

# MANUAL - 4G ROUTER SETUP



G-LTE-PRO



# CONTENTS

<b>A - Basic Router Set Up</b>	<b>2</b>
<b>B - Basic 4G APN Set Up</b>	<b>3</b>
<b>C - Setting up radio</b>	<b>5</b>
<b>D - Setting up the routers LAN interface</b>	<b>9</b>
<b>E - Configuring the routers WAN Settings</b>	<b>10</b>
<b>F - Configuring the routers Firewall Settings</b>	<b>12</b>
<b>G - Router Administration settings</b>	<b>14</b>

# A - Basic Router Set Up

## Connecting the Router

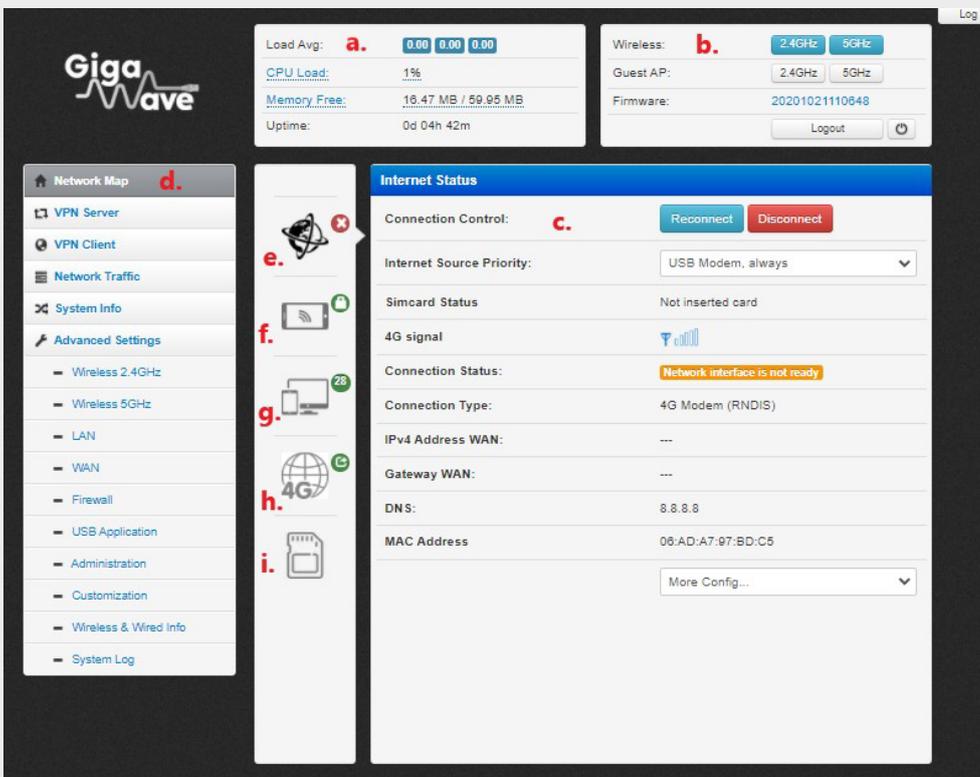
1. Place the SIM card in the SIM card slot on the back of the router.
2. Plug in the 12v PSU that comes with the router. There will be a blue light on the front of the router which means it is powered up but no 4G connection yet.
3. Plug in your computer to one of the 3 yellow LAN ports on the back of the router or connect to the routers Wi-Fi using the below settings.
  - a. Default Wi-Fi I SSID: Giga
  - b. Default Wi-Fi Password: Gigawave

## Accessing the Routers Admin Page

1. Open a web browser such as Google Chrome or Firefox on your computer. In the address bar up the top enter the routers default IP address: `http://192.168.1.1` and press enter. This will pop up a login box. Enter the routers default admin username and password.
  - a. Username: admin
  - b. Password: gigawave

## Routers Homepage

The routers homepage will show the user various options.



**a.** At the top left of the homepage the user can see the system load info. This gives info on the CPU usage; current memory being used and the Uptime of the router.

**b.** This section tells the user whether the 2.4 GHz and 5 GHz radios are enabled. It also tells if the guest 2.4 GHz and 5 GHz radios are enabled. Firmware version is below this. The user can logout and reboot the router from the buttons below the firmware.

**c. Internet status:** This is the status menu of the router. It gives information such as the current state of the sim card, the 4G signal of the sim card and the connection status (orange for not ready green for connected). It will also give the Wan IP addresses, DNS and MAC address of the router.

**d. Routers left-hand Menu Bar:** Users can navigate to different settings of the router using the left-hand menu bar. The options in this bar will covered further on in this manual.

**e. Internet status quick menu:** Quick menu item to get to the internet status page.

**f. Wi-Fi Radios quick menu:** Quick menu item to change Wi-Fi radio options. (Wi-Fi radio options covered in depth further on in this manual)

**g. Client Status quick menu:** Quick menu to see clients currently connected to the routers wired or wireless LAN.

**h. 4G Modem Status:** Overview 4G module installed in router.

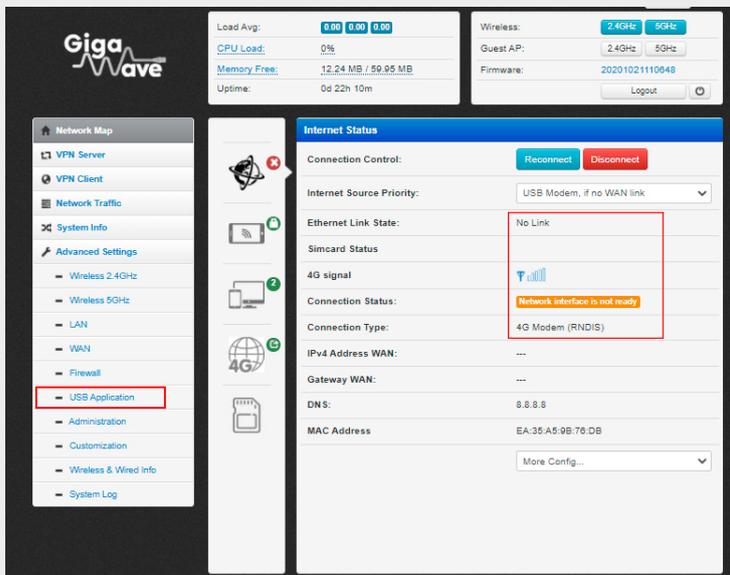
**i. Sim card info:** Info on current sim card inserted in router.

