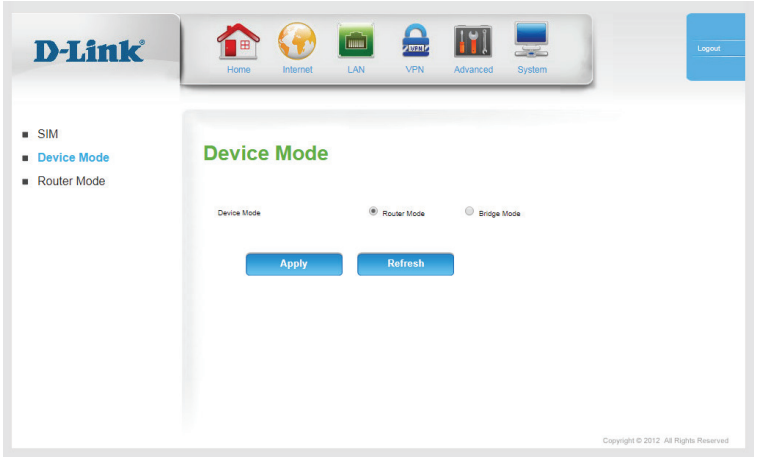
Click **Refresh** to update this page.

Device Mode

Device Mode: **Router Mode** is the default mode, which enables NAT and DCHP. In this configuration, the DWP-902 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 DWP-902 acts as a simple modem, and IPs are assigned directly by the ISP.

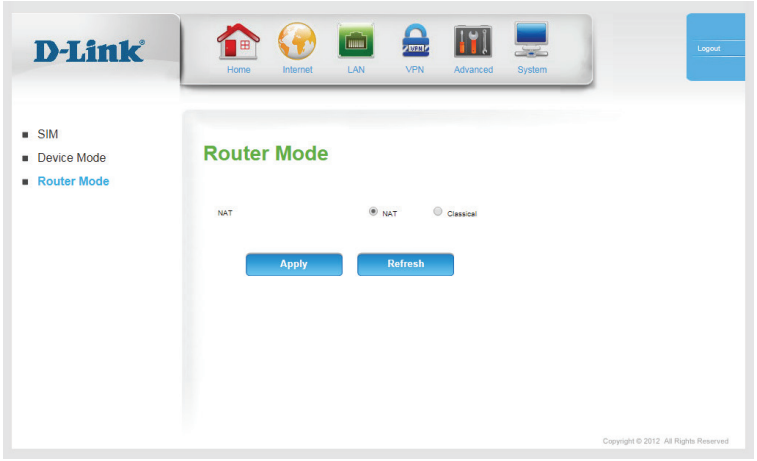
Click **Apply** to save your settings, or **Refresh** to revert to your previous settings.



Router Mode

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

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



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.

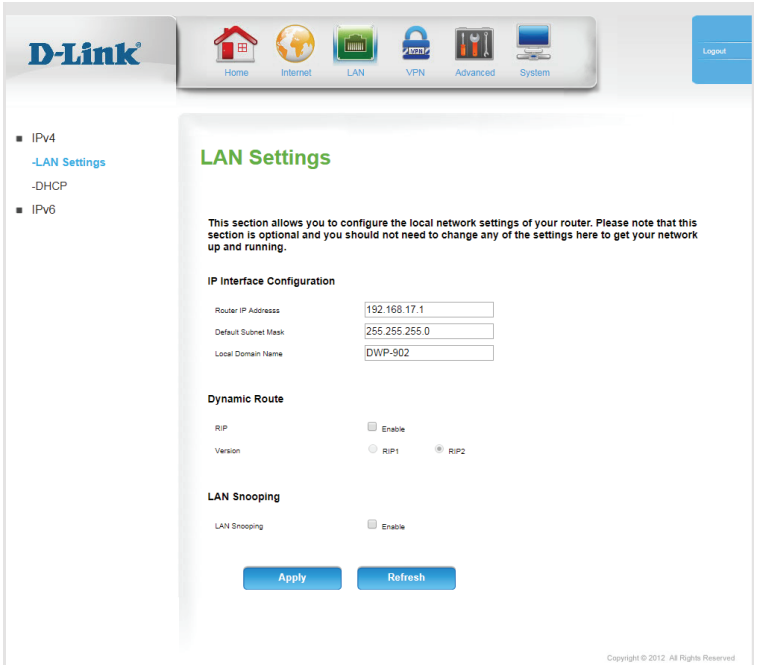
Default Subnet Mask: Enter the subnet mask of the router. The default subnet mask is **255.255.255.0**.

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

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

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

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



DHCP

The DWP-902 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.

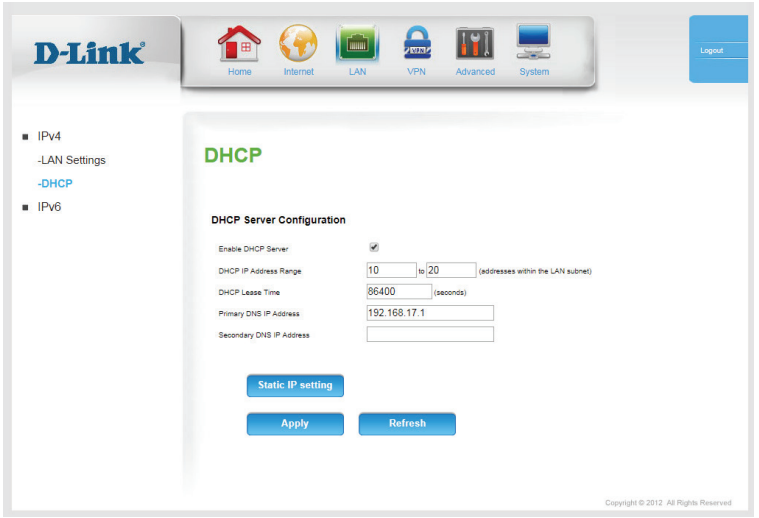
Primary DNS IP Address: Enter the primary DNS IP address that will be assigned to DHCP clients.

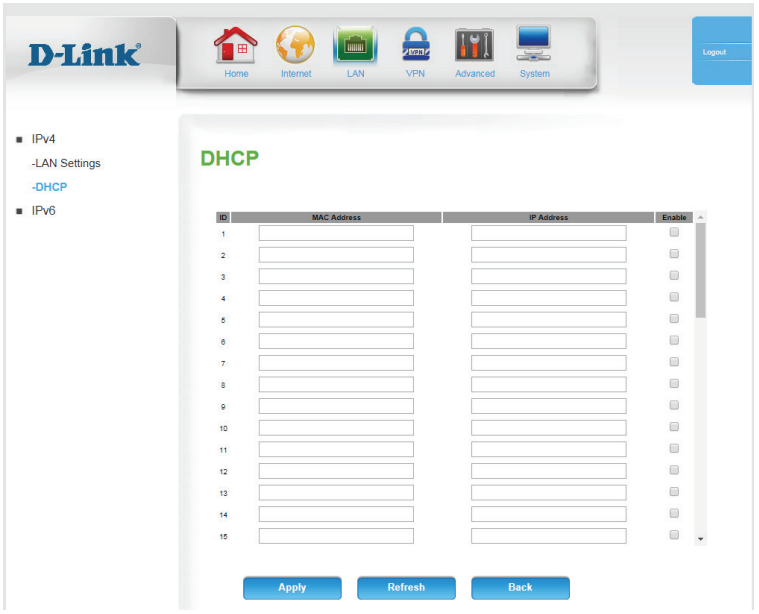
Secondary DNS IP Address: Enter the secondary DNS IP address that will be assigned to DHCP clients.

