Version 1.00 |31/07/2018

User Manual

4G LTE Router

DWR-921

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.

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.

FCC Regulations

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

Changes or modifications not expressly approved by the party responsible for compliance could void the user ‘s authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

Table of Content

Product Overview

Package Contents

- D-Link DWR-921 4G LTE Router
- Power Adapter
- QIG and Warranty Documentations
- Cat5e Ethernet Cable

Note: Using a power supply with a different voltage rating than the one included with the DWR-921 will cause damage and void the warranty for this product.

System Requirements

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

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

Introduction

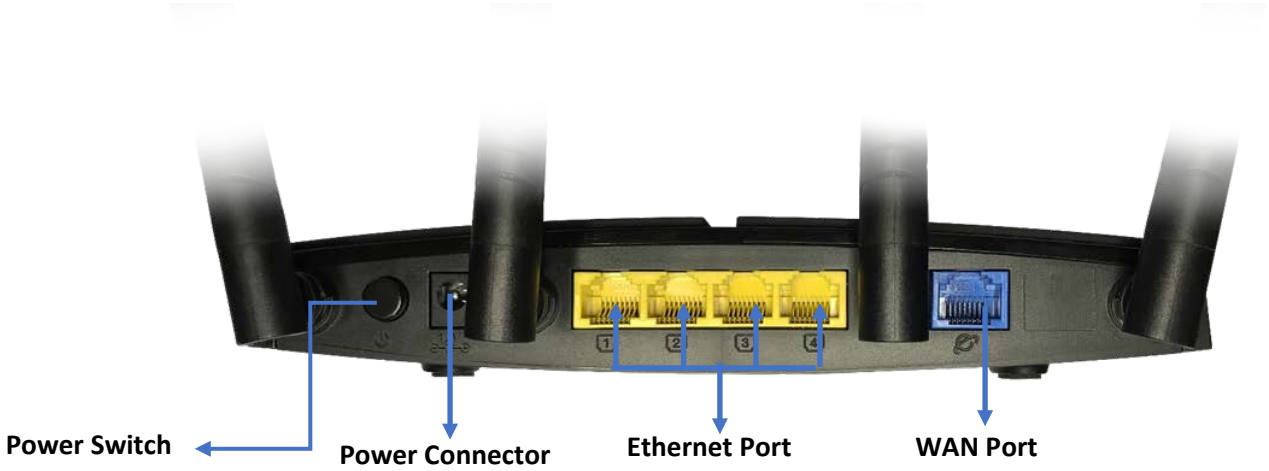
The D-Link 4G LTE Router allows users to access worldwide mobile broadband networks and share them with a number of wired and wireless devices. Once connected, users can transfer data, stream media, and send SMS messages. Simply insert your UMTS/HSUPA SIM card and share your 3G/4G Internet connection through a secure 802.11n wireless network or using any of the four 10/100 Ethernet ports.

The DWR-921 keeps your wireless network safe with WPA/WPA2 wireless encryption, preventing unauthorized users from accessing your network. The DWR-921 utilizes dual-active firewalls (SPI and NAT) to prevent potential attacks across the Internet and includes MAC address filtering to control which clients can access your network, and what content they can access.

The DWR-921 4G LTE Router can be installed quickly and easily almost anywhere. This router is great for situations where an impromptu wireless network is required, or wherever conventional network access is unavailable. The DWR-921 can even be installed in buses, trains, or boats, allowing passengers to access the Internet while commuting.

Hardware Overview

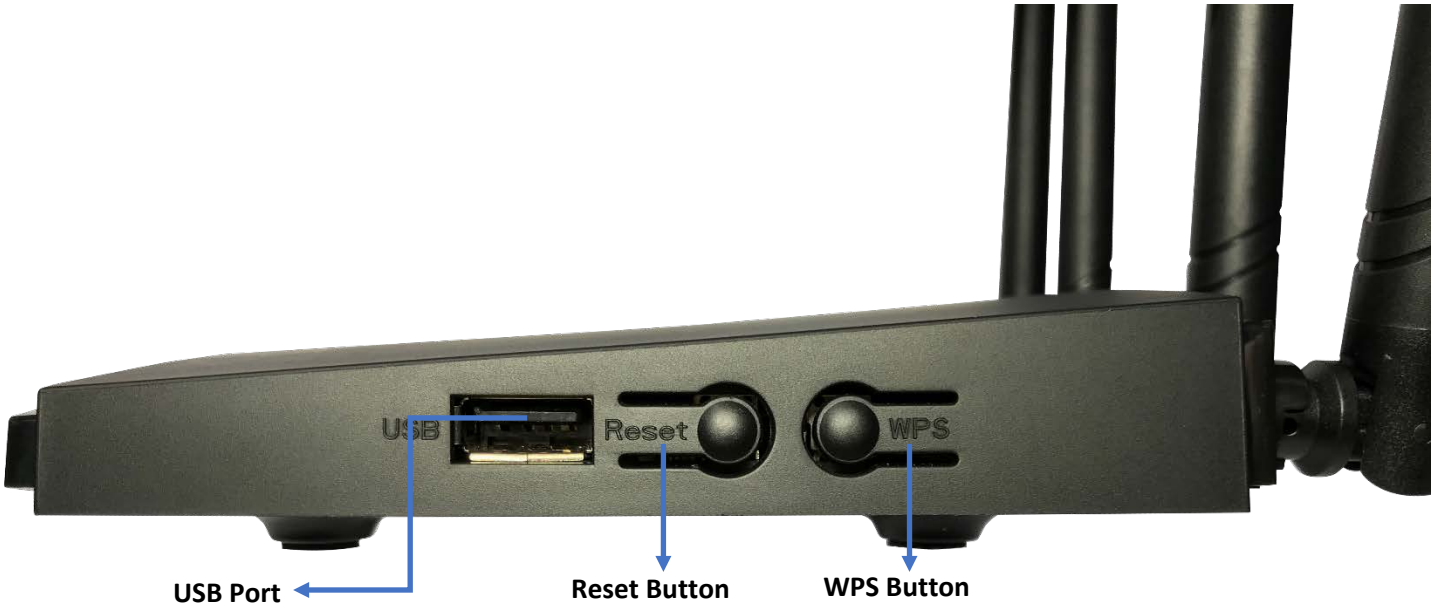
Rear Panel



Port	Function
LAN Ethernet Ports	For connection to a network device such as a desktop or notebook computer.
WAN Ethernet Port	For connection to a DSL/Cable modem or router
Power Connector	Connects to the included power adapter.
Power Switch	Turns the device on or off.

Hardware Overview

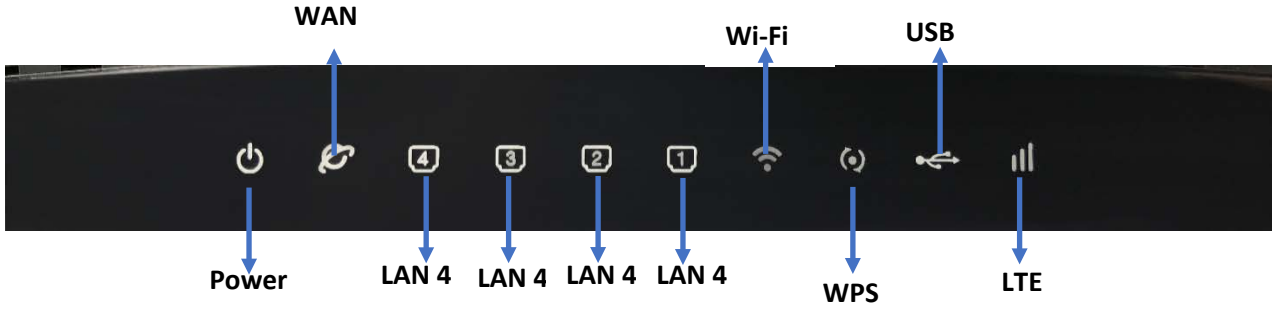
Side Panel



	Function
USB Port	Connect a USB Drive to share Media across the Network
Reset	Press and hold for 10 seconds while device is powered ON to reset device back to factory default settings
WPS	Wireless Protected Setup. Connect Devices using WPS functionality

Hardware Overview

Front Panel



LED	Function
Power	Solid Blue: Power is ON
WAN	Solid Blue: Cable is Connected but no Data transmitted Flashing Blue: Data is being transmitted
LAN 1-4	Solid Blue: Ethernet connection has been established Flashing Blue: Data is being transmitted
Wi-Fi	Solid Blue: Wi-Fi connection is ON Flashing Blue: Data is transmitted over Wi-Fi connection OFF: Wi-Fi function is switched OFF
WPS	Solid Blue: Connection has been established Flashing Blue: Device is looking for other WPS enabled devices OFF: Function disabled or Inactive
USB	Solid Blue: USB connected OFF: No USB drive Connected
LTE	Solid Blue: Mobile connection Established but no Data transmitted OFF: Mobile connection not Established or SIM not attached

Installation

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

Connect to Your Network

1. Ensure that your DWR-921 4G LTE Router is disconnected and powered off.
2. Insert a standard (U)SIM card into the SIM card slot on the bottom of the router. The gold contacts should face downwards.

Caution: Always unplug/power down the router before installing or removing the SIM card. Never insert or remove the SIM card while the router is in use.

3. Insert your Internet/WAN network cable into the WAN port on the back of the router (if applicable).

Note: The 3G/4G connection can also be used as a backup WAN. Once a backup is configured, the router will automatically use 3G for the Internet connection if the Ethernet WAN is not available.

4. Insert the Ethernet cable into the LAN Port 1 on the back panel of the DWR-921 4G LTE Router and an available Ethernet port on the network adapter in the computer you will use to configure the router.

Note: The DWR-921 4G LTE Router LAN Ports are Auto-MDI/MDIX, so both patch and crossover Ethernet cables can be used.

5. Connect the power adapter to the power connecter on the back panel of your DWR-921 4G LTE Router. Plug the other end of the power adapter into a wall outlet or power strip and turn the device on.
    a. The Power LED will light up to indicate that power has been supplied to the router.
    b. After a few moments, if the router is running correctly the following LED's should be on: Power, WAN (when connected), LAN 1-4 (if connected), Wi-Fi, LTE (when mobile sim is attached).

Wireless Installation Considerations

The DWR-921 can be accessed using a wireless connection from anywhere within the operating range of your wireless network. Keep in mind that the quantity, thickness, and location of walls, ceilings, or other objects that the wireless signals must pass through may limit the range of the wireless signal. Ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or office. The key to maximizing the wireless range is to follow these basic guidelines:

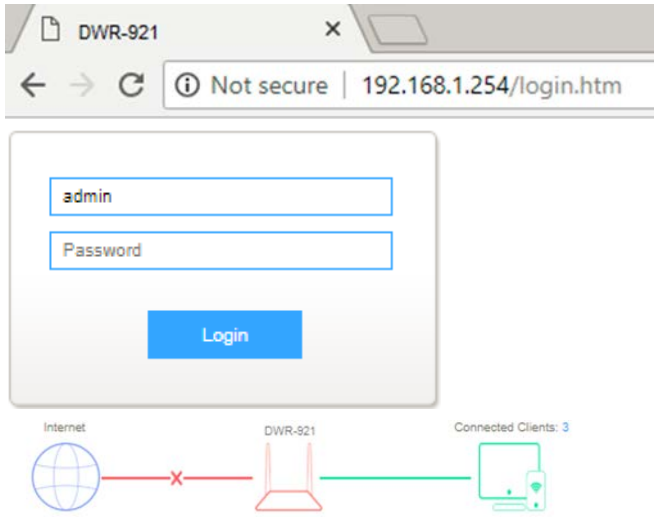
1. Minimize the number of walls and ceilings between the router and other network devices. Each wall or ceiling can reduce your adapter's range from 3 to 90 feet (1 to 30 meters).
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (0.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it can appear 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. Try to position access points, wireless routers, and computers so that the signal passes through open doorways or drywall. Materials such as glass, metal, brick, insulation, concrete, and water can affect wireless performance. Large objects such as fish tanks, mirrors, filing cabinets, metal doors, and aluminium studs may also have a negative effect on range.
4. If you are using 2.4 GHz cordless phones, make sure that the phone base is as far away from your wireless device as possible. The base transmits a signal even if the phone is not in use. In some cases, cordless phones, X-10 wireless devices, and electronic equipment such as ceiling fans, fluorescent lights, and home security systems may dramatically degrade wireless connectivity.

Configuration

This section will show you how to configure your new D-Link mobile router using the web-based configuration utility

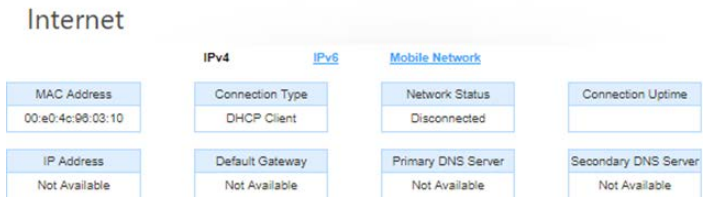
Web-based Configuration Utility

To access the configuration utility, open a web browser such as Internet Explorer and enter the IP address of the router (192.168.1.254 by default).



To login to the configuration utility, enter admin as the username and password and click on Login or press enter.

The configuration utility will open to the Home page. You can view different configuration pages by clicking on the categories at the top of the screen (Home/Settings/Features/Management), and then selecting a configuration page from the bar below the Main Menu categories.

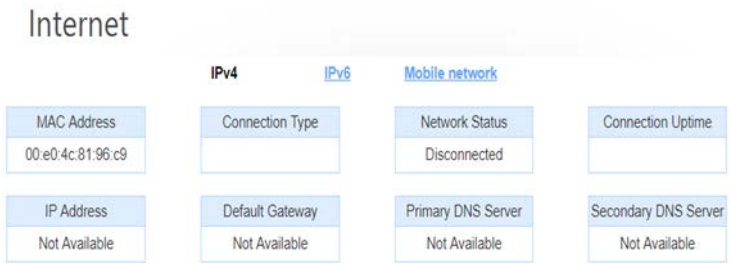


Home

The Home page allows you to view your Internet Connection info, as well as the view the connected devices.

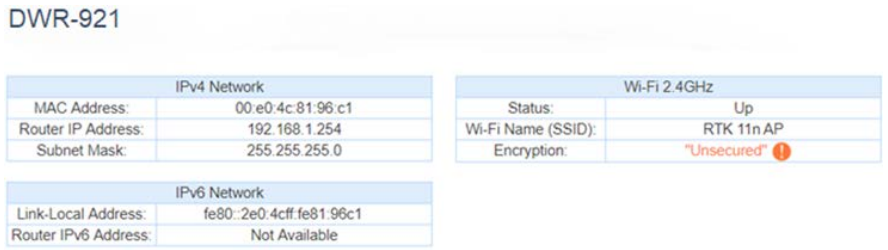
Internet

On this page, you can view information about the Internet status of the DWR-921, including MAC Address, Connection Type, Network Status, Connection Uptime, IP Address, Default Gateway, Primary DNS Server and Secondary DNS Server.



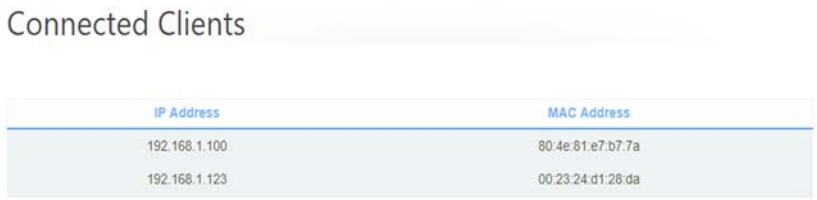
DWR-921

This wizard will guide you through a step-by-step process to configure your router to connect to the Internet.