## B - Basic 4G APN Set Up

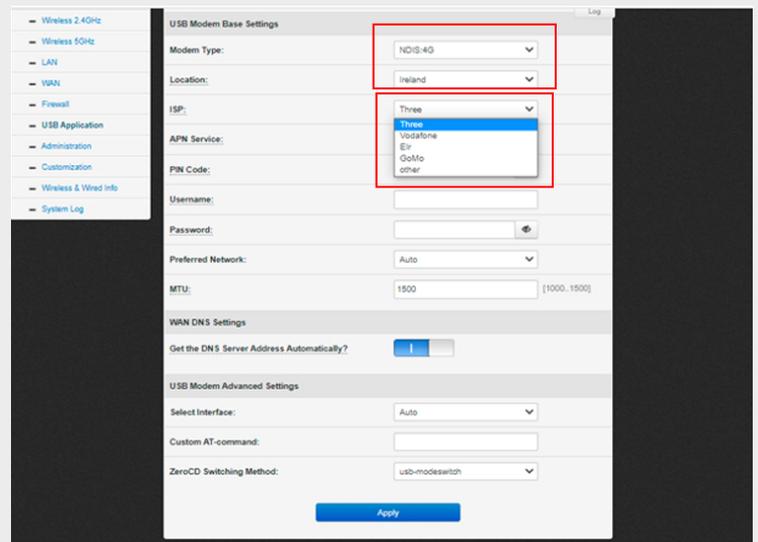
1. On the homepage of the router there will be no 4G connectivity until the 4G Network APN (access point name) details are setup. See image below there is no link upon first set up of the router. The router is pre-loaded with the default APN settings of the 3 network in the Republic Of Ireland. When a 3 sim card is in the router it will work straight away without any additional configuration. The router also has APN settings for other Republic of Ireland networks including Vodafone, Eir and GoMo.

2. The APN can be changed to a different network from the default 3 by following the steps below. If the sim card being used is from a different Republic of Ireland network not in the default list or is from a network in the UK/Northern Ireland the APN settings must be entered manually (see next steps).

### Changing the Default APN



**Step 1** – Click on USB application option under Advanced Settings on the left-hand menu of the homepage. This will open the 4G APN settings page.



**Step 2** - On this page the default modem type for Republic of Ireland and the UK is NDIS: 4G. This is set as default but make sure this type is selected if living in Ireland or the UK.

- a. **Location:** Select the country the 4G Network is in.
- b. **ISP:** Select the 4G network of the sim card that is entered in the router. If using a Republic of Ireland sim card then select the appropriate APN from the list. It will populate the rest of the settings, then press Apply at the bottom of the page.

If using a sim card from Northern Ireland/UK the select other from the list and then enter the correct APN details manually. Select other from the ISP dropdown list and enter the APN details of the sim card you are using. Below is a list of some UK/Northern Ireland APNS:

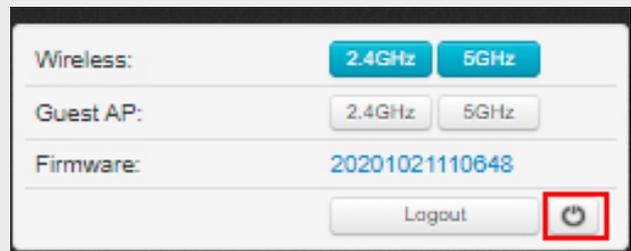
**Vodafone**  
 APN Service:  
 wap.vodafone.co.uk  
 Username: wap  
 Password: wap

**02:**  
 APN Service:  
 mobile.o2.co.uk or wap.o2.co.uk  
 (if using pay monthly sim)  
 Username: 02web  
 Password: password

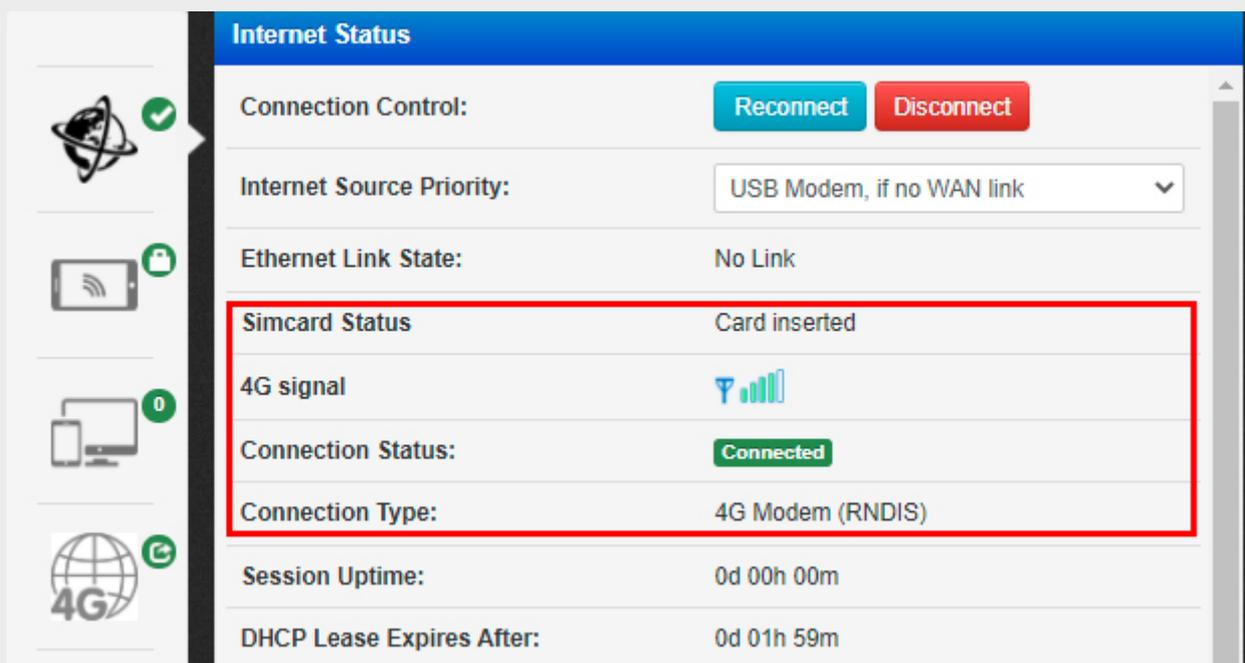
**Three:**  
 APN Service: three.co.uk  
 Username: (leave blank)  
 Password: (leave blank)

All other settings on the USB application page can be left as is.