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.



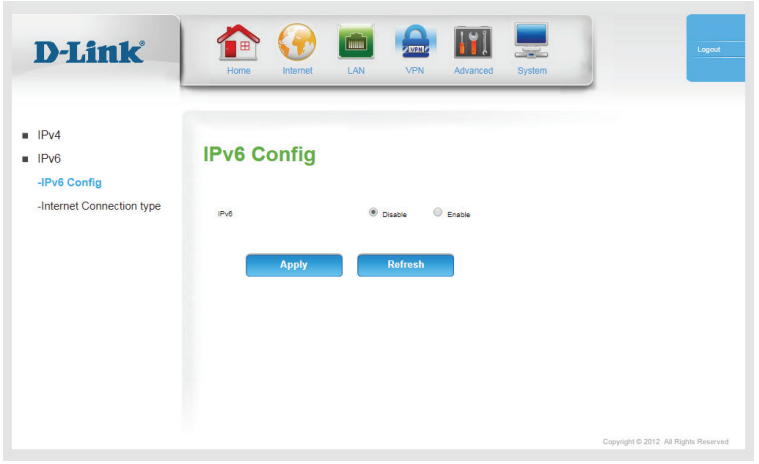


IPv6
IPv6 Config

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 DWP-902 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).

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

VPN

The DWP-902 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. As of this writing, the DWP-902 supports passthroughs for major VPN protocols.

VPN Settings

IPSec Passthrough: Select **Enable** to enable IPSec passthrough.

PPTP Passthrough: Select **Enable** to enable PPTP passthrough.

L2TP Passthrough: Select **Enable** to enable L2TP passthrough.

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

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.

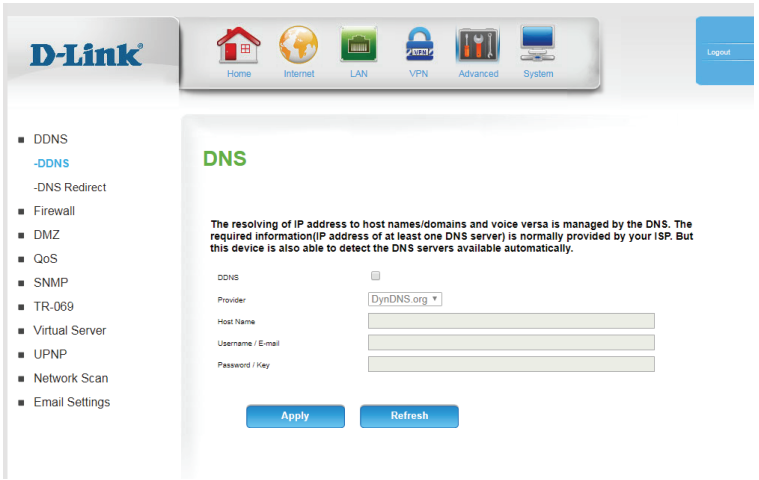
Provider: Select a DDNS service provider to use.

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.



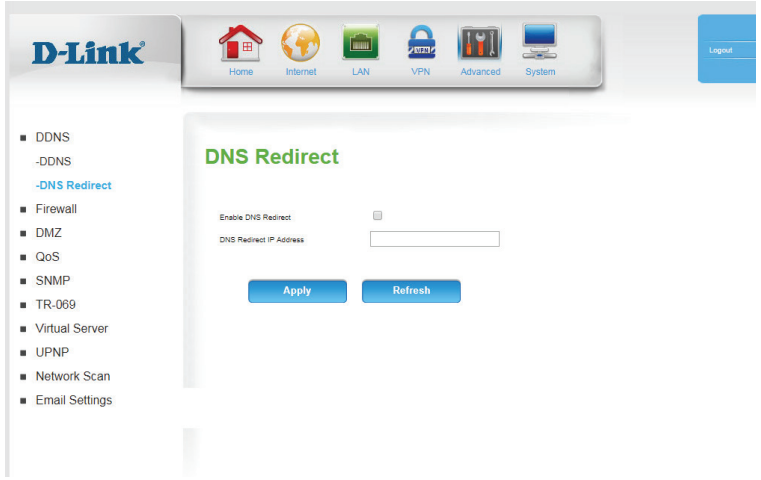
DNS Redirect

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.

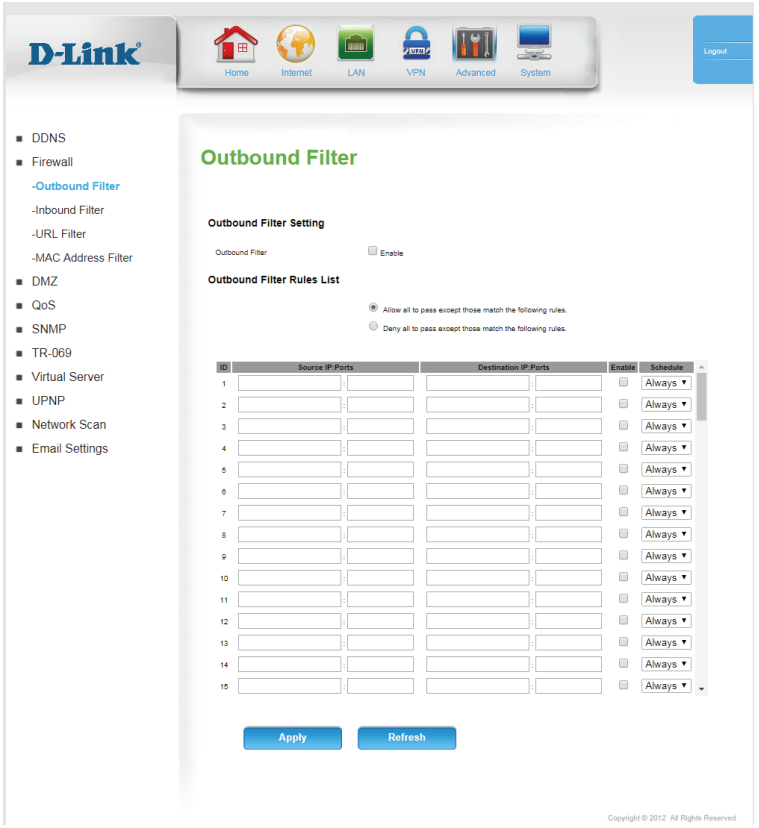
DNS Redirect IP Address: Enter the IP that should be returned whenever a DNS request is sent to the router. All URLs queried through the router's DNS will redirect to the same location.

