



**User Manual**

**4G LTE Outdoor Bridge/Router**

**DWP-902**

# Table of Contents

**Configuration Getting Started .....3**

**Internet.....4**

**LAN.....5**

**VPN .....6**

**Advanced .....7**

**System .....8**

**Specification .....9**

**Regulatory Information .....10**

# 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.



# 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.





# 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.



# 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.



# 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.



The screenshot shows the D-Link DWM 212 web interface. At the top, there's a navigation bar with icons for Home, Status, Logs, Settings, and System. Below this, a sidebar menu lists various configuration options: Administration, Password Settings (highlighted), Remote Login Settings, Configuration Backup, SaaS, Time Settings, Firmware Upgrade, System Log, Schedule, and Network & Flow. The main content area is titled 'Password Settings' and contains three input fields labeled 'Old Password', 'New Password', and 'Confirm Password'. At the bottom of this section are two buttons: 'Apply' and 'Refresh'.



## Specification

<b>Outdoor IP67 LTE router</b>	
<b>LTE module</b>	Sierra EM7455 (M.2 connector) B2/B4/B5/B12 (Cat.6)
<b>Main chip</b>	Dakota IPQ4029* + QCA8072 * Industrial grade, ARM Cortex A7 Quad-Core 710MHz)
<b>LAN</b>	GbE port x1 (802.3af support)
<b>Memory</b>	32M/128M
<b>LED</b>	Signal strength x1, PWR x1 1. On: RSSI> -97 2. Flashing: -97dBm < RSSI < -113dBm 3. OFF: RSSI < -113dBm
<b>SIM slot</b>	2FF (mini SIM)
<b>Reset</b>	One reset button
<b>Water/Dustproof</b>	IP67
<b>Antenna</b>	9dBi patch antenna (320mm x 320mm x 53mm)
<b>Die-cast housing</b>	183mm (L) x 45mm (W) x 91mm (H)
<b>Grounding</b>	Grounding point x1
<b>Surge</b>	6kV
<b>ESD</b>	4kV (contact) 6kV (air)
<b>Operation temp.</b>	-30 to 60° C
<b>PoE injector</b>	Should compatible with DPE-301GI (standard 802.3af/at support)

# 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 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.