User Manual

FIBRE Wi-Fi AC1200 Dual Band Router

DIR-822K

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
2.2	20 Nov 2023	Final

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.

AppleR, Apple logoR, SafariR, iPhoneR, iPadR, iPod touchR and MacintoshR are trademarks of Apple Inc., registered in the U.S. and other countries. App StoreSM is a service mark of Apple Inc.
Chrome™ browser, Google Play™ and Android™ are trademarks of Google Inc.
Internet ExplorerR, WindowsR and the Windows logo are trademarks of the Microsoft group of companies.

Product Overview

Package Contents

DIR-822K router

Power Adapter

Ethernet Cable

Quick Install Guide

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

Note: *Using a power supply other than the one included with the DIR-822K may cause damage and void the warranty for this product.*

System Requirements

Network Requirements

• An active account with an Internet Service Provider using one of the following connection types:
• A broadband device connected using the WAN port

Web-based Configuration Utility Requirements Computer with the following:

• Windows®, Macintosh, or Linux-based operating system
• An installed Ethernet adapter

Browser Requirements:

• Internet Explorer 10 or higher
• Microsoft EDGE Browser 20 or higher
• Firefox 11 or higher
• Safari 5 or higher
• Chrome 17 or higher

Windows® Users: Make sure you have the latest version of Java installed. Visit version of Java installed. Visit www.java.com to download the latest version.

Introduction

The D-Link DIR-822K FIBRE WI-FI AC1200 DUAL BAND ROUTER, share your internet connection over blazing-fast Wireless AC. Equipped with advanced AC beamforming technology to maximize the speed and range of your wireless signal to significantly outperform 802.11n and other older, non-beamforming capable 802.11ac devices. It also has a WAN port, and three 10/100 LAN ports to connect your wired devices. With the addition of Advanced Quality of Service (QoS), data streams are separated, which helps organize and prioritize your network traffic so your video streaming, gaming run smoother over both your wired and wireless network.

The DIR-822K FIBRE WI-FI AC1200 DUAL BAND ROUTER provides incredible speeds, smart antenna technology, and easy mesh features. It also features a clean design and easy installation options.

Features

Faster Wireless Networking -The DIR-822K is dual-band capable and equipped with four antennas to provide wireless speeds of up to 1200 Mbps* for your wireless devices. It operates on both the 2.4 GHz and 5GHz bands to allow separation of traffic so users can participate in high-bandwidth activities, such as video streaming, online gaming, and real-time audio, without affecting low-priority traffic like email and web surfing.

• **Compatible with 802.11n/g/b/a devices** - The DIR-822K is still fully compatible with the 802.11n, 802.11g, and 802.11a standards, so it can connect with existing 802.11n, 802.11g, 802.11b, and 802.11a wireless devices.
• **Advanced Firewall Features** - The web-based user interface allows you to configure a number of advanced network management features including:

- **Content Filtering** - Easily apply content filtering based on MAC address, URL, and/or domain name.

- **Scheduling** - The wireless features can be scheduled to be active on a schedule you define.

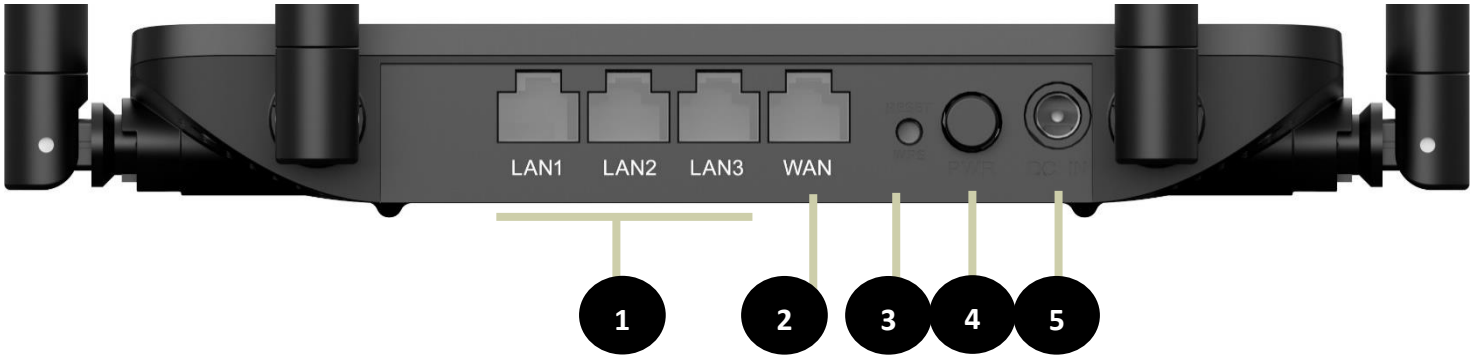
- **Multiple/Concurrent VPN Sessions** - The DIR-822K can pass through VPN sessions. It supports multiple and concurrent L2TP, IPsec and PPTP sessions, so users behind the DIR-822K can access encrypted corporate networks.

• **User-friendly Setup Wizard** - Through its easy-to-use web-based user interface, the DIR-822K lets you control what information is accessible to those on the wireless network, whether from the Internet, or from your company's server. Configure your router to your specific settings within minutes.

* Maximum wireless signal rate derived from IEEE Standard 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

Hardware Overview

Back Panel



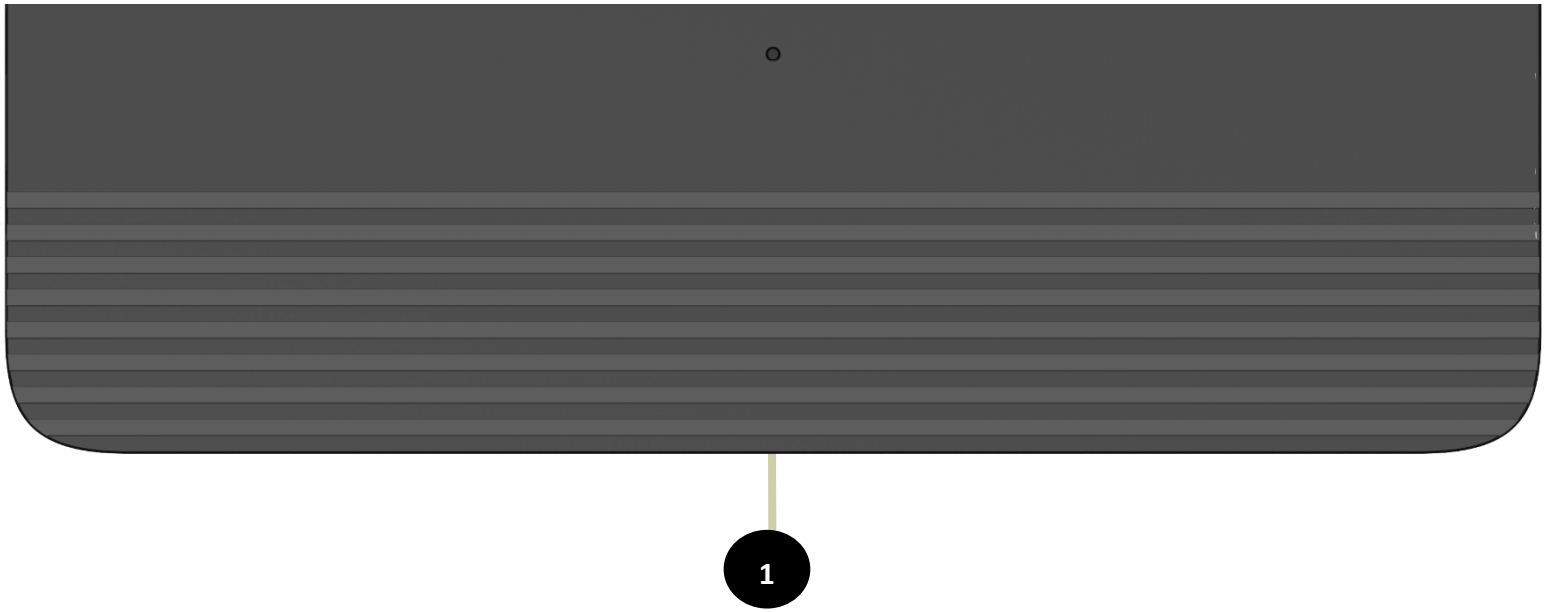
1.	Ethernet Ports	Connects to Ethernet devices such as computers.
2.	WAN Port	Connects to Ethernet WAN devices.
3.	Reset button	Hold Reset button down for 15 Seconds to factory default the Router.
4.	Power Button	Press to switch router ON/OFF.
5.	Power Connector	Connector for the supplied power adapter.

Hardware Overview

Side Panel

Hardware Overview

LEDs



1.	Power/WAN	Solid Red	Device is powered on.
		Solid Green	The WAN is properly connected.
		OFF	No connection or Cable not connected properly.

Installation

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

Note: This installation section is written for users who are setting up their home Internet service with the DIR-822K FIBRE WI-FI AC1200 DUAL BAND ROUTER with Easy mesh for the first time. If you are replacing an existing modem and/or router, you may need to modify these steps.

Before you begin

- Make sure to have your Fibre service information provided by your Internet Service Provider handy. This information is likely to include your Fibre account's Username and Password. Your ISP may also supply you with additional WAN configuration settings which are necessary to establish a connection. This information may include the connection type (DHCP IP, Static IP, PPPoE).
- If you are connecting a considerable amount of networking equipment, it may be a good idea to take the time to label each cable or take a picture of your existing setup before making any changes.
- We suggest setting up your DIR-822K from a single device and verifying that it is connected to the Internet before connecting additional devices.

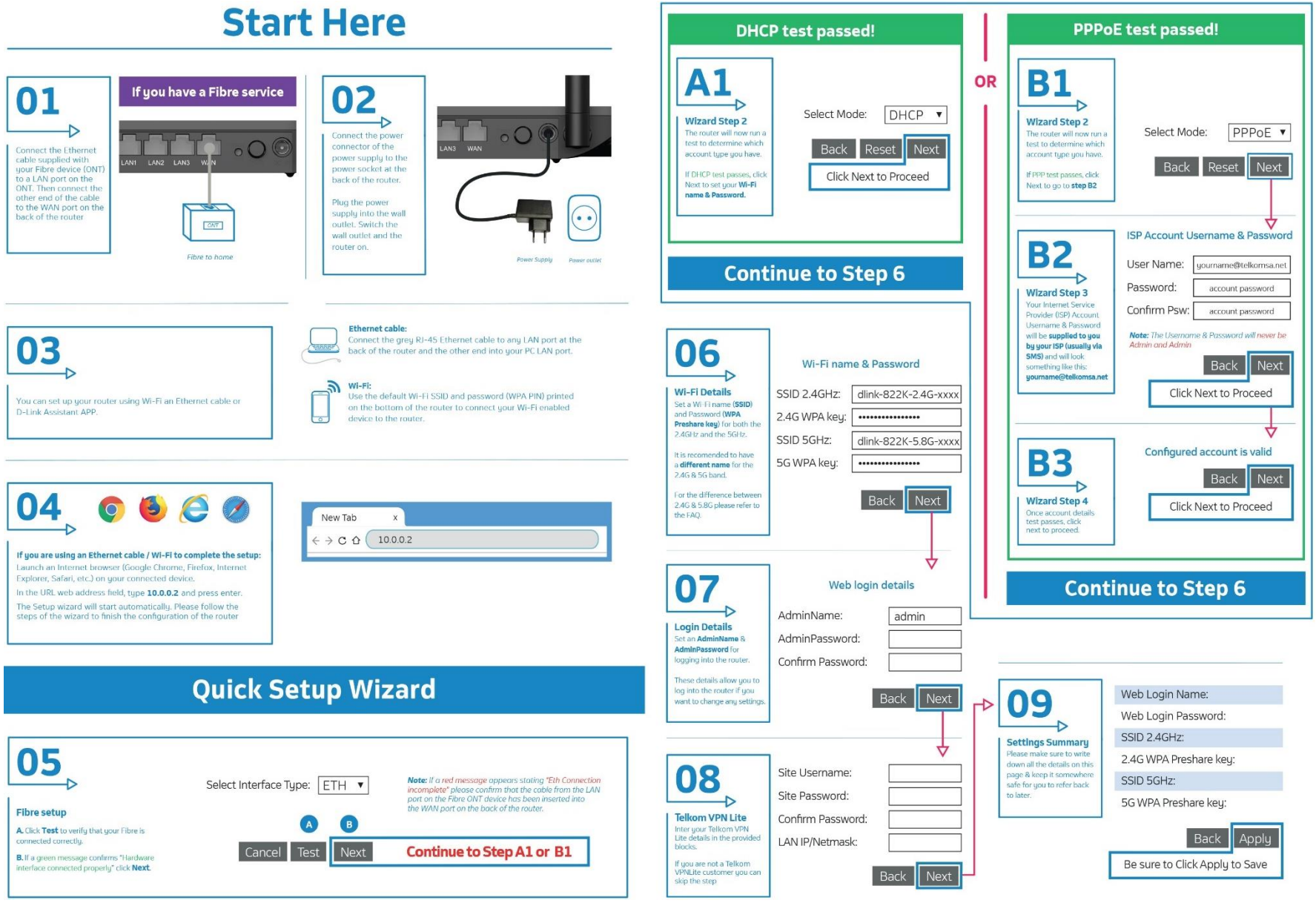
Wireless Installation Considerations

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

1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building materials make a difference. A solid metal door or aluminium studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Manual Setup

Hardware Installation



Getting Started

To connect to the web interface of the router and get started setting it up, refer to **Configuration on page**.

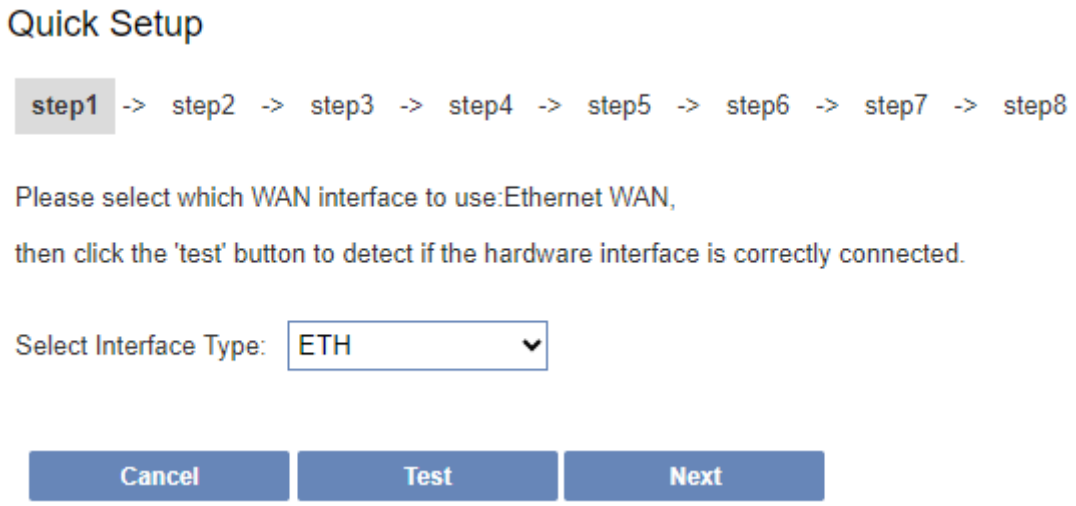
Quick Setup

The Quick Setup menu is used to set up the Internet connection on the DIR-822K. This is the first step in the Quick Setup tool and allows you to choose the connection type.

Step 1
Select WAN Interface Type:

Select ETH as the interface to use: Your ISP should inform you of what method you use to connect to the Internet.

Click **Test** and then **Next** to continue.

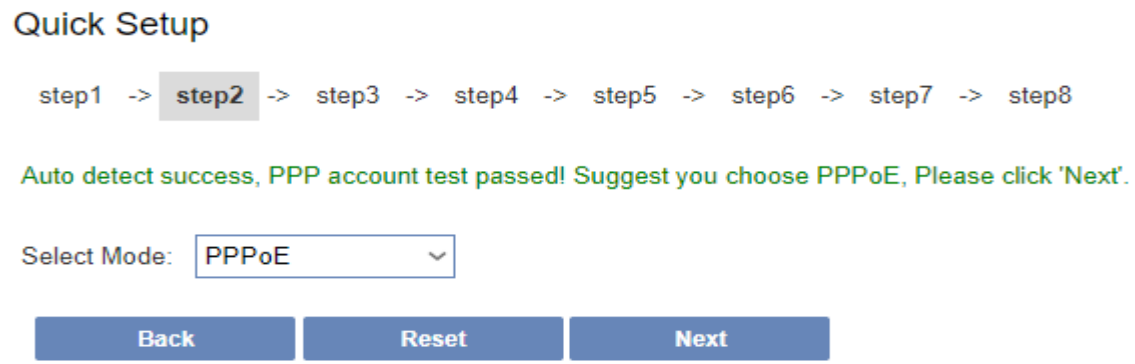


Step 2
Auto detecting

With a Fibre connection you will use either:

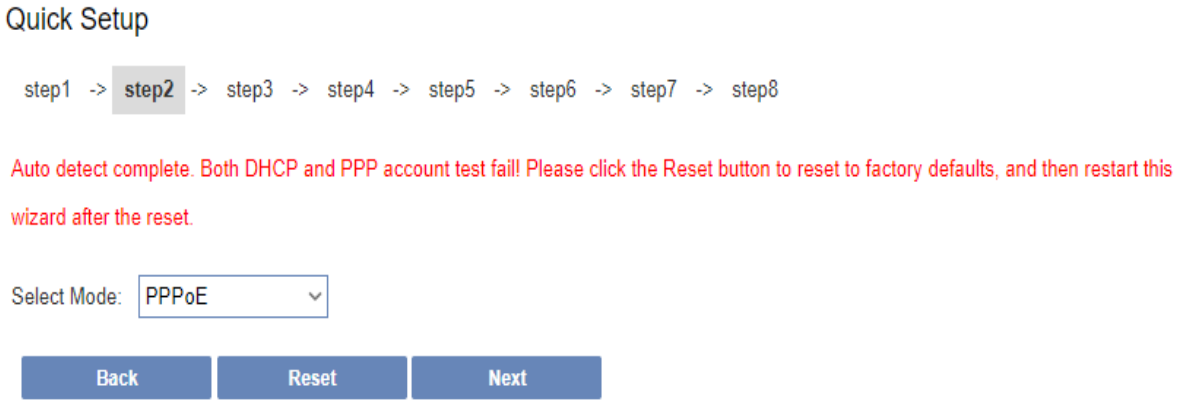
PPPoE or DHCP connection.

If PPPoE or DHCP is successful, please click the next button to continue to next step.



If both DHCP and PPPoE test fails,

Please verify that your fibre is active and the cable from the ONT device is plugged into the **WAN** port at the back of the DIR-822K.



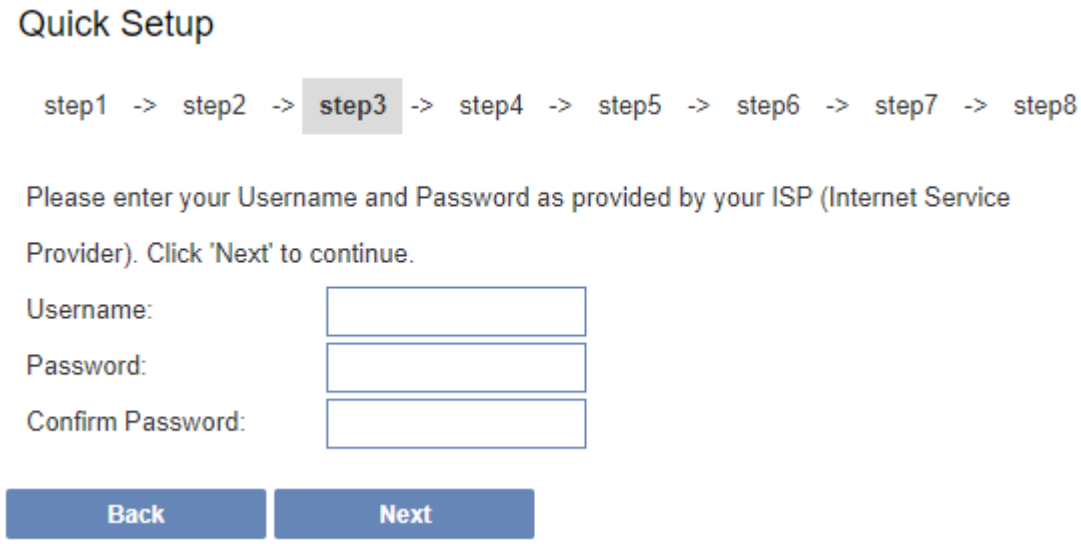
Step 3

IF PPPoE Passed then user will need to enter the Username and Password as provided by the Internet Service Provider (ISP). IF DHCP passed device will automatically skip to step 5.

Username: Enter your Username here. (usually looks like an email address like Yourname@telkomsa.net)

Password: Enter your Password here.

Confirm Password: Enter the same password again here.



Note: *Using admin for the username & password will not work on this step as this is the account details for your Fibre line, which is unique to each client's account.*

Step 4.

If connection is on PPPoE device will now test if the configured account is valid. If the test fails, please click on the back button and double check that the details on step 3 are correct. If the details have been entered correctly and step 4 still fails, please contact your Internet Service Provider and request for them to send you new PPPoE details.
if **successful** click Next to continue to **Step 5.**

Step 5

On Step 5 the user will be able to modify the Wi-Fi SSID and Preshared Key to their requirements.

SSID 2.4GHz: The name of the Wi-Fi network operating on 2.4GHz.

Preshared key: The password for the Wi-Fi network operating on 2.4GHz.

SSID 5GHz: The name of the Wi-Fi network operating on 5GHz.

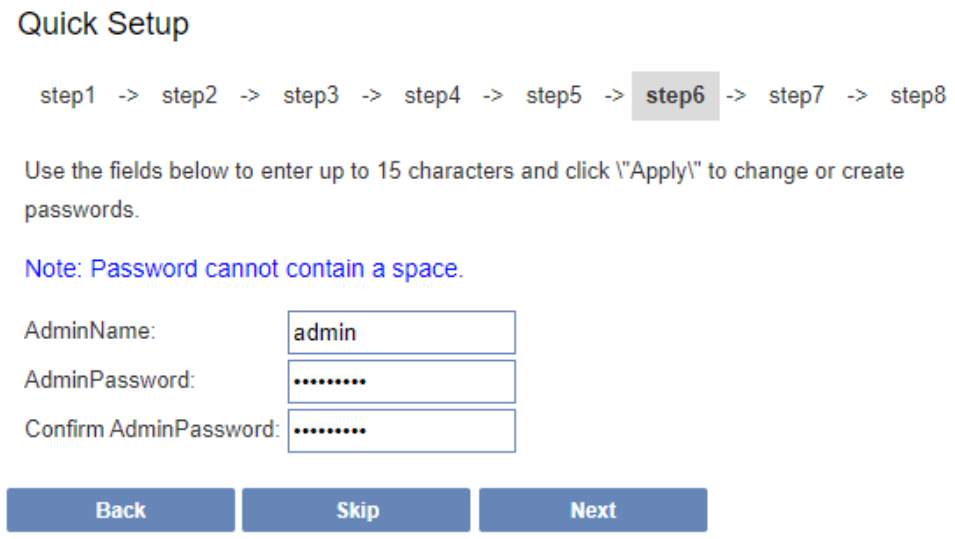
5G WPA Preshared key: The password for the Wi-Fi network operating on 5GHz.

Click **Back** to go back to the pervious page, click **Skip** to skip this configuration

or click **Next** to continue to **Step 6.**

Step 6

In this step you can enter the change the web UI credentials. (The details used to log into the settings page of your router on 10.0.0.2)



Admin Name: The username to log in to the web UI.

Admin Password: Enter the password here for logging into the web UI.

Admin Password: Enter the password for logging in to the web UI again to confirm.

Note: Password cannot contain a space.

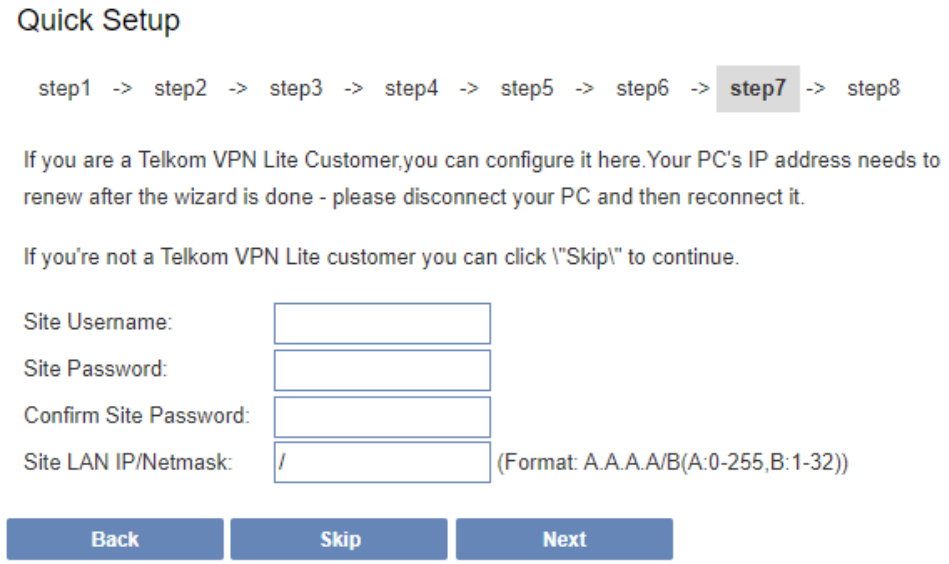
Click **Back** to go back to the pervious page, click **Skip** to skip this configuration (not recommended for security purposes) or click **Next** to continue to **Step 7.**

Step 7

In this step you can enter the Site Username, Site Password, Confirm Site Password and Site LAN IP/Netmask to connect to Telkom VPN lite

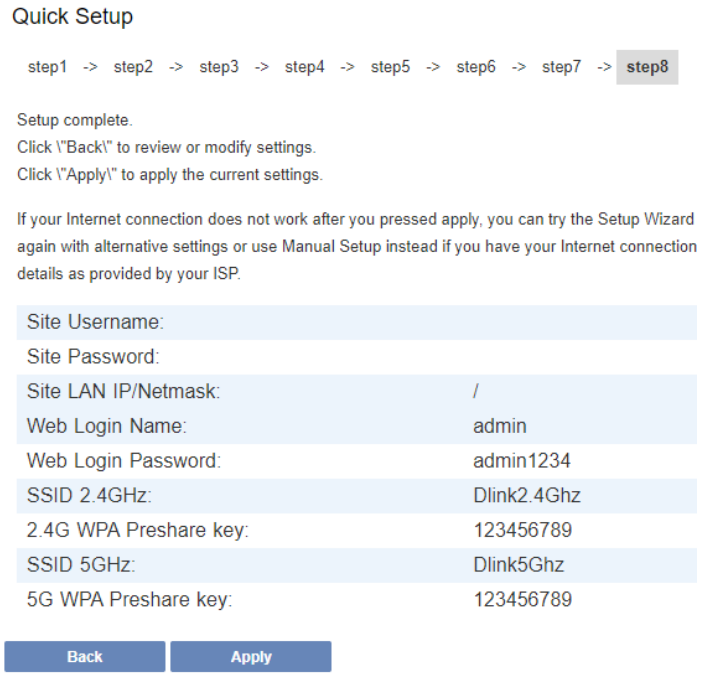
Site Username: The site username.
Site Password: Enter the site password here.
Confirm Site Password: Enter the site password again to confirm.
Site LAN IP/ Netmask: Enter the LAN IP or Netmask for the site here.
Note: *Password cannot contain a space.*

Click **Back** to go back to the pervious page or click **Next** to continue to **Step 8.**



Step 8

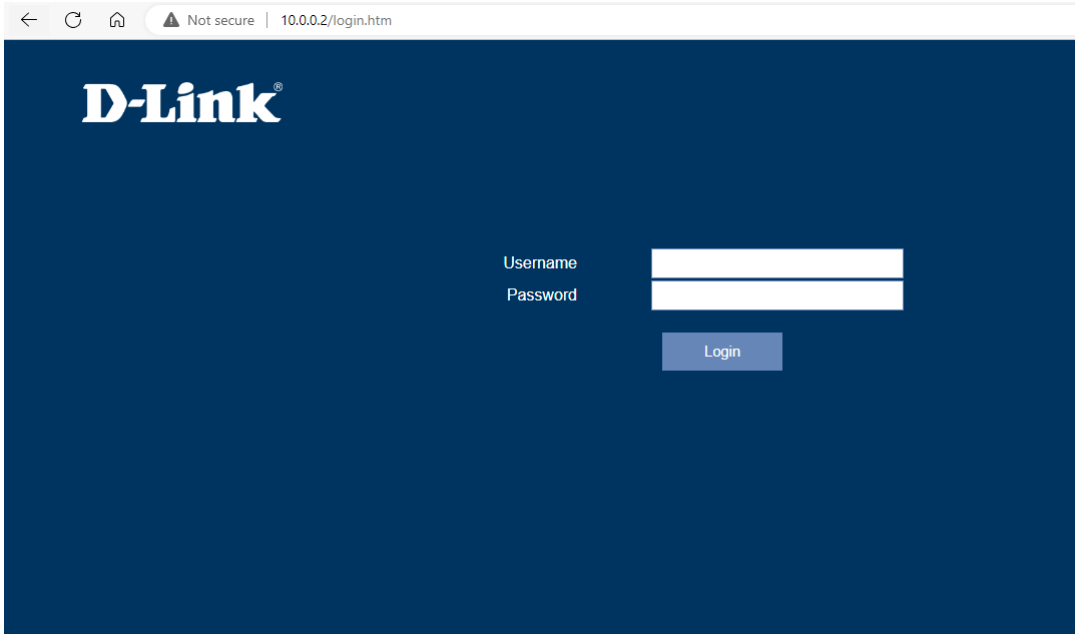
In this step you can you can review everything for accuracy.
Click **Back** to go back to the pervious page or click **Apply** to apply all of the configuration settings.