- c. **Once the APN settings are entered press Apply at the bottom of the page and reboot the 4G router by clicking on the reboot icon in the top right-hand corner:**



**Step 3** - When the router reboots, if the 4G connection is successful the led on the front of the router will have change to solid green meaning 4G router has a solid internet connection. Also, on the homepage of the router it will now say connected:



# C - Setting up radio

## Setting up 2.4GHz Radio including Wi-Fi SSID and Password

**Step 1** - Click on Wireless 2.4 GHz option under Advanced Settings on the left-hand menu of the homepage. This will open the 2.4 GHz wireless radio settings page.

On this General page the following options can be configured:

The screenshot shows the 'Wireless - General (2.4GHz)' configuration page. The left sidebar has 'Advanced Settings' selected, with 'Wireless 2.4GHz' highlighted. The main panel contains the following settings:

- Enable Radio?**:
- Date to Enable Radio (workweek):** Mo, Tu, We, Th, Fr (checked)
- Time of Day to Enable Radio (workweek):** 00:00 - 23:59
- Date to Enable Radio (weekend):** Sa, Su (checked)
- Time of Day to Enable Radio (weekend):** 00:00 - 23:59
- SSID:** Gigawave
- Hide SSID:**
- Wireless Mode:** g/n Mixed (\*)
- Channel Bandwidth:** 20 MHz
- Radio Channel:** 11
- Extension Channel:** Below
- Fixed TX Rate Link Mode:** No (\*)
- Authentication Method:** WPA2-Personal
- WPA Encryption:** AES
- WPA Pre-Shared Key:** [Empty field]
- Network Key Rotation Interval:** 3600 [0..2592000]
- TX Power Adjustment (%):** 100 [0..100]
- Region Code:** Europe (channels 1-13)

Buttons at the bottom: 'Go to 5GHz-Setting' and 'Apply'.

**a. Enable Radio?** Enable or disable the 2.4 GHz radio.

**b. Date to Enable Radio (workweek):** Schedule the radio on or off status based on weekday.

**c. Time of Day to Enable Radio (workweek):** Schedule the radio on/off status based on time.

**d. Date to Enable Radio (weekend):** Schedule the radio on/off status based on weekend.

**e. Time of Day to Enable Radio (weekend):** Schedule the radio on/off status based on time of day during weekend.

**f. SSID:** Set the Wi-Fi name on the 2.4 GHz radio.

**g. Hide SSID:** Enable or disable the SSID (Wi-Fi Name)

**h. Wireless Mode:** Set the 2.4 GHz radio wireless version of the 802.11n interface (b/g/n Mixed by default).

**i. b/g protection:** Enable protection for 11b traffic from 11g or 11n clients. (Auto is default).

**j. Channel Bandwidth:** Select the channel bandwidth of the 2.4 GHz radio. Selecting a wider channel such as 40 MHz maximises throughput and increase speed however is more prone to interference from overlapping channels. If there are issues try the 20 MHz, not as fast but travels further and has fewer overlapping channels.

**k. Radio Channel:** Set 2.4 GHz radio channel, best channels are 1, 6, and 11. (Default is Auto).

**l. Extension Channel:** Select the extension channel used in the 20/40 MHz bandwidth mode. 802.11n uses the extension channel to get extra speed. Select below or above. (Below is default).

**m. Fixed TX Rate Link Mode:** Set a fixed transmission bandwidth limit on the 2.4 GHz radio.

**n. Authentication Method:** Set the authentication method for wireless clients. This can be set to open if you want no Wi-Fi encryption. (Default and standard setting is WPA2-Personal)

**o. WPA Encryption:** Enable the WPA encryption to encrypt the data (default is AES)

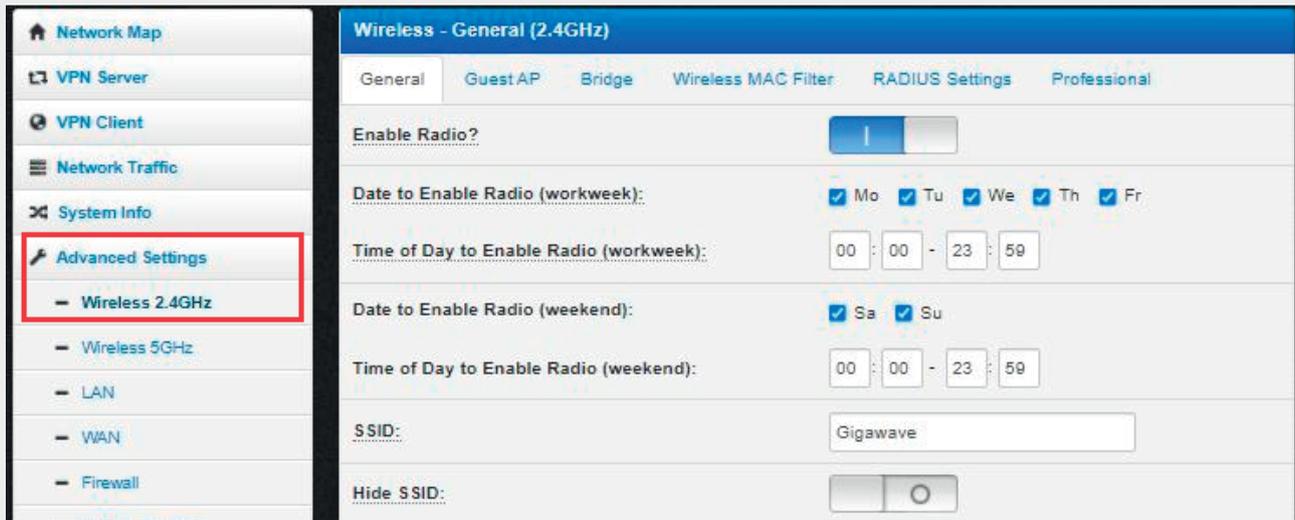
**p. WPA Pre-Shared Key:** This is the 2.4 GHz radio Wi-Fi password. It must be between 8 and 63 characters long. (Default is Gigawave)

**q. Network Key Rotation Interval:** This specifies the interval (seconds) after which a WPA group key is changed. (Can be left at 3600).

**r. TX Power Adjustment (%):** Set the 2.4 GHz radios antenna power. This can be raised or lowered based on the scenario. If there is a lot of interference from wireless devices the output power can lowered accordingly. (Default is set to 100).

**s. Region Code:** Different regions have different regulations for Wi-Fi channels, adjust according to the region that the router is installed in. (Default is Europe channels 1-13).

