1. Inside the box

2. Your LTE Home Router

3. Setting Up Your LTE Router
   3.1 Positioning Your Router
   3.2 Setup Requirements
   3.3 Setting Up

4. Login to Your LTE Router
   4.1 Connect & Login by Mobile App
   4.2 Connect & Login by Computer

5. Web User Interface
   5.1 Home
   5.2 Wi-Fi Settings
      5.2.1 2.4GHz / 5GHz
      5.2.2 Guest
      5.2.3 WPS
   5.3 Parental Control
   5.4 Network
      5.4.1 Network Map
      5.4.2 Status
      5.4.3 LTE Traffic Query
      5.4.4 WAN
      5.4.5 LTE
      5.4.6 LAN
5.4.7 IPv6  
5.4.8 Client List  
5.5 Device Settings  
5.5.1 Admin Settings  
5.5.2 Date & Time  
5.5.3 Backup / Restore  
5.5.4 Firmware  
5.6 Diagnostic  
5.7 Security  
5.7.1 Firewall  
5.7.2 IP / MAC Binding  
5.7.3 Access Control  
5.8 NAT Forwarding  
5.8.1 DMZ  
5.8.2 UPnP  
5.8.3 ALG  
5.8.4 Virtual Servers  

6. Troubleshooting  

7. Technical Specification
1. Inside the box

Inside the product package you should find the following items. Contact Verizon if any item is missing or damaged.

- LTE Home Router
- Power Adapter
2. **Your LTE Home Router**

Your Verizon LTE Home Router provides fast dual-band Wi-Fi for all your devices, and features built-in network security as well as parental controls, guest Wi-Fi and automatic software updates.

Take a moment to familiarize with your product.
**Reset Button**

If you experience difficulties with your router or you want to revert all settings that you have changed, the reset function allows you to reset the router back to its factory default state. Press and hold the reset button for *4-7 seconds* to perform a factory reset (resets all settings back to factory defaults).

**WPS**

WPS is an easy way to add supported Wi-Fi devices to your network. Press the WPS button on the front of the router to activate WPS. You will need to activate WPS on your Wi-Fi device too. Refer to **5.2.3 Wi-Fi Settings > WPS** for more information.

**LEDs**

The LEDs indicate the system and connection status, and WPS activity.

<table>
<thead>
<tr>
<th>Indicator/Scenario</th>
<th>Description</th>
<th>Light type</th>
<th>LED2 (WPS)</th>
<th>LED1 (SYS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>System Off</td>
<td>Off</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power on</td>
<td>Blue</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Booting</td>
<td>Green, Slow Blinking</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Ready (Network searching)</td>
<td>Green, Slow Blinking</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firmware update</td>
<td>Green, Quick blinking (<em>only while firmware is being installed</em>)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Excellent LTE Signal Strength</td>
<td>Green</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Fair LTE Signal Strength</td>
<td>Yellow/Amber</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Poor LTE Signal Strength</td>
<td>Red</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wi-Fi / LTE / FW Error</td>
<td>Red, Slow Blinking</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No SIM Card</td>
<td>Red, Quick Blinking</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

https://www.verizonwireless.com/support/
<table>
<thead>
<tr>
<th>WPS</th>
<th>WPS Pairing</th>
<th>Existing Status</th>
<th>Factory Reset</th>
<th>Reset User data</th>
<th>Existing Status</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Blue, Quick Blinking (blinks until WPS times out)</td>
<td><img src="https://www.verizonwireless.com/support/" alt="Status" /></td>
<td>Yellow/Amber Quick Blinking (only for 2~3 seconds after pressing reset button until device restarts)</td>
<td><img src="https://www.verizonwireless.com/support/" alt="Status" /></td>
<td></td>
</tr>
</tbody>
</table>