Configuration

Log in

To access the web interface, open a web browser and enter the IP address of the router (by default this is **10.0.0.2**) into the address bar.
When the login page of the DIR-822K is displayed, enter the username and password you set on step 6 of the setup wizard. By default, the login details are **admin** for the username and **admin** for the password if you chose to not change the details on the wizard.
Click **Log In** to proceed or **cancel** to clear your input.

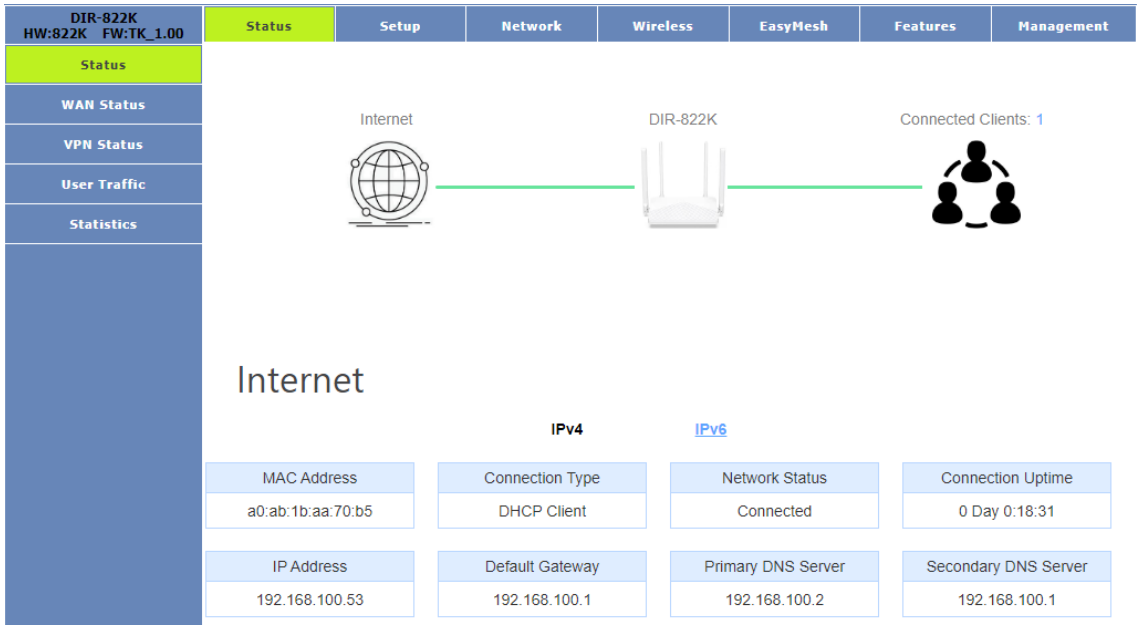


Note: *If you cannot remember your password or cannot log in, follow the factory reset procedure to restore the router to its default settings. The web interface is used to set up and change settings on the DIR-822K. Follow the steps below to access the web interface and start setting up the DIR-822K.*

Status

Device Information

The Status menu is used to display statistics from different functions from the router.
This displays basic system information and the uptime of the router.



Device Information

Product Type: The model number of the router.
Default Gateway: The Default gateway assigned by the ISP to access the Router.
Primary DNS: The Primary DNS of the Router.
Secondary DNS: The Secondary DNS of the Router.
Hardware Version: The hardware version of the router.
Software Version: The Current software version of the router.
MAC Address: The MAC address of the router.
Connection Type: Indicates your Fibre connection type.
Network Status: Indicates if Internet is Connected or Disconnected.
Connected Clients: Indicates the number of connected devices.
Connection up Time: The amount of time that the router has been online and in use.

WAN Status

Network

This displays Network status information.

IPv4 / IPv6 WAN Connection Status

Connection Name: The name of the WAN connection.

Enable: The state of the WAN connection.

Type: The WAN connection type.

VLAN ID: The ID indicating what VLAN the WAN connection is assigned to.

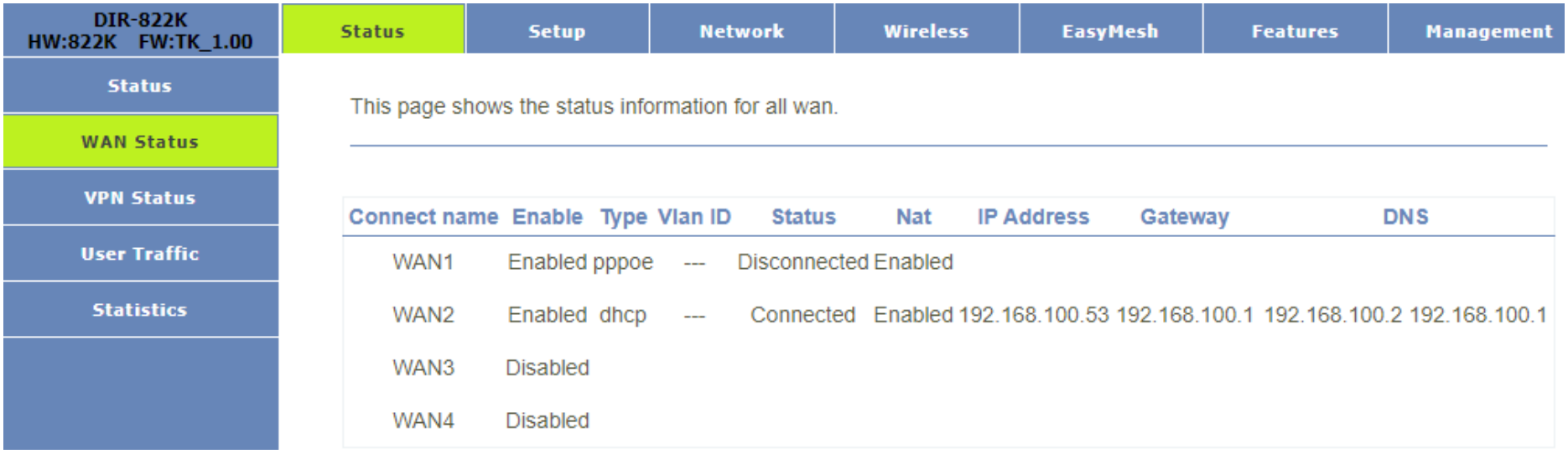
Status: The status of the WAN connection.

NAT: Indicates if the Network Translation address in Enable/Disabled.

IP Address: The IP address of the WAN connection.

Gateway: The default gateway of the WAN connection.

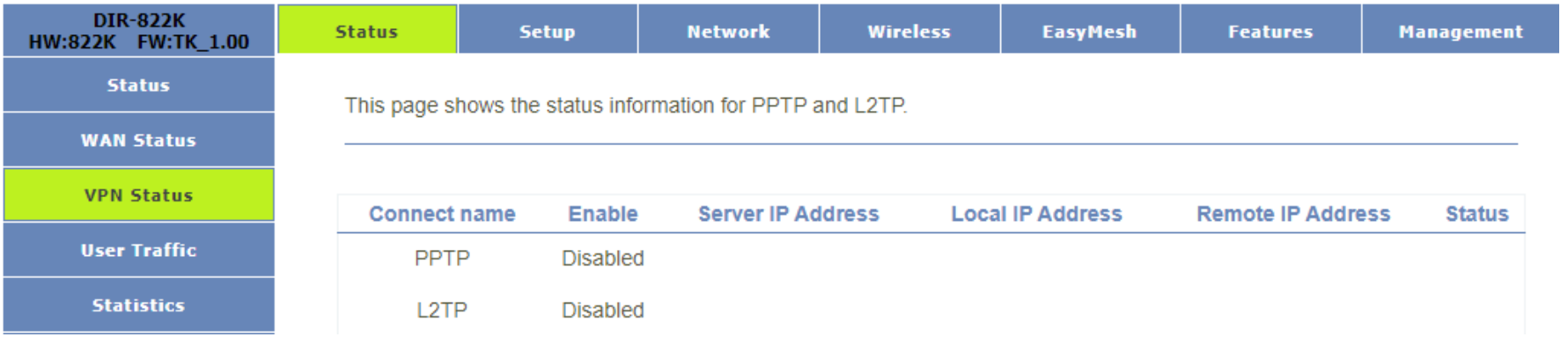
DNS: The primary and Secondary DNS of the WAN connection is displayed.



VPN Status

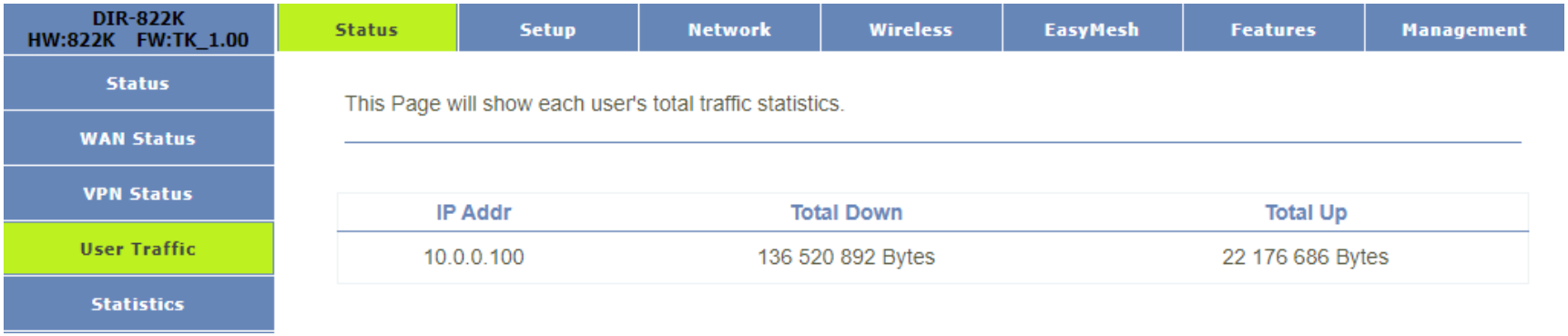
This displays the VPN status information.

PPTP: Enabled/Disabled
L2TP: Enabled /Disabled
Server IP address: IP address attained from the server.
Local IP address: Local IP of attained from your device.
Remote Address: IP address of the Remote access device.
Status: This will state if the connection is connected/disconnected.



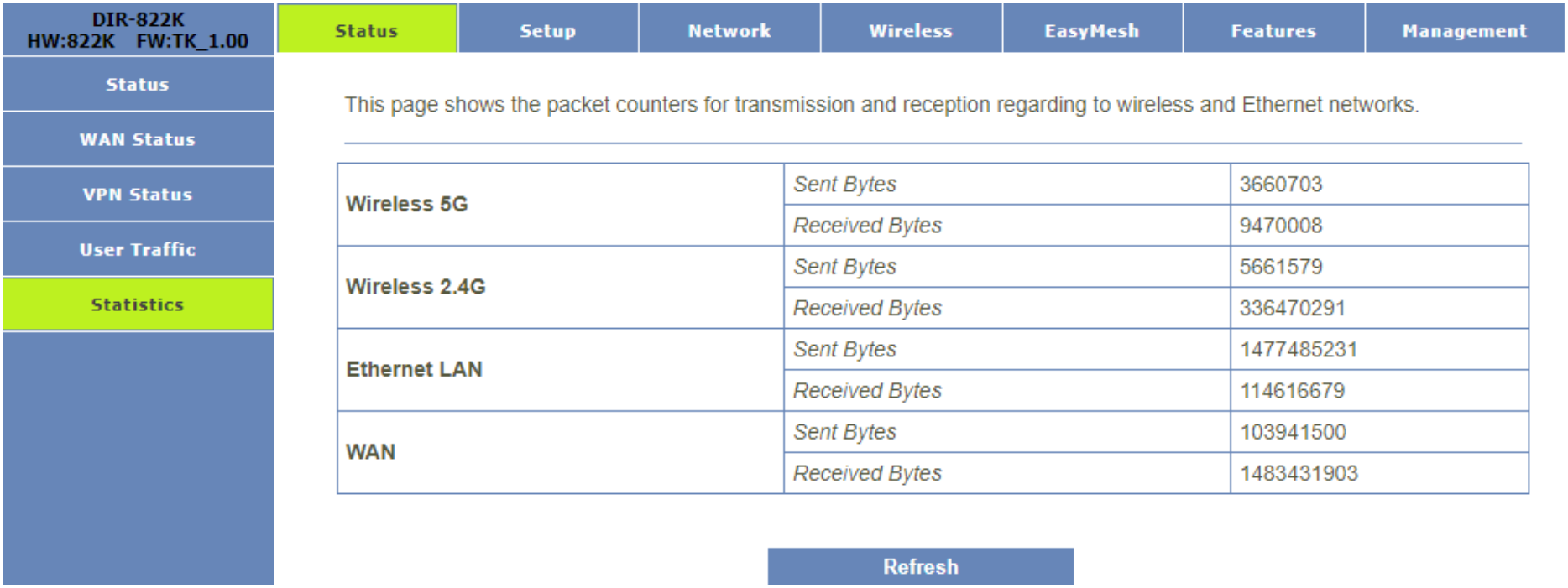
User Traffic

This Displays the User traffic Information such as IP address of connected devices, Total Download/Upload statistics.



Statistics

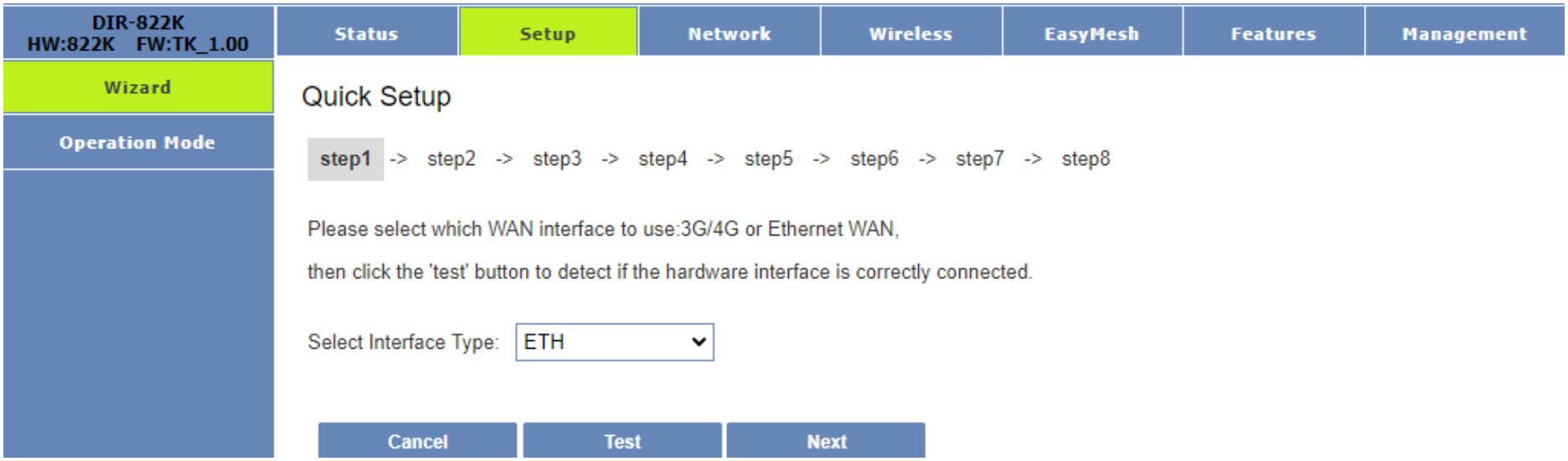
This page shows the packet counters for transmission and reception regarding the wireless and Ethernet networks of the device.



Setup

Wizard

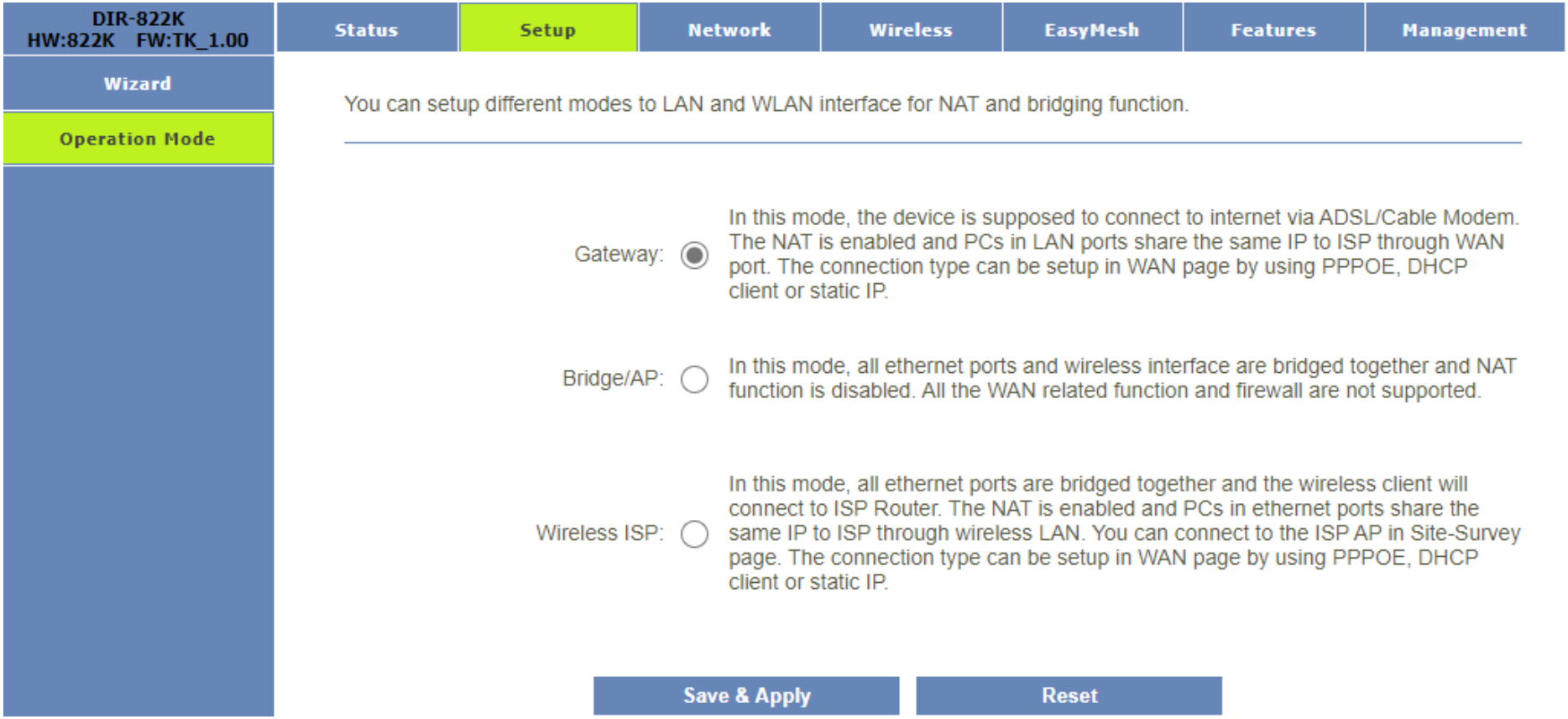
This Section displays the “Quick Setup Wizard” which is used during first time setup.



Operation Mode

This section allows you to setup different modes on the LAN and WAN Interface for NAT and bridging functions.

Gateway: This mode allows the device to connect to the Internet via Ethernet WAN connection, NAT Enabled.
Bridge/AP: This mode bridges all Ethernet ports and wireless interface and Disables NAT.
Wireless ISP: This mode has all Ethernet ports are bridged together and the wireless client will connect to the ISP Router, NAT Enabled.

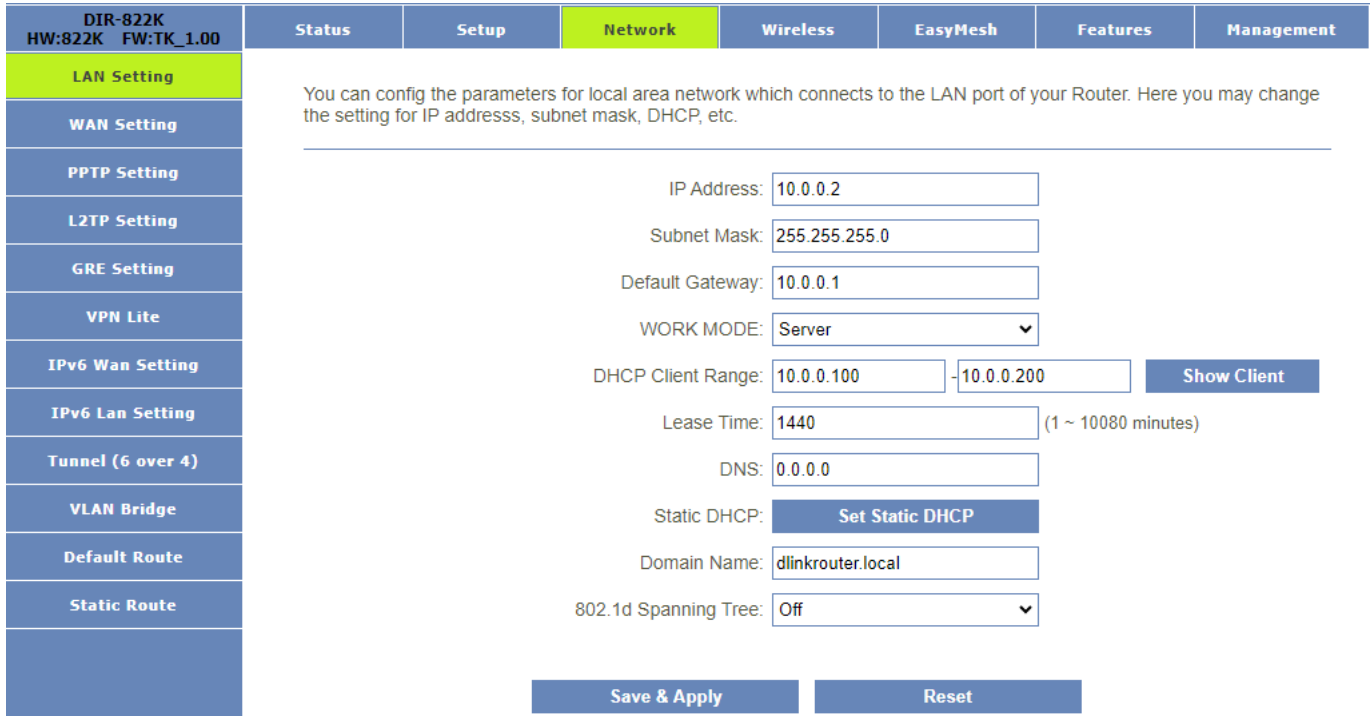


Network

LAN Setting

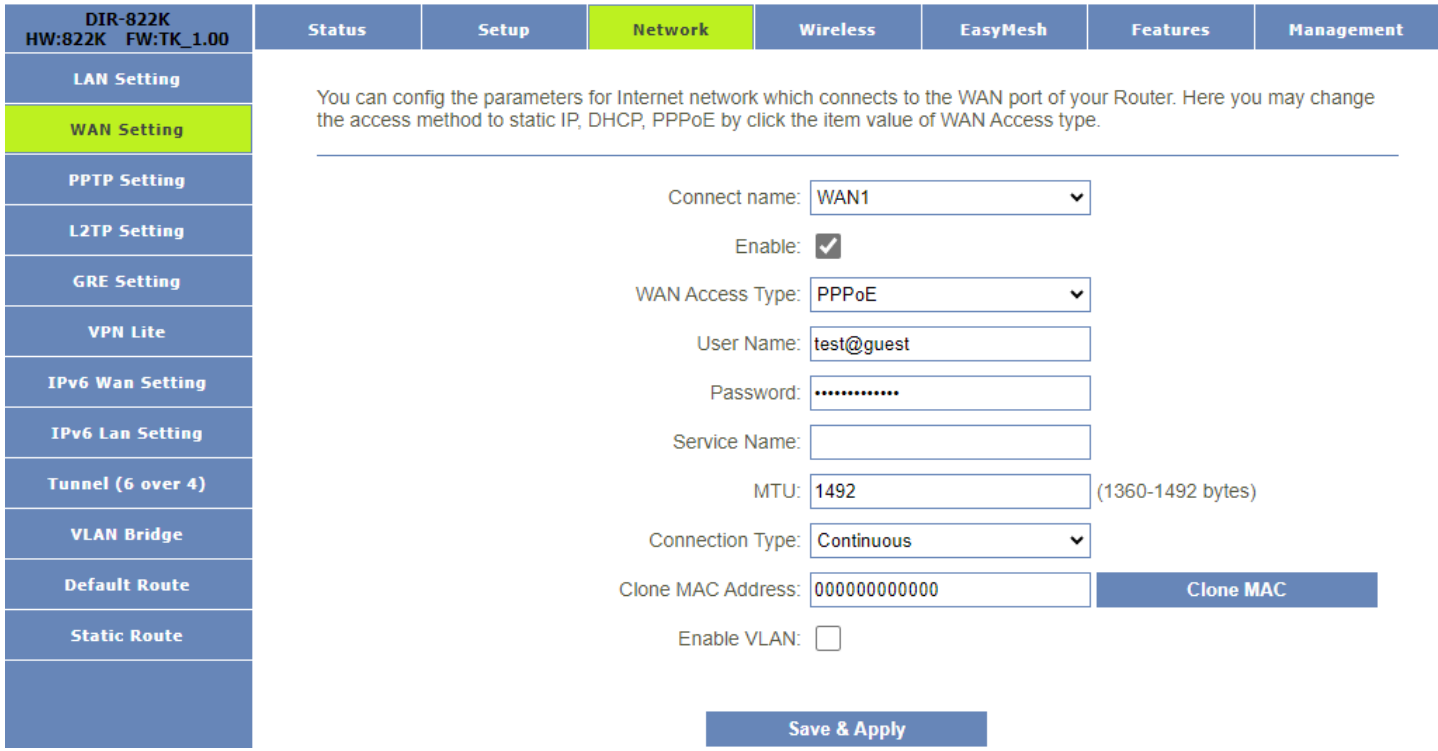
Here you can configure the parameters for local area network.

IP Address: The IP address can be set.
Subnet Mask: The Subnet mask can be set.
Default Gateway: Default Gateway of the Router.
WORK MODE: Can be set to OFF/Client/Server/DHCP Relay.
DHCP Client Range: Set an IP Range for your DHCP clients.
Lease Time: Set a Time limit the DHCP will lease the IP.
DNS: DNS address of Router.
Static DHCP: Set a Static DHCP (Enable/Disable, IP address, MAC address).
Domain Name: Enter a domain name,
Eg: dlinkrouter.local
802.1d Spanning Tree: Enable Spanning tree On/Off.