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 43.

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.

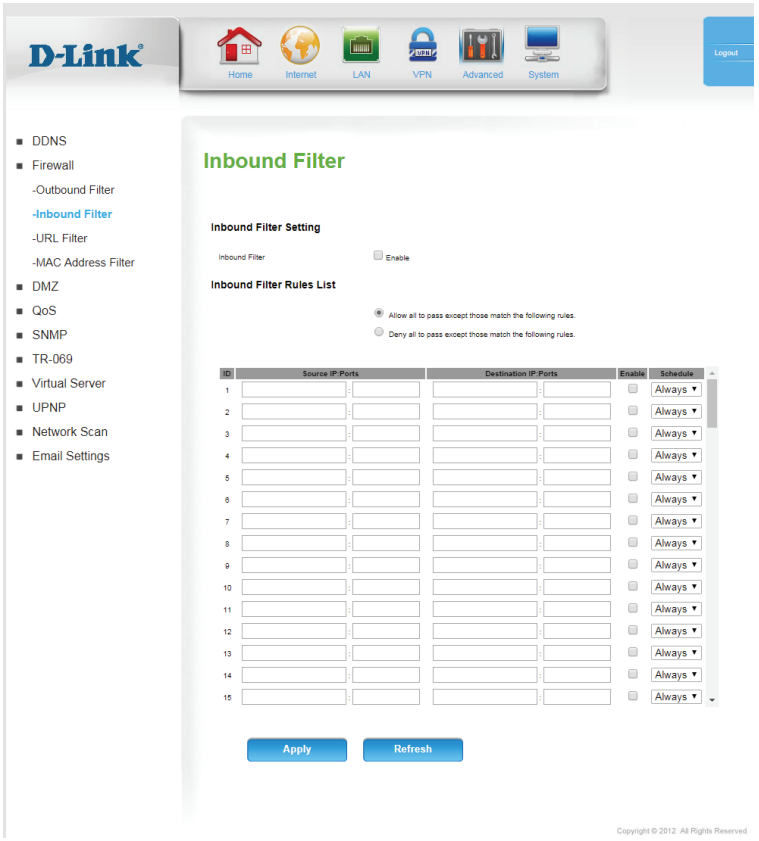
Previous Page: Click to go back to the previous filter page.

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

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

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 43.

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.

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.

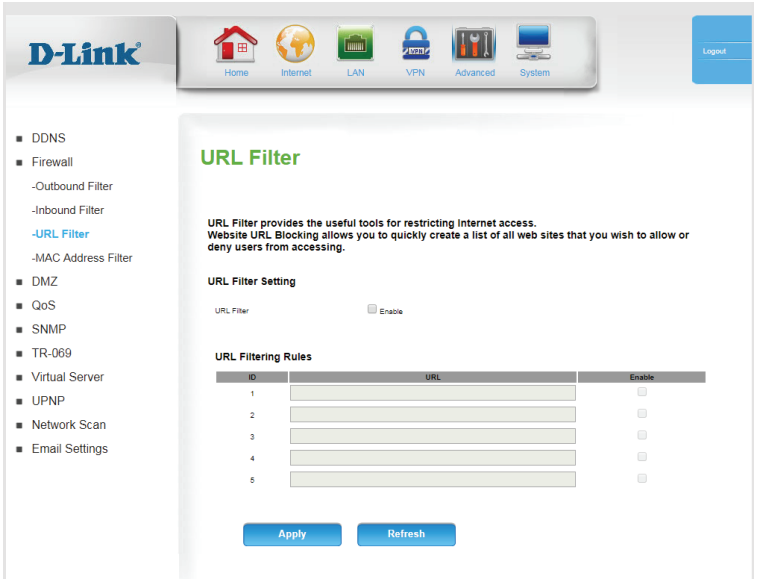
URL FILTERING RULES

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.

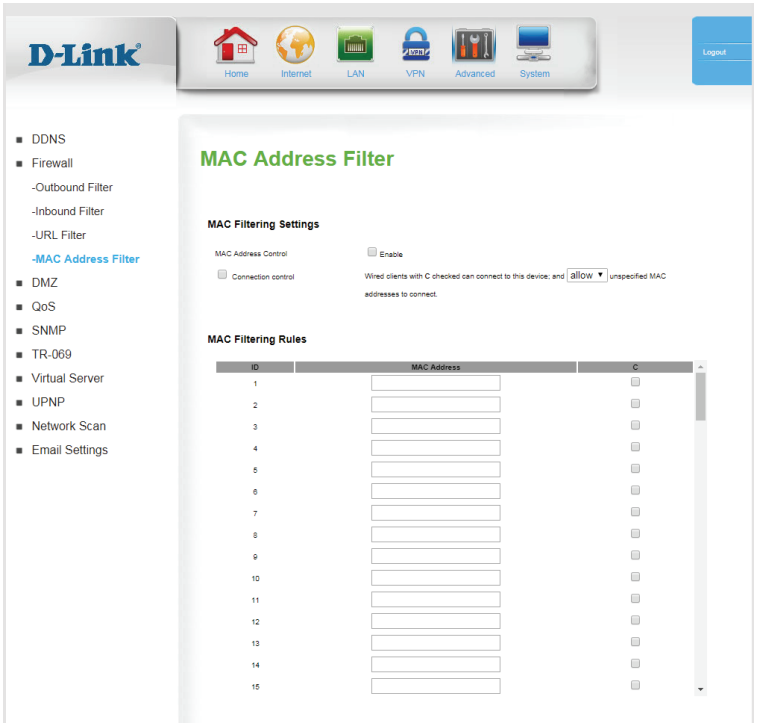
Enable: Check the box to enable the specified rule.

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



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.

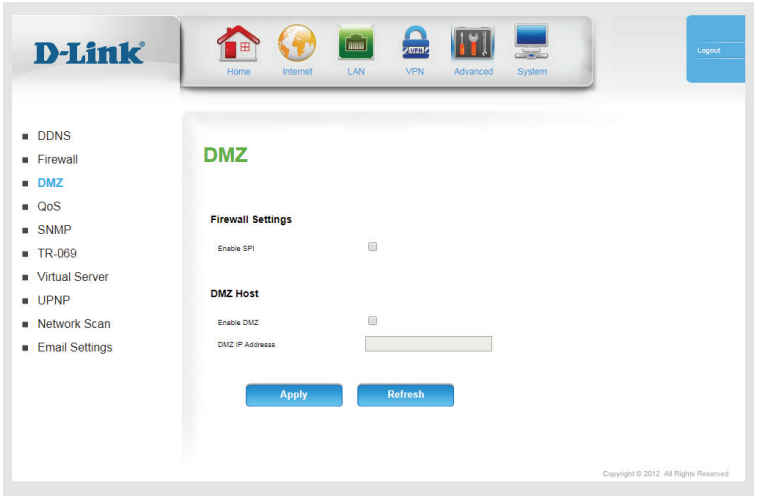
MAC Address: Specify the MAC address of the computer to be filtered.