Connected Clients

This page shows the IP addresses and host names of all the PCs in your network



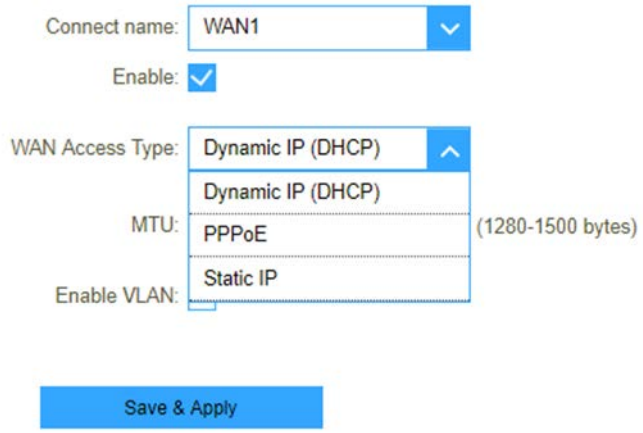
Settings

This Page allows for certain settings to be changed or modified

WAN

On this page, you can configure the parameters of the different WAN connection and view the status for this connection.

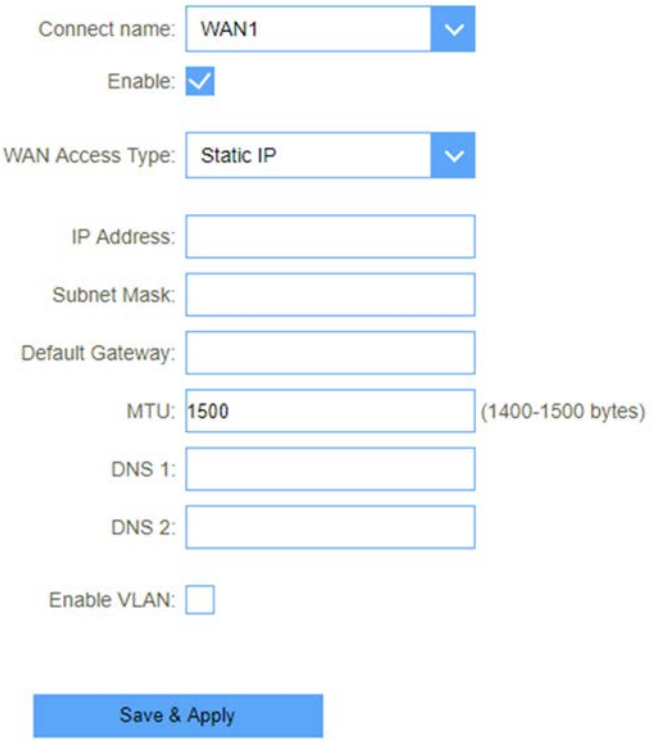
Static IP Address Connections:	Choose this option if your Internet Service Provider provided you with IP address information that has to be manually configured. See “Static IP” on page 13 for information about how to configure this type of connection.
DHCP Client (Dynamic IP Address):	Choose this if your Internet connection automatically provides you with an IP address. Most cable modems use this type of connection. See “Dynamic IP (DHCP)” on page 14 for information about how to configure this type of connection.
Username / Password Connection (PPPoE):	Choose this option if your Internet connection requires a username and password to connect. Most DSL modems use this style of connection. See “PPPoE” on page 15 for information about how to configure this type of connection.



Static IP

Choose this Internet connection if your ISP assigns you a static IP address. After modifying any settings, click Save & Apply to save your changes.

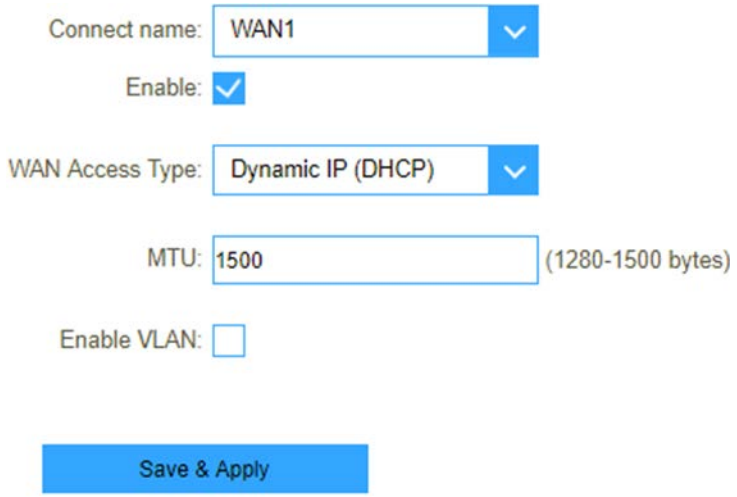
IP Address:	Enter the IP address assigned to your network connection.
Subnet Mask:	Enter the subnet mask.
Default Gateway:	Enter the default gateway.
MTU:	You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 1500.
DNS 1:	Enter the primary DNS server.
DNS 2:	Enter the secondary DNS server.
Enable VLAN:	Enter the VLAN ID value



Dynamic IP (DHCP Client)

This section will help you to obtain IP address information automatically from your ISP. Use this option if your ISP didn't provide you with IP address information and/or a username and password. After modifying any settings, click Save & Apply to save your changes.

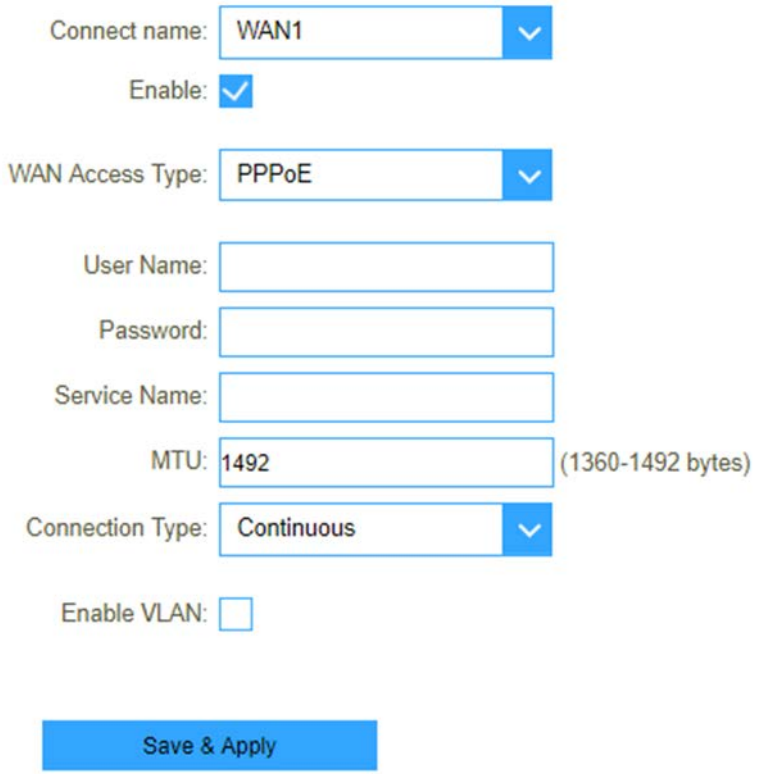
Enable:	Enable or Disable WAN connection
WAN Access Type:	Dynamic IP (DHCP)
MTU:	You may need to change the Maximum Transmission Unit (MTU) for optimal performance. The default value is 1500.
Enable VLAN:	Enable or Disable VLAN (once enable VLAN ID should be entered).



PPPoE

Choose this Internet connection if your ISP provides you with a PPPoE account. After modifying any settings, click Save Settings to save your changes.

WAN Access Type:	Select PPPoE.
Username:	Enter the Username as provided by the ISP.
Password:	Enter the Password as provided by the ISP.
Service Name:	Enter the Service Name (Default blank)
MTU:	Enter the Maximum Transmission Unit default 1492
Connection Type:	Choose between 3 types: • Continuous (default) • Connect on Demand • Manal
Enable VLAN:	Enable or Disable VLAN (If enabled enter VLAN ID).

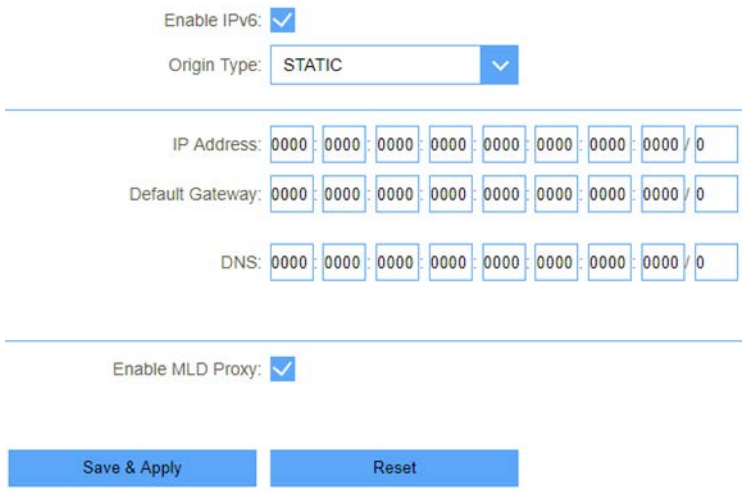


IPv6

You can config IPv6 in this page. It’s support 3 kinds of IPv6 origin types.

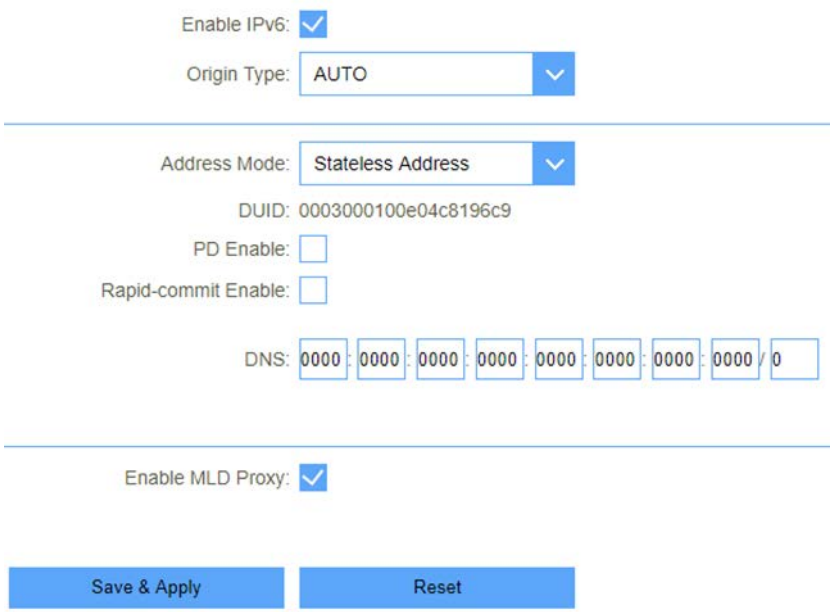
IPv6 Static

Origin Type:	Current IPv6 Mode.
IP Address:	IPv6 WAN IP address.
Default gateway:	IPv6 Default Gateway Address.
DNS:	IPv6 DNS server Address.
Enable MLD Proxy:	Enable or Disable MLD Proxy (Multicast Listener Discovery).



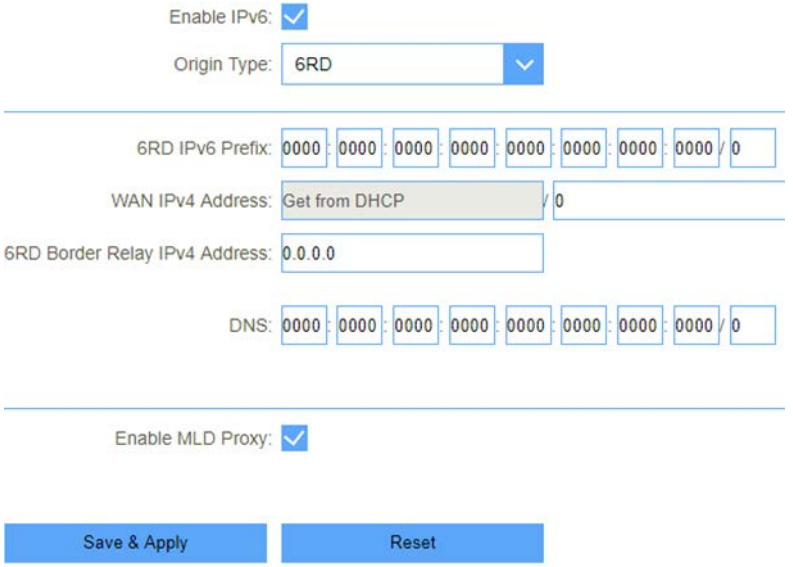
IPv6 Auto

Origin Type:	Current IPv6 Mode is Auto.
Address Mode:	Choose between two options: • Stateless Address. • Stateful Address.
PD Enabled:	Enable or Disable IPv6 WAN prefix delegation.
Rapid-commit Enable:	Enable Rapid Commit Switch. This allows for faster configuration between clients.
DNS:	IPv6 DNS Server Address.
Enabled MLD Proxy:	Enable or Disable MLD proxy (Multicast Listener Discovery).



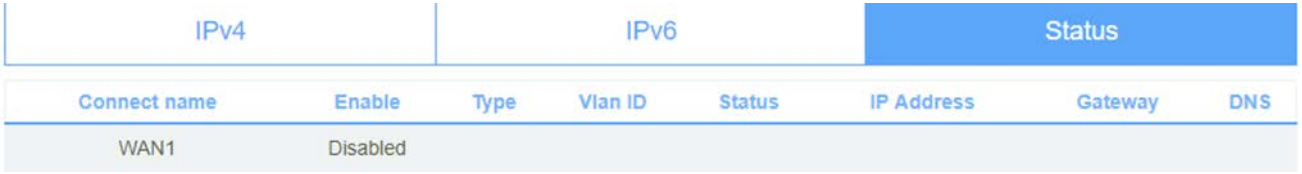
IPv6 6RD

Origin Type:	Current IPv6 mode is 6RD.
6RD IPv6 Prefix:	IPv6 WAN prefix delegation.
WAN IPv4 Address:	IPv4 WAN Address.
6RD Border Relay IPv4 Address:	Border IPv4 IP Address.
DNS:	IPv6 DNS server Address.
Enable MLD Proxy:	Enable or Disable MLD Proxy (Multicast Listener Discovery).



Status

On this page you will be able to view the Status of the Different WAN connections created as on page 12.



Mobile Network

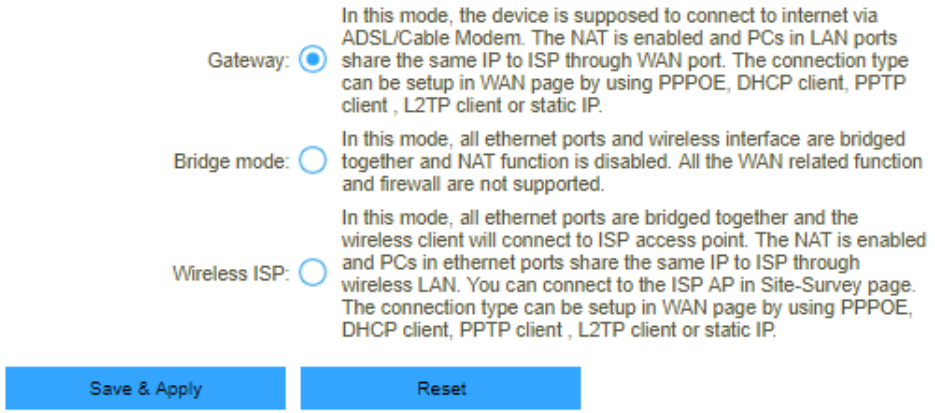
This page allows for settings to be changed on how your router connect to the Mobile Network Services.