WAN Setting

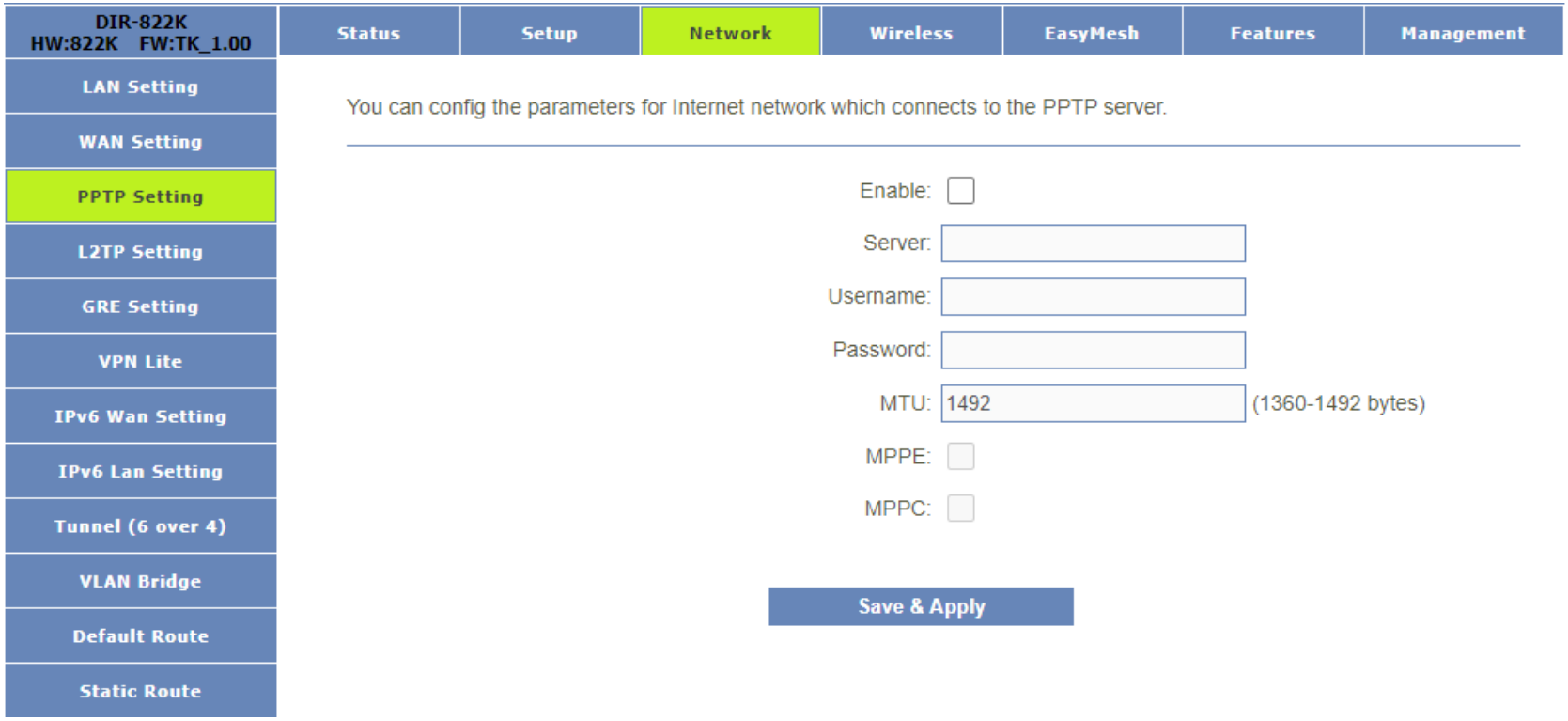
Connection name: Choose a WAN from the drop-down menu.
Enable: Choose to Enable/Disable the profile.
WAN Access Type: Select a WAN type such as PPPOE/DHCP/Static.
User Name: Enter the ISP username if using PPPOE.
Password: Enter the ISP password if using PPPOE.
Service Name: Leave blank or give it a name.
MTU: Please ensure this is set to the value of 1492.
Connection Type: You can set the connection to Continuous/Connect on demand or manual.
Clone MAC Address: This option is used to Clone the Mac address of a device.
Enable VLAN: Choose whether to Enable/Disable the VLAN.



PPTP Setting

Here you can configure the parameters for the PPTP Server

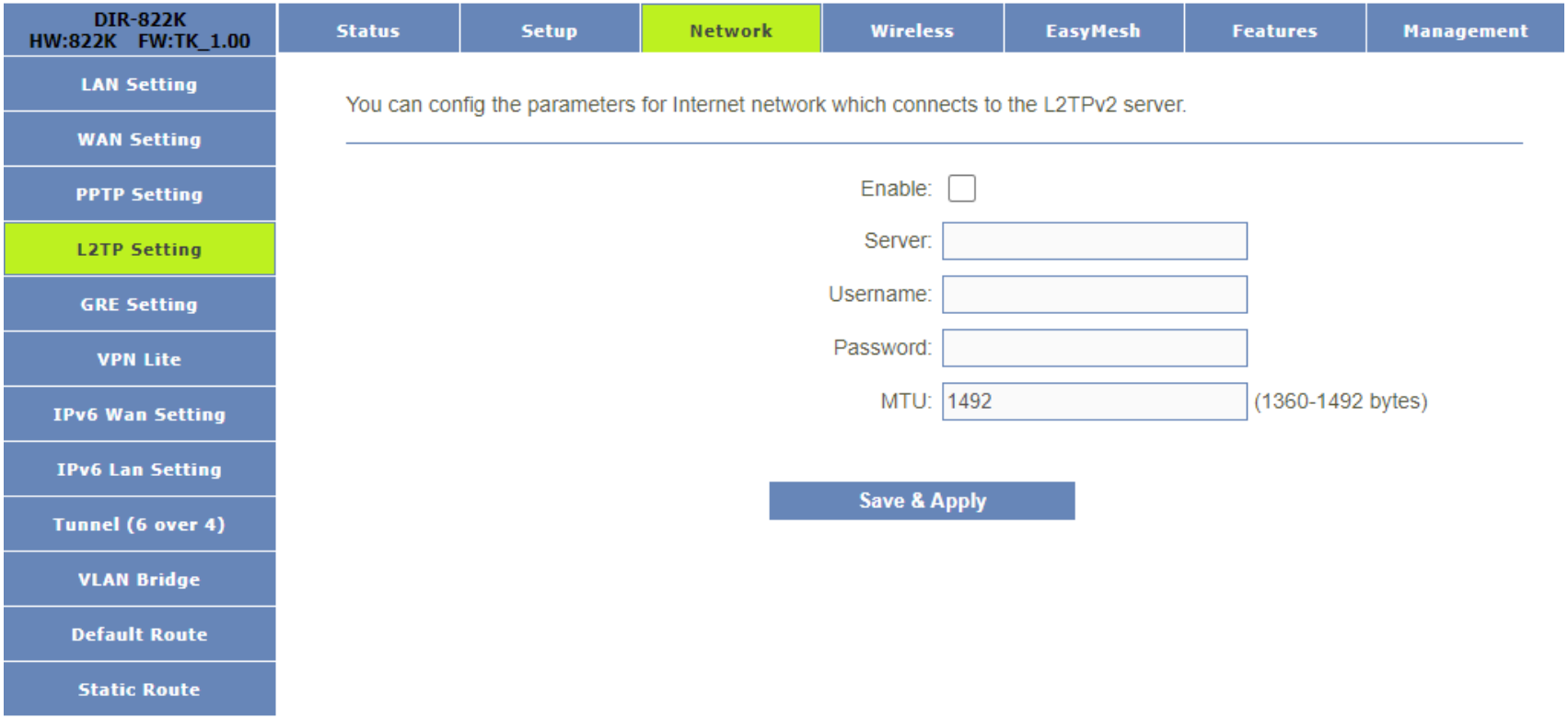
Enable: Choose to Enable/Disable the service
Server: Enter the Server IP address
Username: Enter the username associated
Password: Enter the password associated
MTU: This value must be 1492
MPPE: Enable/Disable (Microsoft Point-to-Point Encryption)
MPPC: Enable/Disable (Microsoft Point-to-Point Compression)



L2TP Setting

Here you can configure the parameters for the L2TPv2 Server

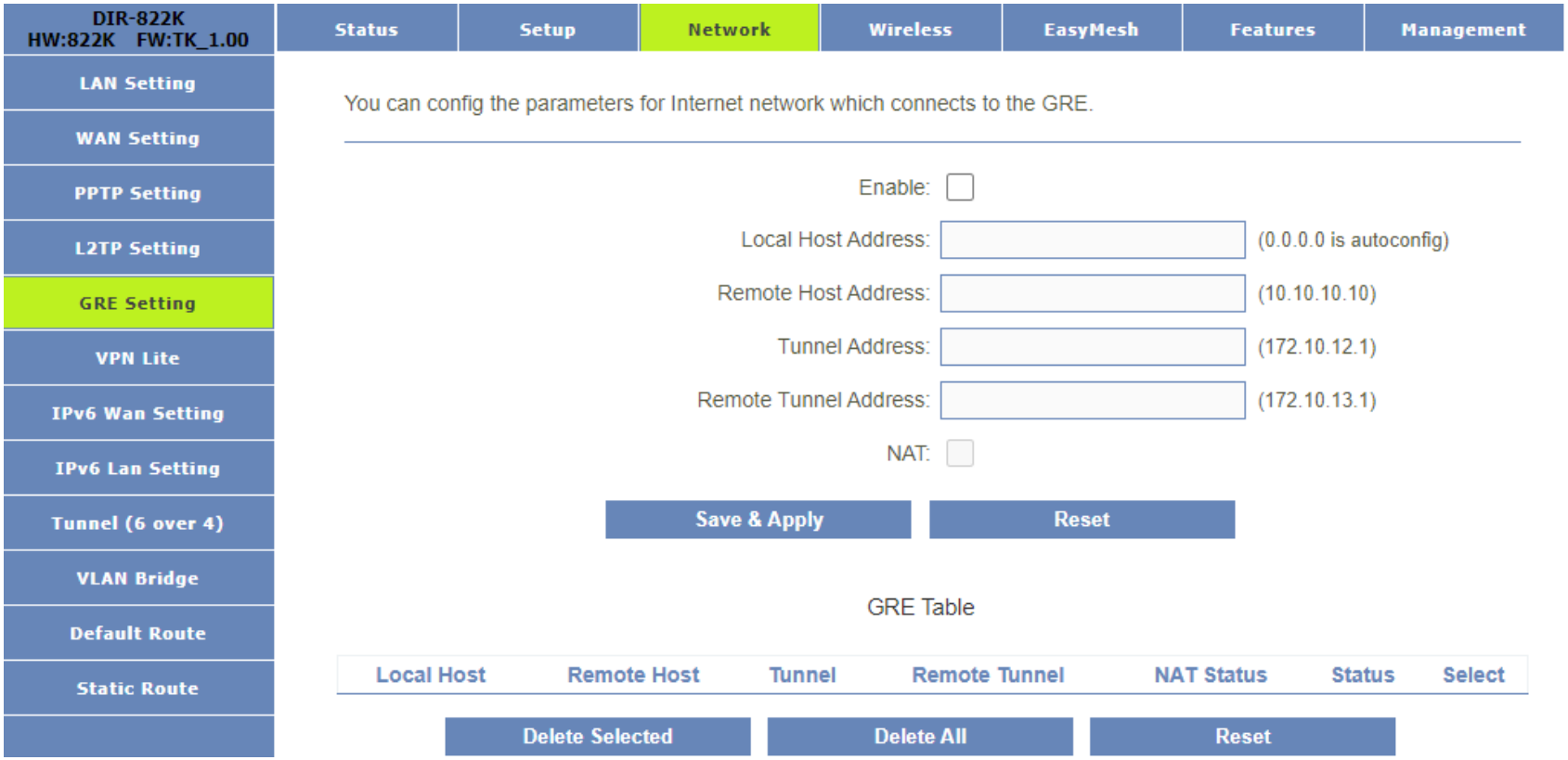
Enable: Choose to Enable/Disable the service
Server: Enter the Server IP address
Username: Enter the username associated
Password: Enter the password associated
MTU: maximum transmission unit, this value is usually 1492 (represents the largest data packet a network device will accept)
MPPE: Enable/Disable (Microsoft Point-to-Point Encryption)
MPPC: Enable/Disable (Microsoft Point-to-Point Compression)



GRE Setting

Here you can configure the parameters to connect to GRE. (Packet encapsulation protocol to route packets over an IP network)

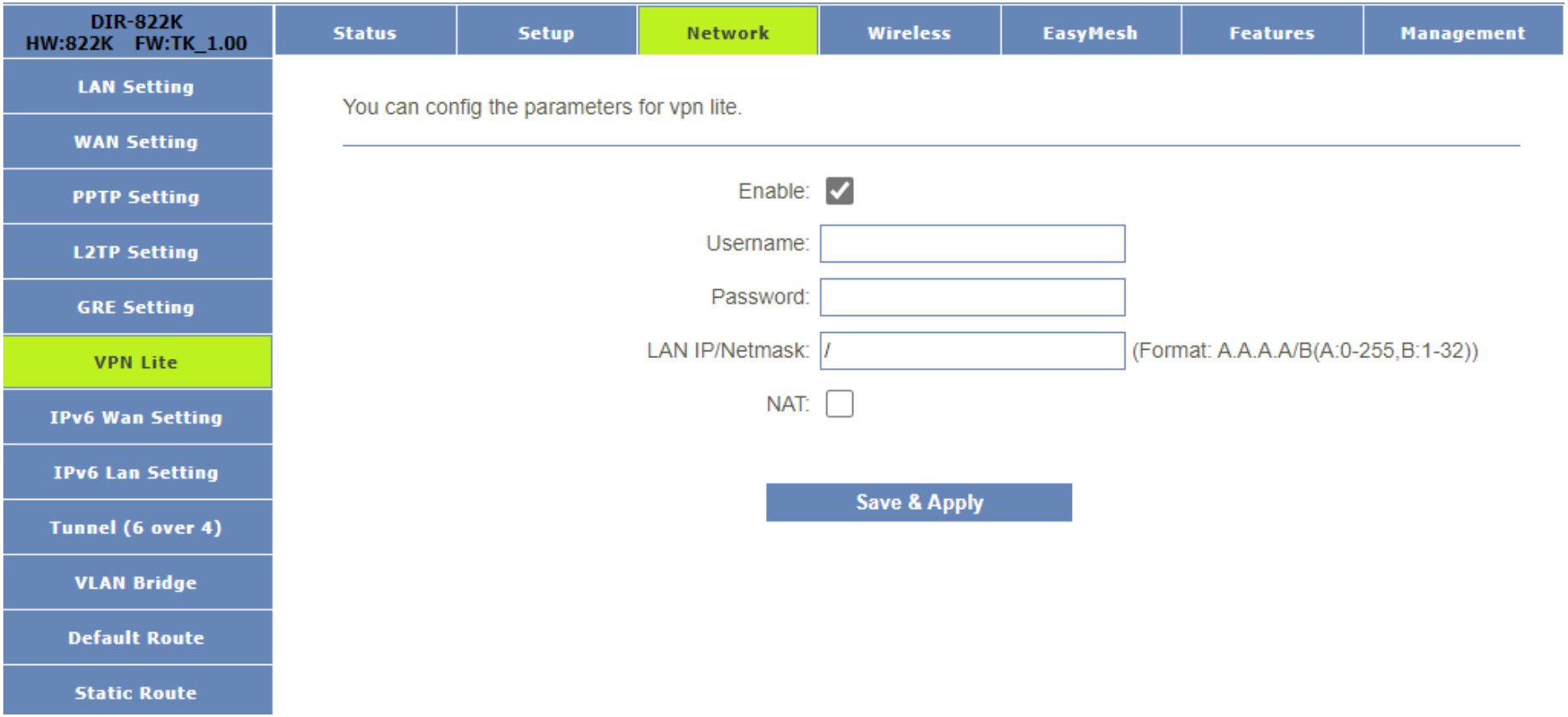
Enable: Enable or disable the function.
Local Host Address: Local IP address.
Remote Host Address: Remote IP address.
Tunnel Address: Insert the Tunnel IP address.
Remote Tunnel Address: Insert the Remote Tunnel IP address.
NAT: Enable or Disable Nat Function.



VPN LITE

Here you can configure your Telkom VPN profile

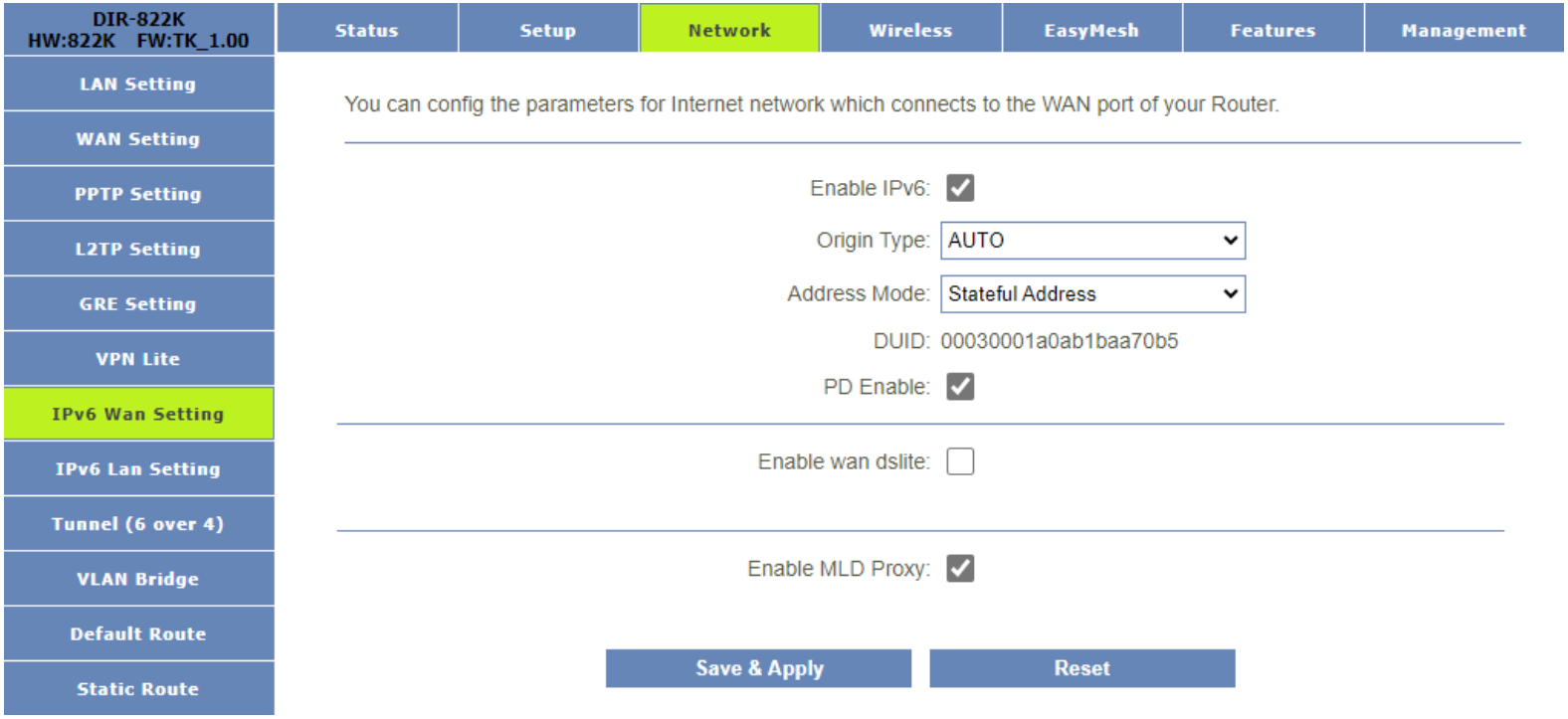
Enable: Enable or Disable the Feature.
Username: Enter your Telkom VPN Lite Username.
Password: Enter your Telkom VPN Lite Password.
LAN IP/Netmask: Here you can Enter the IP or Netmask.
NAT: Enable or Disable the NAT Function.



IPv6 Wan Setting

Here you can configure the parameters of IPv6 Wan settings.

Enable IPv6: Enable/Disable IPv6
Origin Type: This can be set to AUTO/STATIC/6RD
Address Mode: You can set this to a Stateful/Stateless address
PD Enable: Enable or Disable the PD (Prefix Delegation)
Enable wan ds lite: Enable/Disable DS-Lite (Dual-Stack Lite) Allows the user to utilize IPV4 to access Internet via IPv6
Enable MLD Proxy: Enable/Disable Multicast Listener Discovery (used to discover Multicast Listeners)



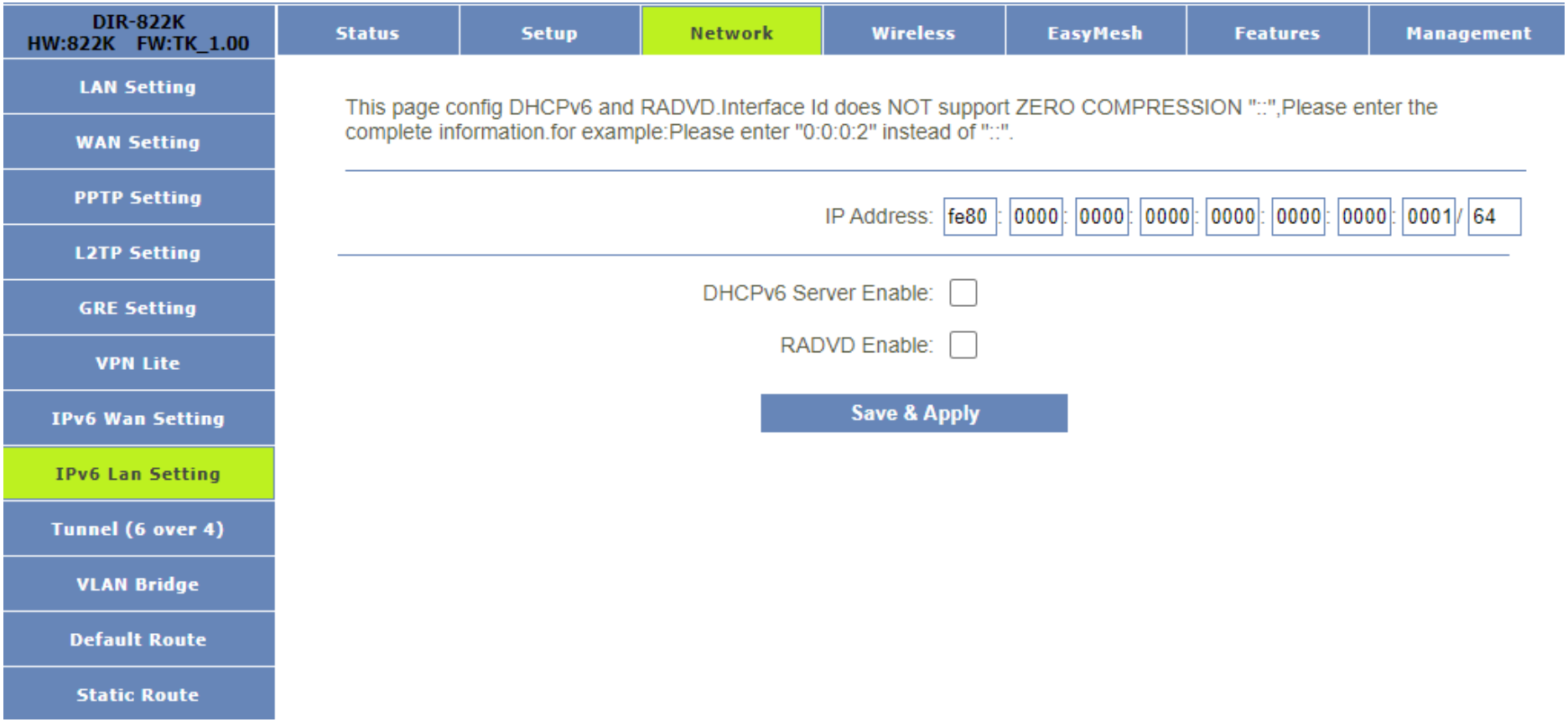
IPv6 Lan Setting

Here you can configure the DHCPv6 and RADVD Parameters

IP address: Enter the IP address.

DHCPv6 Server Enable: Enable or Disable the server.

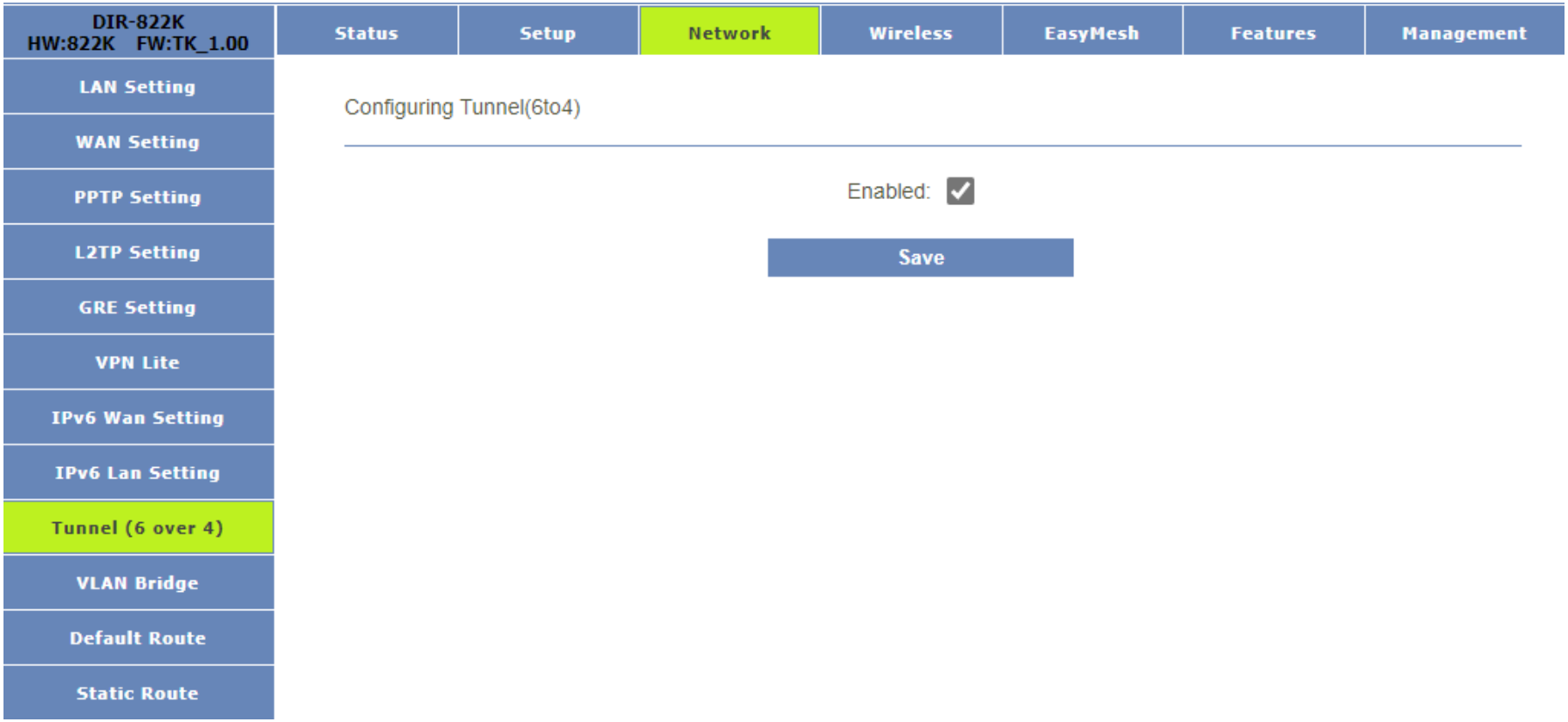
RADVD: Enable or disable RADVD feature (Router advertisement daemon) used for IPv6 auto-configuration.



Tunnel (6 over 4)

Here we can configure Tunnel 6 -4.