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.

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.

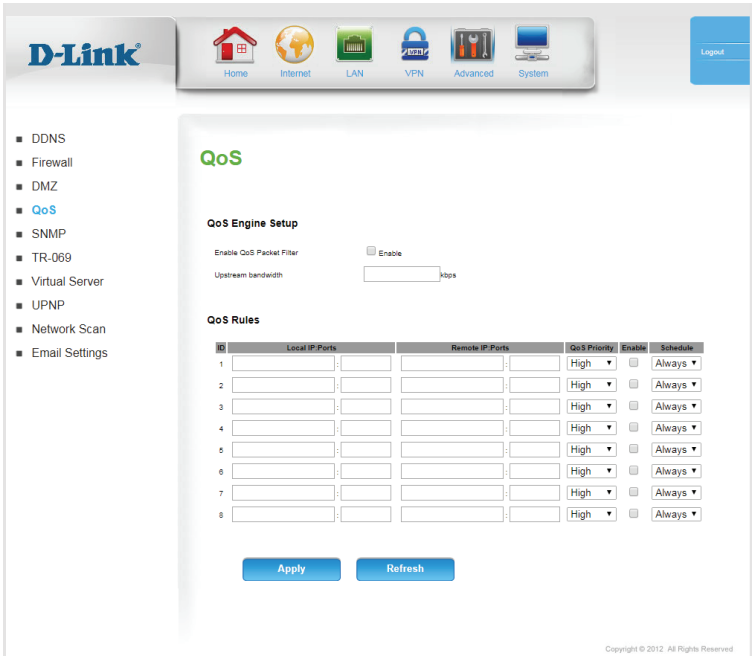
Note: Placing a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is recommended for advanced users only.

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** can 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 Packet Filter: Select this box to enable the QoS feature.

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 43.

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**.

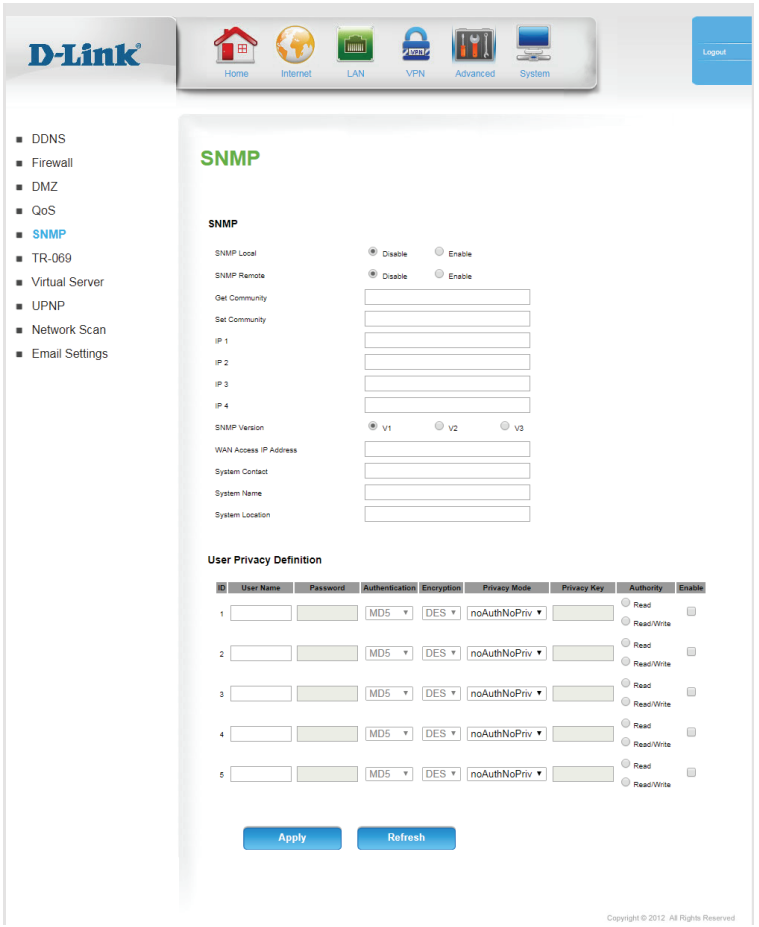
Enable: Check the box to enable the specified rule.

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 43.

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

SNMP

SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol that reports activity on each network device to the administrator of the network. SNMP can be used to monitor traffic and statistics of the DWP-902. The DWP-902 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.

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.

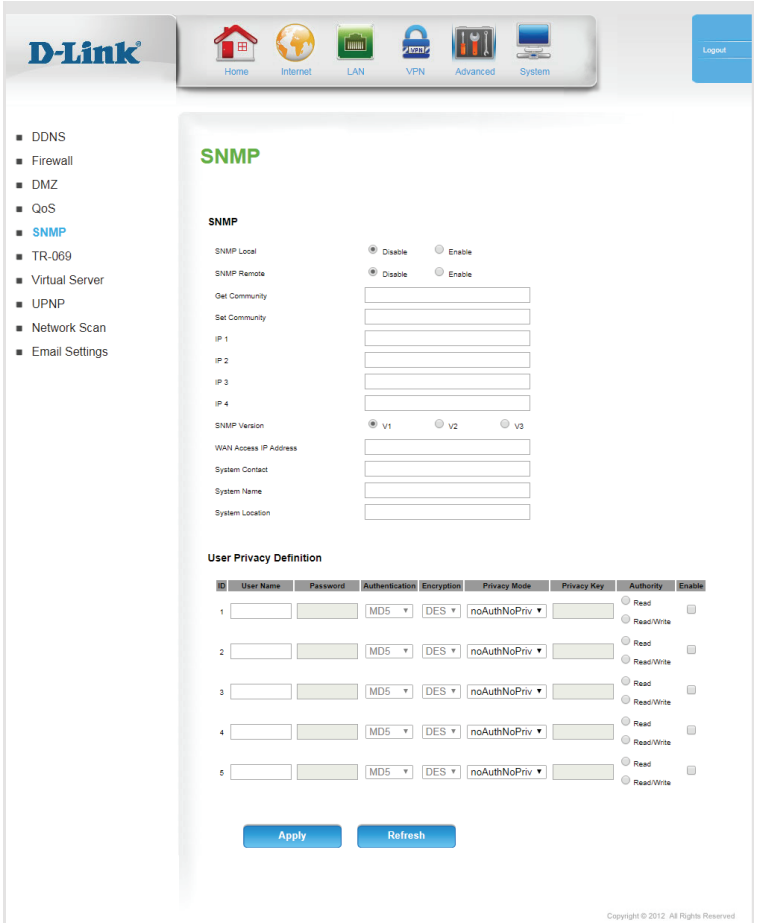
Privacy Key: If encryption is enabled, enter a key between 8 and 27 ASCII characters in length.

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.