Username:	Enter the Username as required by your ISP.
Password:	Enter the Password as required by your ISP.
APN:	Enter the APN for your Mobile Operator.
Dial Number:	Enter the Dial number for your Mobile Operator.
Aut Method:	Choose between PAP and CHAP. Default is Auto
Manual APN:	Choose this option to use the APN entered. If not enabled Router will obtain required information form Mobile operator.

Operation Mode

Choose the mode in which the router will mainly be used.

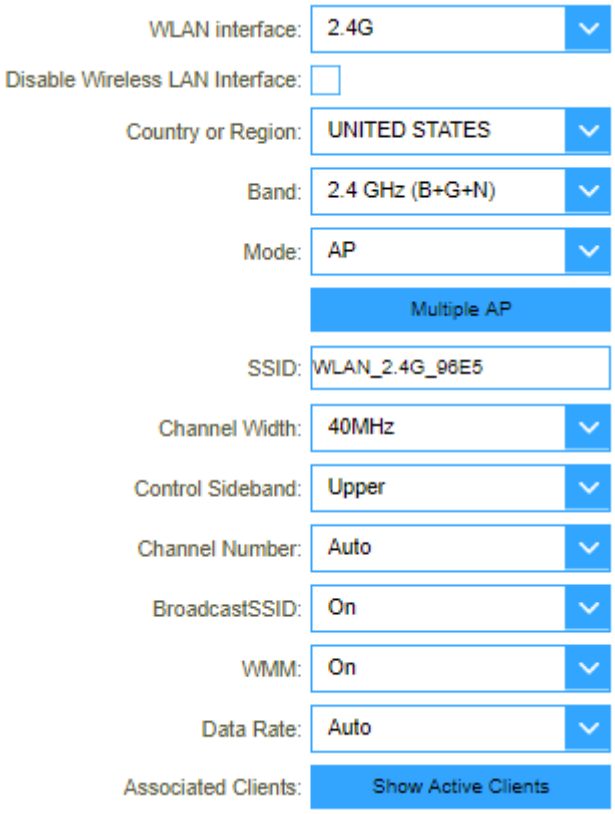
Gateway:	In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.
Bridge Mode:	In this mode, all ethernet ports and wireless interface are bridged together and NAT function is disabled. All the WAN related function and firewall are not supported
Wireless ISP:	In this mode, all ethernet ports are bridged together and the wireless client will connect to ISP access point. The NAT is enabled and PCs in ethernet ports share the same IP to ISP through wireless LAN. You can connect to the ISP AP in Site-Survey page. The connection type can be setup in WAN page by using PPPOE, DHCP client, PPTP client, L2TP client or static IP.



Wi-Fi Settings

This section will help you to manually configure the wireless settings of your router. Please note that changes made in this section may also need to be duplicated on your wireless devices and clients. The Wireless Settings page allows you to configure how your router connects to the Internet. You can also set up a wireless connection to a device automatically or configure your router automatically through Windows by clicking the Wi-Fi Protected Setup button. This is described in "Wi-Fi Protected Setup (WPS) page.

WLAN Interface:	Select the WLAN partition to modify the settings (some models support dual band).
Disable Wireless LAN Interface:	Tick this box if you do not want the selected WLAN partition to be active.
Band:	Select the Wireless Mode (802.11b/g/n) or mixed which includes all the modes. Mixed is by default selected as this provide more compatibility to older Wireless devices.
Mode:	Select the operation mode for the Wi-Fi. Device supports AP, Client, WDS and AP+WDS mode. Default is AP so all devices can Connect.
MultipleAP:	You can configure multiple SSID's when this option is clicked.
Network Type:	You can change the WLAN type (only available on Client mode).
SSID:	Set a name for the Wireless. This is to identify your network among neighbouring wireless devices.
Channel Width:	Select between 20MHz or 40MHz. If using 802.11n select 20/40MHz.
Control Sideband:	Only available on 802.11n mode and when 40MHz is selected.
Channel Number:	For optimal Wireless throughput and performance, it is recommended to select non-interferential channels. Auto will allow the device to automatically switch between channels when interference is detected. (Channel 1, 6, and 11 is non-overlapped channels).
Broadcast SSID:	This option allows you to choose whether you want to hide your wireless name or broadcast your wireless name. If the invisible

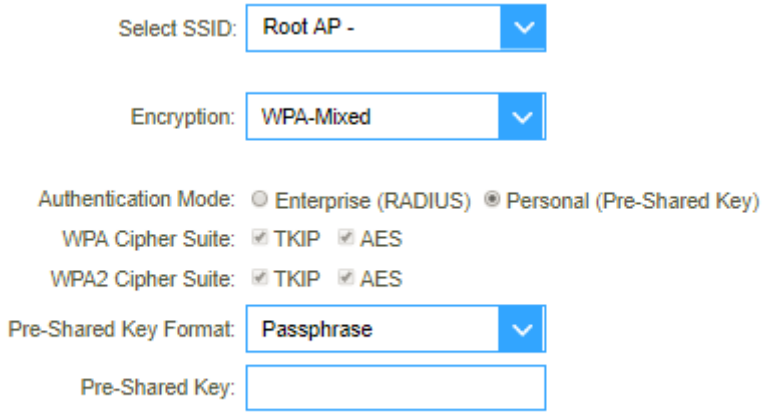


	option is selected, you will need to manually configure your devices to see this network.
WMM:	If this option is selected, it will provide limited Quality of Service (QoS) features to Wireless devices. WMM prioritise traffic according to four categories: Voice, Video, Best effort and background applications.
Associated Clients:	This option will show you all the connected devices to the wireless

Wireless Security Mode

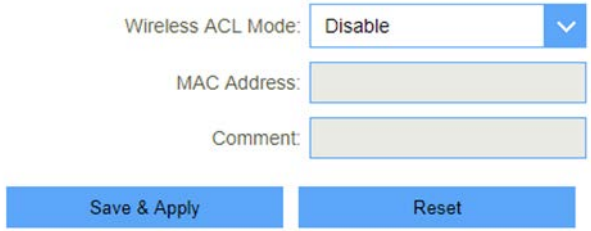
You can choose from several different wireless security modes. After selecting a mode, the settings for that mode will appear. After modifying any settings, click Save & Apply to save your changes.

SSID:	Select the SSID to configure the security settings.
Encryption:	You can choose from 4 different security modes: • Disable: No security will be used. This setting is not recommended. • WEP: WEP encryption will be used. This setting is only recommended if your wireless devices do not support WPA or WPA2. • WPA2: WPA2 is the best encryption for Wireless devices. • WPA-Mixed: WPA-Mixed will Allow older Wireless devices to connect using password which does not support the WPA2 encryption
Authentication Mode:	Choose between Enterprise and Personal. Enterprise requires a server for Authentication whereas Personal a custom password can be created.
WPA Cipher Suite:	Select between TKIP or AES.
Management Frame Protection:	Protects against deauthentication packets from malicious software but may reduce Wi-Fi performance.
Pre-Shared key Format:	Choose between HEX and Passphrase.
Pre-Shared Key:	Enter the desired Wi-Fi password. (Between 8-32 Characters).



ACL

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.



Wireless ACL Mode: A selection of Disable, Allow and Deny is available:

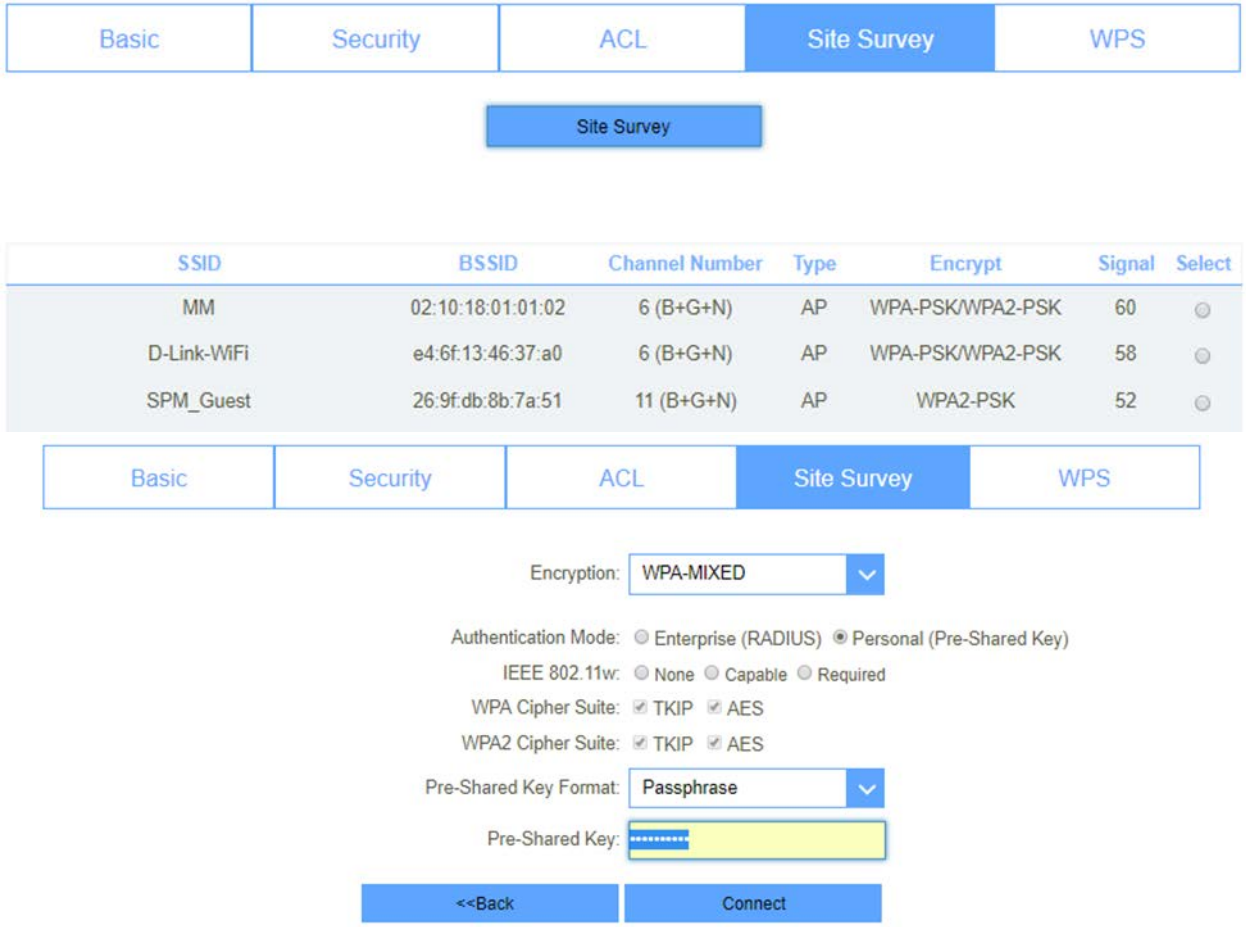
- Disabled - All Wireless devices can connect to the Wi-Fi.
- Allow - Only listed Mac Address will be able to connect to the Wi-Fi.
- Deny - Only the listed devices will be denied from connecting to the Wi-Fi.

MAC Address: Enter the Wireless device Mac Address.

Comment: Enter a description for the device to easily identify the rule.

Site Survey

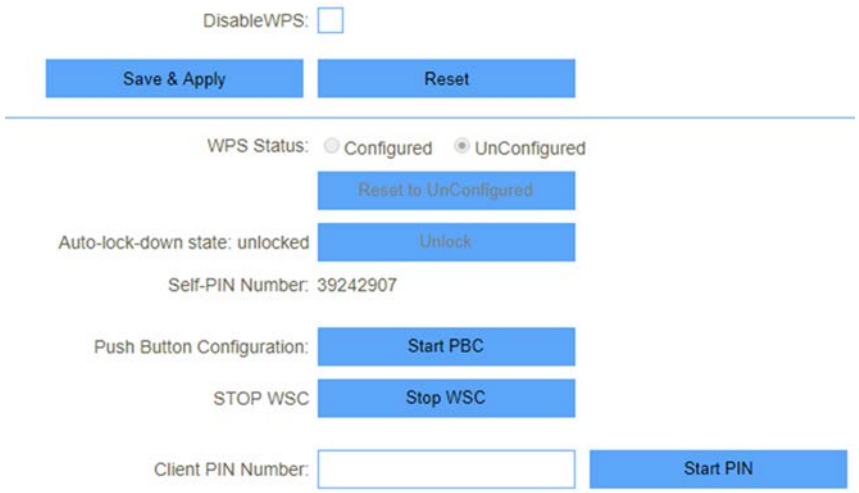
This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled. This is only available when router is set to Client under Basic Wireless. You can choose the network you would like to connect to and then continue with the next button on the bottom of the page. This will take you to the next page where you can enter the Wireless Password which will allow you to connect to the select Wireless network.



Wi-Fi Protected Setup (WPS)

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

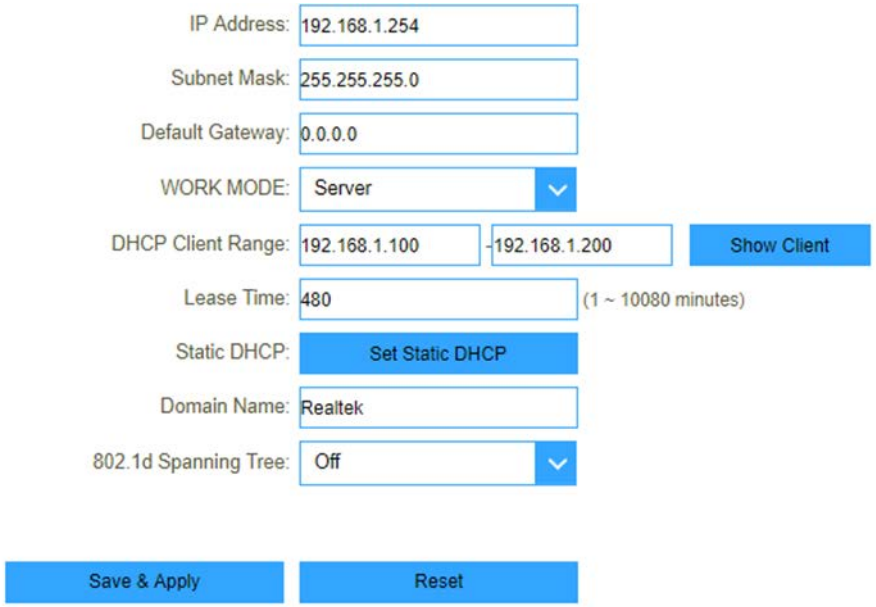
Disable WPS:	Check the DisableWPS box if you do not wish to use this feature.
WPS Status:	If this is set to CONFIGURED, the router will be marked as “already configured” to computers that try to use WPS configuration, such as Windows 7’s Connect to a network wizard. You can click the Reset to Unconfigured button to change the status to UNCONFIGURED to allow for WPS configuration of the router.
Auto-lock-down-state:	Enable this option to prevent clients from connecting to the router using the PIN method. If this option is enabled, clients must use the push-button method to connect.
Self-PIN Number:	This is the number generated by the router for when you use WPS function. This PIN will need to be used when connecting devices using WPS mode and PIN is required by other devices.
Push Button Configuration:	Click this option to start the WPS communication to allow for nearby device to connect to the router.
STOP WSC:	Click on this option to stop the Wi-Fi Simple Config (Mostly used on Linux based operating systems).
Client PIN Number:	You can enter a custom pin code for device to connect which is using WPS setup.