General users usually only need to change the SSID and Password (WPA Pre-Shared Key) to suit client's needs. See pics below:



More advanced users can also click on the GuestAp tab next to General and enable a guest AP network. A guest Wi-Fi SSID and Password (WPA Pre-Shared Key) can be enabled from here. It can be scheduled and isolated from the main LAN network. With this option guest clients will not be able to see LAN device on the main LAN network. Advanced users also have Bridge, Wireless MAC Filter, RADIUS Settings and Professional settings. Settings in these tabs are outside the scope of this basic user guide.

# Setting up 5 GHz Radio including Wi-Fi SSID and Password

The screenshot shows the 'Wireless - General (5GHz)' configuration page. The left sidebar has 'Advanced Settings' and 'Wireless 5GHz' highlighted. The main panel includes the following settings:

- Enable Radio?**: A toggle switch set to 'On'.
- Date to Enable Radio (workweek):** Checkboxes for Mo, Tu, We, Th, Fr are all checked.
- Time of Day to Enable Radio (workweek):** Time range 00:00 - 23:59.
- Date to Enable Radio (weekend):** Checkboxes for Sa, Su are both checked.
- Time of Day to Enable Radio (weekend):** Time range 00:00 - 23:59.
- SSID:** Gigawave
- Hide SSID:** A toggle switch set to 'Off'.
- Wireless Mode:** a/n Mixed (\*)
- Channel Bandwidth:** 20/40 MHz
- Radio Channel:** 36
- Extension Channel:** Auto
- Fixed TX Rate Link Mode:** No (\*)
- Authentication Method:** WPA2-Personal
- WPA Encryption:** AES
- WPA Pre-Shared Key:** A masked password field with a copy icon.
- Network Key Rotation Interval:** 3600 [0..2592000]
- TX Power Adjustment (%):** 100 [0..100]
- Region Code:** Europe (channels 36,40,44,48)

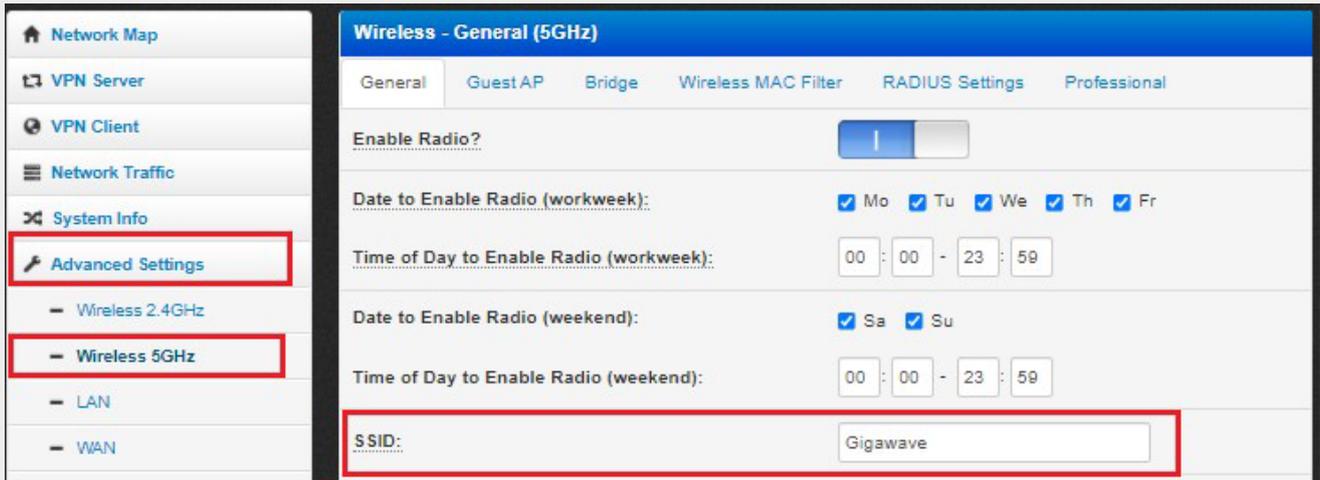
Buttons at the bottom: 'Go to 2.4GHz Setting' and 'Apply'.

On this General page the following options can be configured:

- a. **Enable Radio?** Enable or disable the 5 GHz radio.
- b. **Date to Enable Radio (workweek):** Schedule the radio on or off status based on weekday.
- c. **Time of Day to Enable Radio (workweek):** Schedule the radio on/off status based on time.
- d. **Date to Enable Radio (weekend):** Schedule the radio on/off status based on weekend.
- e. **Time of Day to Enable Radio (weekend):** Schedule the radio on/off status based on time of day during weekend.
- f. **SSID:** Set the Wi-Fi name on the 5 GHz radio.
- g. **Hide SSID:** Enable or disable the SSID (Wi-Fi Name)
- h. **Wireless Mode:** Set the 5GHz radio wireless version of the 802.11a/n interface
- i. **Channel Bandwidth:** Select the channel bandwidth of the 5 GHz radio. Selecting a wider channel such as 40 MHz maximises throughput and increase speed however is more prone to interference from overlapping channels. If there are issues try the 20 MHz, not as fast but travels further and has fewer overlapping channels.
- j. **Radio Channel:** Set 5 GHz radio channel, channels available on 5Ghz are 36, 40, 44, 48. (Default is Auto).
- k. **Extension Channel:** Auto
- l. **Fixed TX Rate Link Mode:** Set a fixed transmission bandwidth limit on the 5 GHz radio.
- m. **Authentication Method:** Set the authentication method for wireless clients. This can be set to open if you want no Wi-Fi encryption. (Default and standard setting set to WPA2-Personal)
- n. **WPA Encryption:** Enable the WPA encryption to encrypt the data (default is AES)

- o. WPA Pre-Shared Key:** This is the 5 GHz radio Wi-Fi password. It must be between 8 and 63 characters long. (Default is Gigawave)
- p. Network Key Rotation Interval:** This specifies the interval (seconds) after which a WPA group key is changed. (Can be left at 3600).
- q. TX Power Adjustment (%):** Set the 5 GHz radios antenna power. This can be raised or lowered based on the scenario. If there is a lot of interference from wireless devices the output power can be lowered accordingly. (Default is set to 100).
- r. Region Code:** Different regions have different regulations for Wi-Fi channels, adjust according to the region that the router is installed in. (Default is Europe channels 36, 40, 44, 48).