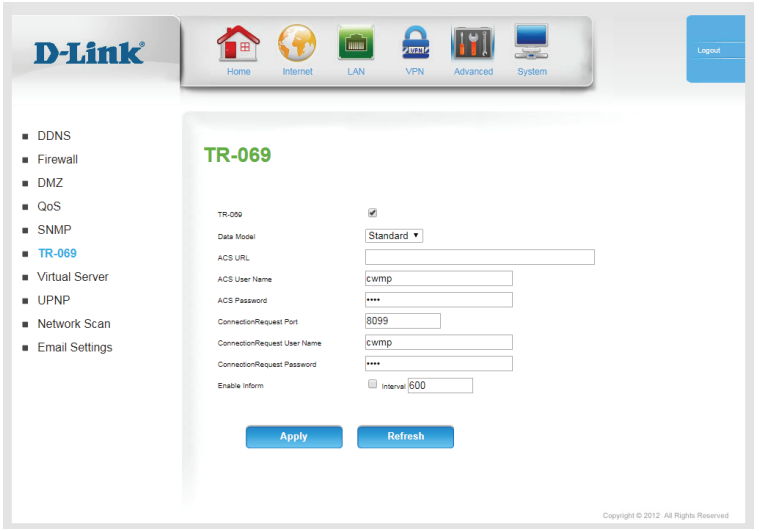
Actions: Click **Edit** to make changes to the corresponding account.

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



TR-069

TR-069 is a WAN a management protocol that allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.



TR-069: Select to enable or disable TR-069 client functionality.

Data Model: Select a data model used to communication with the ACS.

ACS URL: Enter the URL of your ISP's ACS.

ACS User Name: Enter the authentication user name.

ACS Password: Enter the authentication password.

Connection Request Port: Specify a port for the connection request.

Connection Request User Name: Enter the connection user name for the ACS login.

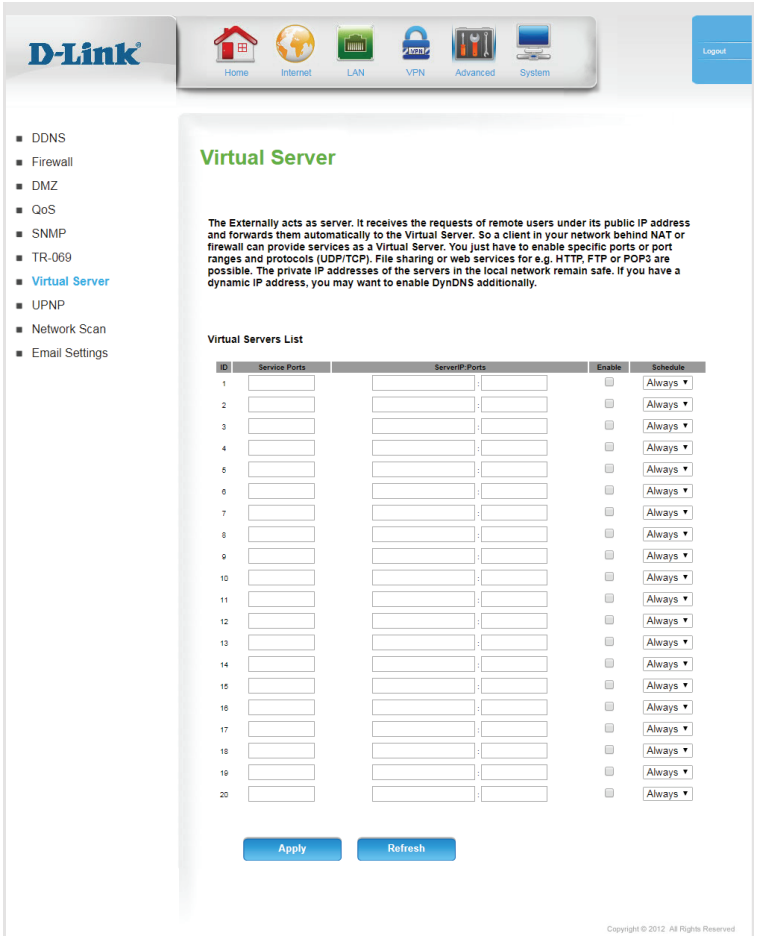
Connection Request Password: Enter the connection password for the ACS to login.

Enable Inform Select to enable TR-069 inform message functionality. If enabled, specify an interval in seconds.

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

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 43.

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.

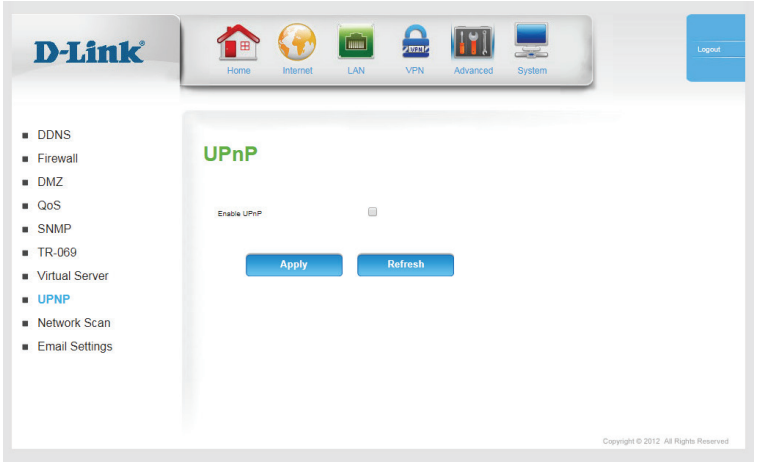
Schedule Rule #: Specify the schedule rule number. To create schedules, click on the **Add New Rule** button. For further information on schedules, please refer to **Schedules** on page 43.

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

UPnP

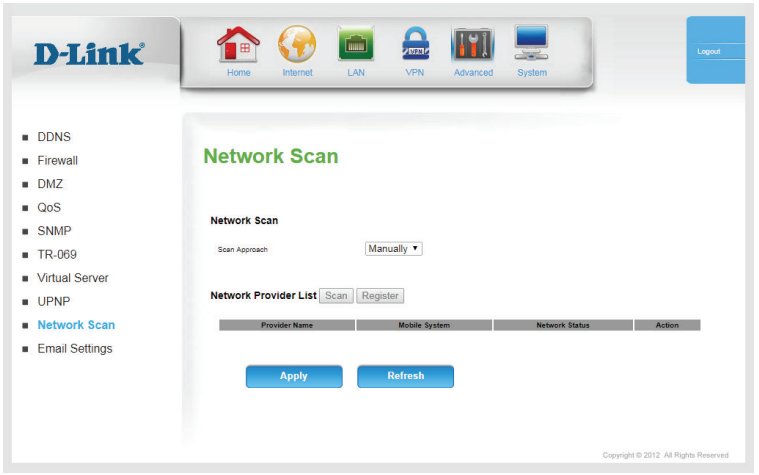
Enable UPnP: Check the box to enable the Universal Plug and Play (UPnP™) feature. UPNP provides compatibility with various networking equipment, software, and peripherals.

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 DWP-902 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 DWP-902 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.

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.