LAN

This section will help you to change the internal network settings of your router and to configure the DHCP Server settings. After modifying any settings, click Save & Apply to save your changes.

IPv4

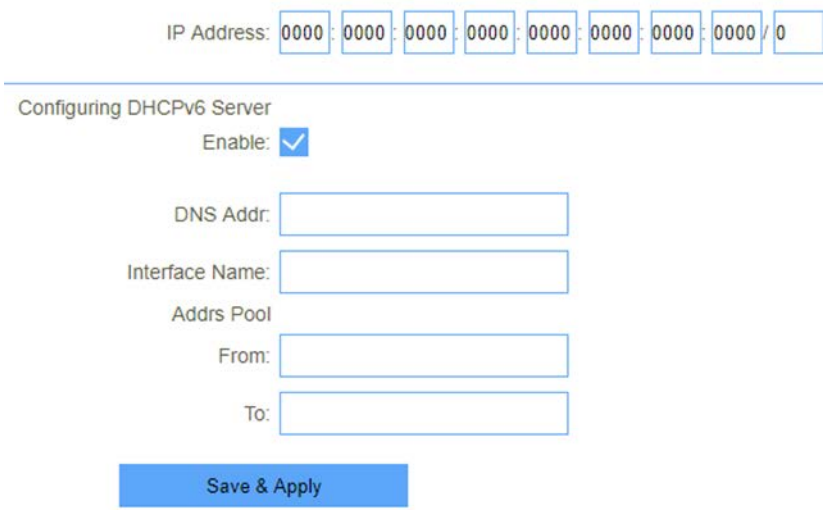


IP Address:	Enter the IP address you want to use for the router. The default IP address is 192.168.1.254.
Subnet Mask:	Enter the Subnet Mask of the router. The default subnet mask is 255.255.255.0.
Gateway:	Enter default gateway address.
Work Mode:	You can select between three different modes: • Server – The router is default set to Server. This will provide IP addresses to connected devices. • Off – Devices connected to the router will have to manually assign an IP address. • Client – The router will receive IP address from connect DHCP server. (Used when Client mode is selected under Wi-Fi).
DHCP IP Client Range:	Enter the range of IPs for the DHCP server to use to assign IP addresses to devices on your network.
Lease Time:	Enter the lease time for IP address assignments.
Static DHCP:	Click this option to assign an IP address with a Mac Address.
Domain Name:	Enter the name of this router or the Domain of your network.
802.1d Spanning Tree:	Enable or Disable spanning Tree. This will switch off the port if a Loop is detected. (Might slow network down if enabled).

IPv6

This page will allow for IPv6 configuration.

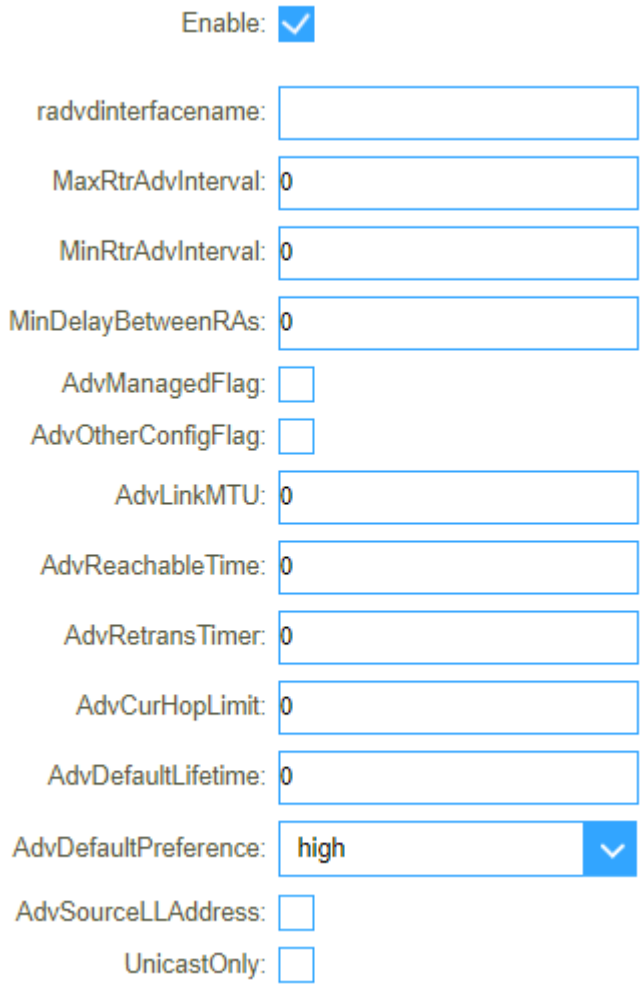
IP Address:	This will be the router's IPv6 address.
DNS Address:	Enter the router LAN IPv6 DNS address.
Interface Name:	If this option is selected, the router will serve as an IPv6 DHCP server and will assign IP's automatically do devices connected to the router.
Address Pool:	Enter the address where the IPv6 server should start to hand out IP addresses as well the last one.



RADVD

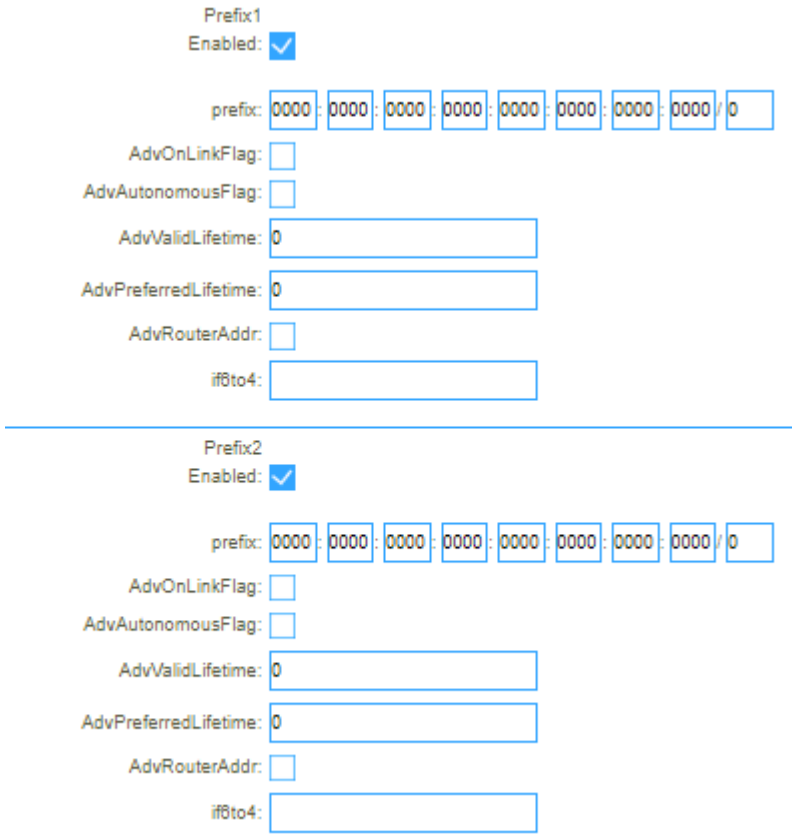
The Router Advertisement Daemon is an open-source software product that implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes using the Neighbour Discovery Protocol.

radvdinterfacename:	Enter the interface Name.
MaxRtrAdvInterval:	Enter the max retry advertisement interval.
MinRtrAdvInterval:	Enter the min retry advertisement interval.
MinDelayBetweenRAs:	Enter the min delay between router advertisement.
AdvManagedFlag:	Enable or disable the advertisement managed flag.
AdvOtherConfigFlag:	Enable or disable the advertisement other config flag.
AdvLinkMTU:	Enter the min retry advertisement interval.
AdvReachableTime:	Enter the advertisement reachable time
AdvRetransTimer:	Enter the advertisement retrains timer.
AdvCurHopLimit:	Enter the advertisement current hop limit.
AdvDefaultLifetime:	Enter the advertisement default life time.
AdvDefaultPreference:	Select from “high”, “medium” or “low” for the advertisement default preference.
AdvSourceLLAddress:	Enable or disable advertisement source link.
UnicastOnly:	Enable or disable unicast only.



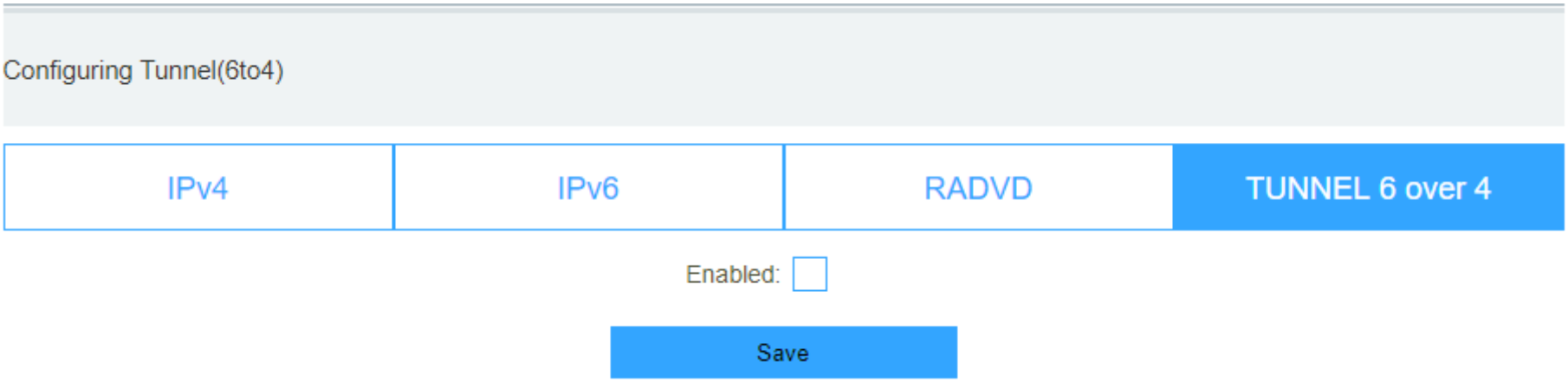
Prefix1 Enabled:	Enable or disable prefix.

prefix:	Enter the prefix and prefix length
AdvOnLinkFlag:	Enable or disable advertisement on link flag.
AdvAutonomousFlag:	Enable or disable advertisement autonomous flag.
AdvValidLifetime:	Enter advertisement valid life time.
AdvPreferredLifetime:	Enter advertisement preferred life time.
AdvRouterAddr:	Enable or disable advertisement router address.
If6to4:	Enter the interface 6to4.
Prefix2 Enabled:	Enable or disable prefix.
prefix:	Enter the prefix and prefix length
AdvOnLinkFlag:	Enable or disable advertisement on link flag.
AdvAutonomousFlag:	Enable or disable advertisement autonomous flag.
AdvValidLifetime:	Enter advertisement valid life time.
AdvPreferredLifetime:	Enter advertisement preferred life time.
AdvRouterAddr:	Enable or disable advertisement router address.
If6to4:	Enter the interface 6to4.



Tunnel 6 over 4

6over4 is an IPv6 transition mechanism meant to transmit IPv6 packets between dual-stack nodes on top of a multicast-enabled IPv4 network. On this page the option can be Enabled or Disabled.

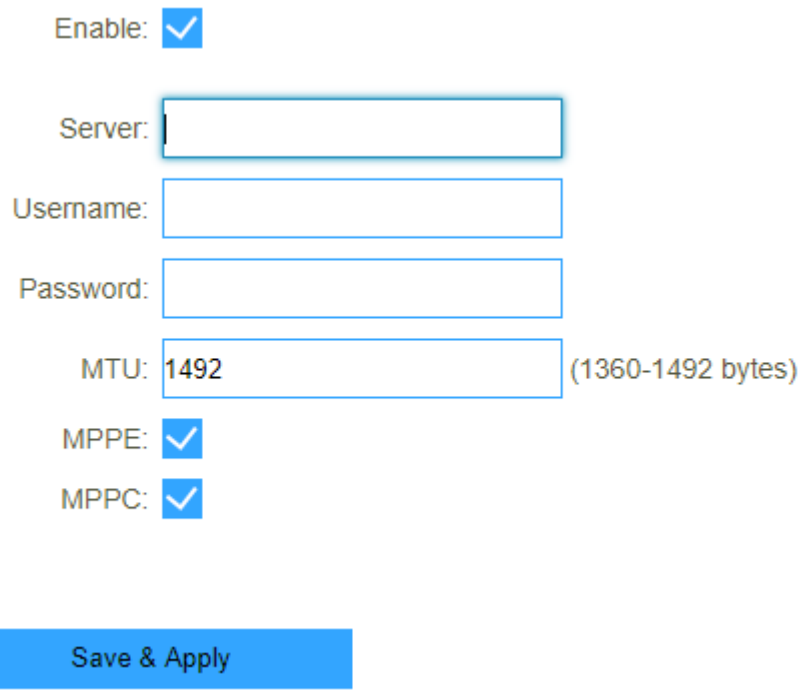


VPN

This page is used to configure the parameters for Internet network which connects to the PPTP and L2TP server.

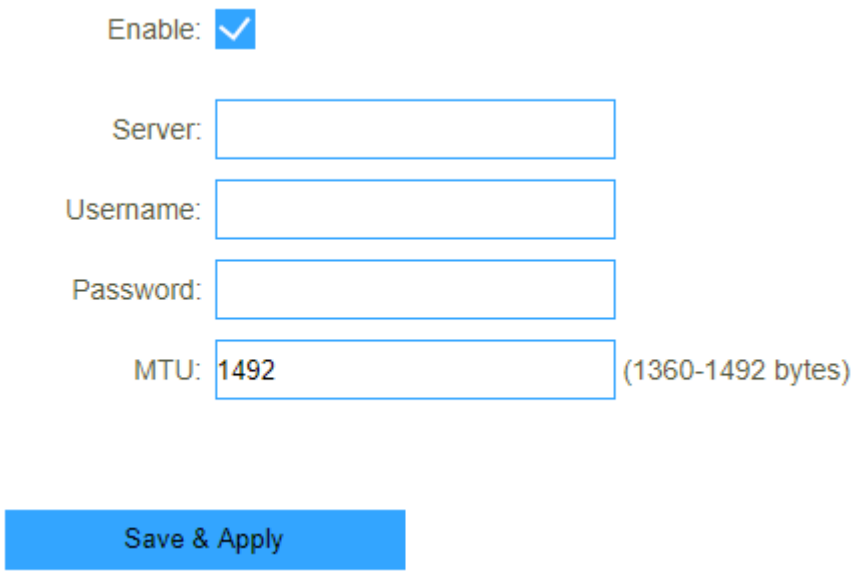
PPTP

Enable:	Enable or Disable the PPTP Connection.
Server:	Enter Server IP Address or FQDN name.
Username:	Enter PPTP VPN Server Username.
Password:	Enter PPTP VPN Server Password.
MTU:	Enter the Maximum Transmission Unit default 1492.
MPPE:	Enable or Disable MPPE.
MPPC:	Enable or Disable MPPC.