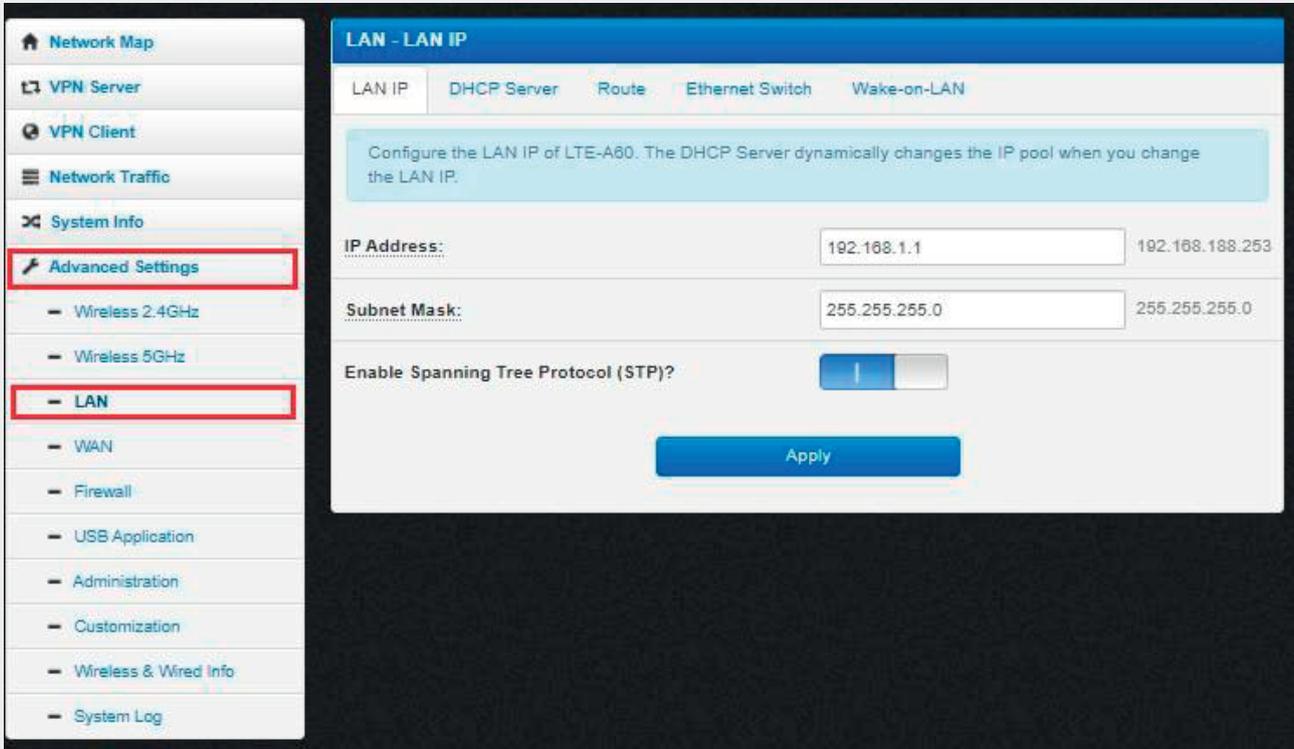
General users usually only need to change the SSID and Password (WPA Pre-Shared Key) to suit client's needs. See pics below:



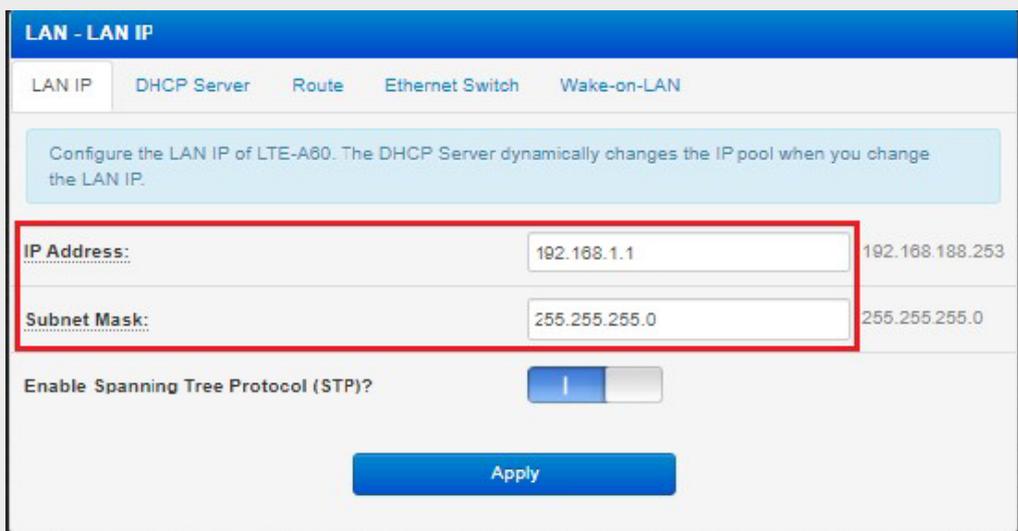
More advanced users can also click on the GuestAp tab next to General and enable a guest AP network. A guest Wi-Fi SSID and Password (WPA Pre-Shared Key) can be enabled from here. It can be scheduled and isolated from the main LAN network. With this option guests clients will not be able to see LAN device on the main LAN network. Advanced users also have Bridge, Wireless MAC Filter, RADIUS Settings and Professional settings. Settings in these tabs are outside the scope of this basic user guide.

# D - Setting up the routers LAN interface

1. Click on the LAN option under Advanced Settings on the left-hand menu of the homepage. This will open LAN IP settings page.



The default LAN IP address of the router is 192.168.1.1 with a subnet mask of 255.255.255.0. When this is changed the router will automatically adjust the DHCP server. Any devices connecting to the router on Wi-Fi or LAN will take a DHCP address automatically from the router based on the range that is specified here:



2. DHCP server settings can be configured by clicking on the DHCP Server tab, see image above. Manual change to the DHCP server can be configured here. The router will support 253 IP addresses for the local network, excluding the broadcast and network address. Manual DNS Server addresses can also be set on this page.

**LAN - DHCP Server**

LAN IP | DHCP Server | Route | Ethernet Switch | Wake-on-LAN

LTE-A60 supports up to 253 IP Addresses for your local network. The IP Address of a local machine can be assigned manually by the network administrator or obtained automatically from LTE-A60 if the DHCP Server is enabled.

**Enable DHCP Server?**

**Domain Name:**

**IP Pool Starting Address:**

**IP Pool Ending Address:**

**DHCP Lease Time (sec):**  [120..604800]

**Default Gateway:**

**DNS and WINS Server Setting**

**DNS Server 1:**

**DNS Server 2:**

**DNS Server 3:**

**WINS Server:**

3. More advanced feature such as IP routing, Bandwidth control per LAN port and Wake-on-Lan (wake up powered down LAN devices connected to the router) can be configured from the Route, Ethernet-Switch and Wake-On-Lan tabs. These advanced features are outside the scope of this manual.