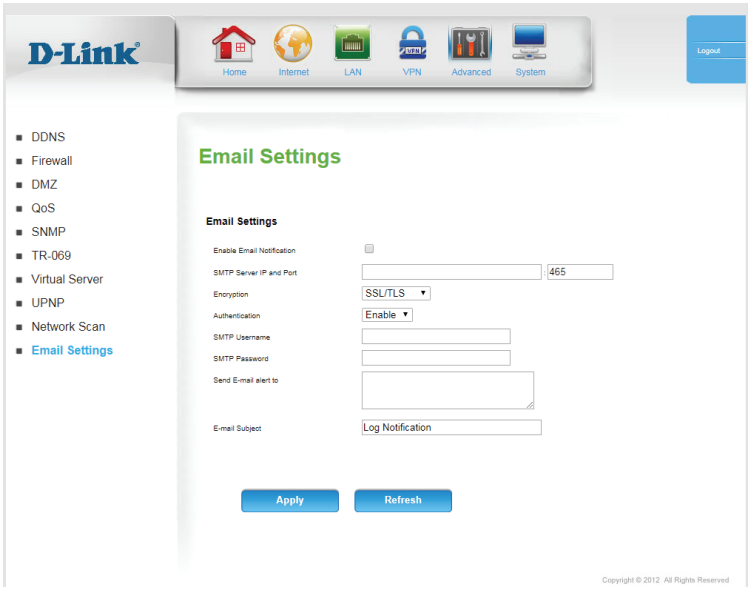
SMTP Password: Enter the password for the SMTP account.

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.

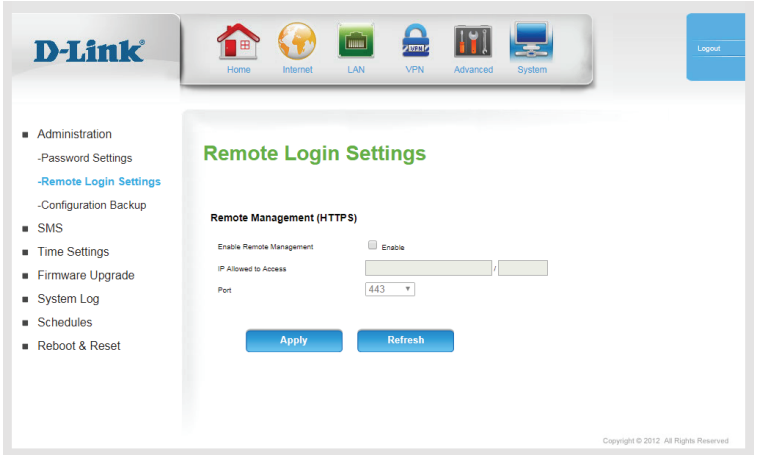
Remote Login Settings

Enable Remote Management: Tick this check box to enable remote management. Remote management allows the DWP-902 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.



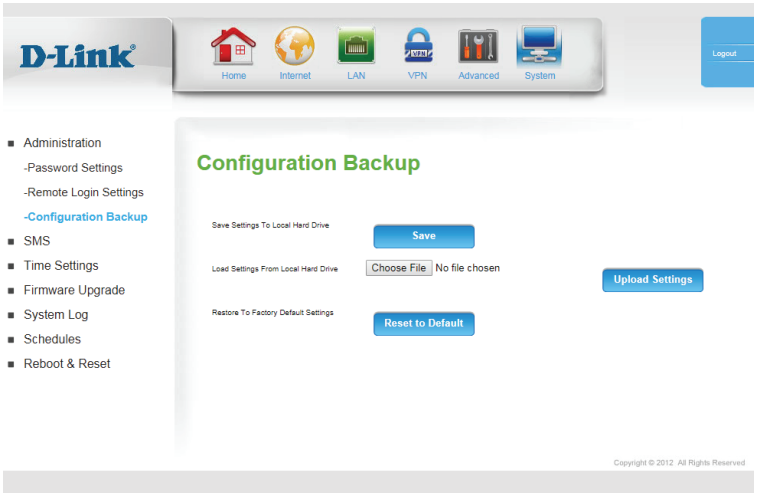
Configuration Backup

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.

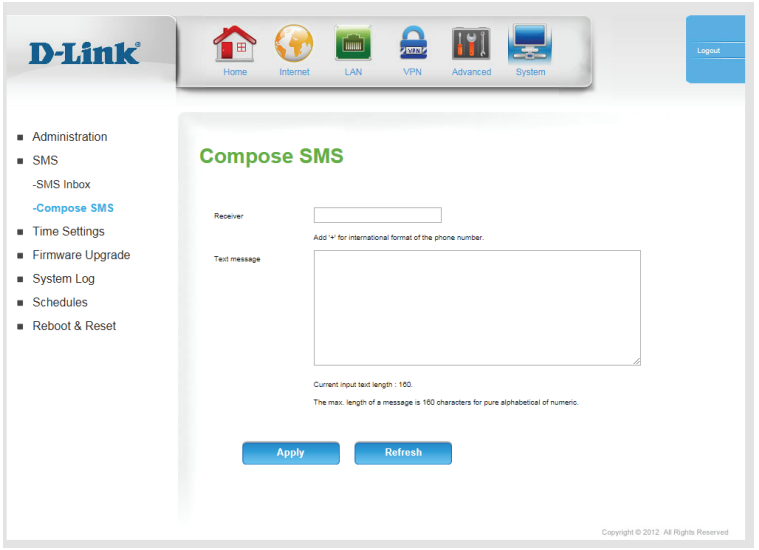
Compose SMS

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.

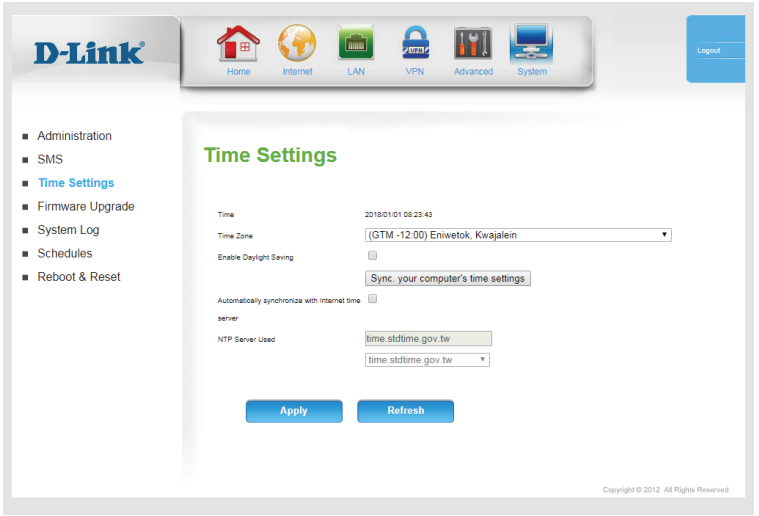
Text Message: Type the message that you would like to send.

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



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.