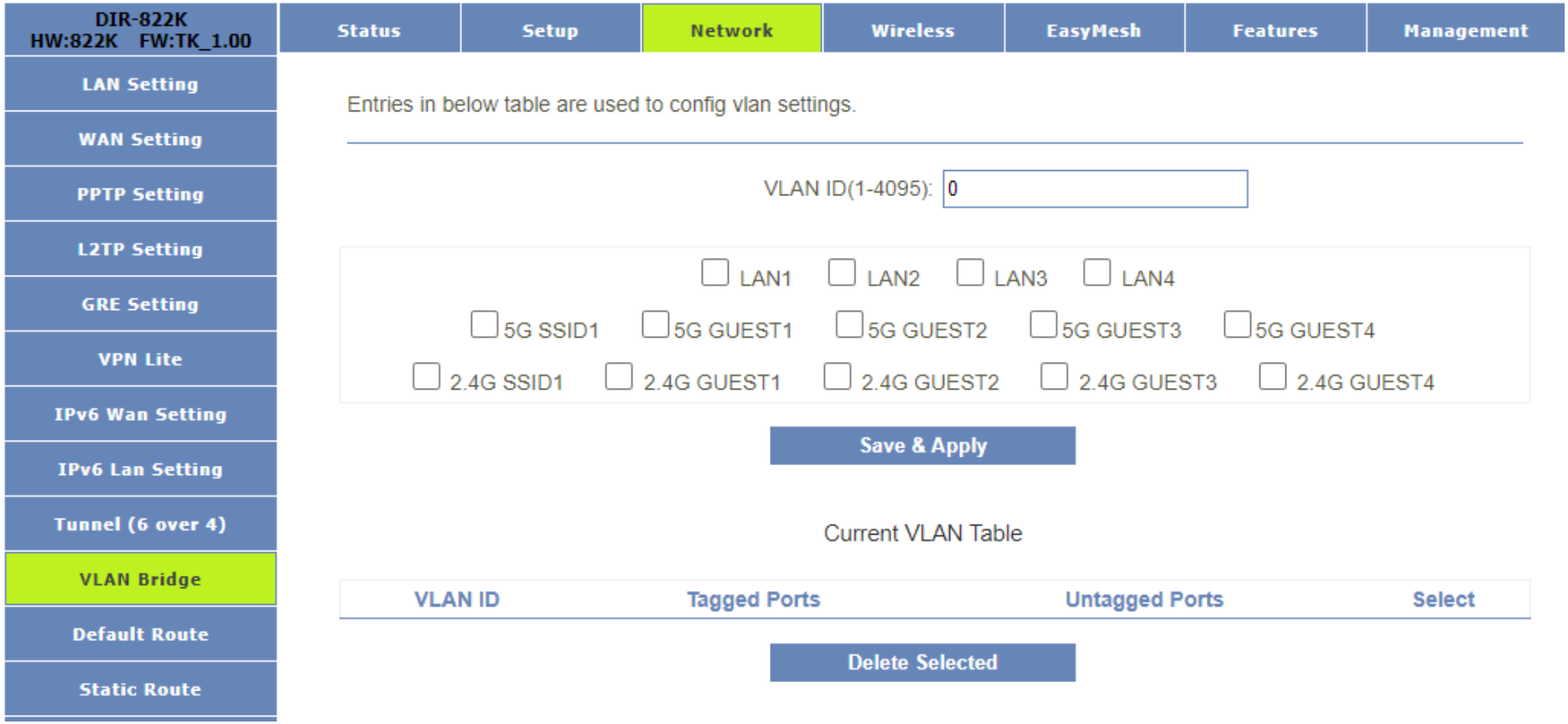
Enable: Enable or Disable the Tunnel.



VLAN Bridge

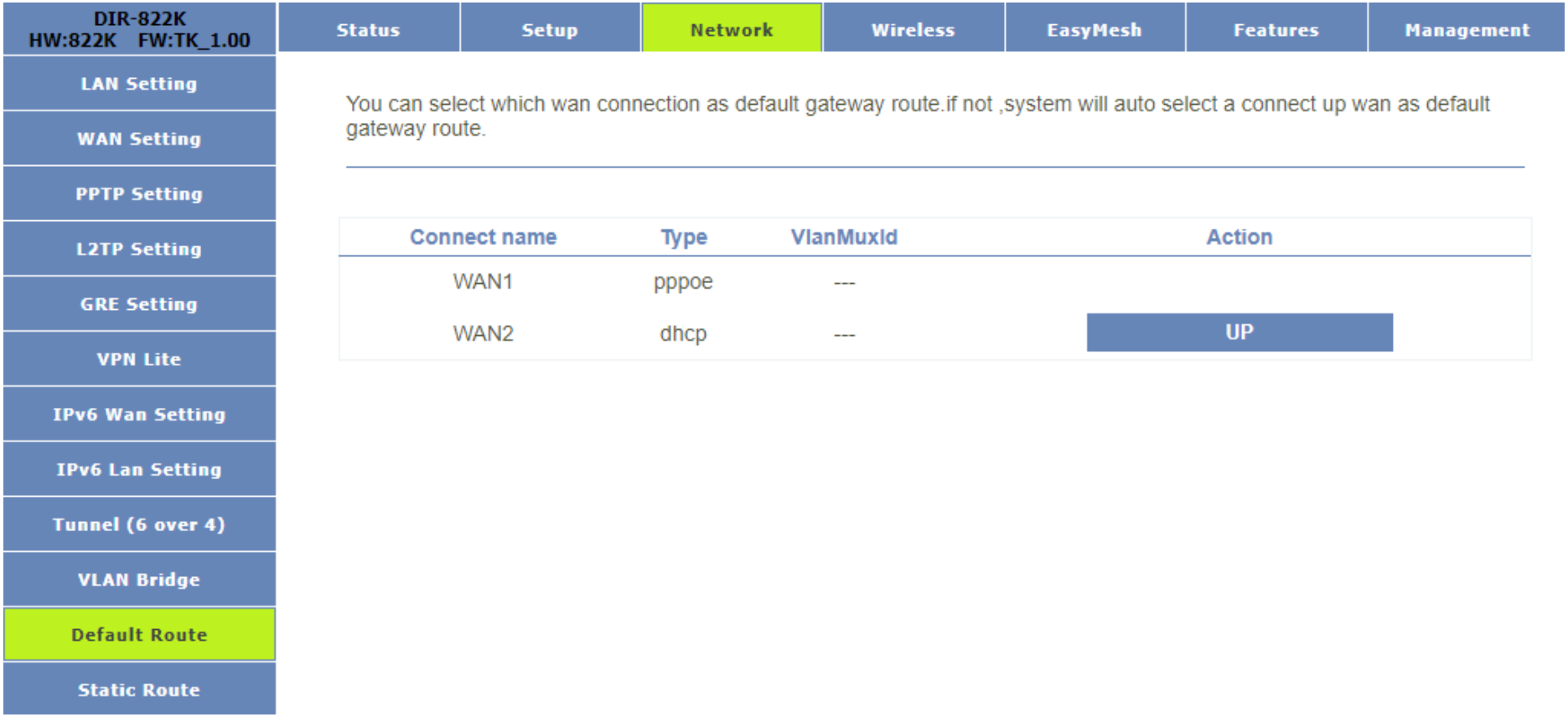
Here we can change the VLAN parameters

VLAN ID: Assign an associated VLAN ID.
LAN1-LAN 4: Select which LAN ports are associated with the VLAN.
SSID Guest 1-4 (2.4Ghz): Select which 2.4Ghz SSID Guest are associated with the VLAN.
SSID Guest 1-4 (5Ghz): Select which 5Ghz SSID Guest are associated with the VLAN .



Default Route

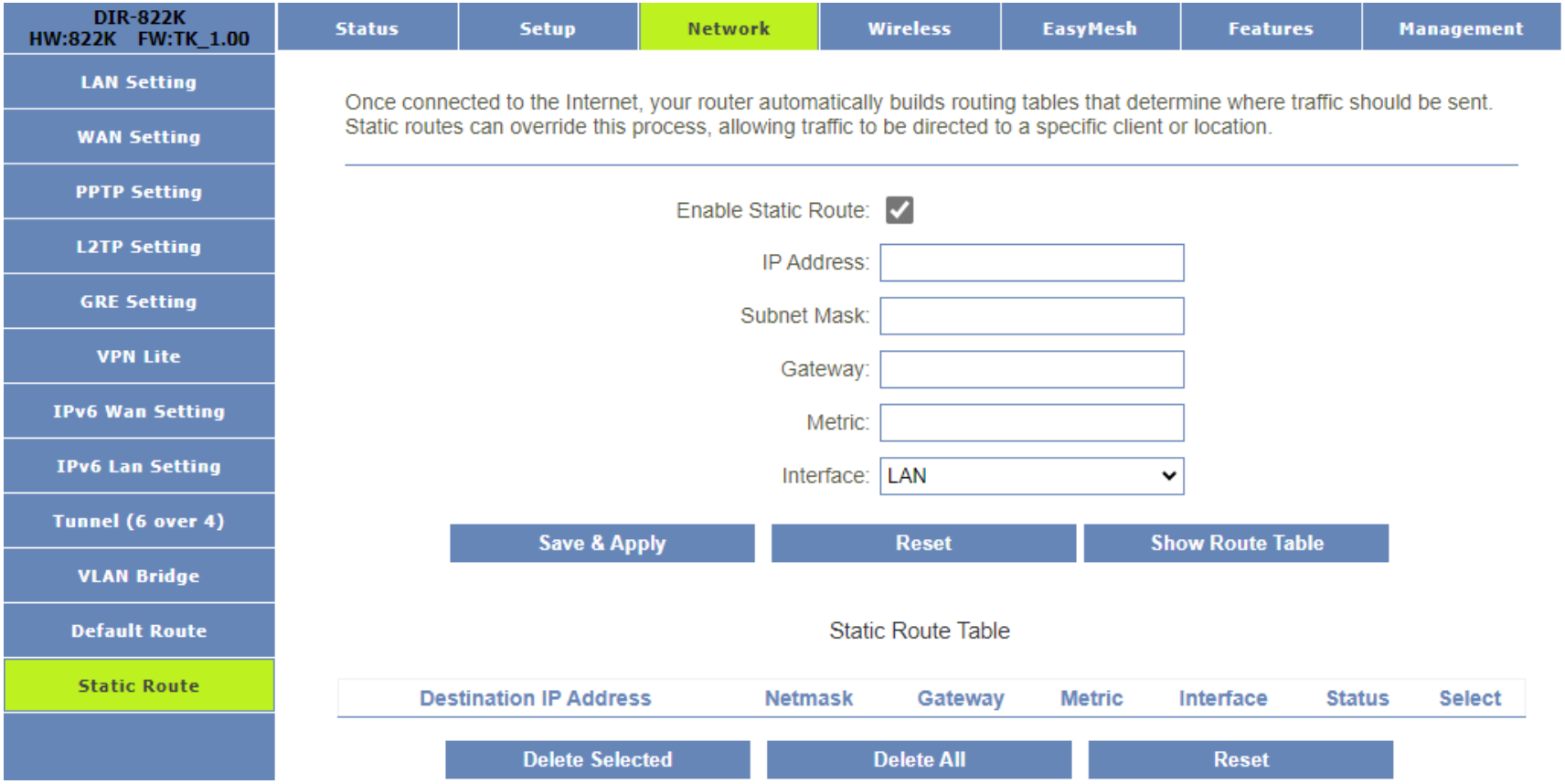
Here you can select which wan connection is set as the default (If no default is set, the current configured wan will be selected as default).



Static Route

Here you can Enable and edit static routing to allow network traffic to be redirected to a specific client its location.

Enable Static Route: Set the Static Route to Enable/Disable.
IP Address: Enter the IP address associated.
Subnet Mask: Enter the Subnet Mask associated.
Gateway: Default Gateway IP address.
Metric: Enter the Metric unit you will utilize.
Interface: Choose LAN/WAN

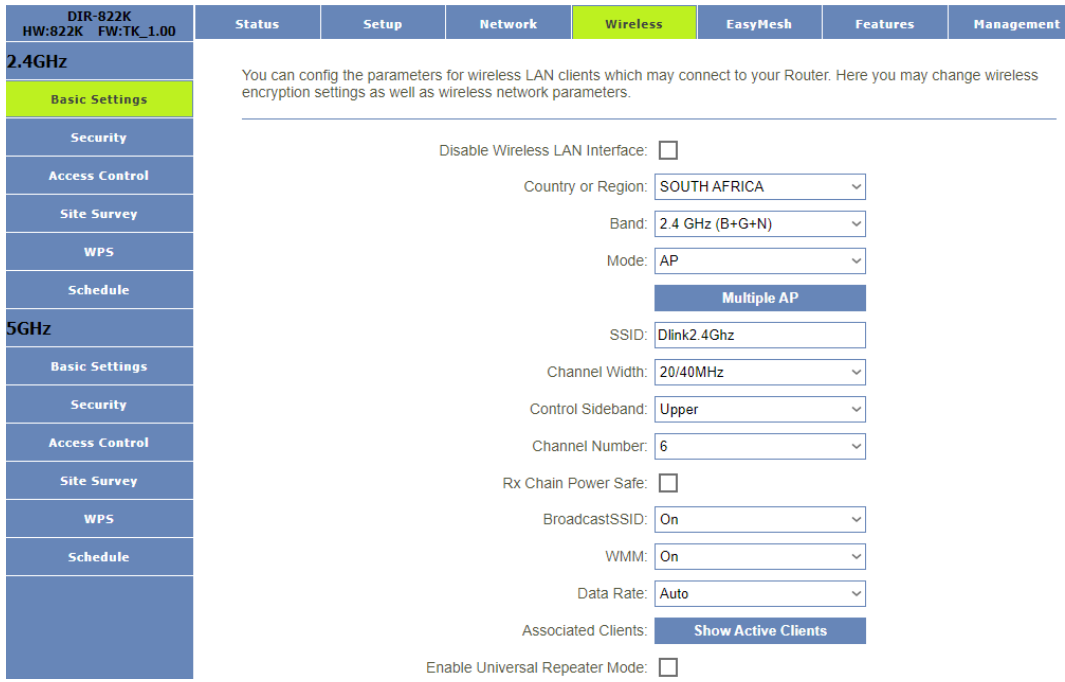


Wireless (2.4GHz)

Basic settings

Here we will configure the settings for the 2.4Ghz Network.

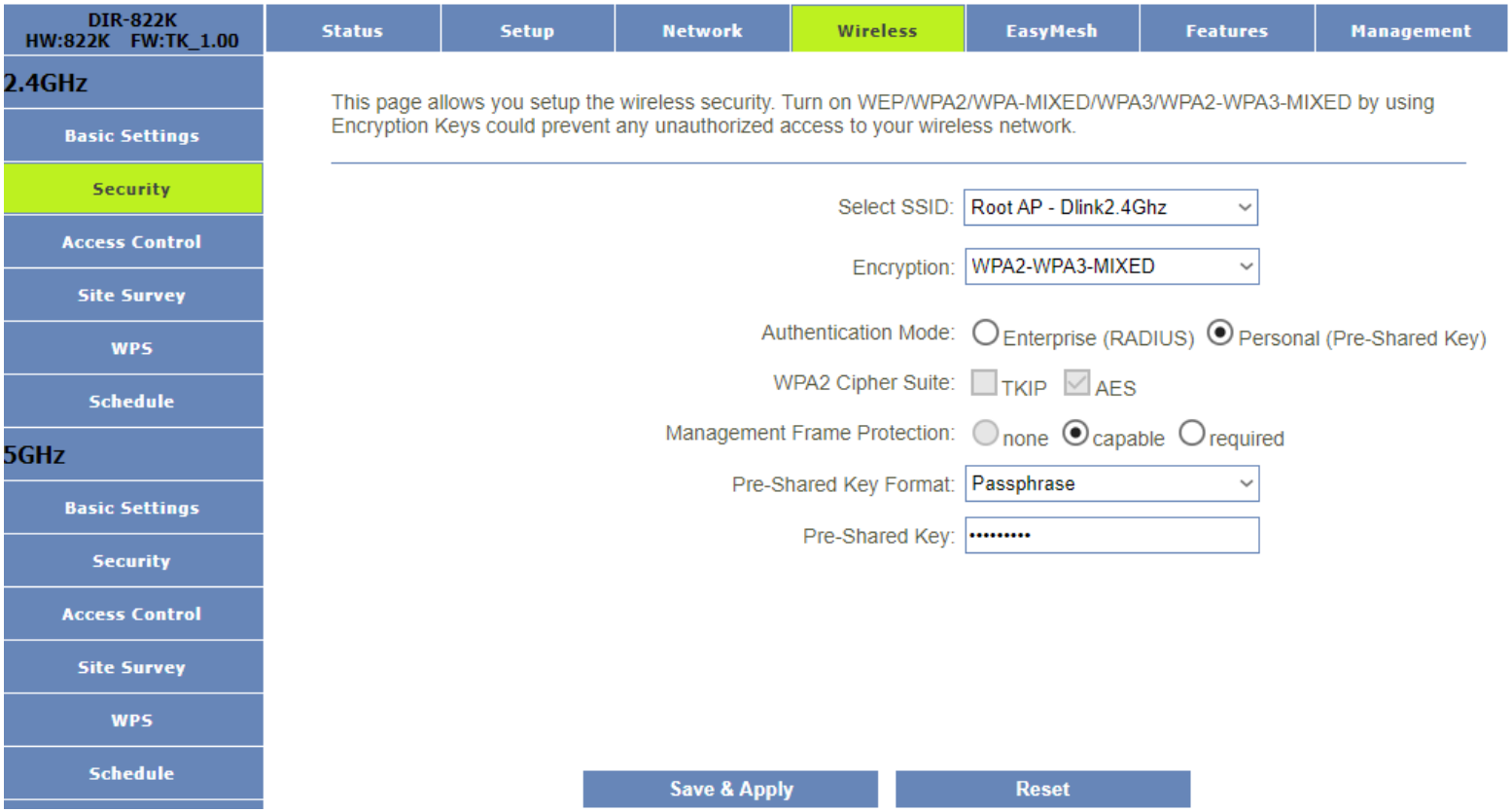
Disable Wireless LAN Interface: Set the Wireless state to Enabled or Disabled.
Country or Region: Choose your country of origin
Band: Select a wireless band
Mode: Select mode AP/Client
SSID: Set a name for your wireless network
Channel Width: Select the channel width of 20Mhz, 40Mhz or 20/40Mhz
Control Sideband: Set the Sideband to Upper or Lower.
Channel Number: Select a wireless channel number between 1-13 (recommended to use 1/6/11)
RX Chain Power Safe: Enable/Disable
Broadcast SSID: Enable to Broadcast the SSID (Wi-Fi Name)
WMM: Turn Wi-Fi Multimedia on/off.
Data Rate: Set the Rate to Auto or a selected value.
Associated clients: Click to show Active wireless clients
Enable Universal Repeater mode: Tick to Enable Universal Repeater mode.



Security

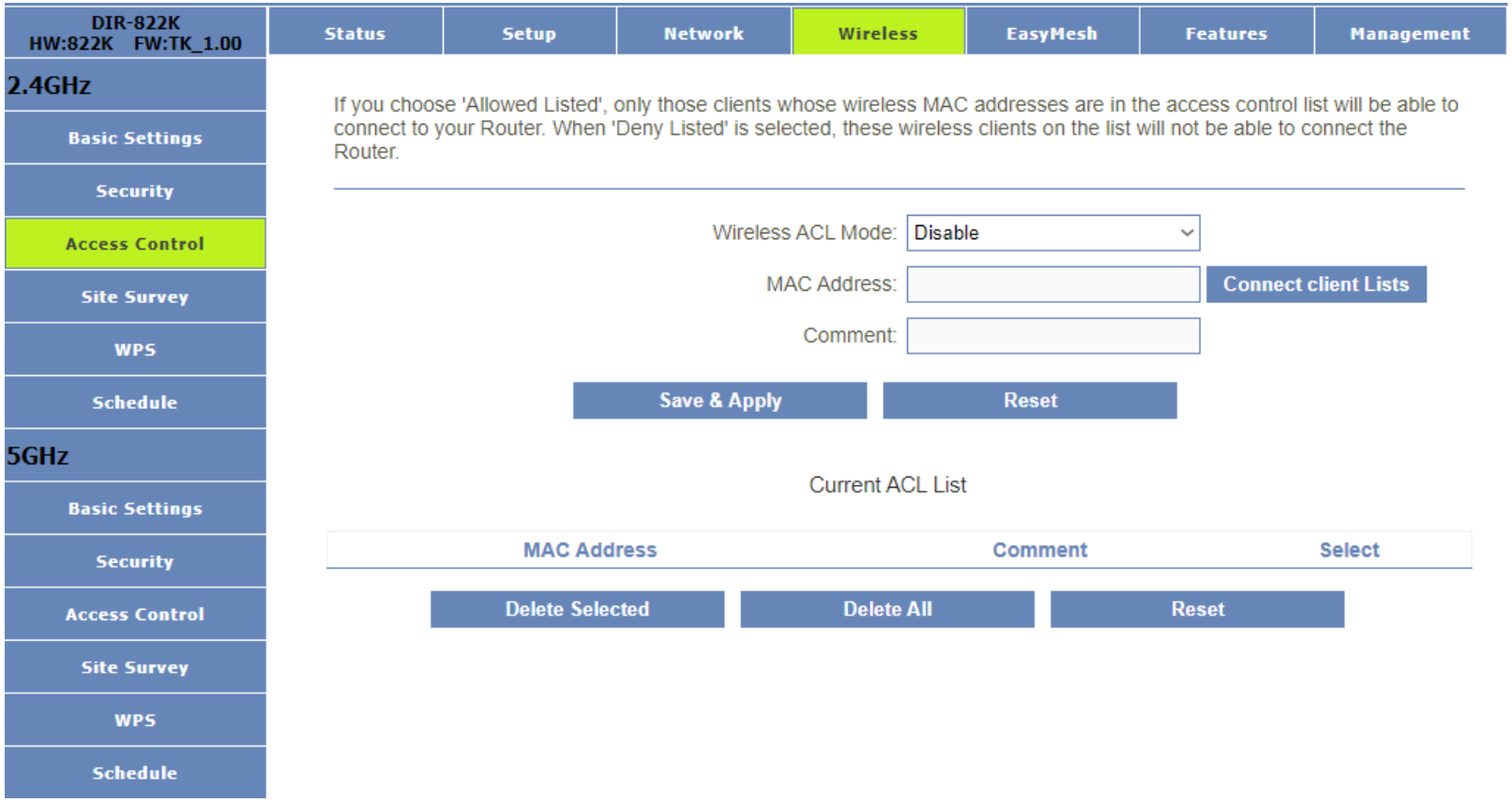
Here you can set and change security parameters

Select SSID: Choose an SSID from the drop-down list.
Encryption: Select an Encryption type.
Authentication Mode: Select between Enterprise or Personal.
WPA2 Cipher Suite: Choose between TKIP/AES.
Management Frame Protection: Select between None/Capable/required.
Pre-Shared Key Format: Select between Passphrase or HEX (64 Characters)
Pre-shared Key: create a Wi-Fi password with a minimum of 8 characters.



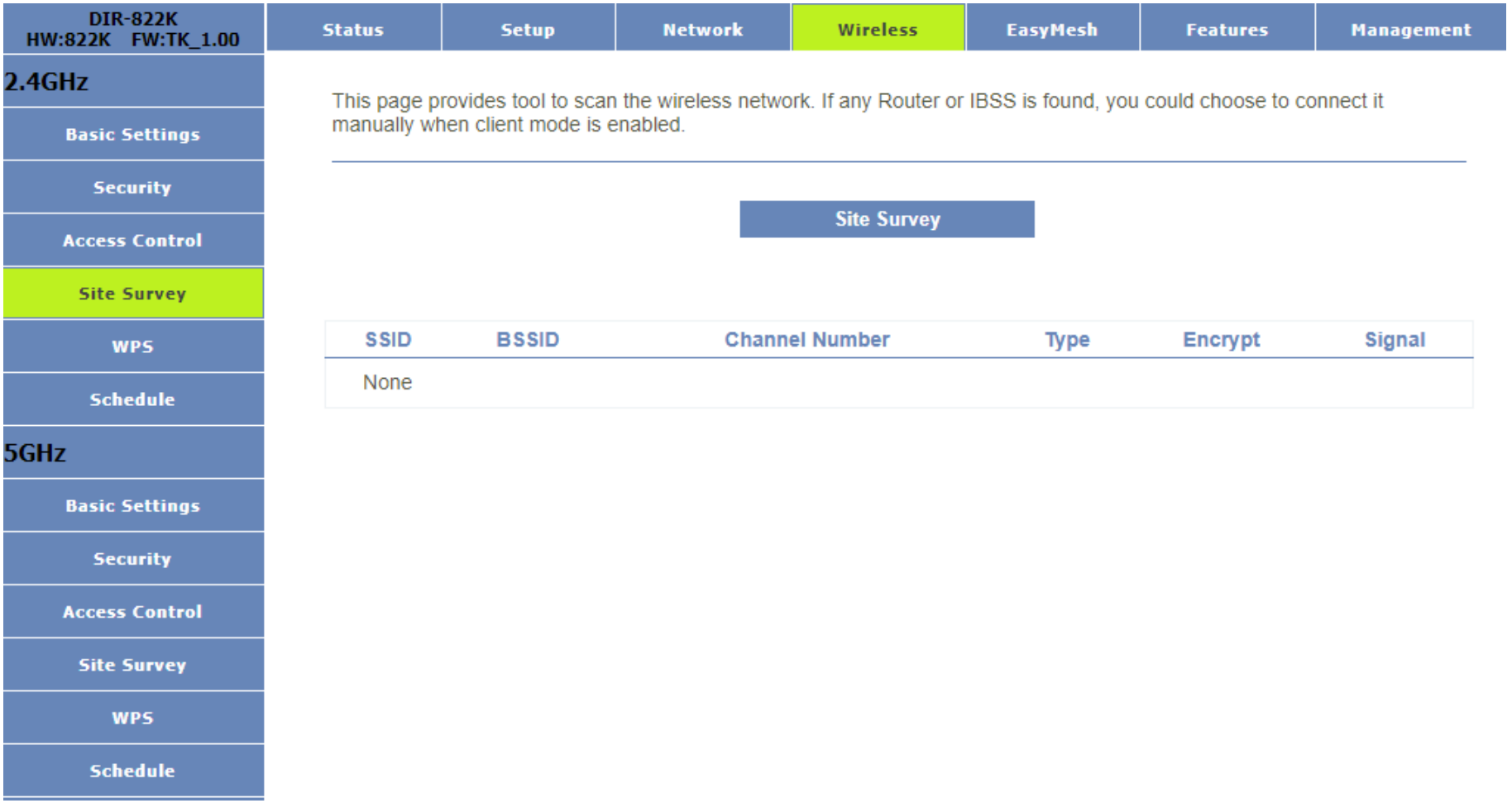
Access Control

Wireless ACL Mode: Set to Disable or choose to Allow or Deny Device access.
Allow: Allows the desired mac address
Disable: fully disables the ACL feature.
Deny: Denies the desired mac address
MAC Address: Enter the MAC of the device or choose it from the connected clients list.
Comment: You may enter a note/name/tag in this field.



Site Survey

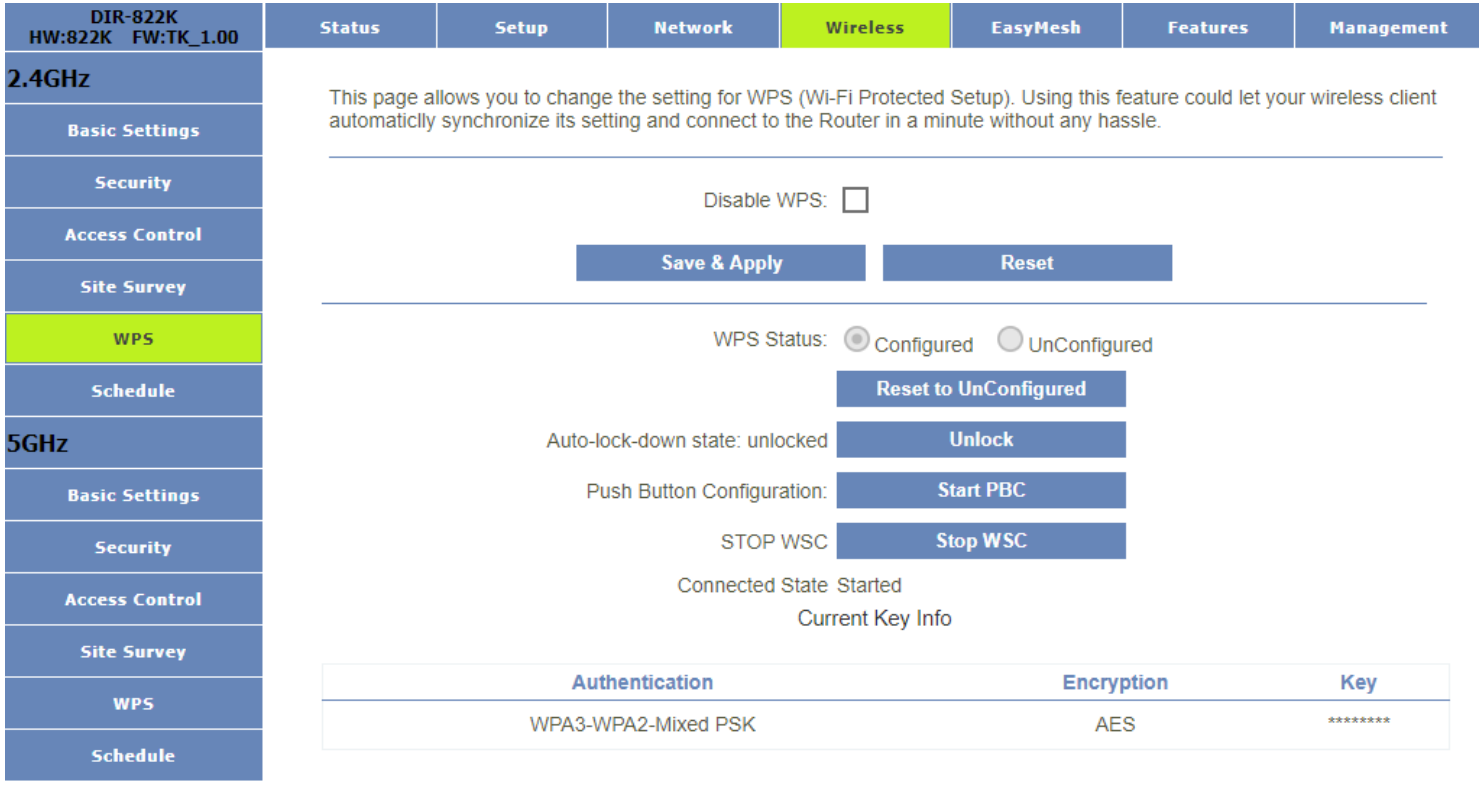
Here you can utilize the site survey tool to scan the wireless network in your area, if any Router or IBSS is found you can choose to connect to it. (Please note wireless client mode must be enabled to connect).