## E - Configuring the routers WAN Settings

Several different connection types can be selected when connecting the router to the WAN. Addresses can be manually or automatically assigned. By default, the router is set to IPoE, when on this setting the router will automatically connect to the ISP. This page can be left as default unless user has specific IP addresses provided by the ISP to configure the router.

The following are some advance WAN settings that may be used by a typical user:

### Port Forwarding

This allows remote computers on the wan connect to a specific device or service within the LAN network. Port forwarding for CCTV etc should be configured here by setting the port forwarding rules.

1. UPnP is the first option on this page; this allows the automatic opening of ports when devices connected to the router also have UPnP enabled. It is not as secure as standard port forwarding.

Click on the Port Forwarding the tab; on this page the following settings may be changed:

- a. **Enable IGD UPnP?** Enable or disable the universal plug and play feature for port forwarding.
- b. **Support Protocols:** Select which protocol router uses for auto port forwarding. (default is UPnP)
- c. **Restrict forwarding rules only to their IP?** Select yes or no to restrict port forwarding only to devices they have UPnP enabled based on their static IP address.
- d. **Allow external Port range:** Select the range UPnP ports allowable to external devices.
- e. **Allow internal Port Range:** Select the range of UPnP ports allowable to internal devices on the LAN.
- f. **Autoclean Rules Interval (sec):** Select the amount of time in seconds to remove inactive UPnP port entries
- g. **Minimum Rules before Autoclean:** Select the minimum amount of UPnP entries before starting autoclean of inactive entries.

## 2. Setting up Manual Port Forwarding

Manual port forwarding can also be set up on this router allow users to open pre-defined ports to enable external access to internal devices on the LAN.

Service Name	Source IP	Port Range	Local IP	Local Port	Protocol
					TCP

a. **Enable Manual Port Forwarding?** Enable or disable the manual port forwarding feature. Below this is also the option to select a protocol from a well know list of server protocols or select a game from a well know list of game servers and this will auto populate entries in the port forwarding list based on what the user selects.

b. **Service Name:** Enter a reference name for your port forwarding rule.

c. **Source IP:** If a specific IP address is being used to port forward from, enter this here. Leave blank to port forward from anywhere. (default is left blank)

d. **Allow external Port range:** Select the range of external ports that the outside (external device is going to connect to).

e. **Local IP:** Enter the LAN IP address of the internal device that ports are being opened on.

f. **Local Port:** Select the internal port to be opened.

g. **Protocol:** Select the TCP or UDP protocol being used. Or select both to use both. UDP is connectionless, less secure (used for video, voip etc.) TCP is a connection orientated protocol which uses a 3-wayhandshake. More secure option especially for CCTV port forwarding. Click the plus sign to add your rule and press apply.

## DMZ

Click on the DMZ tab at the top of the WAN page to configure a DMZ. This will allow the user to expose one device on the local network to the Internet. All ports will be exposed to the outside internet. All inbound packets from the internet will be redirected to this devices IP. (Use with caution).

IP Address of Exposed Station:

## DDNS

Dynamic DNS allows the user to assign an internet domain name to a computer that doesn't have a static IP address. This is useful to access devices remotely whose IP address constantly changes. The DDNS service updates the IP address change periodically. This router supports entering the DDNS client information to access the router from outside the network.

**WAN - DDNS**

Internet Connection Port Forwarding DMZ **DDNS**

Dynamic DNS (DDNS) allows you to assign an Internet domain name to a computer with a dynamic IP Address. Currently, several DDNS services are embedded in LTE-A60.

Enable the DDNS Client?

Service Profile:

Host Name:

Host Name:

Host Name:

DDNS User Name or E-mail Address or Token:

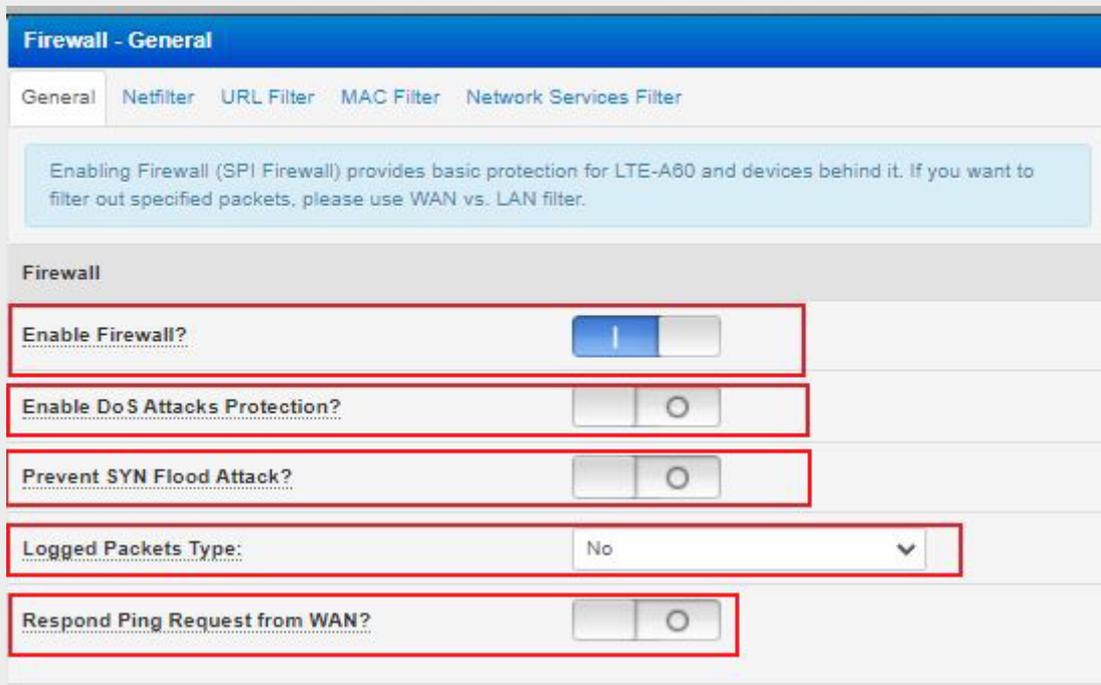
DDNS Password:

Use Secure HTTPS Connection?