**During Firmware Upgrade:**

<table>
<thead>
<tr>
<th>System Status</th>
<th>Light type</th>
<th>LED2 (WPS)</th>
<th>LED1 (SYS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download FW</td>
<td>No LED change</td>
<td>Existing Status</td>
<td>Existing Status</td>
</tr>
<tr>
<td>Reboot recovery</td>
<td>Green, Quick Blinking</td>
<td><img src="https://www.verizonwireless.com/support/" alt="Status" /></td>
<td></td>
</tr>
<tr>
<td>Initial boot</td>
<td>Blue</td>
<td><img src="https://www.verizonwireless.com/support/" alt="Status" /></td>
<td></td>
</tr>
<tr>
<td>FW updating</td>
<td>Green, Quick blinking</td>
<td><img src="https://www.verizonwireless.com/support/" alt="Status" /></td>
<td></td>
</tr>
<tr>
<td>Power On</td>
<td>Blue</td>
<td><img src="https://www.verizonwireless.com/support/" alt="Status" /></td>
<td></td>
</tr>
<tr>
<td>System Booting</td>
<td>Green, Slow blinking</td>
<td><img src="https://www.verizonwireless.com/support/" alt="Status" /></td>
<td></td>
</tr>
<tr>
<td>System ready</td>
<td>Green, Slow blinking</td>
<td><img src="https://www.verizonwireless.com/support/" alt="Status" /></td>
<td></td>
</tr>
<tr>
<td>(Network Searching)</td>
<td></td>
<td><img src="https://www.verizonwireless.com/support/" alt="Status" /></td>
<td></td>
</tr>
</tbody>
</table>

https://www.verizonwireless.com/support/
3. Setting Up Your LTE Router

Your Verizon LTE Router comes with a pre-installed SIM card and can be up and running in just a couple of minutes.

3.1 Positioning Your Router

For the best wireless signal transmission from the router to your network devices:

- Place the router in a central area.
- Keep the router away from metal obstructions and away from direct sunlight.
- Keep the router away from 802.11g or 20MHz only Wi-Fi devices, 2.4GHz computer peripherals, Bluetooth devices, cordless phones, transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment to prevent signal interference or loss.

3.2 Setup Requirements

To configure your wireless network via computer, you need a computer that meets the following system requirements:

- Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX/1000BaseTX)
- IEEE 802.11a/b/g/n/ac wireless capability
- An installed TCP/IP service
- Web browser such as Internet Explorer, Firefox, Safari, or Google Chrome
3.3 Setting Up

1. Plug the router into a power outlet with the included power adapter.

2. Wait for a couple of minutes for the router to power up and establish an LTE connection. The system LED should display a solid red, orange or green according to signal strength.

3. That’s it! You can connect your Internet devices to the router’s Wi-Fi networks named **LTE-Home-xxxx** (check your router’s product label for your unique Wi-Fi password). You can also connect Internet devices to your router by Ethernet cable, by connecting your device’s LAN ports.

4. Go to 3. **Login to your LTE Router** to login to your router and configure settings such as Wi-Fi security.

You should immediately change your Wi-Fi password and Web UI login password.
4. Login to Your LTE Router

You can log in to your router’s Web User Interface (Web UI) to access and change any of your router's settings and functions, such as Parental Controls and Wi-Fi security. You can also access network information such as connected devices and data usage.

You can log in to the Web UI using a computer or mobile app.

First connect your device to your router, then access the Web UI, as shown below.

Your router is pre-set with WPA2 security, but it is always recommended to change the default Wi-Fi password, as well as the Web UI login password.

4.1 Connect & Login by Mobile App

1. Scan available Wi-Fi networks with your mobile device:

2. Select either of the networks named WiFi-2.4G or WiFi-5G

3. Enter your password, which can be found on your router’s product label.

5. Log in using the default password (Check your router’s product label for your unique GUI Password).

6. Go to Wi-Fi Settings to change your Wi-Fi password and Device Settings > Admin Password to change your Web UI login password, and remember to save your settings.

7. Check 5. Web User Interface in this guide for more information about your router’s settings.
4.2 Connect & Login by Computer

1. Scan available Wi-Fi networks with your computer.

2. Select either of the networks named LTE-Home-xxxx (2.4G) or LTE-Home-xxxx (5G).

3. Enter your password, which can be found on your router’s product label.

4. If preferred, you can use an Ethernet cable to connect your computer to the router’s LAN port for configuration (instead of Wi-Fi). Simply connect the two devices’ LAN ports by Ethernet cable.

5. Open a web browser and enter the router’s default address http://192.168.1.1 in the address bar.

6. Log in to the Web UI using the default password (Check your router’s product label for your unique GUI Password).

7. Go to Wi-Fi Settings to change your Wi-Fi password and Device Settings > Admin Password to change your Web UI login password, and remember to save your settings.