WPS

Here you can change the settings for the 2.4Ghz WPS (Wi-Fi Protected Setup), using this feature you can let your wireless client connect and synchronize all its settings and connect to the Router.

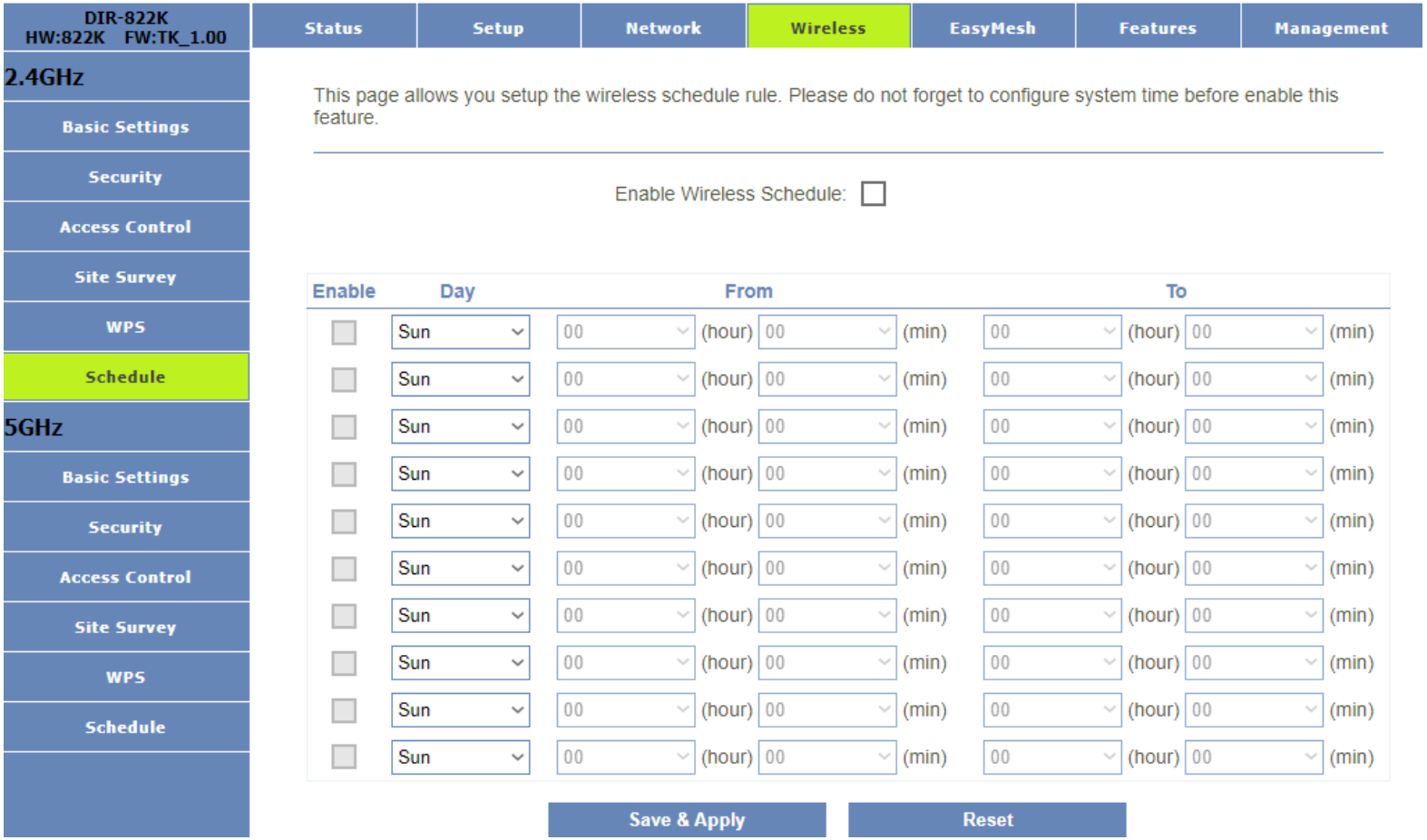
Disable WPS: Choose to Disable/Enable the WPS Function
WPS Status: This will state if the device is configured or unconfigured. (You can manually reset the configuration here)
Auto-lock-down state: Lock or Unlock your wireless network to prevent unauthorized access and keep your data secure.
Push Button Configuration: Connect multiple devices to the network and enable data encryption by pushing the button.
STOP WSC: Stop the WPS function by pressing this button.
Connected State: Shows the current State of the WPS connection as (Started/Stopped)



Schedule

Here you can setup the wireless schedule rule (Please note to configure system time)

Enable: Enable or Disable the Rule.
DAY: Select a day in which you want the rule to be active.
FROM: Set start time.
TO: Set end time.

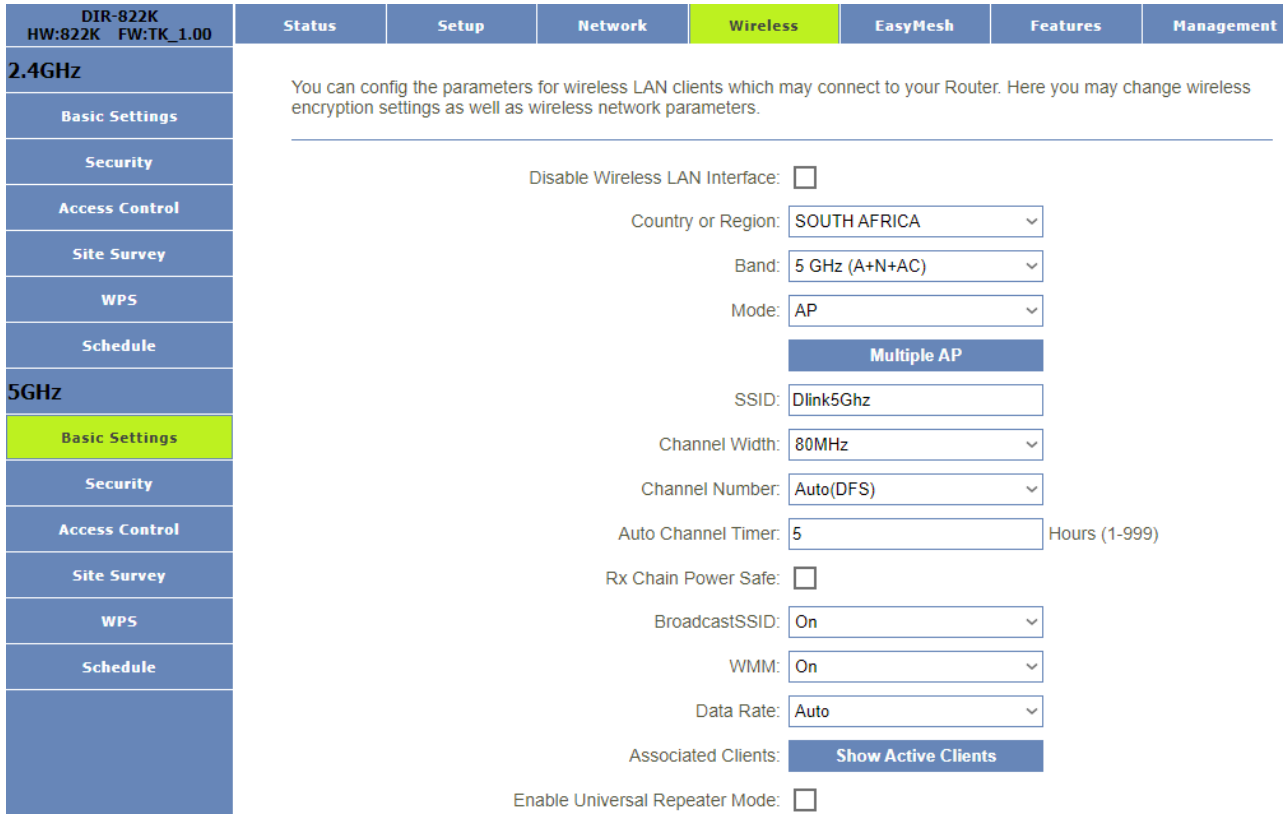


Wireless (5GHz)

Basic settings

Here we will configure the settings for the 5Ghz Network.

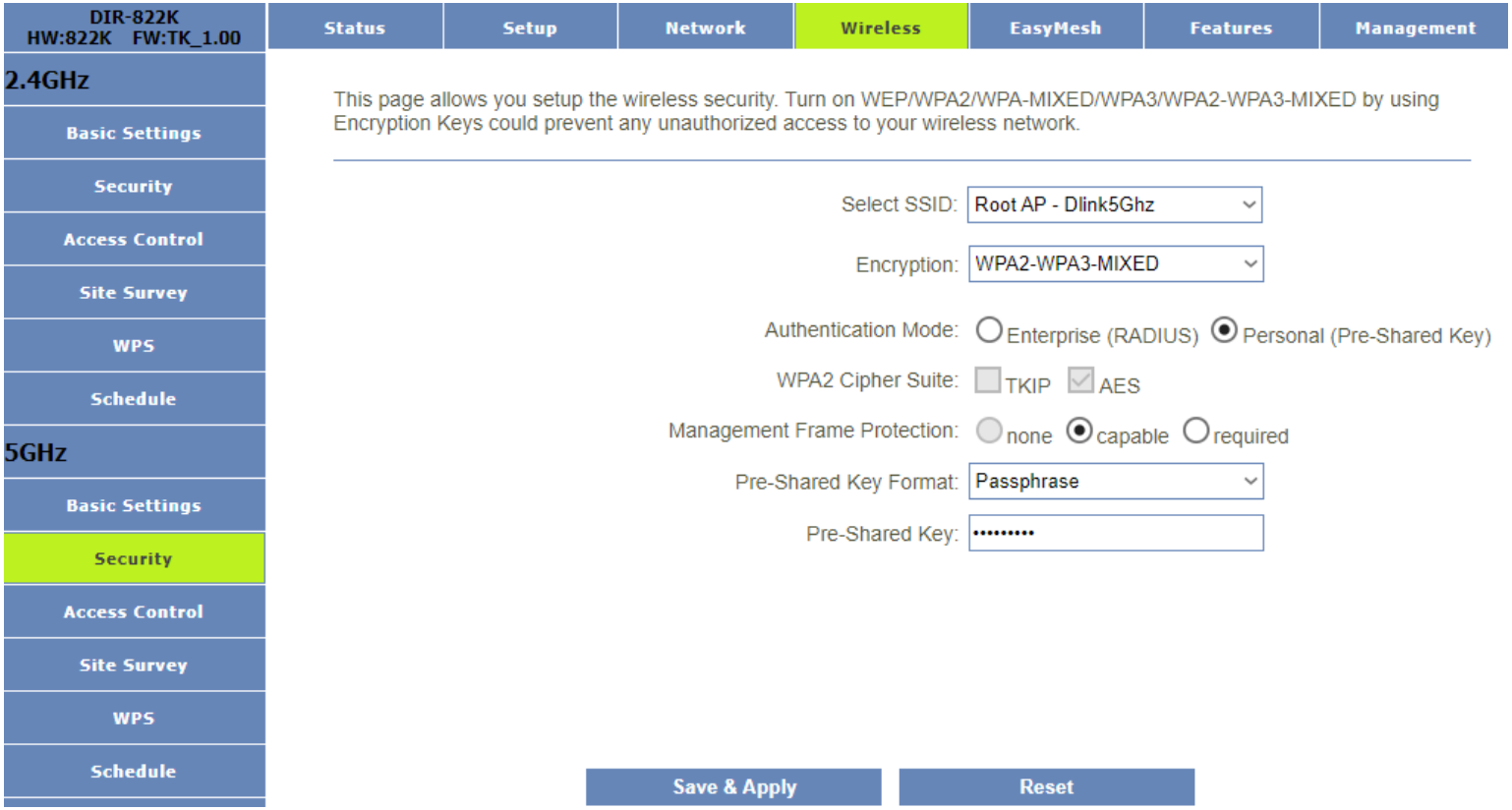
Disable Wireless LAN Interface: Set the Wireless state to Enabled or Disabled.
Country or Region: Choose your country of origin
Band: Select a wireless band
Mode: Select mode AP/Client
SSID: Set a name for your wireless network
Channel Width: Select the desired channel width
Control Sideband: Set the Sideband to Upper or Lower.
Channel Number: Select a wireless channel number between 1 -13 (recommended to use 1/6/11)
RX Chain Power Safe: Enable/Disable
Broadcast SSID: Enable to Broadcast the SSID (Wi-Fi Name)
WMM: Turn Wi-Fi Multimedia on/off.
Data Rate: Set the Rate to Auto or a selected value.
Associated clients: Click to show Active wireless clients
Enable Universal Repeater mode: Tick to Enable Universal Repeater mode.



Security

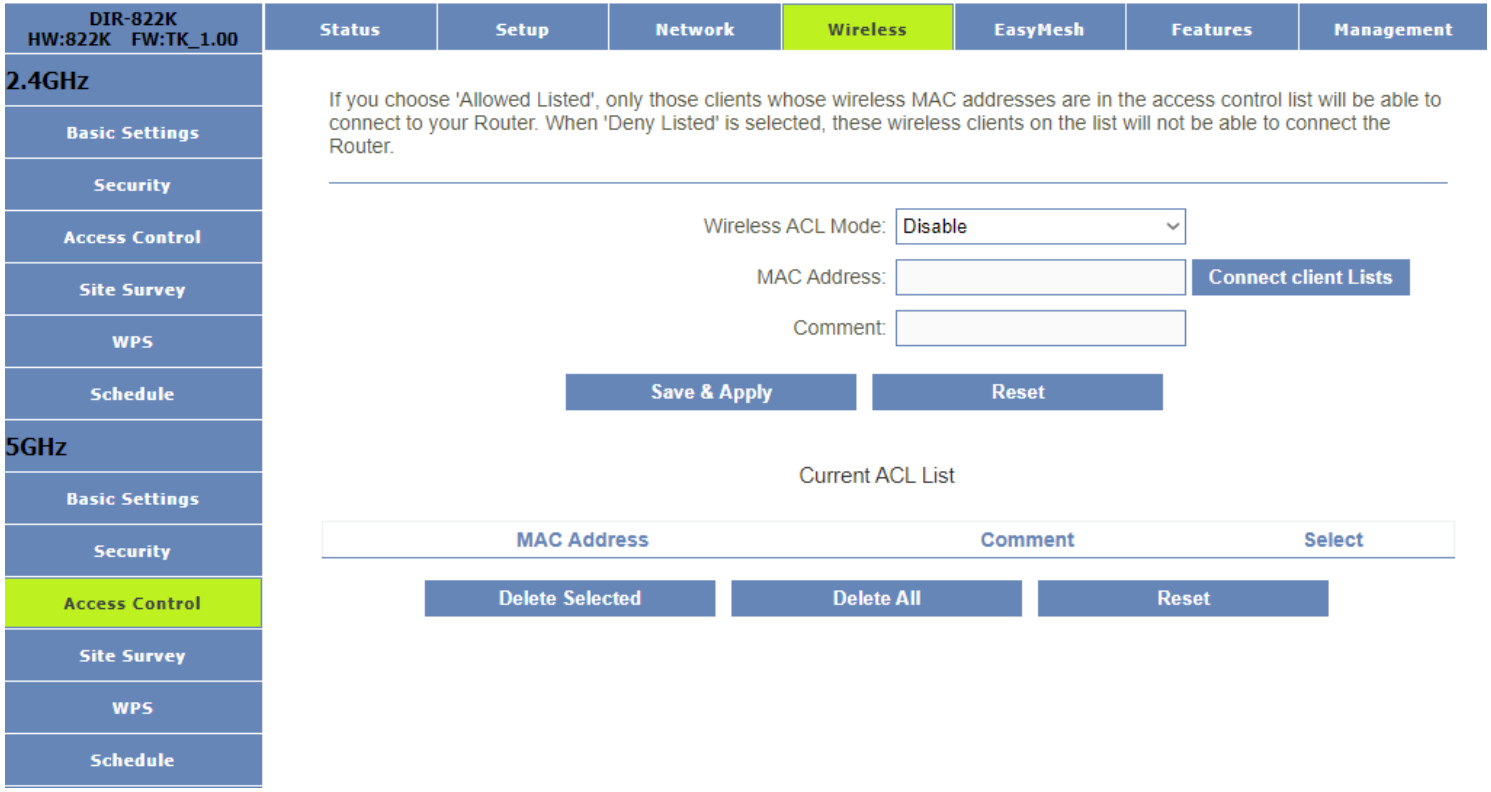
Here you can set and change security parameters.

Select SSID: Choose an SSID from the drop-down list.
Encryption: Select an Encryption type.
Authentication Mode: Select between Enterprise or Personal.
WPA2 Cipher Suite: Choose between TKIP/AES.
Management Frame Protection: Select between None/Capable/required.
Pre-Shared Key Format: Select between Passphrase or HEX (64 Characters)
Pre-shared Key: create a Wi-Fi password with a minimum of 8 characters.



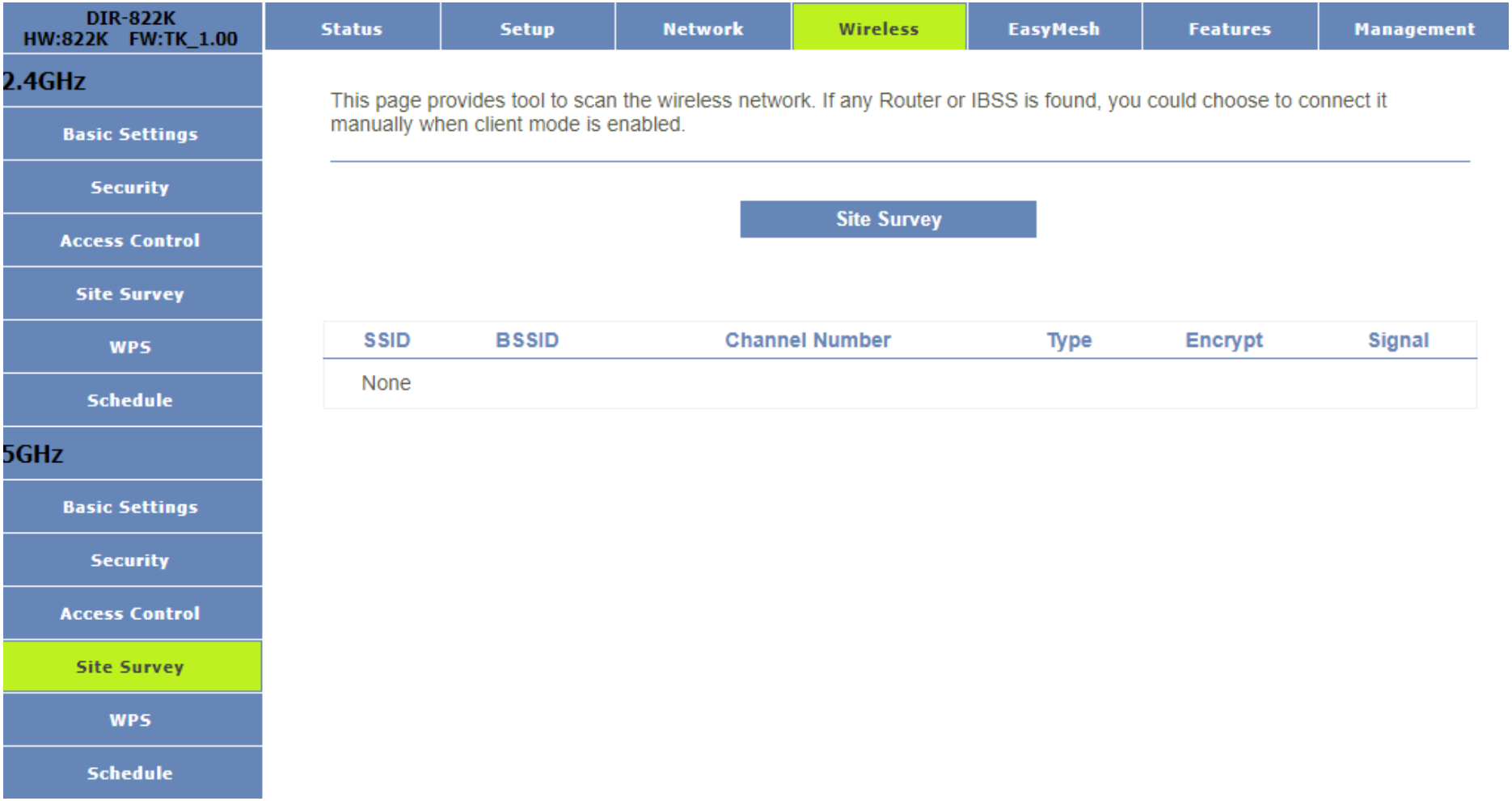
Access Control

Wireless ACL Mode: Set to Disable or choose to Allow or Deny Device access.
Allow: Enables the ACL mode.
Disable: Disables the ACL mode.
Deny: Deny any Mac Address on the ACL list.
MAC Address: Enter the MAC of the device or choose it from the connected clients list.
Comment: You may enter a note/name/tag in this field.



Site Survey

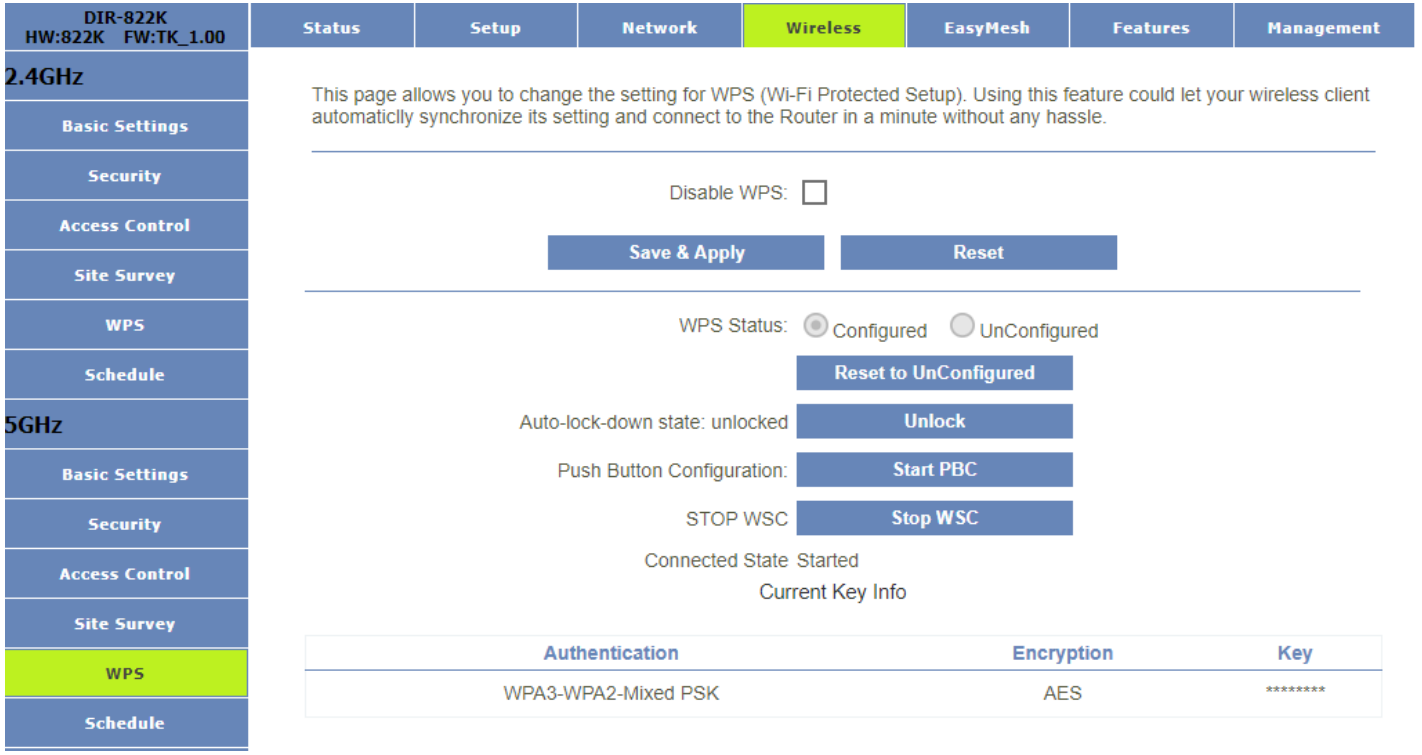
Here you can utilize the site survey tool to scan the wireless network in your area, if any Router or IBSS is found you can choose to connect to it. (Please note wireless client mode must be enabled to connect).



WPS

Here you can change the settings for 5Ghz WPS (Wi-Fi Protected Setup), using this feature you can let your wireless client connect and synchronize all its settings and connect to the Router.

Disable WPS: Choose to Disable/Enable the WPS Function
WPS Status: This will state if the device is configured or unconfigured. (You can manually reset the configuration here)
Here you can change the settings for WPS (Wi-Fi Protected Setup), using this feature you can let your wireless client connect and synchronize all its settings and connect to the Router.
Auto-lock-down state: Lock or Unlock your wireless network to prevent unauthorized access and keep your data secure.
Push Button Configuration: Connect multiple devices to the network and enable data encryption by pushing the button.
STOP WSC: Stop the WPS function by pressing this button.
Connected State: Shows the current State of the WPS connection as (Started/Stopped)



Schedule

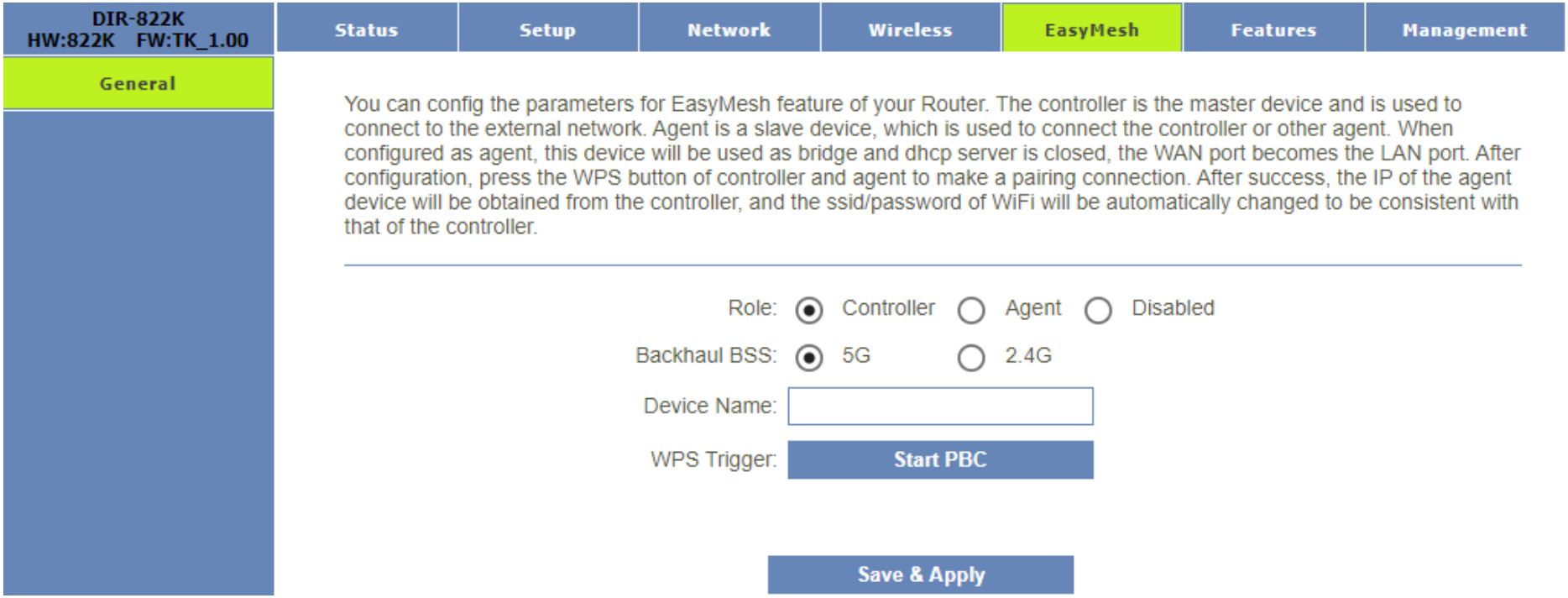
Here you can setup the wireless schedule rule (Please note to configure system time)

Enable: Enable or Disable the Rule.
DAY: Select a day in which you want the rule to be active.
FROM: Set start time.
TO: Set end time.