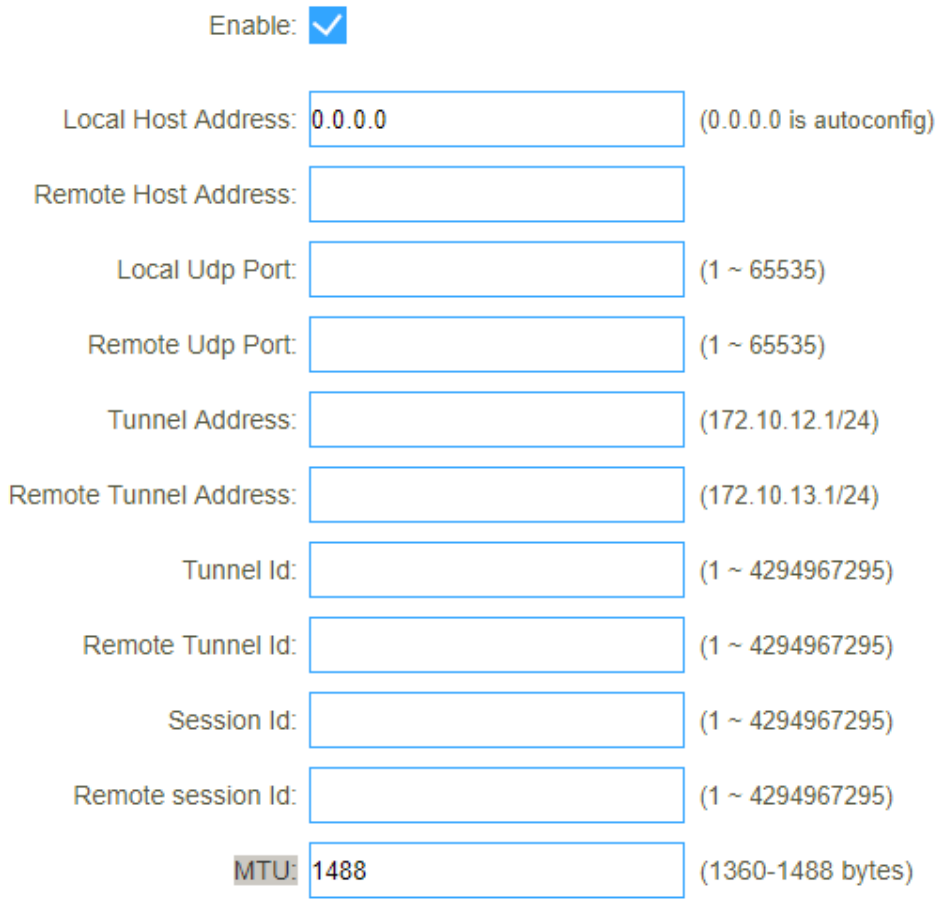
L2TPv2

Enable:	Enable or Disable the PPTP Connection.
Server:	Enter Server IP Address or FQDN name.
Username:	Enter PPTP VPN Server Username.
Password:	Enter PPTP VPN Server Password.
MTU:	Enter the Maximum Transmission Unit default 1492.



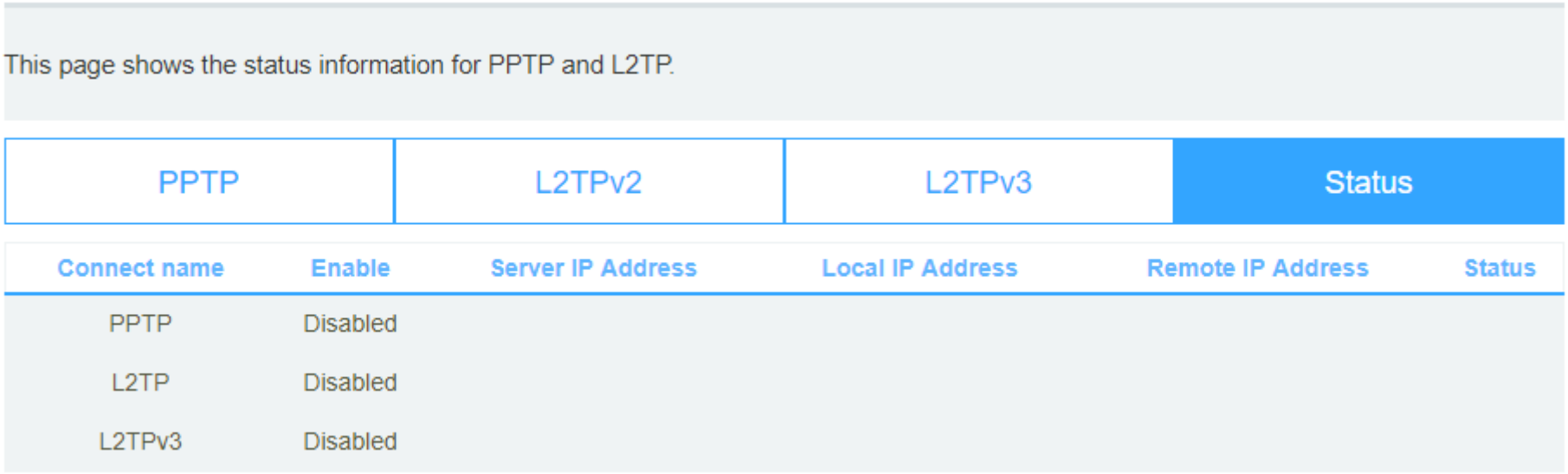
L2TPv3

Enable:	Enable or Disable L2TPv3.
Local Host Address:	Enter the Local IPv4 Address (0.0.0.0 will obtain IP automatically according to L2TP server settings).
Remote Host Address:	Enter Remote IPv4 address assigned by L2TP server.
Local Udp Port:	Enter local L2TP server port.
Remote Udp Port:	Enter remote UDP port of the L2TP server.
Tunnel Address:	Enter the L2TP server Address.
Remote Tunnel Address:	Enter the Remote L2TP server Address.
Tunnel Id:	Enter the Tunnel ID as per the L2TP server.
Remote Tunnel Id:	Enter the Remote Tunnel ID as per the L2TP server.
Session Id:	Enter the Session ID as per the L2TP server.
Remote session Id:	Enter the Remote Session ID as per the L2TP sever.
MTU:	Change the Maximum Transmission Unit (default 1488).



Status

On this page you will see the connection status of the VPN connections.

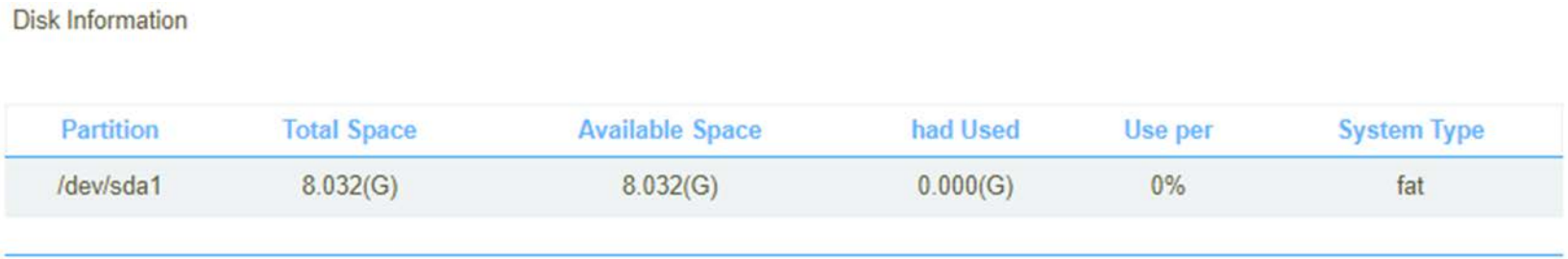


USB

The DWR-921 has a built-in USB port which can be connected to an external USB storage device for file sharing.

Disk Information

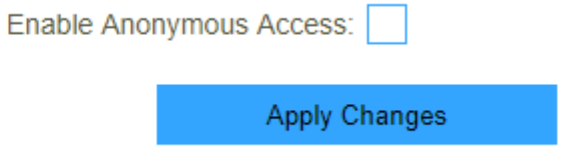
This page will show information about the USB drive connected.



Partition:	This will show information regarding the partition of the USB drive.
Total Space:	Shows the total amount of space on the USB drive.
Available space:	Shows the available space on the USB drive.
Had Used:	Amount of spaced used on USB drive.
Use Per:	Amount of space used in percentage.
System Type:	Format of USB drive (The DWR-921 only supports FAT32).

Account Management

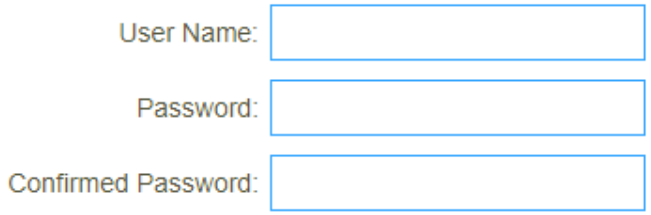
If enable anonymous access, client can only access specific directory [public], the [public] directory located in the first partition of the first disk.



Samba Account

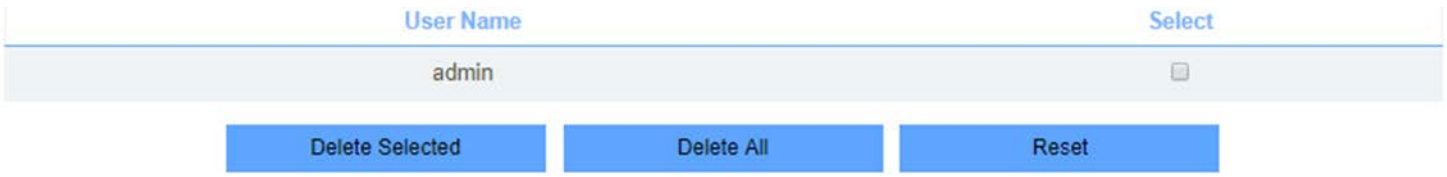
Here an account can be created for additional users to access file on the shared USB drive.

User Name:	Enter a Username.
Password:	Enter a Password for the specified Username.
Confirm Password:	Confirm the Password entered for the specified Username.



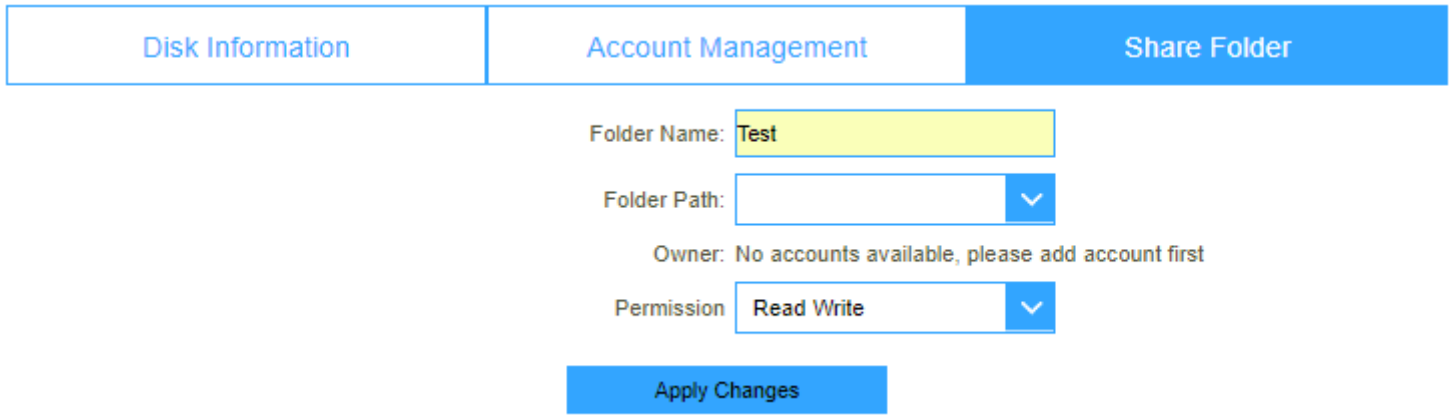
Account Table

This will show all accounts configured for USB shares.

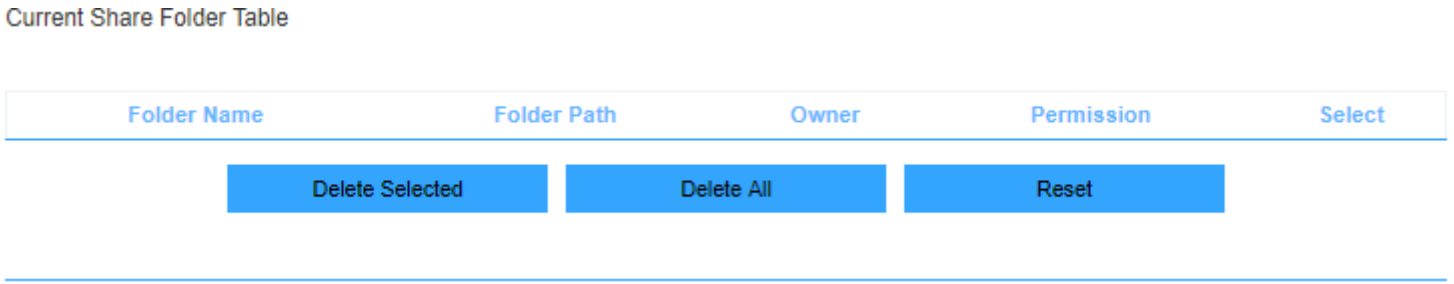


Share Folder

This page used for add/delete share folder.



Current Share Folder Table



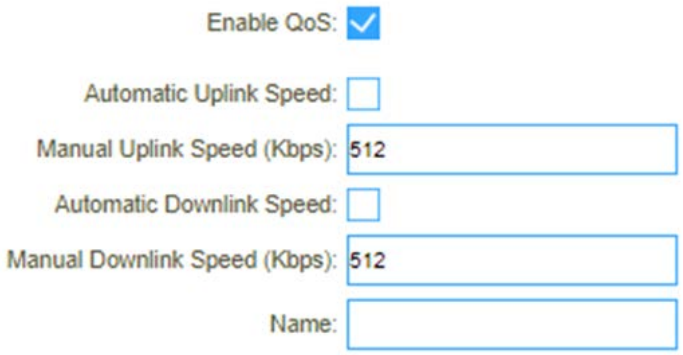
Features

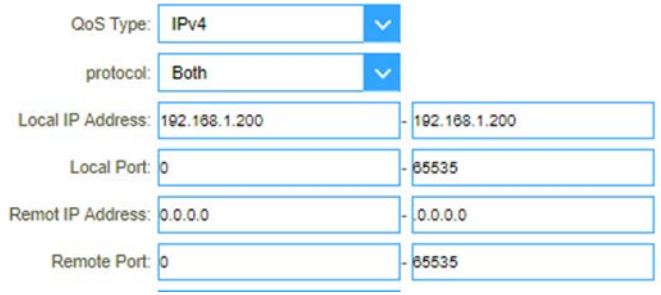
This section of the router will allow you to modify and change settings according to the features that is listed here.

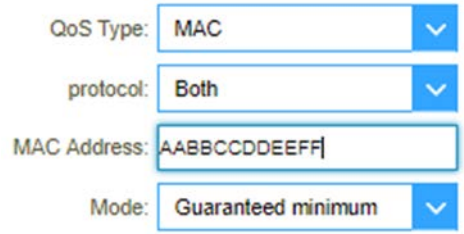
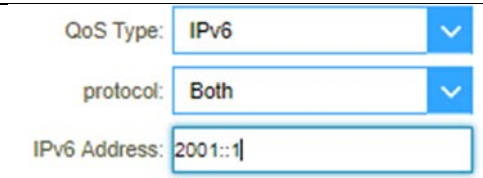
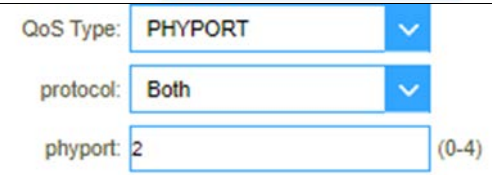
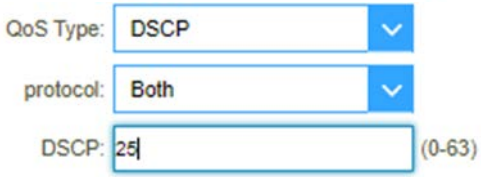
Quality of Service (QoS)

This feature will allow you to configure QoS for device on you network.