Generally the only details the user will need to enter here is the DDNS service being used (www.no-ip.com, www.dyndns.org, www.easydns.com etc.), the hostname, and the username and password of the DDNS service. Free or paid accounts can be set up on many DDNS websites. When enabled user must also enable (Web Access from Wan?)In the Firewall menu under advanced settings.

# F - Configuring the routers Firewall Settings

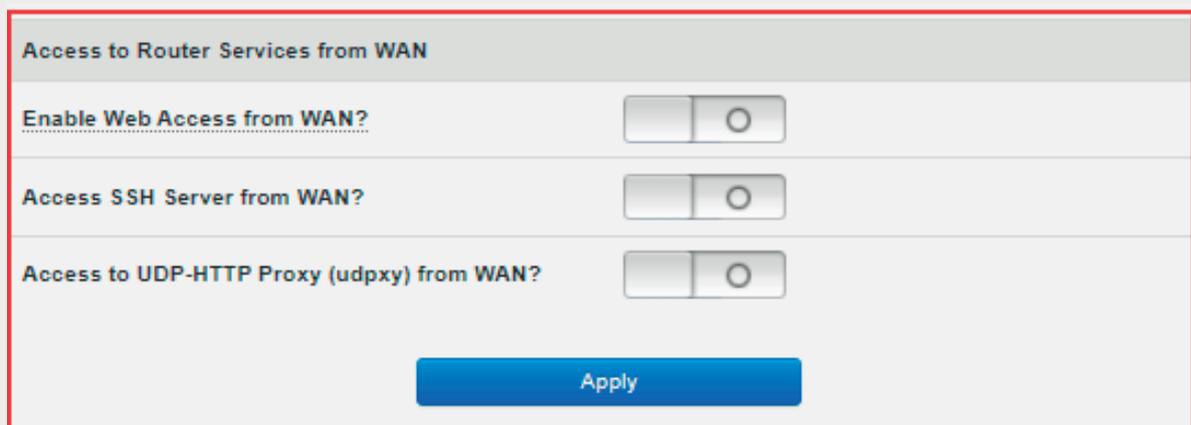
To configure these settings click on the Advanced Settings option on the left-hand side menu and click on Firewall. The basic Firewall on the router is enabled by default. To this provides basic protection for LAN devices behind the router from the internet.



The user can enable more advanced settings from the setting above for more protection:

- a. **Enable Firewall?** Enable or disable the basic firewall protection.
- b. **Enable DoS Attacks Protection?** This option once enabled will enable protection from Denial-of-service attacks from the internet.
- c. **Prevent SYN Flood Attack?** This option once enabled will prevent SYN floods (attempts to flood a system with requests in order to consume resources and disable it).
- d. **Logged Packets Type:** Select whether user wants the router to log dropped, accepted or all packets between the LAN and WAN.
- e. **Respond Ping Requests from WAN?** Enabling this option will mean the router will respond back to a "ping" that comes from outside your network. (Used generally for testing, turned off by default)

The routers services can also be accessed from the Wan. Settings relating to this can be configured on the bottom of the general firewall page. See pic below:

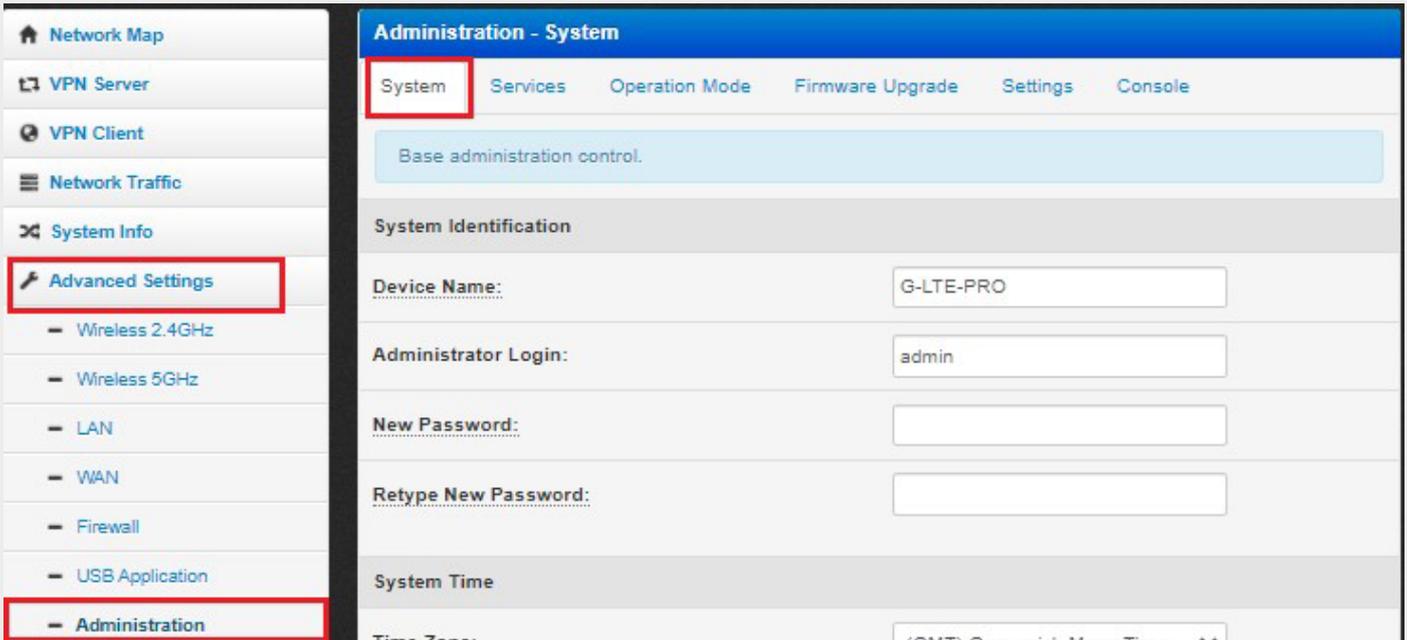


- a. **Enable Web Access from WAN?** Enable or disable remote access to the router from the wan. Once enabled select the port that the external device will use to connect to the router. This option must be enabled if using the DDNS service.
- b. **Access SSH server from WAN?** If a secure shell server is being used, this can also be accessed from the wan once this option is enabled. Once enabled select the port that the external device will use to connect to secure shell server.

More options for advanced users include Netfilter, URL Filter (block access to certain websites), MAC Filter (block certain mac addresses from accessing the router) and Network services are configurable. These options are outside the scope of this document.