Easy Mesh

You can configure the Easy Mesh feature here and makes changes to the settings.

Role: Choose to Disable or make it the Controller or Agent.
Backhaul BSS: Choose which SSID you want to use.
Device name: Give the Device a unique name.
WPS Trigger: Click to start WPS process.



Features

Advanced

You can utilize the Routers high-performance features, monitor internet traffic and protect your network from malicious internet attacks.

Enable DMZ: Enabling this feature will add a perimeter network that adds an extra layer of security to internal local-area network from untrusted traffic

Enable UPNP: Enabling this feature will allow Universal plug and play ,this network protocol allows network devices to seemingly discover each other's presence and establish functional network service.

Enable IGMP Proxy: Enabling this feature will allow several devices to share one IP address so they can all receive the same data.

Enable Ping Access on WAN: Enable this feature to PING the WAN interface of the firewall/Router when troubleshooting connectivity issues when outside the office or home LAN.

Enable Web Server Access on WAN: Enable this feature to allow access to the router interface remotely.

Enable Web Server HTTPS Access on WAN: Enable this feature if you want to connect to the Web Server using an HTTPS address.

Web Lan Http access port: Choose a HTTP port to access the Web.

web Lan Https access port: Choose a HTTPS port to access the Web.

Enable IPsec pass through on VPN connection: Enable if you want to use IPsec on a VPN connection.

Enable PPTP pass through on VPN connection: Enable if you want to use PPTP on a VPN connection.

Enable L2TP pass through on VPN connection: Enable if you want to use L2TP on a VPN connection.

RTSP ALG: Enable this to control the delivery of data with real time properties.

SIP ALG: Enable this to prevent traffic from interfering with VoIP packets

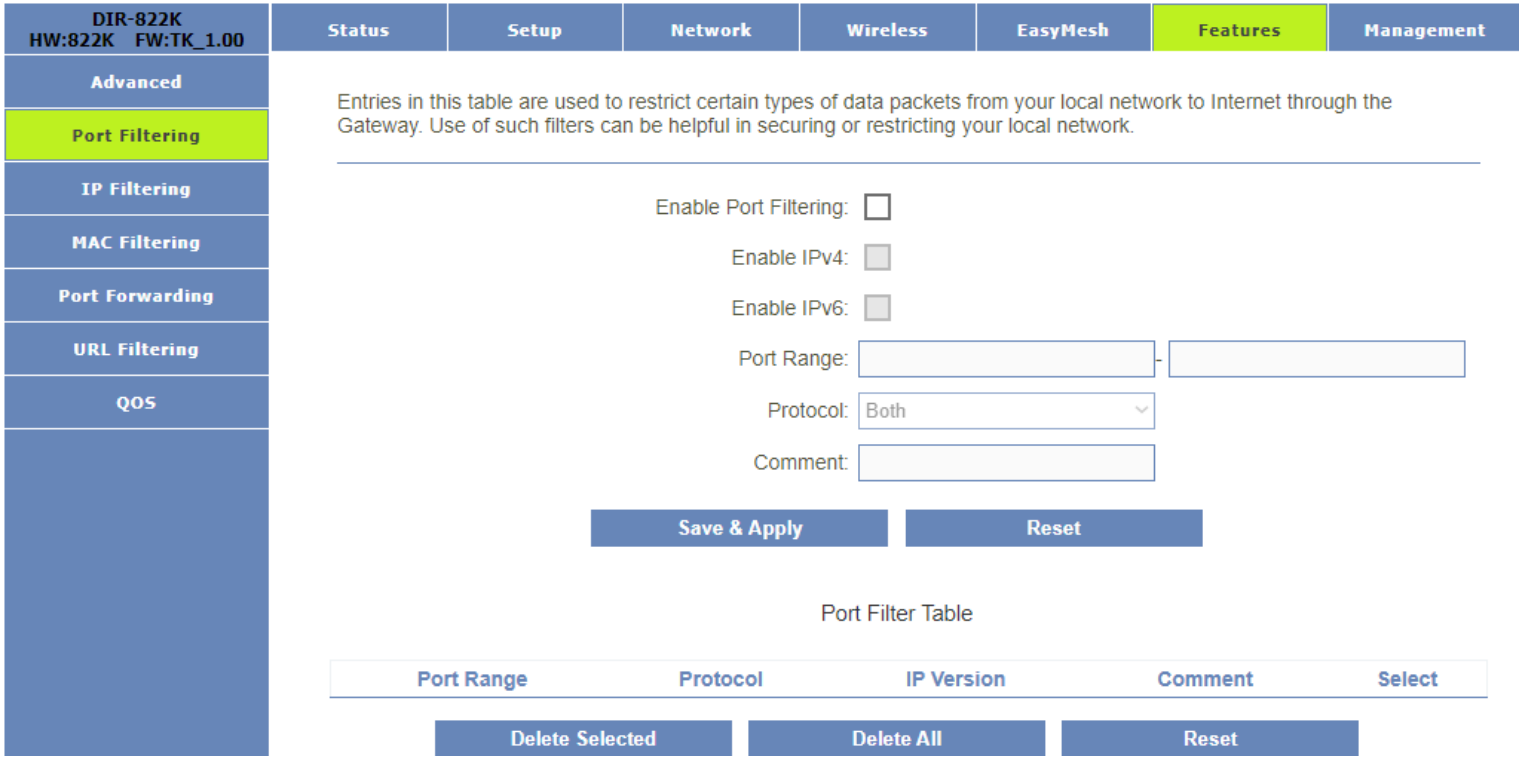
Wi-Fi Guest Access Router: Enable this to allow Wi-Fi Guest access on Guest Profiles.


DIR-822K
HW:822K FW:TK_1.00
Status
Setup
Network
Wireless
EasyMesh
Features
Management
Advanced
Port Filtering
IP Filtering
MAC Filtering
Port Forwarding
URL Filtering
QOS
Your router's high-performance firewall feature continuously monitors Internet traffic, protecting your network and connected devices from malicious Internet attacks
Enable DMZ:
Enable UPNP:
Enable IGMP Proxy:
Enable Ping Access on WAN:
Enable Web Server Access on WAN:
Enable Web Server HTTPS Access on WAN:
Web Lan Http Accessed port: 80
Web Lan Https Accessed port: 443
Enable IPsec pass through on VPN connection:
Enable PPTP pass through on VPN connection:
Enable L2TP pass through on VPN connection:
RTSP ALG:
SIP ALG:
Wifi Guest Access Router:
Save & Apply
Reset

Port Filtering

You can restrict certain types of data packets from your local network to the internet. This can secure or restrict your local network.

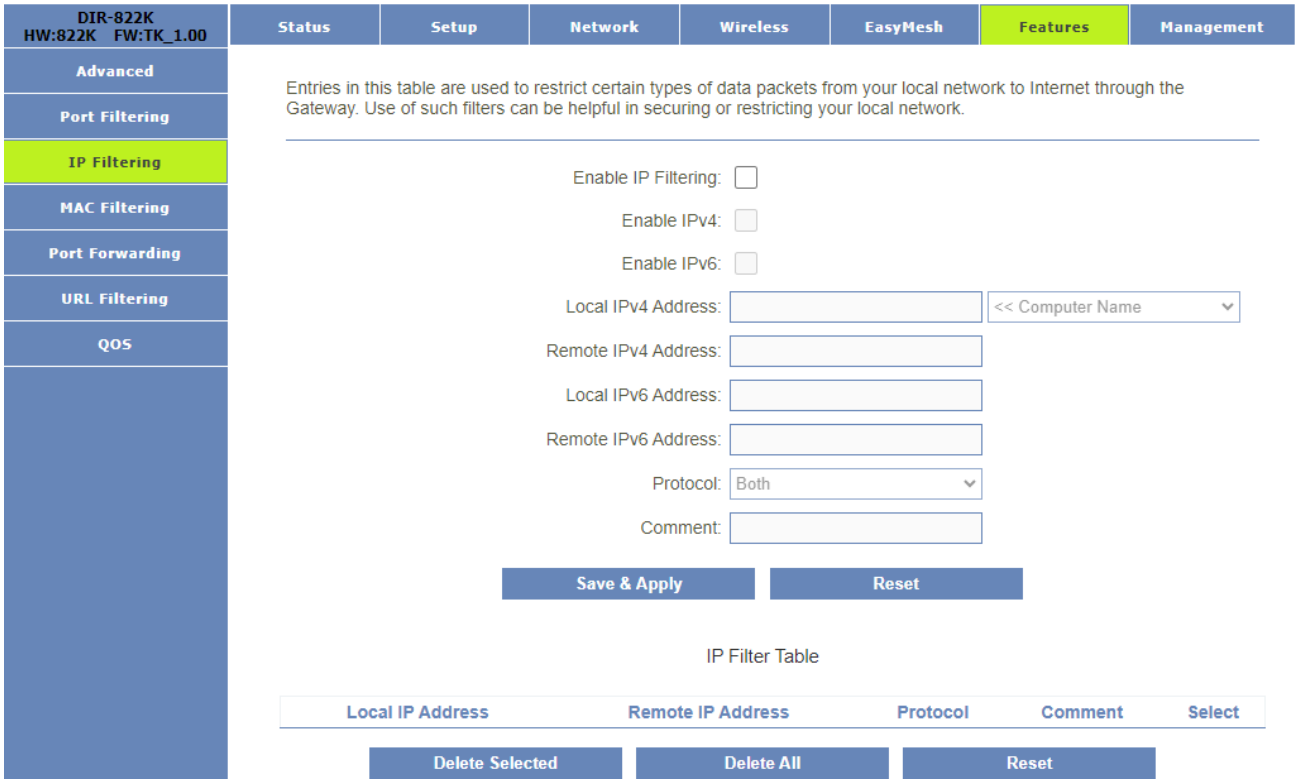
Enable Port Filtering: This feature will enable port filtering.
Enable IPv4: This will Enable Port filtering to be done on IPv4
Enable IPv6: This will Enable Port filtering to be done on IPv6
Port Range: You can set the Port Range here (1 – 65535) – e.g.: (Http Port 80, Https Port 443)
Protocol: Select Protocol type (Both, UDP, TCP)
Comment: Input a name / tag.



IP Filtering

You can restrict certain types of data packets from your local network to the internet. This can secure or restrict your local network.

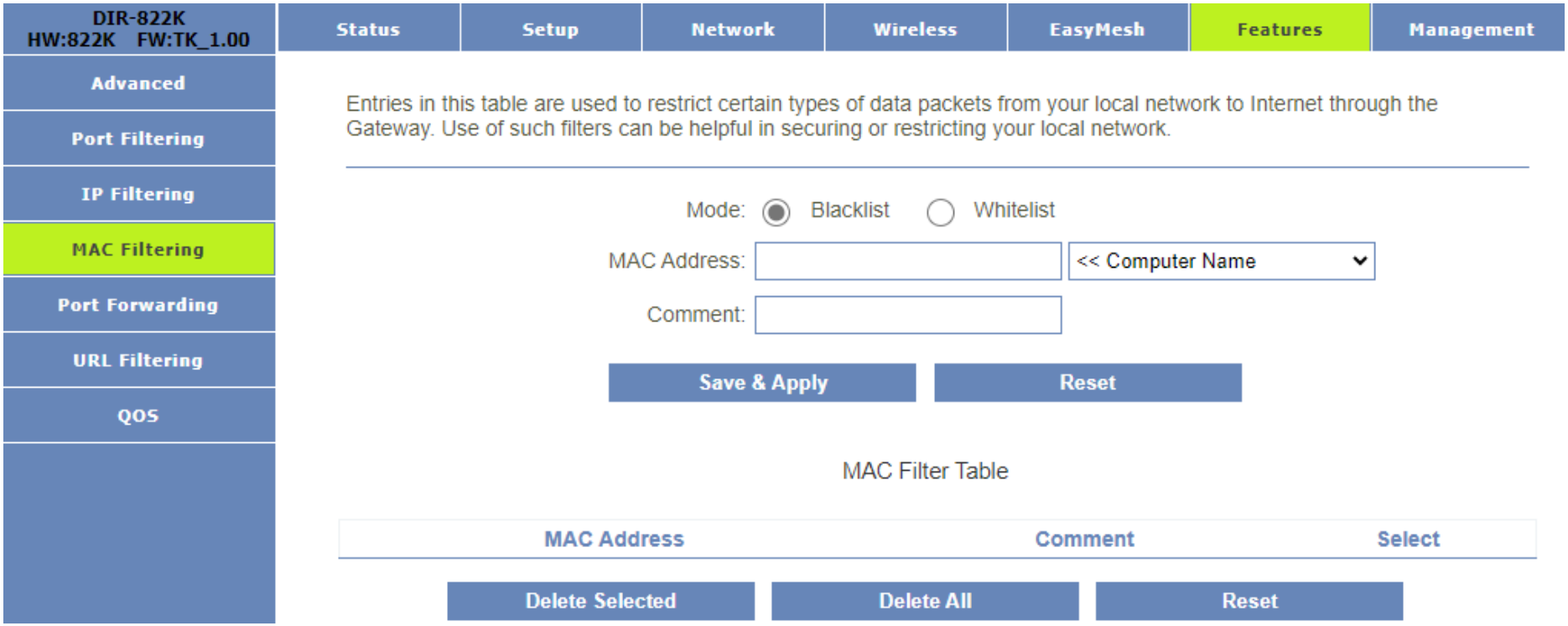
Enable IP Filtering: Enable this feature to use IP Filtering.
Enable IPv4 : Enable this Feature to utilize IP Filtering over IPv4
Enable IPv6 : Enable this Feature to utilize IP Filtering over IPv6
Local IPv4 Address : Enable this to use IPv4 on the local IP.
Remote IPv4 Address : Enable this to use IPv4 on the Remote IP.
Local IPv6 Address : Enable this to use IPv6 on the local IP
Protocol : Choose a Protocol to use (Both, UTP, TCP)
Comment : Enter a name or tag.



MAC Filtering

You can restrict certain types of data packets from your local network to the internet, use of such filters can secure or restrict your local network.

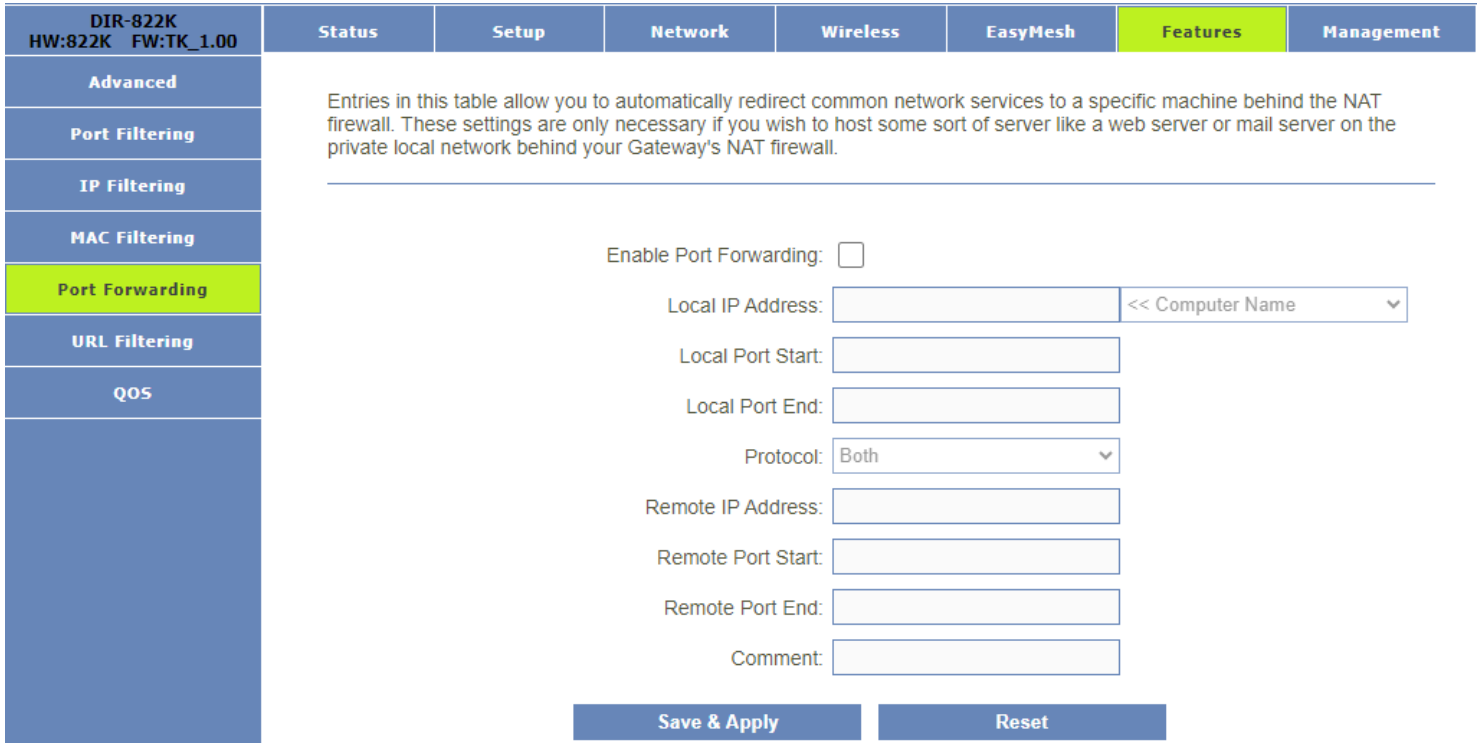
Mode: Choose to Blacklist or Whitelist a MAC address.
MAC Address: Select the device from the drop-down menu and type in its corresponding Mac address.
Comment: Enter a name or tag.



Port Forwarding

You can setup your port forwarding rules here, this will allow you to connect to a specific device behind the NAT firewall.

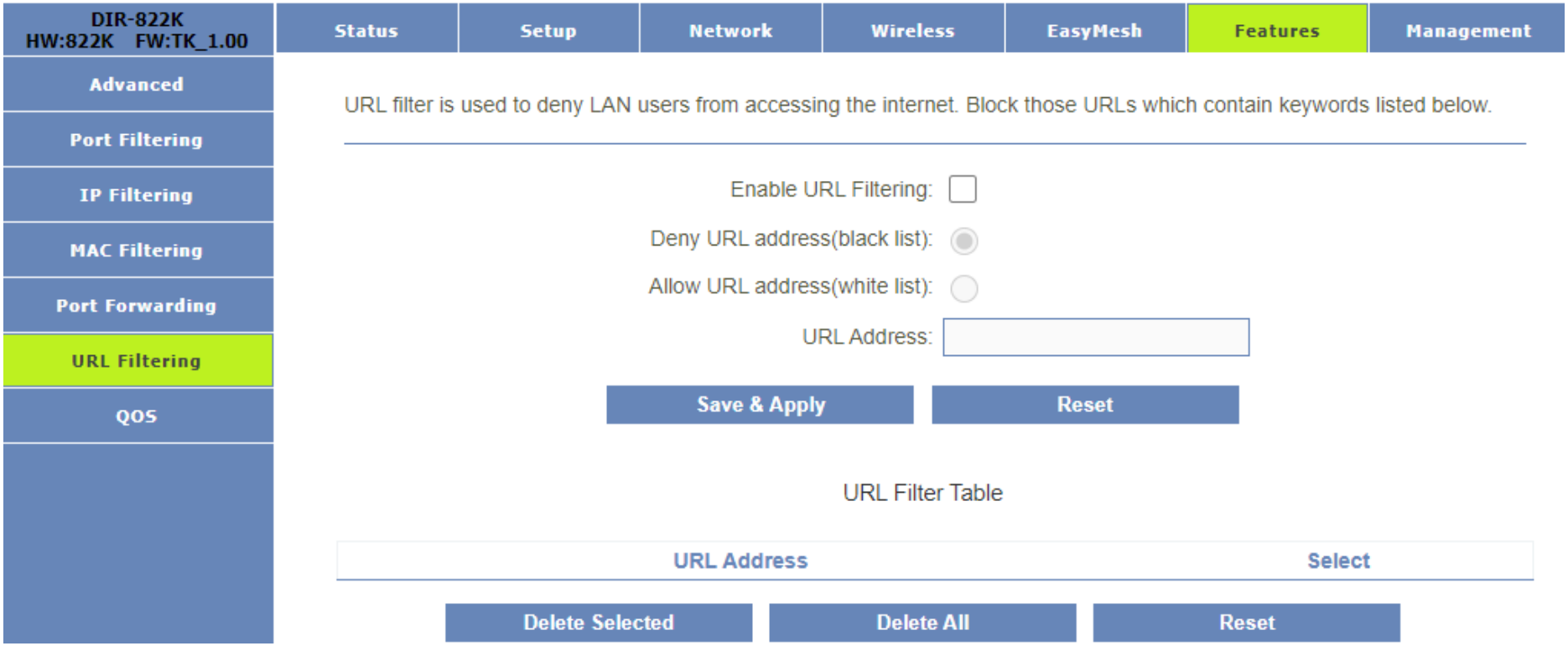
Enable Port Forwarding: Use this feature to Enable Port Forwarding on the device.
Local IP Address: Internal IP address of the Router.
Local Port Start: Enter the Port Number
Local Port End: Enter the Port Number
Protocol: Choose a Protocol (BOTH , UDP,TCP)
Remote IP address: Enter a remote IP address if you want an individual device to connect, if not leave it blank.
Remote Port Start: Enter Port Number.
Remote Port End: Enter Port Number.
Comment: Enter a name or tag.



URL Filtering

You can use the URL Filter to deny LAN users access to certain Internet sites by blocking URL's which contain certain keywords.

Enable URL Filtering: Use this to Enable or Disable the URL Filtering rules.
DENY URL address (Black list): Enable this to use "Black-List" (Denies all access to the URL)
Allow URL address (white list): Enable this to use "White-List" (Allows access to the URL)
URL address: Enter the Web-Address you wish to Block content viewing.



QOS

You can use this Feature to improve all round network traffic and prioritize network packets to improve online gaming / FTP or WEB services.

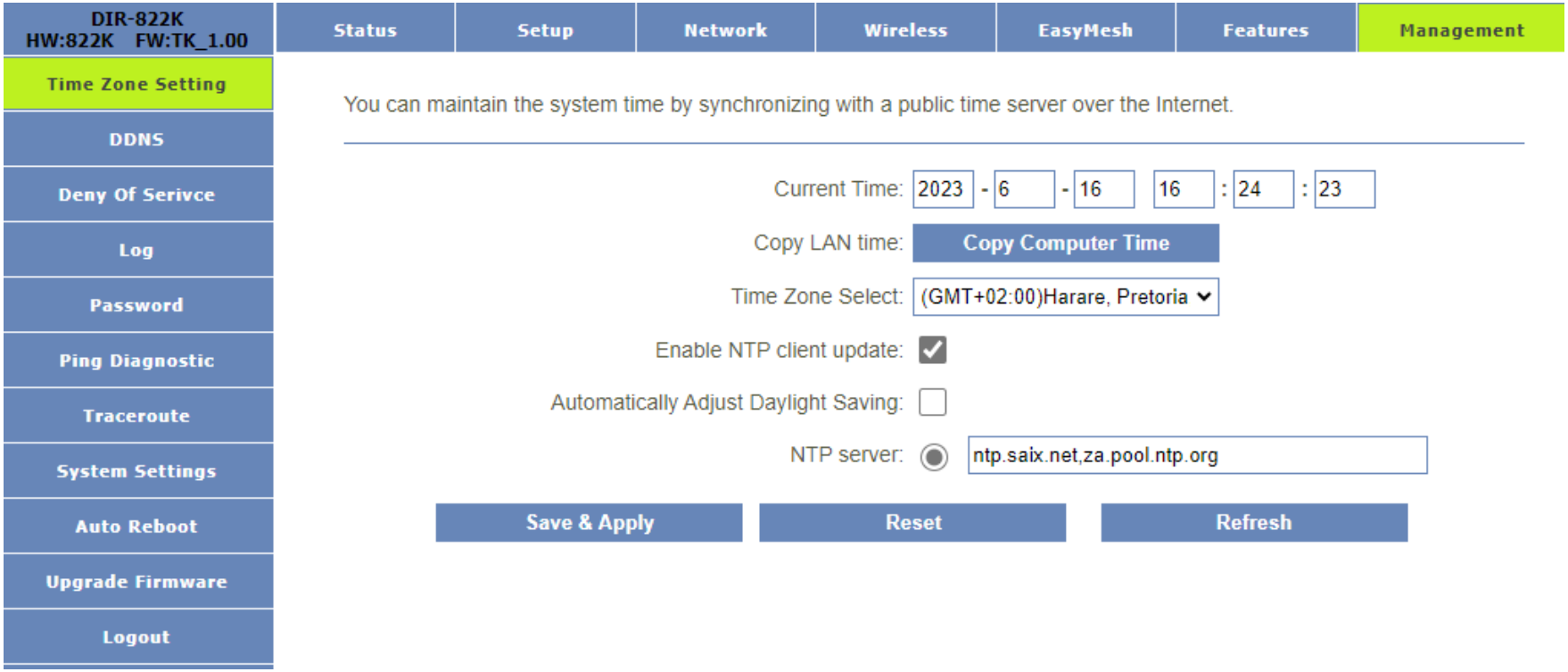
Enable QoS: Enable or Disable the Rule.
Automatic Uplink Speed : Enable or Disable .
Automatic Downlink Speed : Enable or Disable.
Name: : Give the Rule a name.
QoS Type: : Choose a type (IPv4,IPv6,MAC,PHYPORT,DSCP)
Protocol : Choose a protocol (Both, TCP,UDP)
Local IP Address : IP address of the Router.
Local Port : Enter the Local port you will be using.
Remote IP Address : Enter the IP you will be using to send and receive traffic.
Remote Port : Enter the Remote Port you will be using.
Mode : Guaranteed minimum or Restricted maximum bandwidth.
Uplink Bandwidth : Set a Uplink bandwidth limit.
Downlink Bandwidth : Set a downlink bandwidth limit.
Priority : Set a priority between 1 -7 (higher the number = higher the priority)
Remark DSCP : you can re-mark differentiated service codes to prioritize IP packets.
Comment : Enter a name or tag.

Management

Time Zone Setting

Here you can maintain the system time settings by synchronizing with a public time server over the internet.

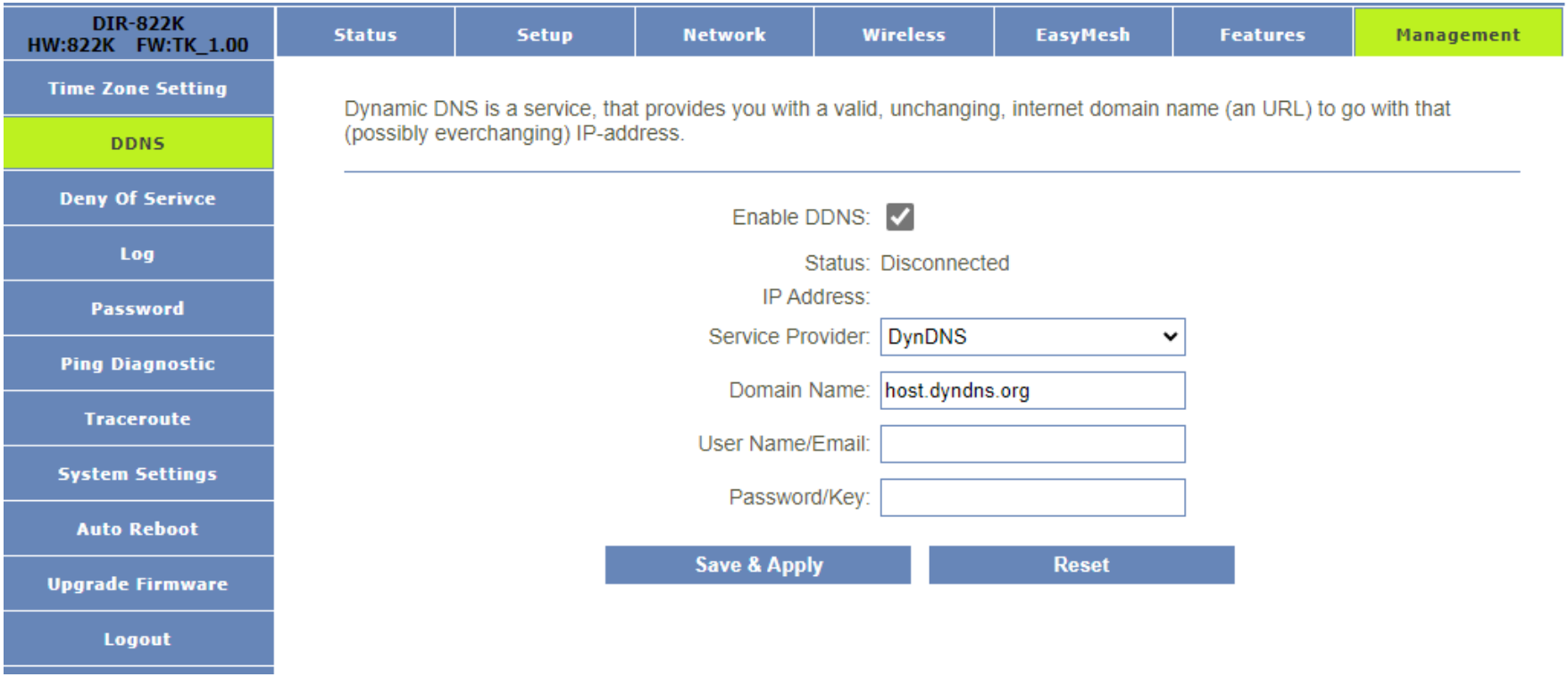
Current time: set the current time manually.
Copy LAN time: Automatically Copies the Computer time from your device.
Time Zone Select: Select a time zone based on your location.
Enable NTP Client Update: Enable this to periodically keep the Time server up to date.
Automatically Adjust Daylight Saving: Select this if your country practices daylight saving.
NTP Server: Enter the NTP server address.