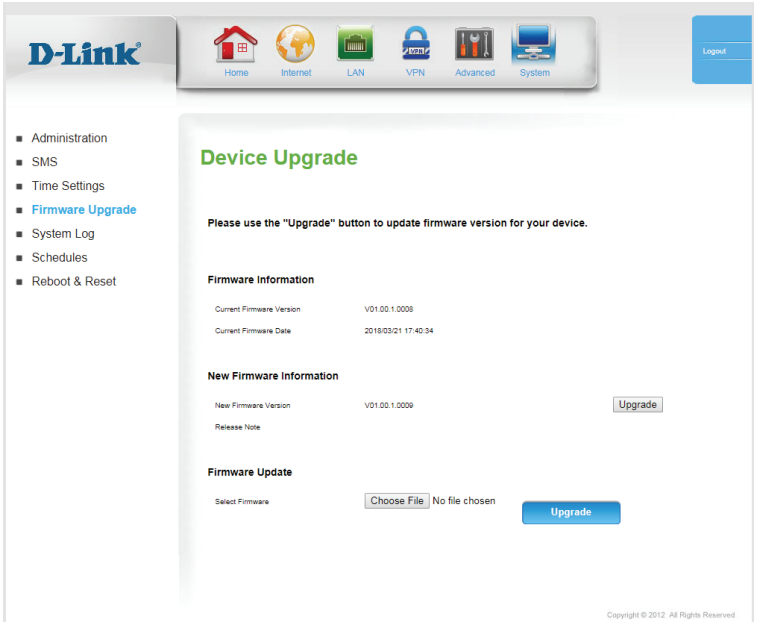
NTP Server Used: Enter an NTP server to use for time synchronization, or use the drop-down box to select one. Click the **Update Now** button to synchronize the time with the NTP server.

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

Firmware Upgrade

Device Upgrade

Here, you can upgrade the firmware of your router. The DWP-902 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.

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

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

New Firmware Version: This will appear if your device detects new firmware available over the Internet. Click the **Upgrade** button to begin the update process.

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

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

System Log

The DWP-902 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.

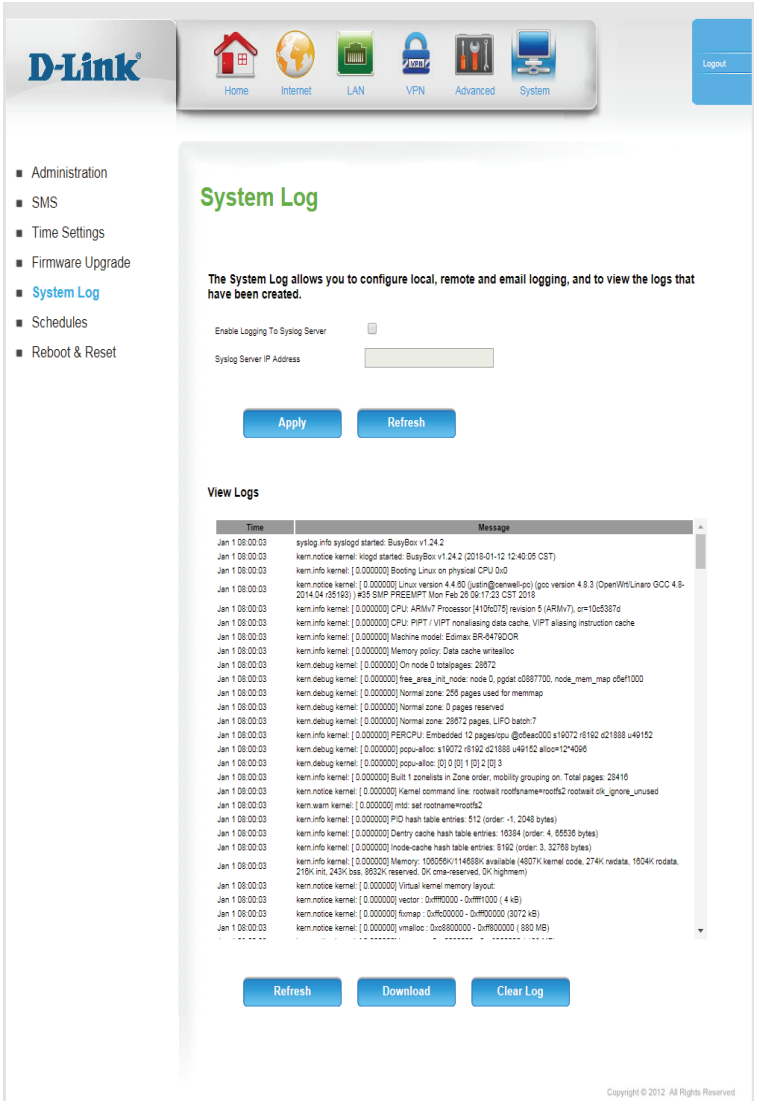
First Page: Click to go to the first page of logs.

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.

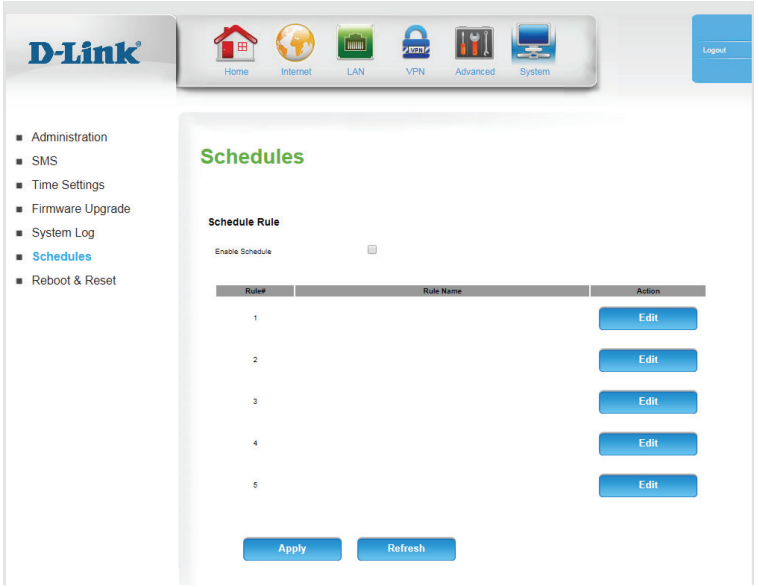


Schedules

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)



Schedule Rule Setting

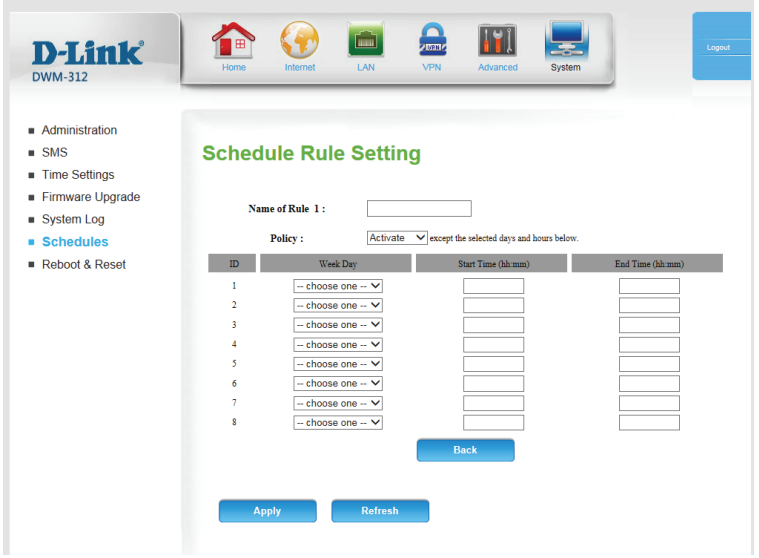
Name of Rule #: Enter a name for your new schedule.