# G - Router Administration settings

To configure the routers administration settings, click on the Advanced Settings Tab on the left-hand side menu and then click on Administration. From here users can configure system settings.



## System

The following settings can be configured from this menu:

- a. **Device Name?** This is the routers reference name. It will be what comes up on IP scanners etc when users are trying to find the device. (Default is G-LTE-PRO)
- b. **Administration login:** Username for logging into the router. (Default is admin)
- c. **New Password:** Password for logging into router. Password cannot be greater than 32 characters (default is gigawave).
- d. **Retype New Password?** Enter password confirmation.
- e. **Time Zone:** Enter the standard time zone for your country.
- f. **NTP Synchronization Period:** Select time interval that the router will sync the time with the NTP server.
- g. **NTP Server 1:** Enter the NTP server that the router will use to sync the time. (Default is time.windows.com)
- h. **NTP Server 2:** Enter backup NTP server for time sync if needed.
- i. **Remote Log Server:** This allows the user to enter a server address and port for remotely storing the log of the router.
- j. **Enable Syslog Floating Toolbar?** Select yes or no to show the log tab in the toolbar.
- k. **Enable context help:** Enable or disable tooltips.

## Services

Click on the service tab at the top of the administration menu to control various system services.

The screenshot shows the 'Services' configuration page. It is divided into three main sections, each outlined with a red border:

- HTTP Web Server:**
  - Web Server Protocol: HTTP (dropdown)
  - Port of Web Access from LAN: 80 (input field, with [80..65535] range indicator)
  - Restricting Web Access from LAN: No (\*) (dropdown)
- Terminal Services:**
  - Enable Telnet Server? (checked toggle)
  - Enable SSH Server? No (\*) (dropdown)
- Miscellaneous Services:**
  - LLTD (Link Layer Topology Discovery)? (checked toggle)
  - Cron Daemon (Scheduler)? (disabled radio button)
  - Hardware Watchdog Timer: (disabled radio button)

An 'Apply' button is located at the bottom center of the page.

On this services page the following settings can be configured:

- a. **Web server protocol?** This is the protocol that will be used when the router is accessed from a web browser. HTTP is default. When this option is selected with port 80 users will only have to type the routers ip address into the browser and they will automatically land on the router's admin login page. This can be changed to HTTPS or HTTP and HTTPS. HTTPS is more secure than HTTP. (Default is HTTP)
- b. **Port of Web Access from LAN:** This is the web port that will be used by browser to connect to the router. (HTTP default is 80).
- c. **Restricting Web Access from LAN?** Users have the option of blocking either wired or wireless lan clients from accessing the routers login page. (No is the default)
- d. **Enable Telnet Server?** Enable or disable the routers telnet server.
- e. **Enable SSH Server?** Enable or disable the routers secure shell server.
- f. **LLTD (Link Layer Topology Discovery)?** This enables network topology discovery. Provides a graphical map of the devices on the network.
- g. **Cron Daemon (Scheduler)?** Allows the scheduling of tasks on the router. For more advanced users. (Rarely used by standard users).
- h. **Hardware Watchdog Timer:** Enabling this option will reboot the router within the first 15 second of a system crash.

## Operation Mode

Click on the service tab at the top of the administration menu to control various system services.

**Administration - Operation Mode**

System Services **Operation Mode** Firmware Upgrade Settings Console

Wireless Router Mode (Default)  Access Point Mode (AP)

LTE-A60 connects to the Internet via IPoE/PPPoE/PPTP/L2TP protocol and provides Internet sharing for Wired/Wireless clients. In this mode, NAT, Firewall, UPnP, DHCP Server are available and enabled by default.

Wireless Clients G-LTE-PRO 4G Wireless Router Internet

Save

## Firmware Upgrade

The router can be upgraded with a firmware upgrade file provided by the manufacturer if needed. This firmware file can be uploaded to the router and after upgrade router will reboot.

**Administration - Firmware Upgrade**

System Services Operation Mode **Firmware Upgrade** Settings Console

Follow instructions listed below:

1. Download a proper version to your local machine.
2. Specify the path of and name of the downloaded file in the [New Firmware File].
3. Click [Upload] to upload the file to router. Uploading process takes about 2-3 minutes.
4. After receiving a correct firmware file, router will automatically start the upgrade process. The system reboots after the upgrading process is finished.

Firmware Version: 202010211110648

New Firmware File: Choose File No file chosen

Upload

**Note:**

1. For a configuration parameter existing both in the old and new firmware, its setting will be kept during the upgrade process.

## Settings

On this page users have various system options for defaulting and backing up config of the router.

Router Settings (NVRAM)	
Factory Default:	<input type="button" value="Reset"/>
Save Setting to a File:	<input type="button" value="Save"/>
Restore Settings from a File:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/>
NVRAM to Flash Memory Committing Mode:	Always after changes (*) ▼
Commit NVRAM Content to Flash Memory Now:	<input type="button" value="Commit"/>
Router Internal Storage (/etc/storage)	
Factory Default:	<input type="button" value="Reset"/>
Storage Backup:	<input type="button" value="Save"/>
Restore Storage from a Backup file:	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/>
Save Network Traffic History to Internal Storage?	Yes, w/o commit to flash (*) ▼
Save Current System Time to Internal Storage?	Yes (*) ▼
Commit Internal Storage to Flash Memory Now:	<input type="button" value="Commit"/>

The following options can be used for such tasks:

- Factory Default:** Restore the router completely to its default settings. Router will reboot after default is complete.
- Save Setting to a File:** Backup current router configuration to a file.
- Restore Settings from a File:** Use the file uploader to upload a previous backup configuration file to the router. Router will reboot after committed upload is complete.
- NVRAM to Flash Memory Committing Mode:** Write the config to —flash memory after changes are committed.
- Commit NVRAM Content to Flash Memory Now:** Commit to restoring backup. Wait while router reboots.

Router internal Storage options:

- Factory Default:** Factory default routers internal storage only.
- Storage Backup:** Backup current routers storage folder to the computer.
- Restore Storage from a Backup file:** Choose backup to restore a backup of the router's internal storage.
- Save Network Traffic History to Internal Storage?** Users can save the history of the routers network traffic to the internal storage of the router. (This is set to yes by default)
- Save Current System Time to Internal Storage?** When set to yes this will store the routers time configuration to the internal storage. (Yes, by default)

The last tab is the console of the router which is a more advanced feature not covered by the scope of this document.

Other advanced options include the System log of the router, log of wireless and wireless clients connecting to the router and led customization features which can be changed under the Advanced Settings section on the left-hand side menu of the router.