8. Check 5. Web User Interface in this guide for more information about your router’s settings.
5. **Web User Interface**

Your router’s Web User Interface (Web UI) allows you to setup and configure its various functions. You can access the Web UI anytime by entering the router’s default address `http://192.168.1.1` in the address bar of web browser, or by using the Verizon Router App, on a device connected to the router. The default password could check your router’s product label for your unique GUI Password.

**Menu**

Use the left side menu to navigate:

- **Home**
- **Wi-Fi Settings**
- **Parental Control**
- **Network**
- **Device Settings**
- **Diagnostic**
- **Security**
- **NAT Forwarding**

**Save**

Remember to save your settings with the save button after making changes.
5.1 Home

The Home page shows your network status and key system information. Network Status should display **Connected** to indicate an LTE connection. If you don’t see this, check the router’s LEDs and refer to **Troubleshooting** for more help.

---

**System Information**

<table>
<thead>
<tr>
<th>Network Status</th>
<th>Displays the status of your router’s LTE connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WPS</td>
<td>The WPS status of your router is shown here, indicating whether WPS is active or off.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Your router’s public IP Address is displayed here.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Displays the MAC address of your router. A MAC Address is a unique fixed identifier for any device on a network.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Displays the current software version your router is running.</td>
</tr>
</tbody>
</table>
5.2 Wi-Fi Settings

The Wi-Fi Settings screen displays advanced settings for your router’s Wi-Fi as well as WPS settings. Your router is dual-band and uses two Wi-Fi frequencies (2.4GHz & 5GHz) for better wireless performance on your devices.
5.2.1 2.4GHz / 5GHz

> Wi-Fi Settings > 2.4GHz / 5GHz

You can edit advanced settings for 2.4GHz or 5GHz frequency bands by selecting the respective tab.

### 2.4 GHz Wi-Fi Settings

- **Wi-Fi 2.4G**: On
- **Wi-Fi Name (SSID)**: WIFI-24GHz
- **Wi-Fi Password**: *********
- **Security**: WPA/WPA2-PSK (Recommended)
- **Version**: Mixed WPA/WPA2
- **Encryption**: Mixed WEP/AES

### 5 GHz Wi-Fi Settings

- **Wi-Fi 5G**: On
- **Wi-Fi Name (SSID)**: WIFI-5GHz
- **Wi-Fi Password**: *********
- **Security**: WPA/WPA2-PSK (Recommended)
- **Version**: Mixed WPA/WPA2
- **Encryption**: Mixed WEP/AES

### Channel Settings

- **Mode**: 802.11a/b/g/n mixed
- **Channel**: Auto
- **Channel Bandwidth**: Auto

### 2.4 / 5 GHz Wi-Fi Settings

[Link to Verizon Wireless Support]

https://www.verizonwireless.com/support/
### Wi-Fi 2.4GHz/5GHz

**Toggle to enable or disable this Wi-Fi frequency.**

**Wi-Fi Name (SSID)**
This is the name of your Wi-Fi network for identification, also sometimes referred to as “SSID”. The SSID can consist of any combination of up to 32 alphanumeric characters.

**Hide SSID**
Check the box to hide your SSID. When hidden, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden SSID is typically more secure than a visible SSID.

**Wi-Fi Password**
Enter your Wi-Fi password. A complex, hard-to-guess key is recommended.

**Security**
Select a Wi-Fi security type from the drop-down menu. WPA/WPA2 is the default setting and the most secure. Security can be disabled by selecting None but this is not recommended.

**Version**
Select which version of security type to use. WPA2 is the most secure but not supported by all wireless clients. Selecting Mixed WPA/WPA2 ensures wireless client compatibility.

**Encryption**
Displays encryption type according to version. AES encryption is the default setting for WPA2, while Mixed TKIP+AES is default for Mixed WPA/WPA2.

### 2.4 / 5 GHz Channel Settings

**Mode**
Select the wireless standard used for the router’s Wi-Fi. 802.11b/g mixed means 802.11b and 802.11g wireless clients can connect to the router, 802.11g/n mixed means 802.11g and 802.11n wireless clients can connect to the router.

**Channel**
Select a wireless radio channel or use the default “Auto” setting from the drop-down menu. Changing radio channel can improve Wi-Fi signal depending on how crowded the channel is with other radio signals and interference.