DDNS

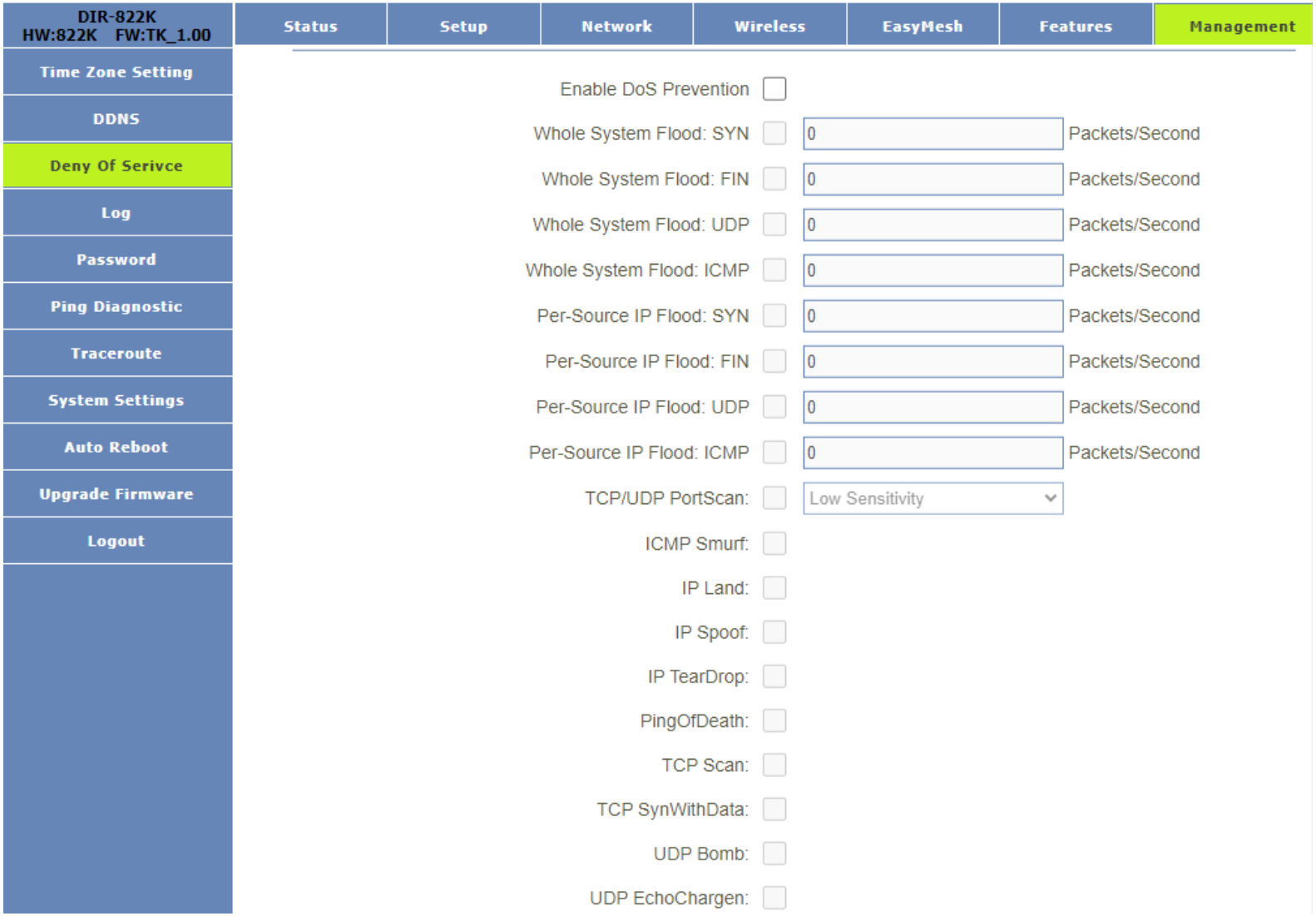
Here you can setup you're existing DDNS account

Enable DDNS: This feature will allow you to Enable or Disable the DDNS account.
Status: this will show the DDNS account as Connected/Disconnected.
IP Address: this will show the IP address associated with the DDNS account.
Service Provider: Select your DDNS service provider from the drop down menu.
Domain Name: Enter your DDNS host name.
User Name/Email: Enter the DDNS name or email associated with your account.
Password Key: Enter the DDNS password associated with your account.



Deny of Service

Here you can manage parameters to prevent Denial of Service attacks (DDOS)

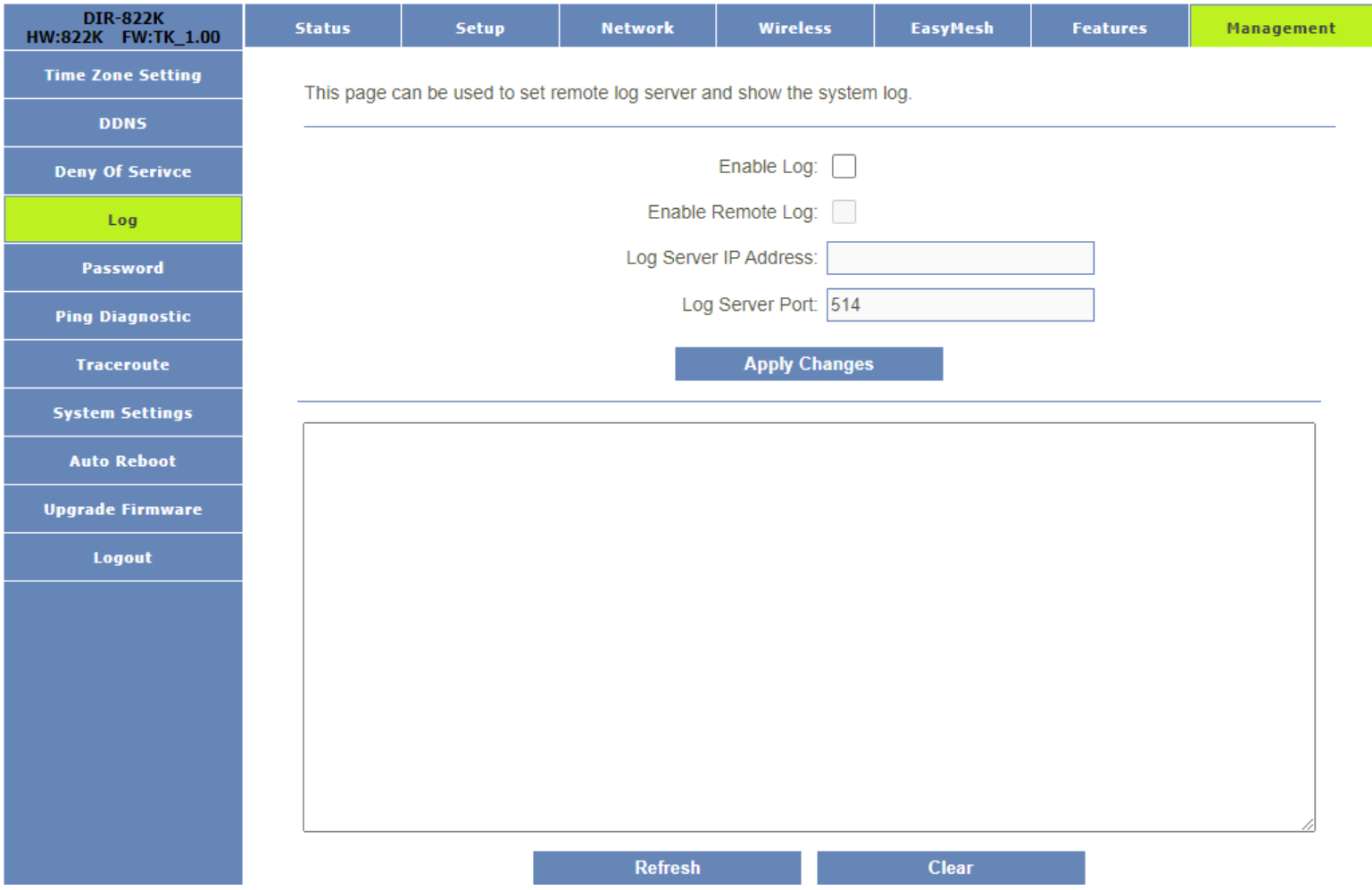


Enable DoS Prevention: You can enable the DDOS prevention Feature here to stop malicious attacks.
Whole System Flood: SYN: enable this to Prevent attacks affecting traffic denial to a server.
Whole System Flood: FIN: enable this to Prevent attacks affecting Packet traffic .
Whole System Flood: UDP: enable this to Prevent attacks that cause packet flooding to overwhelm or stop device ability to function.
Whole System Flood: ICMP: enable this to Prevent attacks that cause echo-requests (pings) to overwhelm device stability.
Per-Source IP Flood SYN: enable this to Prevent attacks that cause massive number of SYN requests to a server with open connections.
Per-Source IP Flood FIN: enable this to Prevent attacks that cause disruption of network activity due to bandwidth saturation.
Per-Source IP Flood UDP: enable this to Prevent attacks that cause UDP packets to overwhelm or stop a device ability to function.
Per-Source IP Flood ICMP: enable this to Prevent attacks that cause ICMP packets to overwhelm a device and the connection to it.
TCP/UDP Port Scan: enable to Prevent a port from being scanned or have its network status checked.
ICMP Smurf: enable to Prevent a flood of ICMP request packets.
IP Land: enable to Prevent attacks that can consist of sending special poison spoofed packets to a computer causing a lock-up.
IP Spoof: enable to Prevent the creation of IP packets with a false source Ip to impersonate another computer.
IP Teardrop: enable to Prevent attacks that flood the computer resource and cause instability.
Ping of Death: enable to Prevent attacks that can crash, destabilize or freeze a computer by sending oversized packets.
TCP Scan: enable to Prevent attacks that can sneakily scan open ports for intrusion.
TCP Syn With Data: enable to Prevent attacks that allow a server and client to pair or exchange message data.
UDP Bomb: enable to prevent Spoof IP to generate packets to overload the target the server.
UDP Echo Chargen: enable to Prevent and attack that can trigger the Echo-Chargen by spoofing a conversation between the Echo request/Reply service.

Log

Here you can view and set the remote log server.

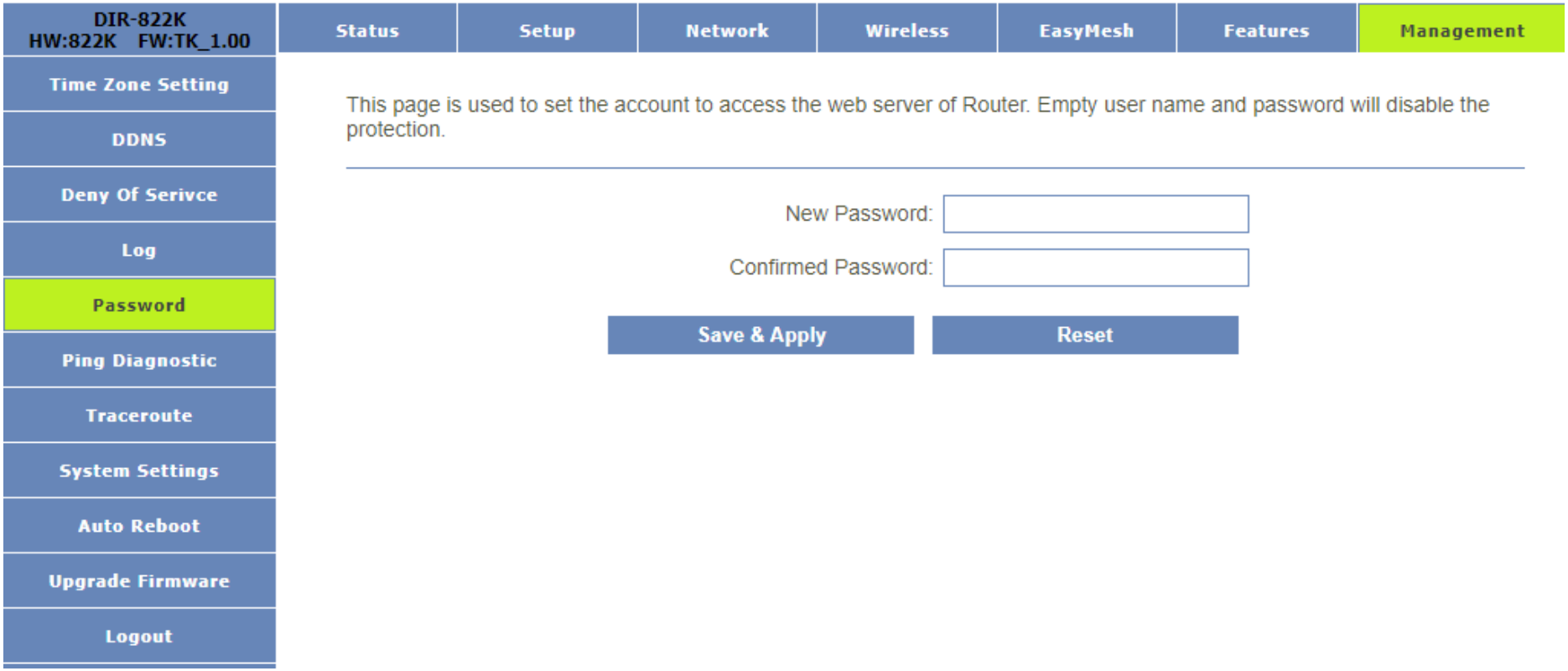
Enable Log: This Feature Enable's Logging.
Enable Remote log: This Feature Enable's Remote logging.
Log Server IP Address: Enter the Server IP.
Log Server Port: Enter the Log Port.



Password

Here you can change the default Router password to enhance security.

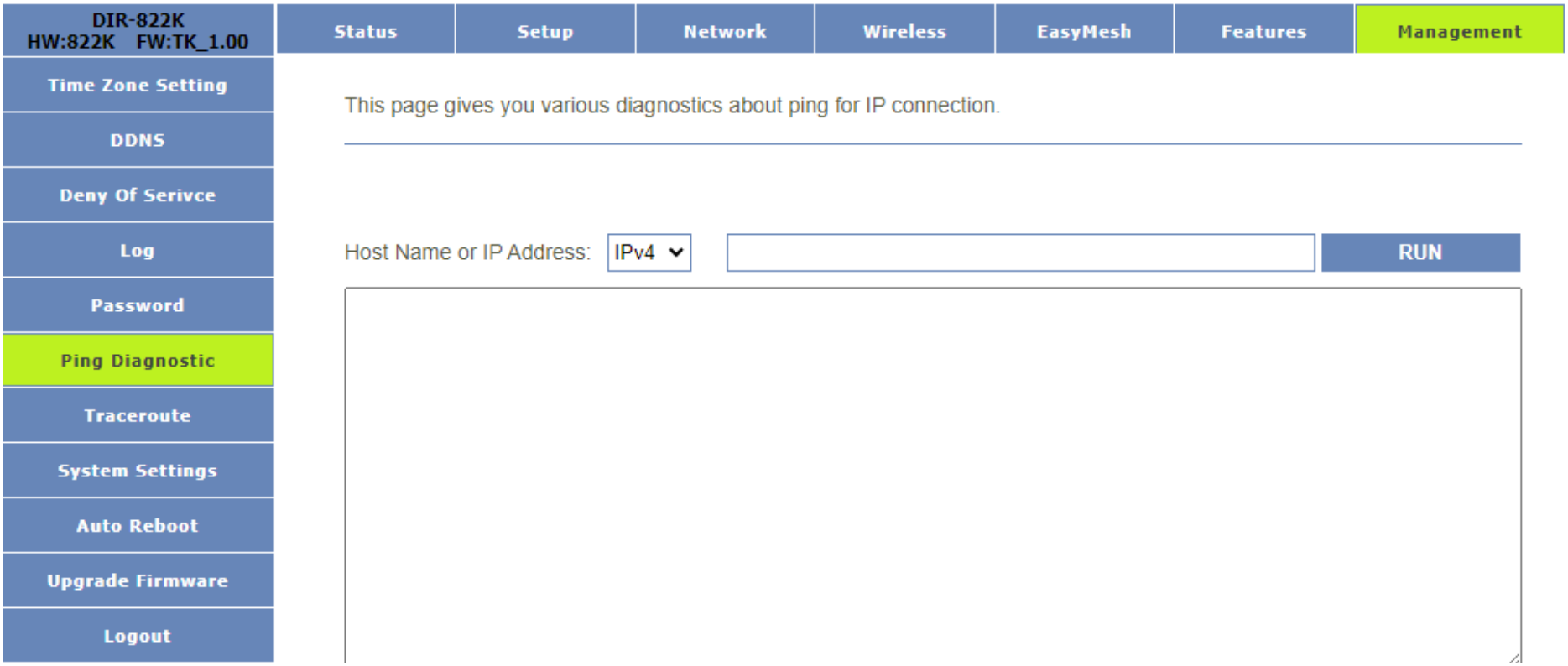
New Password: Enter a password of at least 6 characters long, this can contain Numbers, Letters, Special characters.
Confirm Password: Confirm the above password.



Ping Diagnostic

Here you can Ping an IP and Run diagnostics.

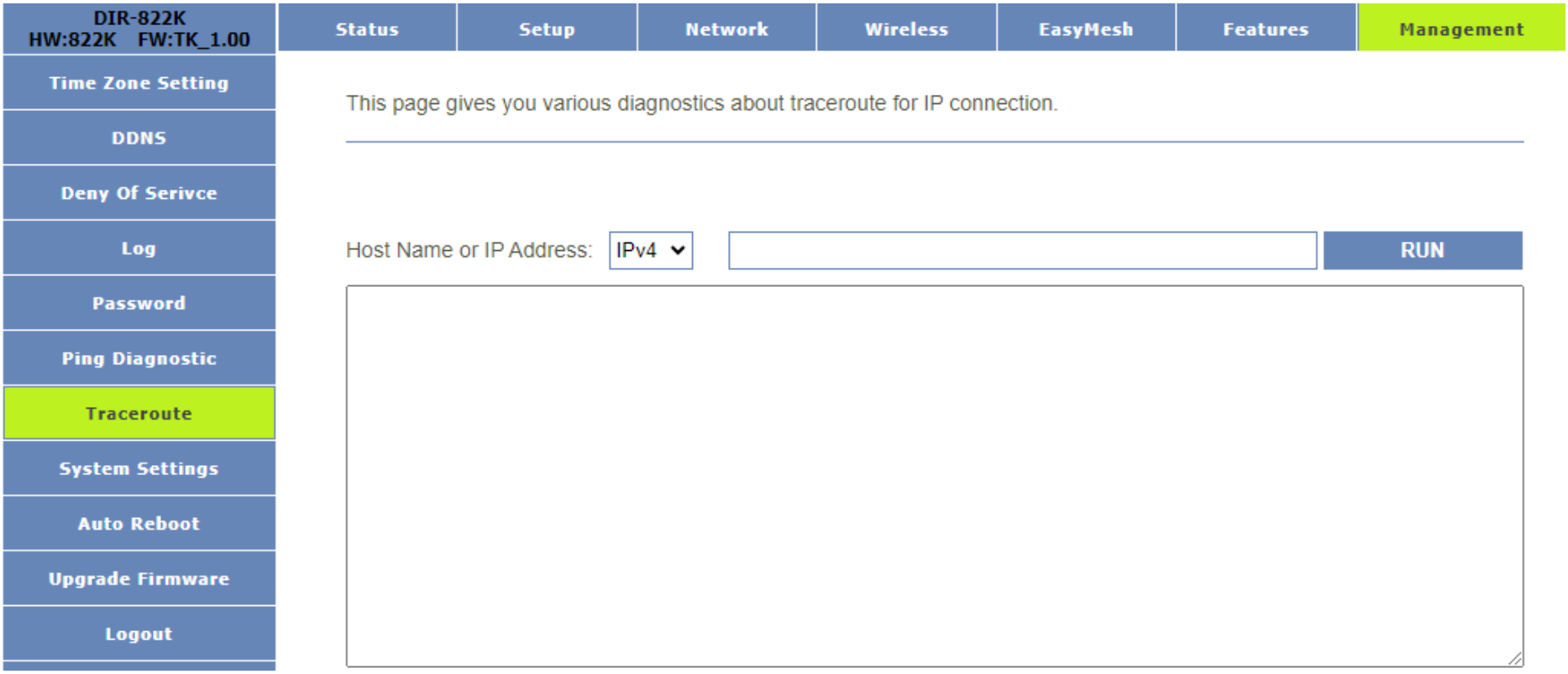
Host Name or IP Address: Choose IPv4 or IPv6 and “Click Run”



Traceroute

Here you can use the Traceroute tool and Run Diagnostics.

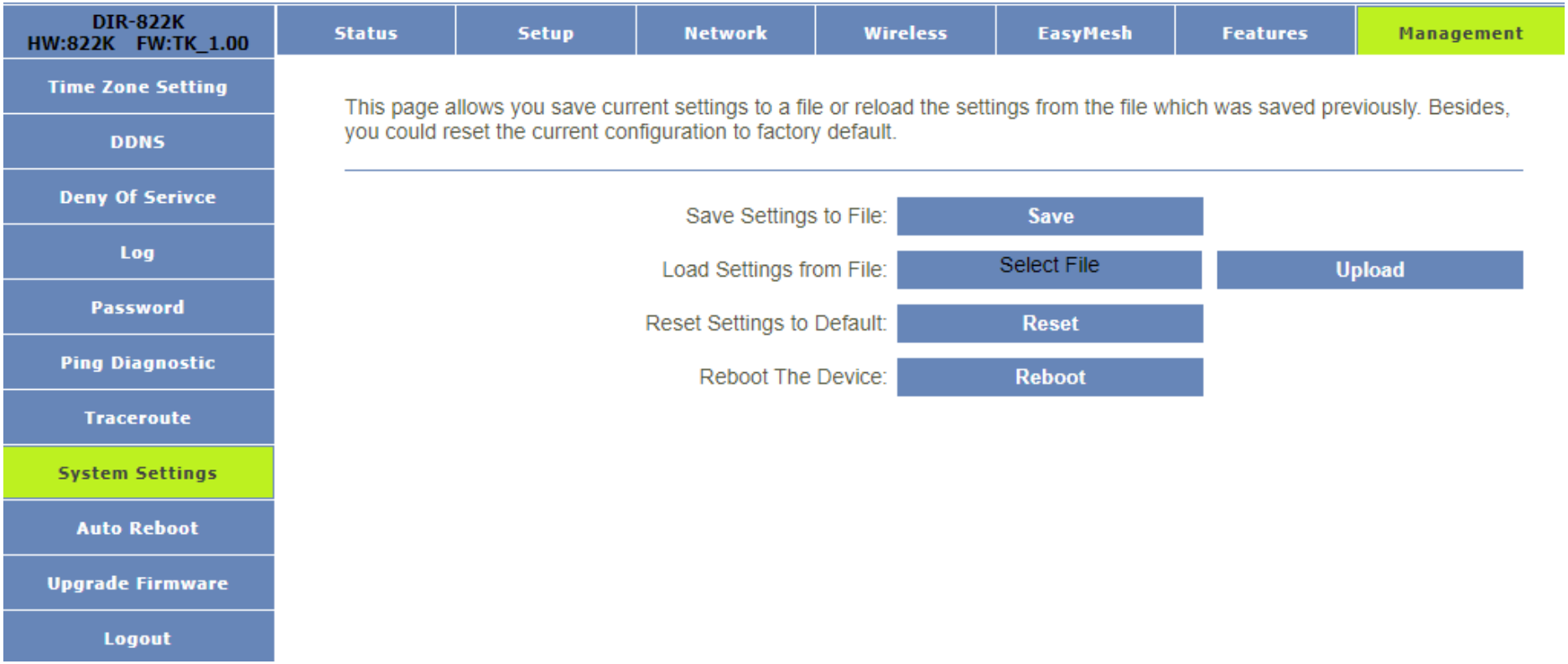
Host Name or IP Address: Choose IPv4 or IPv6



System Settings

Here you can save current settings or configurations, Reboot/Reset the Device, or load a Config file onto the Router.

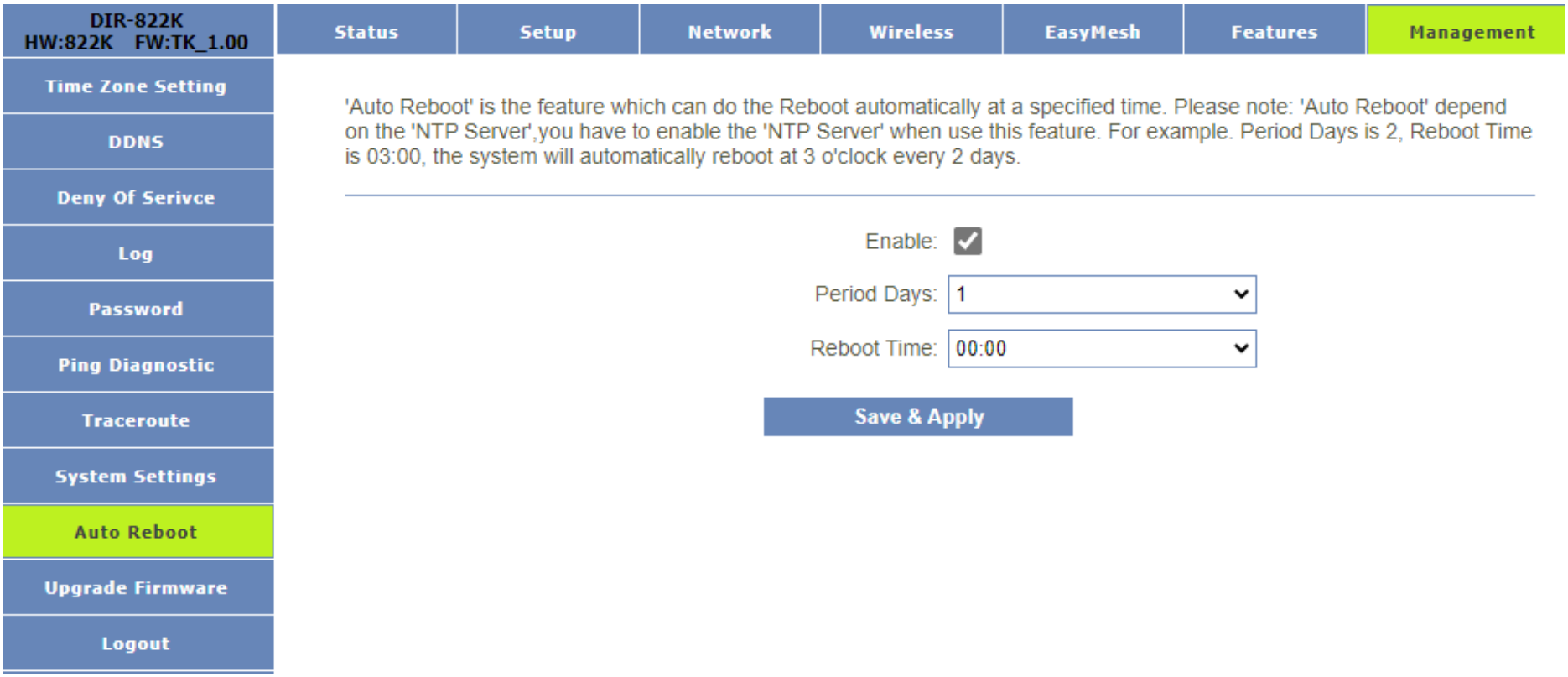
Save Settings to File: Save the Router config locally to your PC/Laptop.
Load Settings from File: Load a config backup previously saved.
Reset Settings to Default: Reset the Router to Factory default settings.
Reboot the Device: Reboot the Device using the Web Gui here.