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.

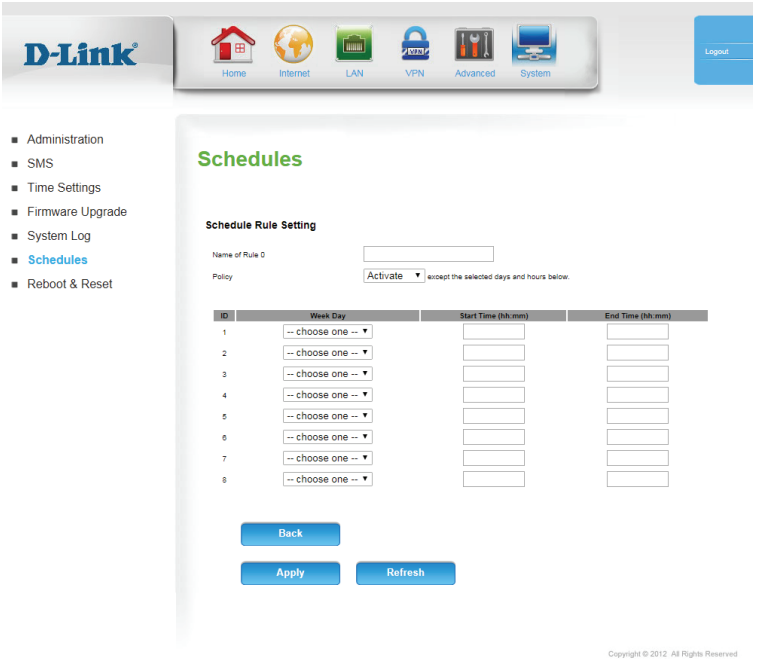
Reboot-Schedule: If the connection reset feature is enabled, select the hour and minute it should be triggered using the dropdown boxes.

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

Weekly Schedule Day of Week: Select this option if you want the connection reset feature to activate only on a certain day of the 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 DWP-902. 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 (**192.168.17.1** 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® version 12.0,or higher
  - Google™ Chrome 20 or higher
  - Safari 4.0 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 bottom 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 **192.168.17.1**. When logging in, leave the password box empty.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C:\>
```

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

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

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

- Navigate to the Internet configuration page (see **Internet** on page 7 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

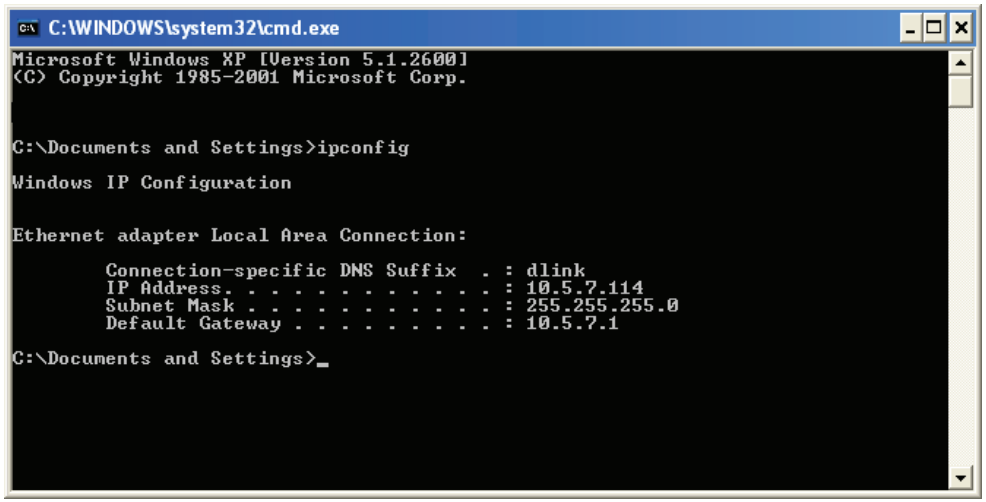
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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.



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

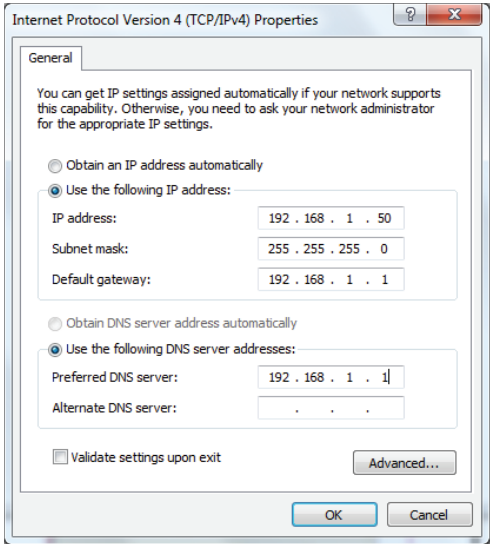
Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

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]	• LTE Cat. 6 Bands 2/4/5/12	
Data Throughput[1]	• LTE Throughput up to 300 Mbps down/50 Mbps up	
Device Interfaces	• 1 x 10/100/1000 PoE Gigabit Ethernet port	• 1 x 2FF Mini-SIM slot
Standards	• IEEE 802.3i • IEEE 802.3af	• IEEE 802.3u
Advanced Features	• QoS engine (Quality of Service) • L2TP/PPTP/IPSec VPN Passthrough	• Firmware Over-the-Air (FOTA) upgrades • Web-based UI
Physical		
LED Indicators	• Power	• Connection status
Surge Protection	• 6 kV	
ESD Protection	• 4 kV	
Power	• 48 V Power over Ethernet	
Enclosure	• Dustproof, water-resistant enclosure	• Compatible with IP67 standard
Dimensions	• 321 x 322 x 185 mm (12.64 x 12.68 x 7.28 in)	
Weight	• 3.18 kg (7 lbs)	
Temperature	• Operating: -30 to 60 ˚C (-22 to 140 ˚F)	• Storage : -40 to 85 ˚C (-40 to 185 ˚F)
Humidity	• Operating: 5% to 85% non-condensing	• Storage: 0% to 95% non-condensing
Certifications	• FCC	
Order Information		
Part Number	*Description*	
DWP-902	Outdoor Internet Antenna	
DPE-301GI	1 Port Gigabit PoE Injector	

[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.
Updated 2018/05/15

Regulatory Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Non-modification Statement

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

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.