**Channel Bandwidth**
Set the channel bandwidth: 20MHz (lower performance but less interference), 40MHz (better performance but likely more interference), or Auto (automatically select based on interference level).

### 5.2.2 Guest

> Wi-Fi Settings > Guest

https://www.verizonwireless.com/support/
You can setup additional “Guest” Wi-Fi networks (2.4GHz and/or 5GHz) so guest users can enjoy Wi-Fi connectivity without accessing your primary networks. The “Guest” tab displays settings for your guest Wi-Fi networks.

### Guest

- **Guest Network**
  - Toggle to enable or disable all guest networks.

- **2.4GHz / 5GHz Guest Network**
  - Toggle to enable or disable guest network for displayed frequency, either 2.4GHz or 5GHz.

- **Wi-Fi Name (SSID)**
  - This is the name of your Wi-Fi network for identification, also sometimes referred to as “SSID”. The SSID can consist of any

https://www.verizonwireless.com/support/
combination of up to 32 alphanumerical characters.

| **Hide SSID** | Check the box to hide your SSID. When hidden, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden SSID is typically more secure than a visible SSID. |
| **Wi-Fi Password** | Enter your Wi-Fi password. A complex, hard-to-guess key is recommended. |
| **Security** | Select a Wi-Fi security type from the drop-down menu. WPA/WPA2 is the default setting and the most secure. Security can be disabled by selecting None but this is not recommended. |
| **Version** | Select which version of security type to use. WPA2 is the most secure but not supported by all wireless clients. Selecting Mixed WPA/WPA2 ensures wireless client compatibility. |
| **Encryption** | Displays encryption type according to version. AES encryption is the default setting for WPA2, while Mixed TKIP+AES is default for Mixed WPA/WPA2. |
5.2.3 WPS
> Wi-Fi Settings > WPS

Wi-Fi Protected Setup (WPS) is a simple way to establish connections between WPS compatible devices. WPS can be activated on compatible devices by pushing a WPS button on the device or from within the device’s firmware/configuration interface (known as PBC or “Push Button Configuration”). When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. “PIN code WPS” is a variation of PBC which includes the additional use of a PIN code between the two devices for verification.

Follow the instructions on screen.
The **Parental Control** feature allows you to restrict Internet access to selected devices on your network at specified times e.g. disabling Internet access for a child’s smartphone.

1. Click **Add New** to add and setup a new device for parental controls.
2. Toggle **Enable This Entry** to enable/disable this parental control setup.
3. Toggle **Schedule Internet Access** to enable/disable the schedule for Internet access.
4. Select a device from the Client menu or enter the MAC address manually below.

5. Specify a Device Name and enter a Description of the device for easy reference.

6. Click to select and specify which days to apply the parental control restrictions, and set the start and end times.

7. Click **Save** to save the schedule and the device’s Internet access will now be restricted according to the schedule.
5.4 Network

The **Network** menu provides quick links to the networking functions of your router. When you select the Network menu, the Network Map page is displayed as below.
5.4.1 Network Map

The **Network Map** provides a visual overview and status information of the network and devices on the network, with quick links to LAN & WAN settings and connected device / client lists. Green check marks indicate everything is working correctly.
Network Status displays the status of the network across six categories: Internet v4, Internet v6, LTE, LAN, Wireless & System Information.

<table>
<thead>
<tr>
<th>Internet (V4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Subnet Mask</td>
</tr>
<tr>
<td>Default Gateway</td>
</tr>
<tr>
<td>Primary DNS</td>
</tr>
<tr>
<td>Secondary DNS</td>
</tr>
<tr>
<td>Connection Type</td>
</tr>
</tbody>
</table>

Internet v4 Displays IPv4 Wide Area Network WAN information about your router's LTE connection. IPv4 is the default Internet protocol widely used across the Internet.
Internet v6
Displays IPv6 Wide Area Network WAN information about your router’s LTE connection. IPv6 is an alternative Internet protocol which is not yet widely supported. To setup IPv6 go to Network > IPv6.

LTE
Displays LTE information including signal strength. To edit LTE settings go to Network > LTE.

LAN
Displays the router’s Local Area Network (LAN) information including MAC Address, IP Address and Subnet Mask, and DHCP Server status. To edit LAN settings go to Network > LAN.