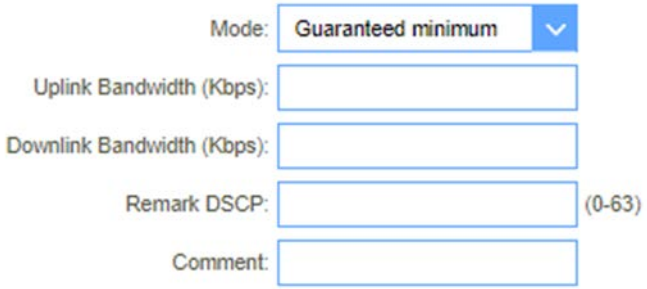
Enable QoS:	Enable or Disable QoS.
Automatic Uplink Speed:	Enable Automatic upload link.
Manual Uplink Speed:	Enter the upload speed limit.
Automatic Downlink Speed:	Check this box to enable Automatic speed control.
Manual Downlink Speed:	Enter the Download limit.
Name:	Enter a Name for this rule.
QoS Type:	Choose between six QoS types: • IPv4 – Specify IPv4 address or range and service ports.





	• MAC – Specify device MAC for which QoS rule should be enabled. 
	• IPv6 – Specify IPv6 address. 
	• PHYPORT – Specify Ethernet port number between 0-4. 
	• DSCP – Specify DSCP rule number between 0-63. 
Protocol:	Choose between three options for the rule: • Both – TCP/UDP • TCP • UDP
Mode:	Choose between two options for the rule: • Guaranteed Minimum Bandwidth • Restricted Maximum Bandwidth
Uplink Bandwidth:	Enter the Upload speed limit in Kbps.
Downlink Bandwidth:	Enter the Download speed limit in Kbps.
Remark DSCP:	Enter the DSCP remark rule number 0-63.

Comment: Enter a comment for this rule.

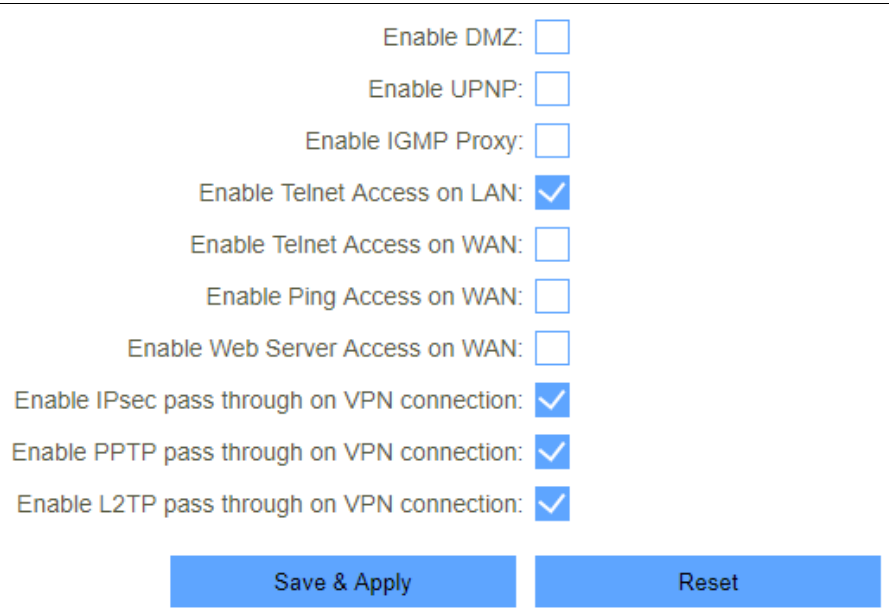


Firewall

Your router's high-performance firewall feature continuously monitors Internet traffic, protecting your network and connected devices from malicious Internet attacks.

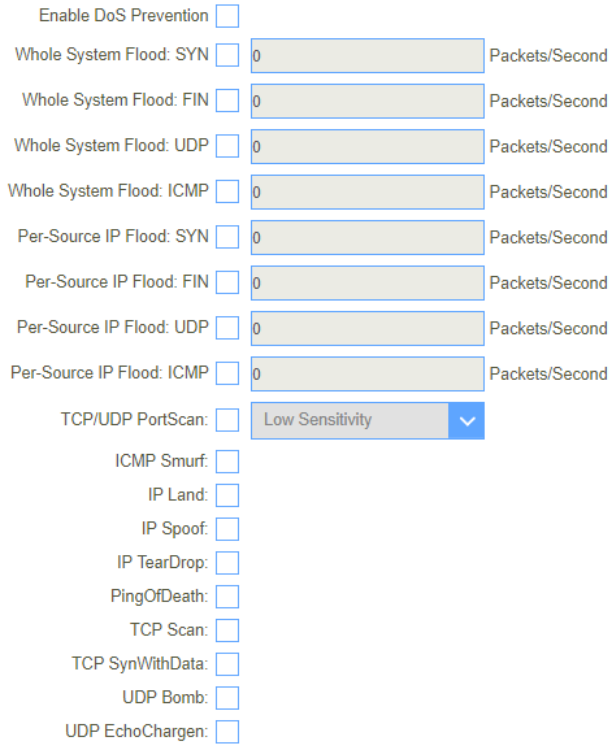
Advance Firewall Settings

Enable DMZ:	Enable or disable DMZ function (You will need to specify the IP off the device).
Enable UPnP:	Enable or disable UPnP function.
Enable IGMP Proxy:	Enable or disable IGMP Proxy function.
Enable Telnet Access on LAN:	Enable or disable Telnet for Local access.
Enable Telnet Access on WAN:	Enable or disable Telnet for WAN access.
Enable Ping Access on WAN:	Enable or disable Enable Ping Access on WAN function.
Enable Web Server Access on WAN:	Enable or disable Enable Web Server Access on WAN function.
Enable IPsec pass through on VPN connection:	Enable or Disable this option to allow or block IPsec connections to pass through the device.
Enable PPTP pass through on VPN connection:	Enable or Disable this option to allow or block PPTP connections to pass through the device.
Enable L2TP pass through on VPN connection:	Enable or Disable this option to allow or block L2TP connections to pass through the device.



DDOS

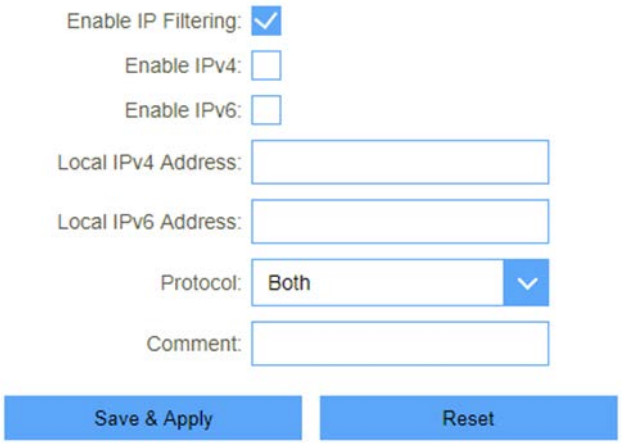
A denial-of-service (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service.



IP Filtering

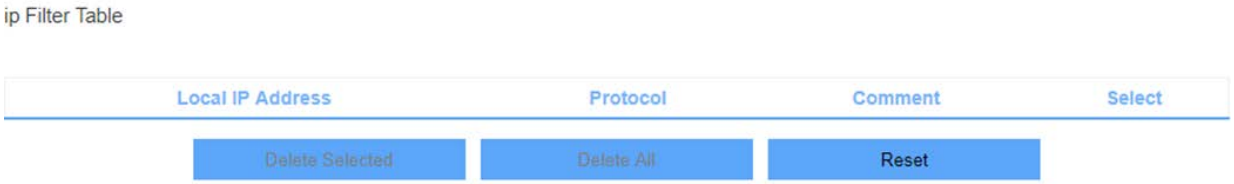
Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Enable IP Filtering:	Enable or Disable the IP Filtering function.
Enable IPv4:	Enable or disable the IPv4 Filtering feature.
Enable IPv6:	Enable or Disable the IPv6 Filtering feature.
Local IPv4 Address:	Enter the local IP address of the device.
Local IPv6 Address:	Enter the local IPv6 address of the device.
Protocol:	Select between TCP, UDP or Both.
Comment:	Add a comment to Identify the rule.



IP Filtering Table

This table will show a summary of any IP filtering rules added.



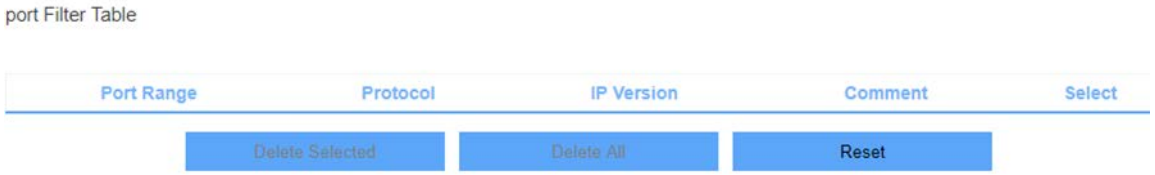
Port Filtering

This will allow to create a router to open a specific port or port range when an Application requires the port to be open when going outside of the local network.

Enable Port Filtering:	Enable or Disable Port Filtering Function.
Enable IPv4:	Enable the Port Filtering rule for IPv4.
Enable IPv6:	Enable the Port Filtering rule for IPv6.
Port Range:	Enter the Port number or port rage to be opened when device request for port.
Protocol:	Choose between TCP, UDP or Both.
Hop:	Add a comment to identify the rule.

Port Filtering Table

This table will show a summary of all Port Filtering rules created.

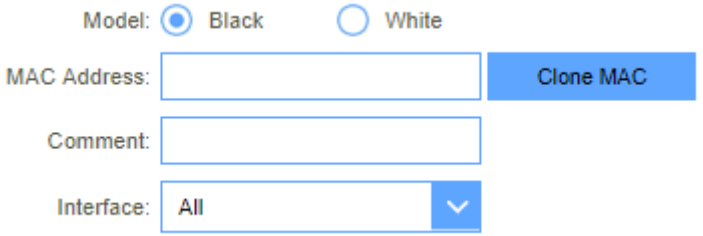


Mac Filtering

Mac Filtering will allow the device to block or allow certain devices based on their Mac Address (Physical network address).

Model: Choose between Blacklist and whitelist:

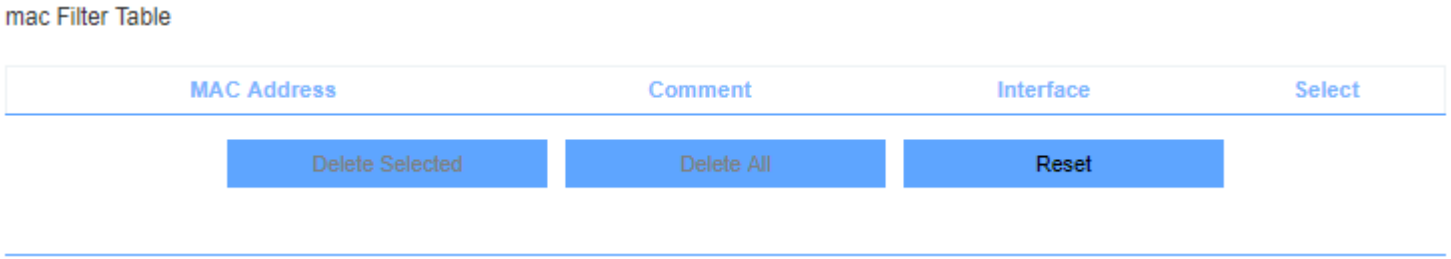
- Blacklist – Allows all devices to connect accept listed MAC address.
- Whitelist – Block all devices to connect accepts listed MAC addresses.



MAC Address:	Enter the device MAC address.
Comment:	Add a comment to the MAC filtering rule.
Interface:	WAN interface for the rule.

Mac Filtering Table

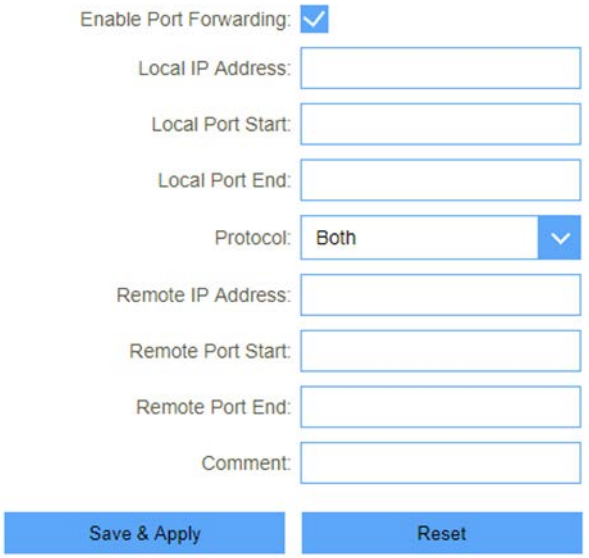
This table will show all configured Mac Filtering Rules.



Port Forwarding

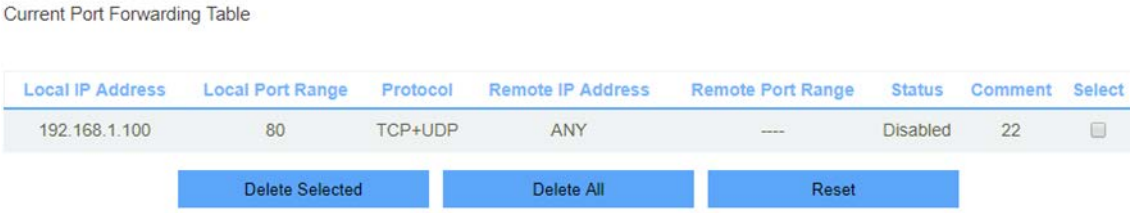
This allows for port to be open for incoming traffic from the internet for application which requires to be seen from the internet (ex. Opening port 80 for your camera system for remote monitoring).

Enable Port Forwarding:	Enable or Disable the Port Forwarding function.
Local IP Address:	Enter the Local IP address of the device for which the ports should be open.
Local Port Start:	Enter local port start.
Local Port End:	Enter local port end.
Protocol:	Select TCP, UDP or both.
Remote IP Address:	Enter the remote IP address which is allowed to access the port (Default blank or 0.0.0.0 can be used).
Remote Port Start:	Enter the remote Port start.
Remote Port End:	Enter the remote Port end.
Comment:	Enter a Comment for the rule.



Current Port Forwarding Table

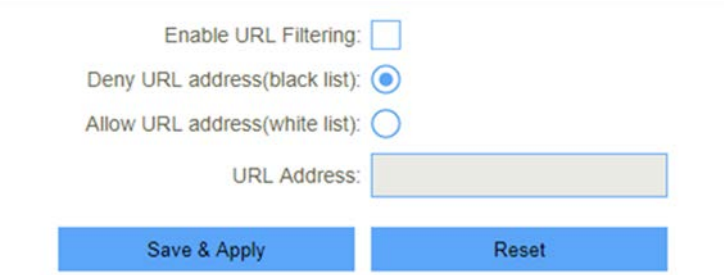
This table will show all configured Port Forwarding rules.