Auto Reboot

Here you can Enable and Manage automatic Reboot for your Device.

Enable: Set the state to Enabled/Disabled.
Period Days: Set how many day intervals you want the device to reboot.
Reboot Time: Set a daily time you want the device to reboot.

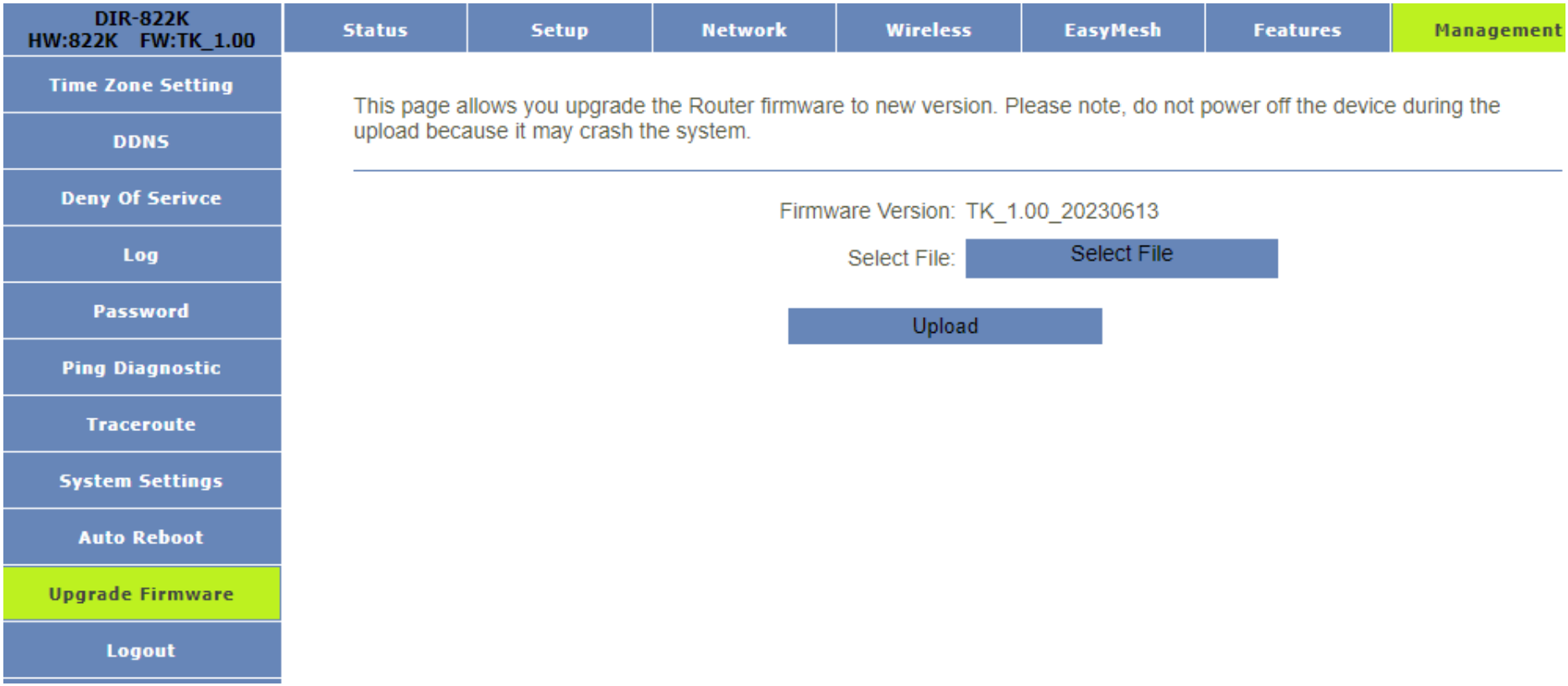


Upgrade Firmware

Here you can update the Routers firmware, by downloading and selecting the correct firmware file.

Firmware Version: this will display the current Firmware version of the device.
Select file: Click here to browse your local PC/Laptop for the downloaded firmware file.
Upload: Click this button to start the firmware update process.

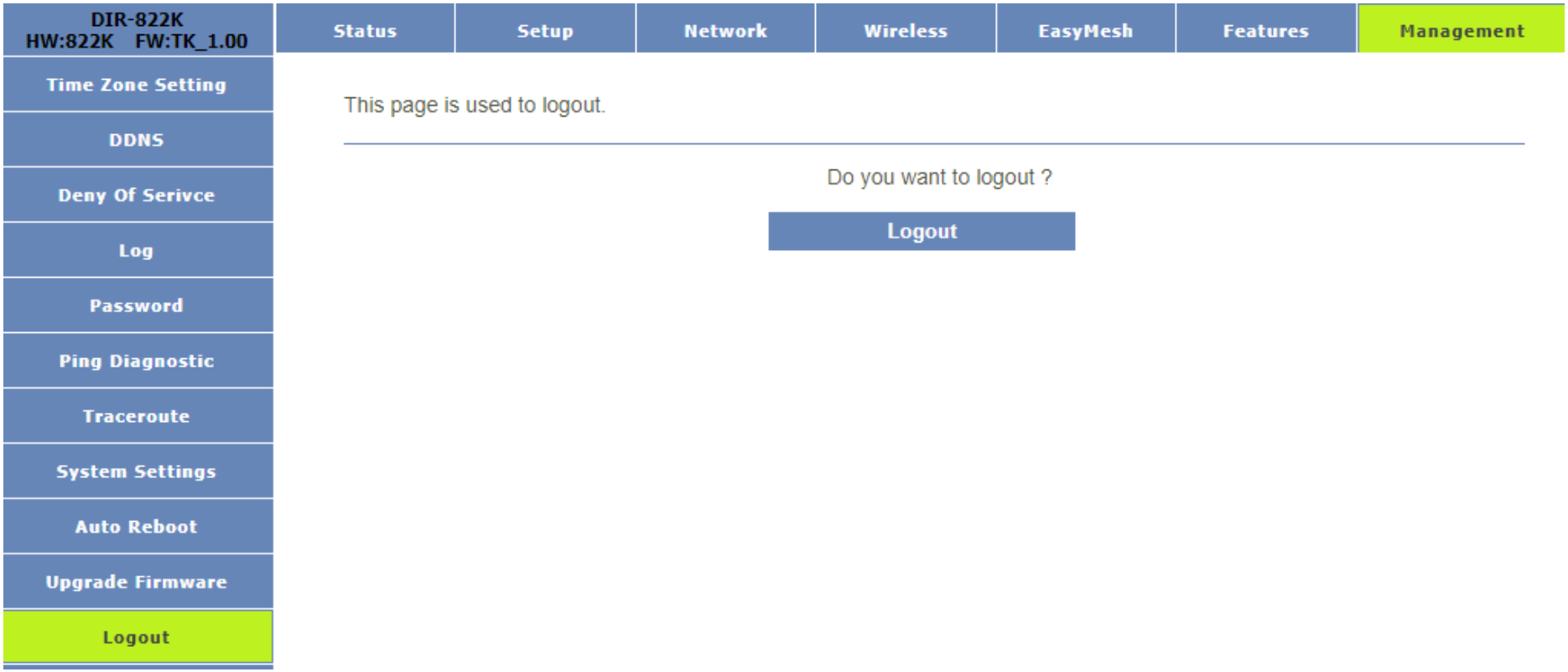
(It is recommended to never do a firmware upgrade over Wi-Fi but to rather utilize an Ethernet cable to ensure update stability)



Logout

Here you can safely and manually logout of your device after changing any settings or parameters.

Logout: Click this button to Exit the Web-Management page of the Router.

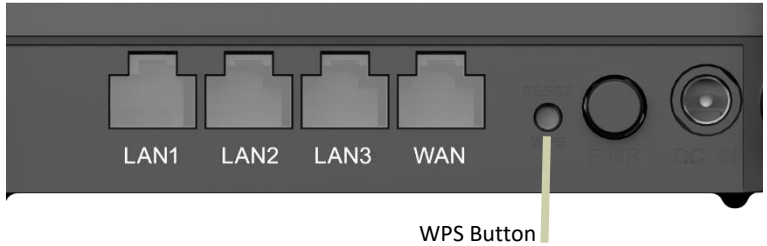


Connect a Wireless Client to your Router

WPS Button

The easiest way to connect your wireless devices to the router is with WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DIR-822K router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the WPS button on the DIR-822K for about 1 second. The WPS LED on the front will start to blink.



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

Step 3 - Allow up to 1 minute for your connection to be configured. Once the WPS LED stops blinking, you will be connected and your wireless connection will be encrypted with WPA2.

Windows® 10

When connecting to the DIR-822K wirelessly for the first time, you will need to input the wireless network name (SSID) and Wi-Fi password (security key) of the device you are connecting to. If your product has a Wi-Fi configuration card, you can find the default network name and Wi-Fi password here. Otherwise refer to the product label for the default Wi-Fi network SSID and password, or enter the Wi-Fi credentials set during the product configuration.

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

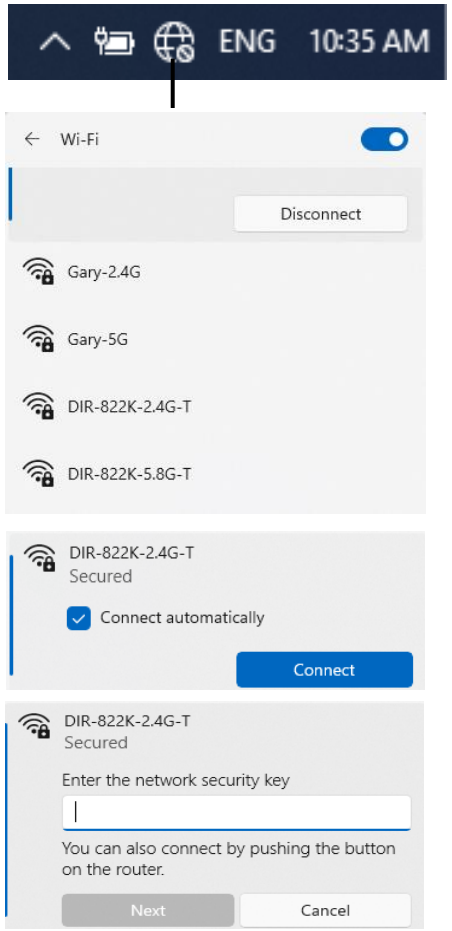
2. Clicking on this icon will display a list of wireless networks which are within range of your computer. Select the desired network by clicking on the SSID.

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

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

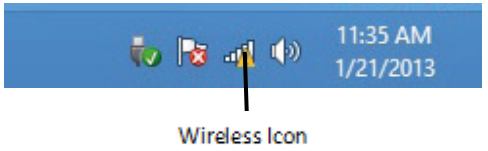
5. You will then be prompted to enter the Wi-Fi password (network security key) for the wireless network. Enter the password into the box and click **Next** to connect to the network. Your computer will now automatically connect to this wireless network when it is detected.

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



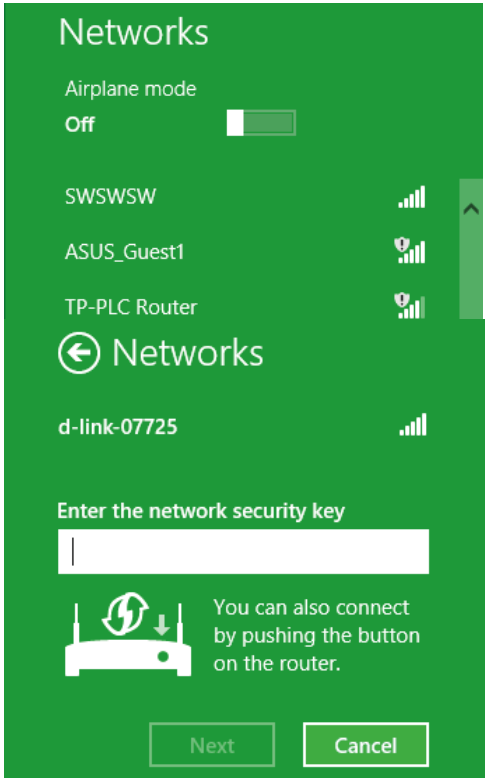
Windows® 8

It is recommended that you enable wireless security (WPA/WPA2/WPA3) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.



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

2. Clicking on this icon will display a list of wireless networks that are within connecting proximity of your computer. Select the desired network by clicking on the network name.



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

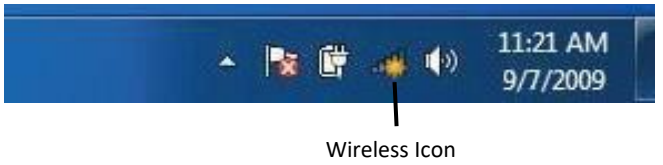
4. If you wish to use Wi-Fi Protected Setup (WPS) to connect to the router, you can also press the WPS button on your router during this step to enable the WPS function.

5. When you have established a successful connection to a wireless network, the word **Connected** will appear next to the name of the network to which you are connected to.

Windows® 7

It is recommended that you enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

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



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

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

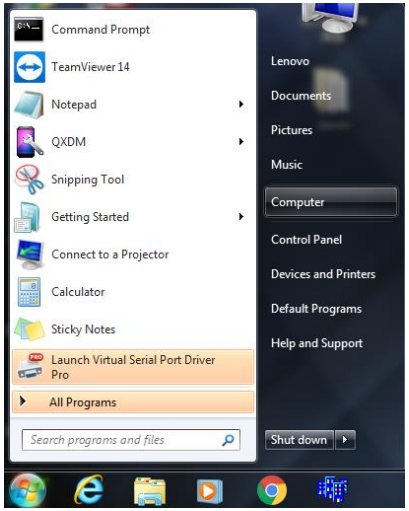
If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.

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

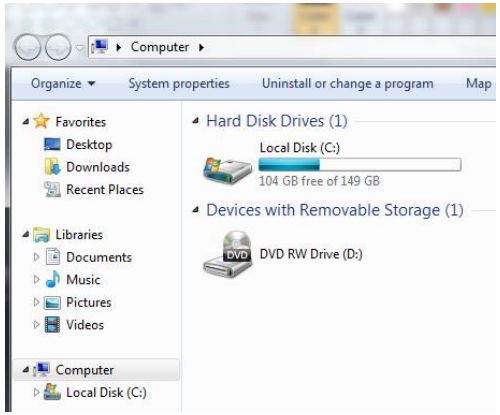
WPS

The WPS feature of the DIR-822K can be configured using Windows 7.
Carry out the following steps to use Windows 7 to configure the WPS feature:

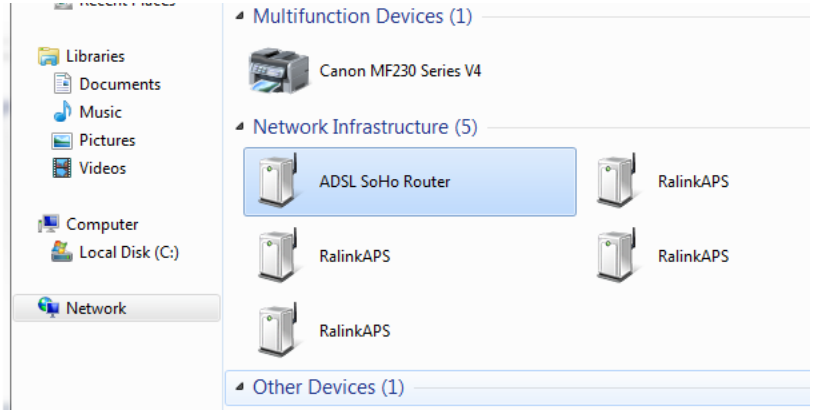
1. Click the **Start** button and select **Computer** from the Start menu.



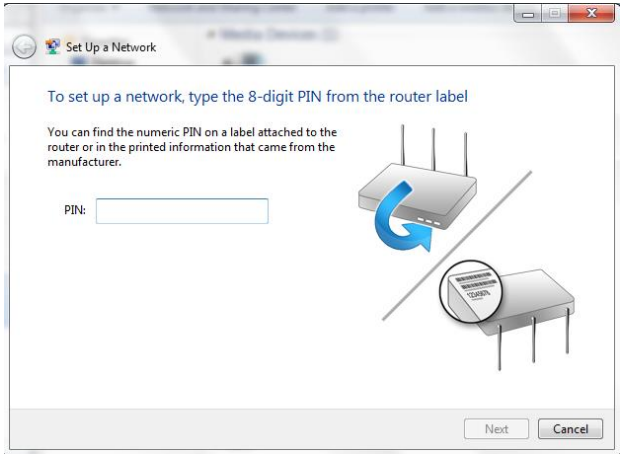
2. Click **Network** on the left side.



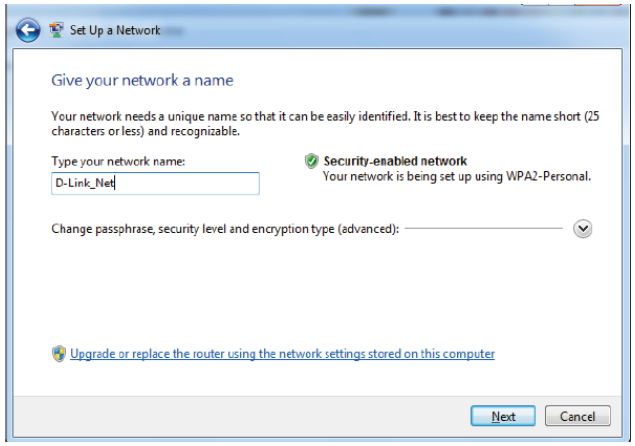
3. Double-click the DIR-822K (Will be displayed as RAlinkAPS).



4. Input the WPS PIN number (on the router label) in the **Setup** > **Wireless Setup** menu in the Router's Web UI) and click **Next**.

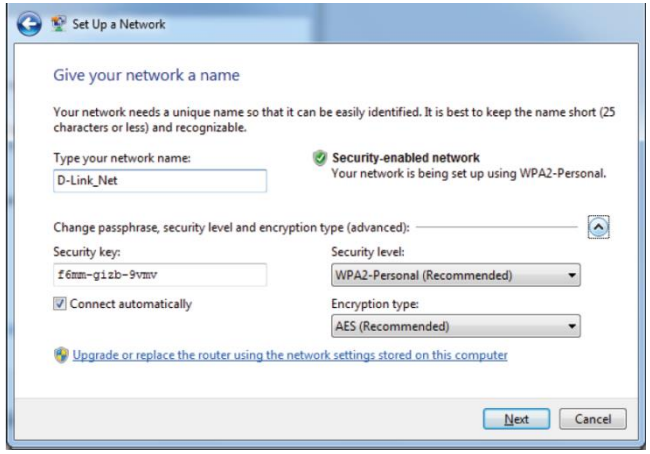


5. Type a name to identify the network.



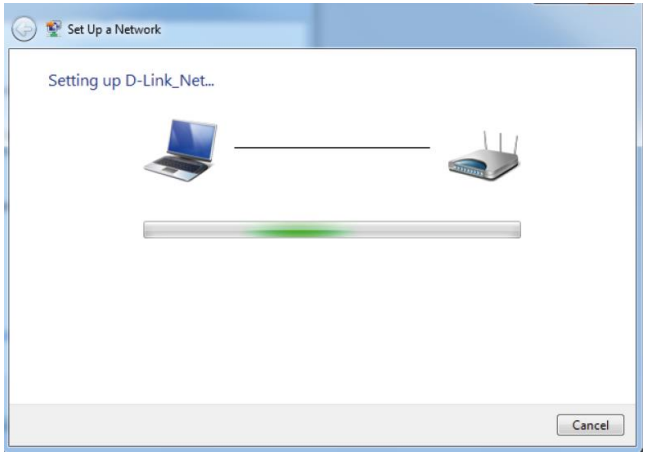
6. To configure advanced settings, click the Arrow icon.

Click **Next** to continue.



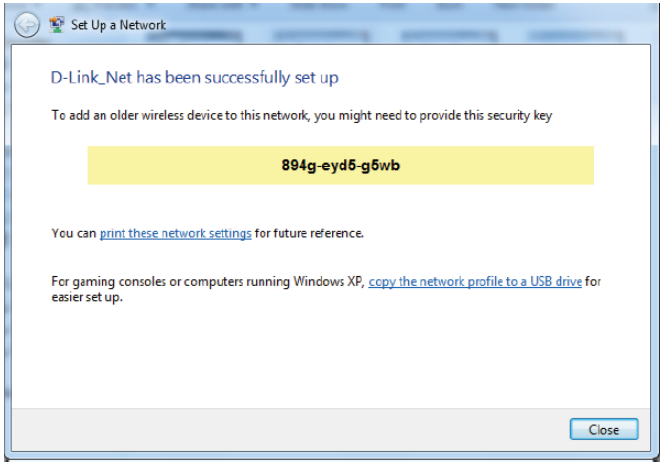
7. The following window appears while the DIR-822K is being configured.

Wait for the configuration to complete.



8. The following window informs you that WPS on the DIR-822K has been set up successfully.

Make a note of the security key as you may need to provide this security key if adding an older wireless device to the network in the future.



9. Click **Close** to complete WPS setup.

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-822K. Read the following descriptions if you are having problems. The examples below are illustrated in WindowsR 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 (**10.0.0.2** for example), make sure you are not connected to a website, you don't 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 ExplorerR 10 or higher
  - Microsoft EDGE Browser 20 or higher
  - Mozilla Firefox 11 or higher
  - Google™ Chrome 17 or higher
  - Apple Safari 5 or higher
- Verify physical connectivity by checking for solid LAN lights on the device. If you do not get a solid LAN light, try using a different cable, or connect to a different port on the device. 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 WindowsR 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?

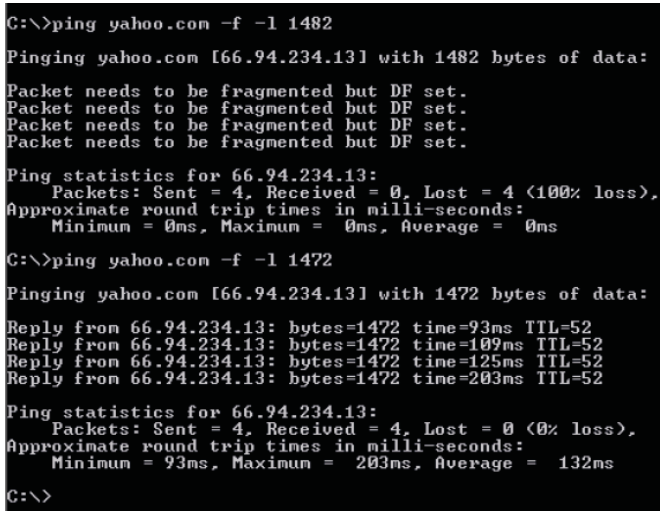
If you forgot your password, you must reset your router. This process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, press and hold the the rest button down for 20-25 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 **10.0.0.2**. When logging in, the default username is admin and the default password it admin.

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** (WindowsR NT, 2000, XP, VistaR, 7, 8.x, and 10 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**

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:

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

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business, or public access wireless networks. Strictly adhering to the IEEE standard, the D-Link wireless family of products will allow you to access the data you want, when, and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

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

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards. Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A wireless router is a device used to provide this link.

What is Wireless?

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

Why D-Link Wireless?

D-Link is the worldwide leader and award-winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

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

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point the signal can travel up to 100m. With an outdoor access point the signal can reach out up to 15km to serve places like manufacturing plants, industrial locations, university and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away.

Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power. This makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

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

Home Uses/Benefits

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

Small Office and Home Office Uses/Benefits

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

Where is wireless used?

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

Using a D-Link USB adapter with your laptop, you can access the hotspot to connect to the Internet from remote locations like: airports, hotels, coffee shops, libraries, restaurants, and convention centres.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your router or access point

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

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

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-hoc** – Directly connecting to another computer for peer-to-peer communication using wireless network adapters on each computer, such as two or more DIR-822K wireless network USB adapters.

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

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

Networking Basics

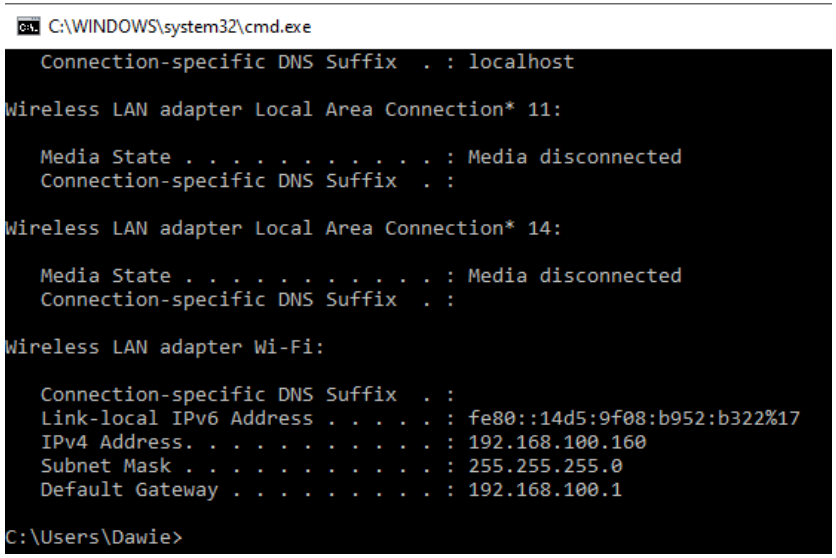
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start** > **Run**. In the run box type ***cmd*** and click **OK.** (WindowsR 7/VistaR 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

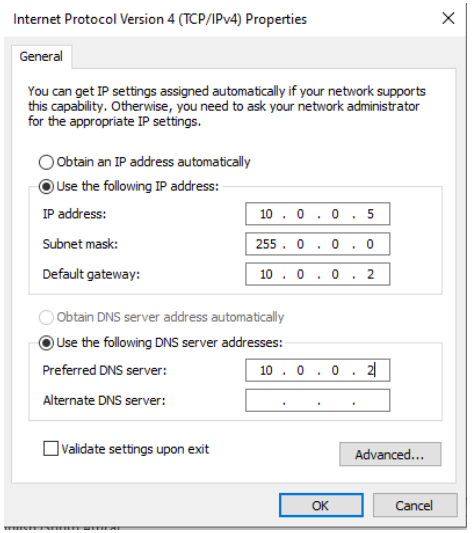
Windows® 7- Click on Start > Control Panel > Network and Internet > Network and Sharing Center > Change Adaptor Options
Windows® 8,10 - Click on Start > Search for Control Panel > Network and Internet > Network and Sharing Center > Change adaptor settings.

Step 2

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

Step 3

Highlight **Internet Protocol version 4 (TCP/IP)** and click **Properties.**



Step 4

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

Example: If the router´s LAN IP address is 10.0.0.2, make your IP address 10.0.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set the Default Gateway the same as the LAN IP address of your router (I.E. 10.0.0.2).

Set Primary DNS the same as the LAN IP address of your router (10.0.0.2). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

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

Wireless Security

This section will show you the different levels of encryption you can use to help protect your data from intruders. The DIR-822K offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA2-PSK (Pre-Shared Key)
- WPA (Wi-Fi Protected Access)
- WPA-PSK (Pre-Shared Key)

What is WPA?

WPA (Wi-Fi Protected Access), is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more robust public-key encryption system to ensure that only authorized network users can access the network.

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

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

Technical Specifications

Device Interfaces

- 3 x RJ-45 10/100 Ethernet LAN ports
- 1 x RJ-45 10/100 Ethernet WAN port
- 2.4 GHz and 5 GHz wireless for 802.11 a/b/g/n/ac

Antenna Types

- 4x external dual band fixed antennas

Standards

- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n
- IEEE 802.11ac
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3az
- IEEE 802.3x
- IEEE 802.11e
- IEEE 802.1p

Wi-Fi Encryption

- WPA™ - Personal/Enterprise
- WPA2™ - Personal/Enterprise
- WPA3™ Personal/Enterprise
- Wi-Fi Protected Setup (WPS) PIN/PBC

Power

- Input: 100 to 240 V AC, 50/60 Hz
- Output: 12 V DC, 1 A

Operating Temperature

- 0 to 40 °C (32 to 104 °F)

Storage Temperature

- -20 to 80 °C (-4 to 176 °F)

Operating Humidity

- 5% to 85% maximum (non-condensing)

Certifications

- CE

Dimensions

- 230 x 150 x 35 mm (8.26 x 5.91 x 1.46 in)

Weight

- 227g (1.05 lbs)

Regulatory Information

CE EMI Class A Warning

This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

CE

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