URL Filtering

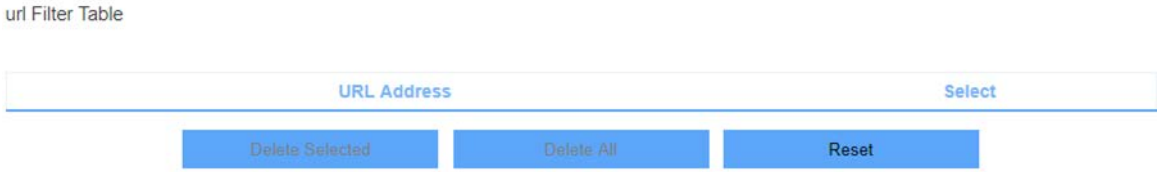
This section will allow the router to block certain web sites (DWR-921 can't block URL that starts with "https://".)

Enable URL Filtering:	Enable or Disable URL filtering.
Deny URL Address (Blacklist):	Enter the Website URL which needs to be blocked.
Allow URL Address (Whitelist):	Enter the Website URL which is allowed (All other websites will be blocked).
URL Address:	Enter the Website URL address for the above options.



URL Filter Table

This section shows the current list of configured URL Filters.



Route

This menu shows you the current default route and static route. Static Route reduces route selection problems and corresponding data overload and accelerates data packet forwarding.

Default Route

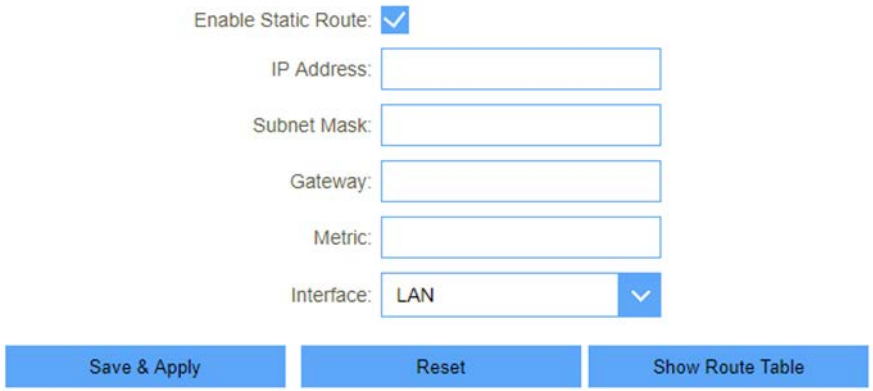
This option shows the current configured internet connections which the internet passes through

Connect name	Type	VlanMuxId	Action
LTE	dhcp	---	

Static Route

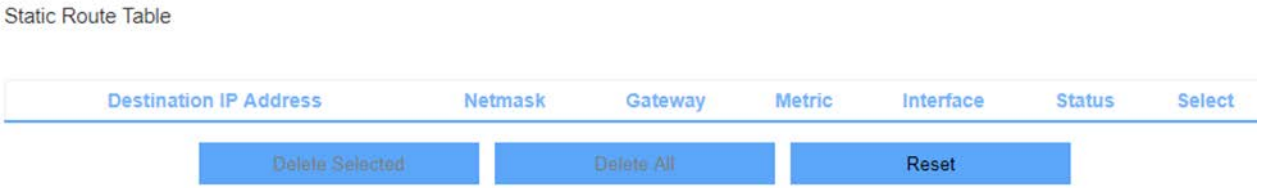
Once connected to the Internet, your router automatically builds routing tables that determine where traffic should be sent. Static routes can override this process, allowing traffic to be directed to a specific client or location.

Enable Static Routing:	Enable to Disable Static Route function.
IP Address:	Enter the Destination IP Address.
Subnet Mask:	Enter the Destination Subnet Mask.
Gateway:	Enter the Network gateway Address.
Metric:	Enter the routing metric.
Interface:	Select the interface for the routing to pass through.



Static Route Table

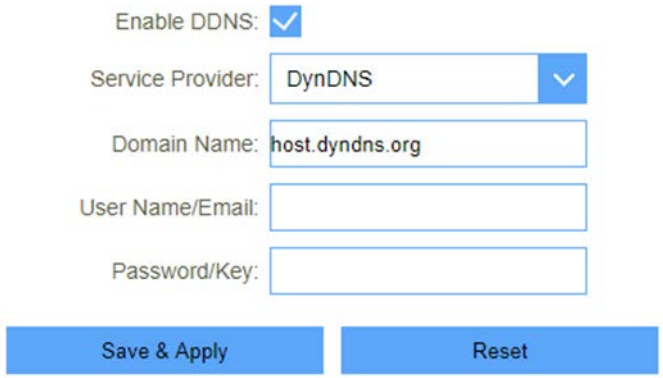
The table will show all static routes configured.



Dynamic DNS

The DWR-921 supports Dynamic Domain Name Service (DDNS). The dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains and allows access to a specified host from various locations on the Internet. Click a hyperlinked URL in the form of hostname.dyndns.org and allow remote access to a host. Many ISPs assign public IP addresses using DHCP, so locating a specific host on the LAN using the standard DNS is difficult. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet even if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS service providers

Enable DDNS:	Enable Dynamic DNS service.
Service Provider:	Select between two service Providers: • DynDNS • TZO
Domain Name:	Enter the Host Name from the DDNS provider.
User Name/Email:	Enter User Name as per the DDNS provider.
Password/Key:	Enter password as per the DDNS provider.



Management

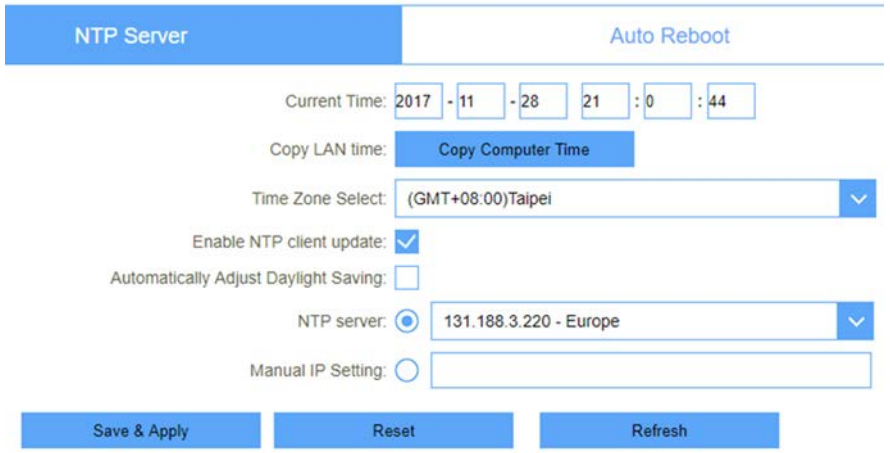
This section allows a user have more control on how to manage certain aspects of the DWR-921.

Time

NTP Server

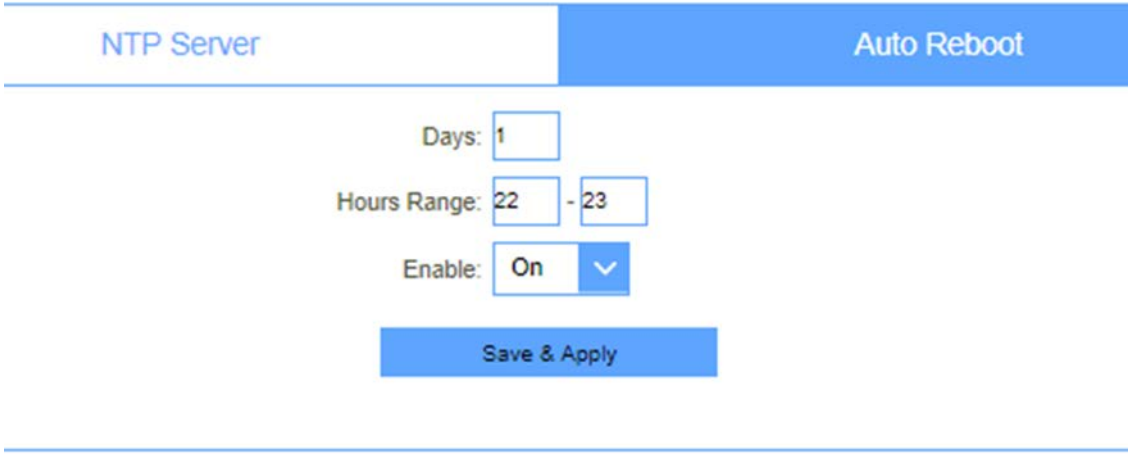
This section is to modify the DWR-921-time server settings so that the router can stay up to date for rules such as Schedules.

Current Time:	This is the current time of the router. You can manually change the values.
Copy LAN Time:	If clicked, it will copy your computer time settings.
Time Zone Select:	Select your current time zone.
Enable NTP client update:	Enable or Disable Automatic update.
Automatically Adjust Daylight Saving:	Enable or Disable of Automatic Daylight-Saving functions.
NTP Server:	Select the NTP server.
Manual IP Settings:	Manually add NTP server IP Address.



Auto Reboot

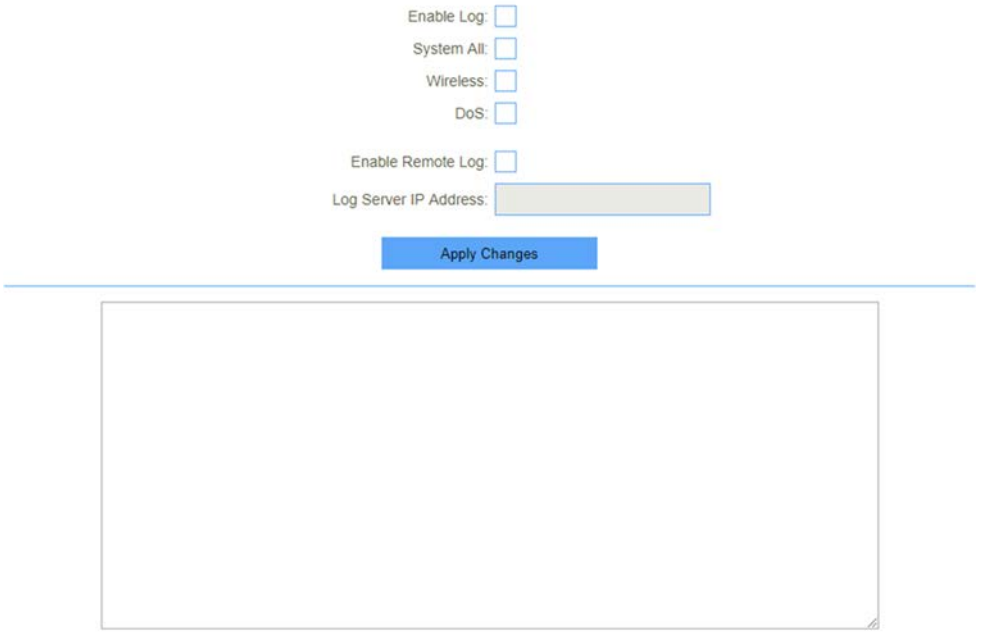
This feature can do the Reboot automatically at a specified time. Please note: “Auto Reboot” depend on the “NTP Server”, you have to enable the 'NTP Server' when using this feature.



System Log

This page allows for the user to enable the logs for this router as well as remote logs to monitor the router for fault or certain activities.

Enable Log:	Enable or Disable System Log.
System All:	Display all log files.
Wireless:	Enable log for Wireless activity.
DoS:	Enable log for DoS activity.
Enable Remote Log:	Enable or Disable remote logging.
Log Server IP Address:	Enter remote Syslog server IP address.

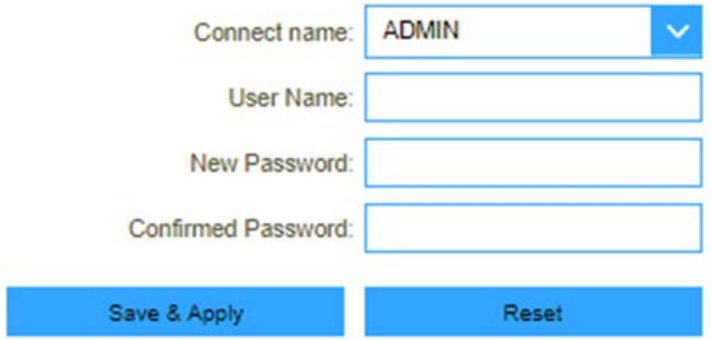


System Settings

On this page, the user will be able to change the routers login credentials as well as restore the device to Factory settings, Backup the Configuration and restore previously made configurations.

Administrator

Connect name:	Select between which privilege you would like the user to have: • ADMIN – Administrator level settings • USER – Can view certain settings
User Name:	Create a new User Name.
New Password:	Create a new password for the User Name.
Confirmed Password:	Confirm for the User Name.



System

This screen allows you to back up, restore, and erase the router's current settings. Once you have the router working correctly, you should back up the information to have it available if something goes wrong. When you back up the settings, they are saved as a file on your computer. You can restore the router's settings from this file.

Save Settings to File:	Save router settings to Local PC.
Load Settings from File:	Upload Save settings from Local PC.
Reset Settings to Default:	Restore device back to factory settings.
Reboot the device:	Reboot the router.

Statistics

User Statistics

This page shows each user's total traffic statistics and LTE traffic statistics.

IP Addr	Total Down	Total Up	Lte Down	Lte Up
192.168.1.123	0 Bytes	0 Bytes	0 Bytes	0 Bytes
192.168.1.100	0 Bytes	591 158 Bytes	0 Bytes	0 Bytes
192.168.1.101	0 Bytes	0 Bytes	0 Bytes	0 Bytes

Interface Statistics

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

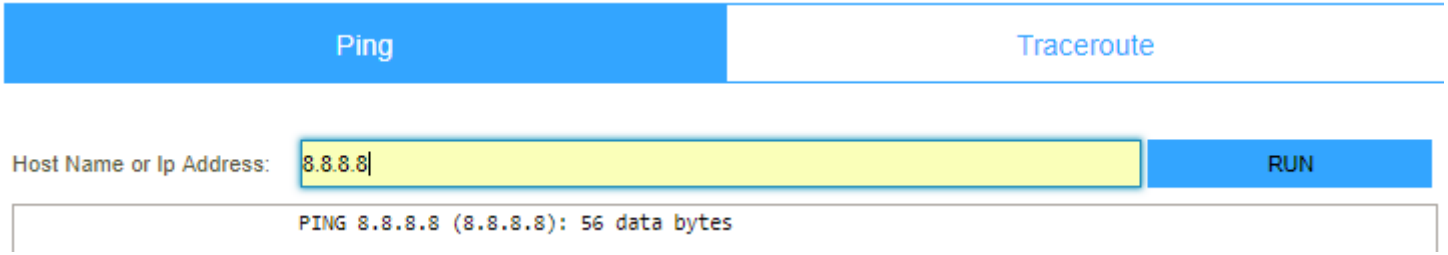
Wireless LAN	*Sent Bytes*	4954123
	Received Bytes	130946343
Ethernet LAN1	*Sent Bytes*	0
	Received Bytes	0
Ethernet LAN2	*Sent Bytes*	140291521
	Received Bytes	10556552
Ethernet LAN3	*Sent Bytes*	0
	Received Bytes	0
Ethernet LAN4	*Sent Bytes*	0
	Received Bytes	0
WAN	*Sent Bytes*	0
	Received Bytes	0

Refresh

Diagnostics

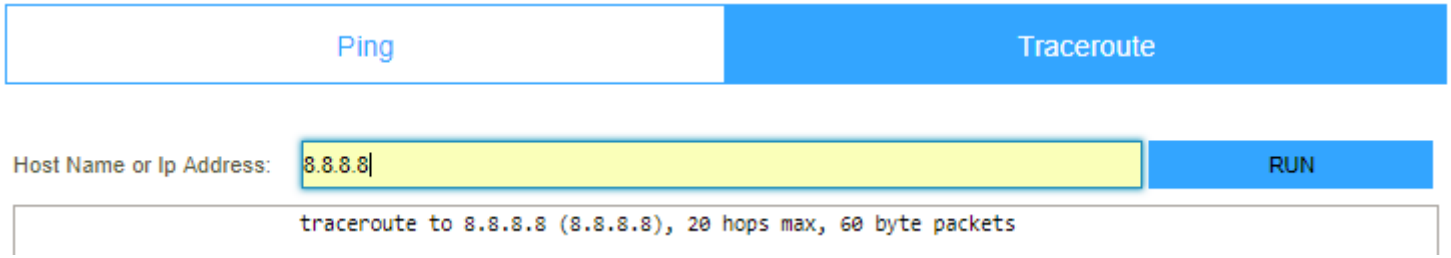
Ping

This page gives you various diagnostics about ping for IP connection.



Traceroute

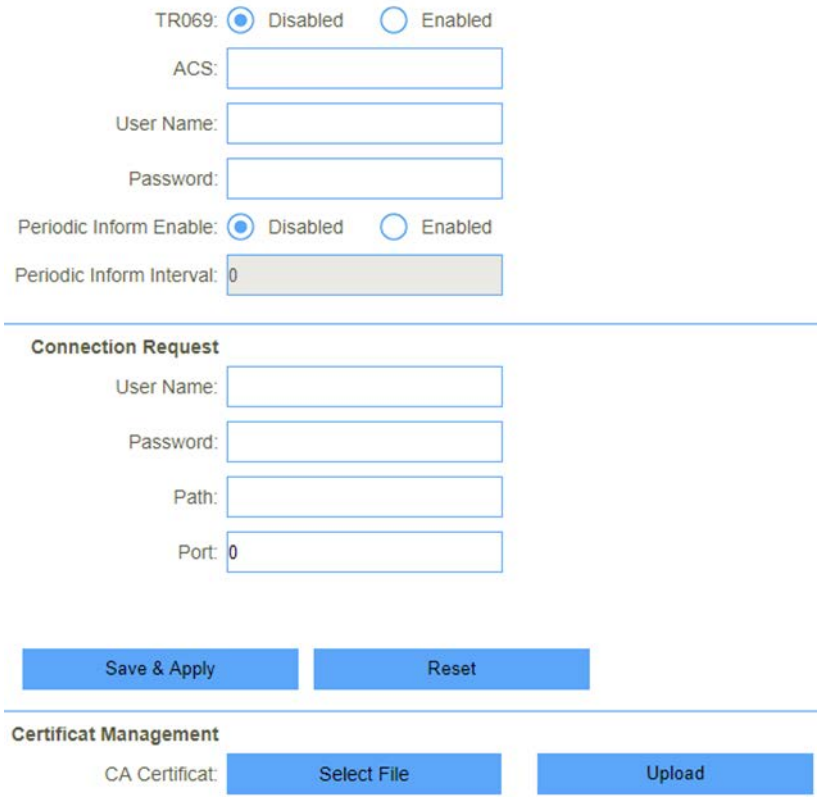
This page gives you various diagnostics about traceroute for IP connection.



TR069

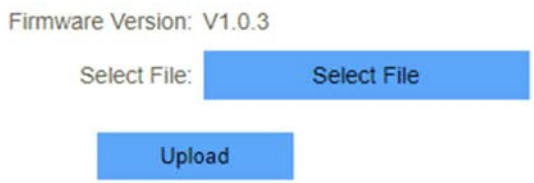
This page is used to configure the TR069. Here you may change the setting for the ACS's parameters.

TR069:	Enable or Disable TR069 Function.
ACS:	ACS Server Domain or IP Address.
Username:	Username for Connection to ACS Server.
Password:	Password for Connection to ACS Server.
Periodic Inform:	Enable or Disable periodic inform.
Periodic Inform Interval:	Periodic inform interval.
User Name:	Username used for ACS connection to TR069.
Password:	Password used for ACS connection to TR069.
Path:	Connection request path.
Port:	Connection port.
Certificate Management:	Upload CA certificate if required by ACS server.



Upgrade

You install new version of the router’s software using this page. From time to time, we may release new versions of the Router's firmware. Firmware updates contain improvements and fixes the current problems. On this page, you can check the firmware version and upgrade firmware.



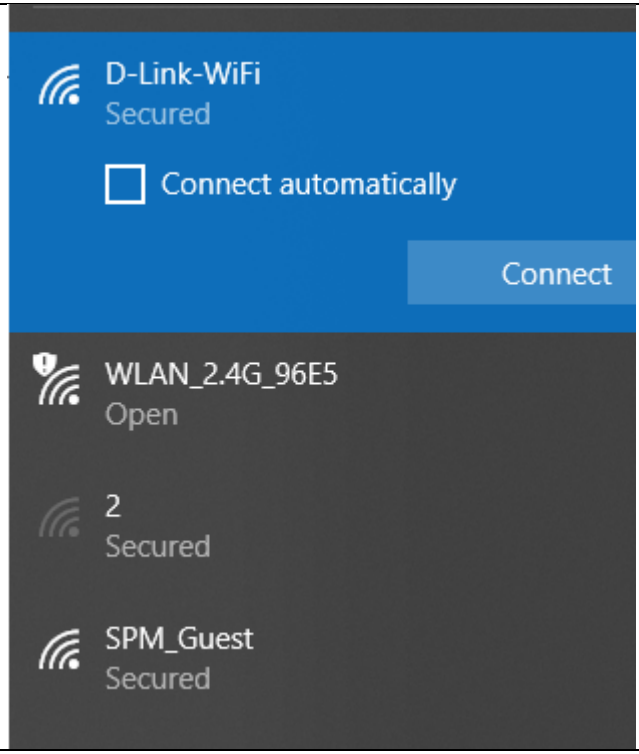
Connecting to a Wireless Network

Using Windows 10/8.1/8

Windows 10/8.1/8 users may use the built-in wireless utility to connect to a wireless network. If you are using another company's utility or windows 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey "option similar to the Windows 10/8.1/8 utility as seen below.

If you receive the Wireless Networks Detected bubble, click on the centre of the bubble to access the utility. You can also click on the wireless icon in your system tray (lower-right corner).	

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

Highlight the wireless network (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 “Networking Basics” for more information.	

Using Windows 7

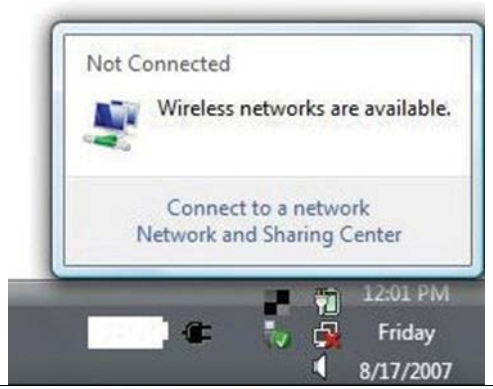
Windows 7 users may use the built-in wireless utility to connect to a wireless network. If you are using another company's utility or Windows 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey "option similar to the Windows 7 utility as seen below.

If you receive the Wireless Networks Detected bubble, click on the centre of the bubble to access the utility. You can also click on the wireless icon in your system tray (lower-right corner).	
The utility will display any available wireless networks in your area.	

Highlight the wireless network (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 “Networking Basics” on page 80 for more information.	

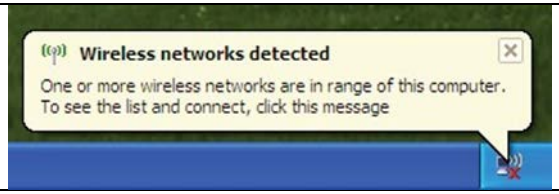
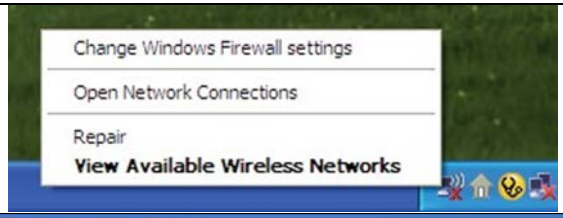
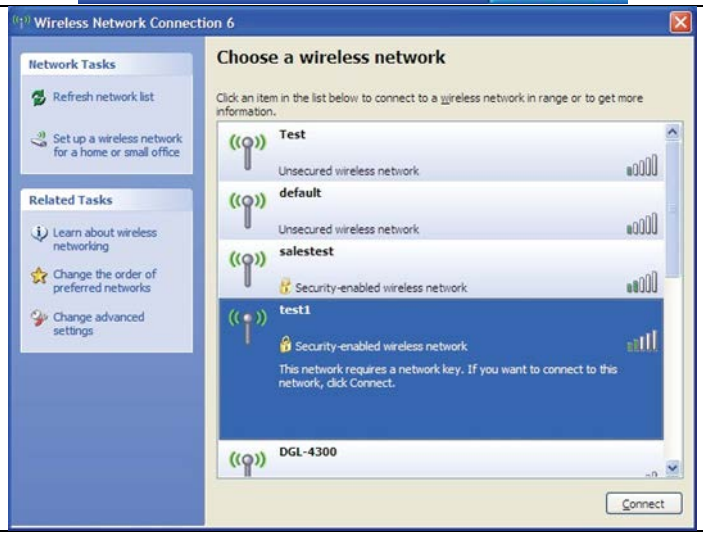
Using Windows Vista™

Windows® Vista™ users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey "option similar to the Windows® Vista™ utility as seen below.

If you receive the Wireless Networks Detected bubble, click on the centre of the bubble to access the utility. Or Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select Connect to a network.	
The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the Connect button. If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to "Networking Basics" on page 80 for more information.	

Using Windows® XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

If you receive the Wireless Networks Detected bubble, click on the centre of the bubble to access the utility.	
or	
Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select View Available Wireless Networks.	
The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the Connect button. If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to "Networking Basics" for more information.	

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DWR-921. Read the following descriptions if you are having problems.

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

When entering the IP address of the D-Link router (192.168.1.254 for example), you are not connecting to a website on the Internet or 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:

- Internet Explorer 6 or higher
- Mozilla 1.7.12 (5.0) or higher
- Opera 8.5 or higher
- Safari 1.2 or higher (with Java 1.3.1 or higher)
- Camino 0.8.4 or higher
- Firefox 1.5 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 Zone Alarm, Black Ice, 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:

1. Go to Start > Control Panel. Double-click the Internet Options Icon. From the Security tab, click the Reset All Zones to Default Level button to restore the settings to their defaults.
2. 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.
3. Go to the Advanced tab and click the button to restore these settings to their defaults. Click OK three times.
4. 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 the 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. Please note that this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.1.254, and the default username is admin and the password should be admin.

Tips

Here are a few things to keep in mind when installing 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 and 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.

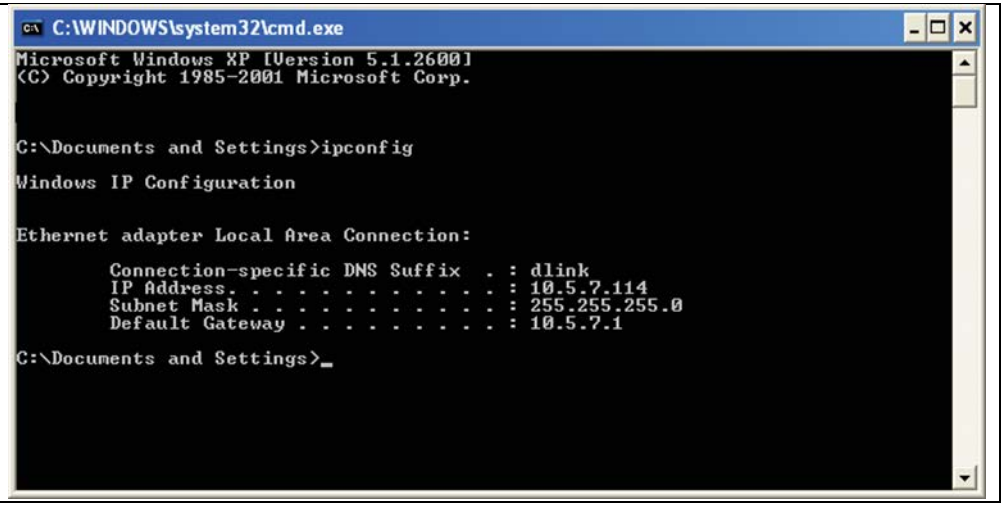
Security

Don’t let you unauthorized users connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to “Wireless Settings” for detailed information on how to set up wireless security.

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® Vista™, 7/8/8.1/10 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 10 - Click Start -> Type Control Panel -> Network and Sharing Center -> Left Panel look for Change Adaptor Settings.

Windows 7 - Click Start -> Type Control Panel -> Network and Sharing Center -> Left Panel look for Change Adaptor Settings.

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.

Step 2

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

Step 3

Highlight Internet Protocol (TCP/IP) or 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 192.168.0.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 Default Gateway the same as the LAN IP address of your router (192.168.0.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). 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.

Technical Specifications

LTE Band • 800 / 900 / 1800 / 2600 MHz	VPN • L2TP/PPTP/IPSEC/VPN Pass-through • PPTP/L2TP/L2TPv3 client
UMTS/HSDPA/HSUPA Band • 900 / 2100 MHz • Power Class 3	Antenna • 2x 5dBi 2.4g external antenna • 2x5dBi LTE external antenna
Data Rates • 2.4GHz up to 300Mbps • 11b (11Mbps): -79dBm • 11g (54Mbps): -68dBm • 11n (20M) mode: -67dBm • 11n (40M) mode: -64dBm	Ports • 1 x 10/100 Mbps auto MDI/MDI-X RJ45 port • 4 x 10/100 Mbps auto MDI/MDI-X RJ45 port (LAN1~4) • 1 x USB 2.0, Type A, 5V 500mA
Standards • IEEE 802.11n (2T2R, up to 300Mbps) • IEEE 802.11g • IEEE 802.11b • IEEE 802.11i • IEEE 802.3 10BASE-T • IEEE 802.3u 100BASE-TX	USIM Slot • Standard 6-pin SIM card interface
Wireless Security • 802.11a/g/n: OFDM (BPSK / QPSK / 16QAM / 64QAM) • 802.11b: DSSS (DBPSK / DQPSK / CCK) • WEP • WPA/WPA2 personal mixed mode	LED Status Indicators • POWER • WAN • LAN 1-4 • WI-FI • WPS • USB • LTE

Firewall • NAT firewall, SPI firewall • Built-in NAT server which supports Port Forwarding and DMZ • Built-in firewall with URL filtering, and MAC address filtering	Dimensions (W x D x H) • 200 X 128 33 MM
Operating Temperature • Operating: 0 ~ 40 degrees C • Storage: -40 ~ 70 degrees C	Certifications • CE, RoHS, WEEE • Wi-Fi Certified
Operating Humidity • Operating: 10 ~ 90% (non-condensing) • Storage: 5 ~ 95% (non-condensing)	

Supported frequency band is dependent upon regional hardware version.

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