Wireless 2.4GHz & 5GHz
Displays your router’s Wi-Fi information for both 2.4GHz & 5GHz frequencies. Includes network name (SSID) and radio & channel information. To edit these Wi-Fi settings go to Wi-Fi Settings.

System Information
Displays system identifiers unique to your hardware.
### LTE Traffic Query

**Traffic Query** displays your network data usage, with upload, download and total traffic displayed in MB. Ensure that your router’s date and time settings are correct in **Device Settings > Date / Time** for accurate Monthly usage information.

<table>
<thead>
<tr>
<th>Monthly Usage</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upload</strong></td>
<td>00.36MB</td>
</tr>
<tr>
<td><strong>Download</strong></td>
<td>623.34MB</td>
</tr>
<tr>
<td><strong>Total Traffic</strong></td>
<td>673.70MB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Current Usage</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Query Range</strong></td>
<td>2020-05-04 00:00 - 00:59</td>
</tr>
<tr>
<td><strong>Upload</strong></td>
<td>50.36MB</td>
</tr>
<tr>
<td><strong>Download</strong></td>
<td>623.34MB</td>
</tr>
<tr>
<td><strong>Total Traffic</strong></td>
<td>673.70MB</td>
</tr>
</tbody>
</table>
5.4.4  WAN

The WAN Settings screen allows you to configure the settings of various Wide Area Network (WAN) connection types.

**WAN Type**

**Connection Type:** Choose your Internet Service Provider type: Dynamic IP or Static IP – and enter the appropriate IP Address, Subnet Mask and Default Gateway if using Static IP. Consult your ISP if the router is unable to obtain a valid IP address or if you are unsure the WAN connection type.

**Dynamic IP Advanced Settings**

**DNS Address:** Allows this router to get the DNS IP address from the ISP automatically or you can specify preferred primary and secondary DNS address. A DNS is a host on the Internet that translates Internet names to numeric IP addresses.
LTE settings are pre-configured by default. You can disconnect the LTE connection using the Disconnect button if needed, and the connection and SIM status are displayed accordingly. It’s not recommended to modify APN Setting unless instructed by your ISP.

## LTE Settings

### LTE Status

<table>
<thead>
<tr>
<th>Internet Status</th>
<th>Connected</th>
</tr>
</thead>
</table>

| SIM Status   | Ready   |

### APN Setting

<table>
<thead>
<tr>
<th>APN</th>
<th></th>
</tr>
</thead>
</table>
The **LAN Settings** page allows you to configure your router on your Local Area Network (LAN). You can specify a static IP address for your router, and configure your router as a DHCP server to assign IP addresses to other devices on your LAN.

### Basic

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>5e:6e:e5:fa:72:3e</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.0.0.1</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

### Advanced

<table>
<thead>
<tr>
<th>DHCP</th>
<th>Off</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address Pool</td>
<td>192.168.1.100 - 192.168.1.150</td>
</tr>
<tr>
<td>Address Lease Time (Hours)</td>
<td>24</td>
</tr>
<tr>
<td>Primary DNS (Optional)</td>
<td></td>
</tr>
<tr>
<td>Secondary DNS (Optional)</td>
<td></td>
</tr>
</tbody>
</table>

**Basic**

- **MAC Address**: Displays the MAC address of your router. A MAC address is a unique fixed identifier for every device on a network.
- **IP Address**: Specify the IP address here. This IP address will be assigned to your router and will replace the default IP address.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask</td>
<td>Specify a subnet mask. The default value is 255.255.255.0</td>
</tr>
<tr>
<td>Advanced</td>
<td></td>
</tr>
<tr>
<td>DHCP</td>
<td>Toggle the switch to enable or disable DHCP server.</td>
</tr>
<tr>
<td>IP Address Pool</td>
<td>Enter the start and end IP address of the IP address range which your router’s DHCP server will assign to devices on the network.</td>
</tr>
<tr>
<td>Address Lease Time</td>
<td>Enter an address lease time in hours. IP addresses will be assigned for this period of time before being reassigned.</td>
</tr>
<tr>
<td>Primary DNS Address</td>
<td>Enter a primary DNS address.</td>
</tr>
<tr>
<td>Secondary DNS Address</td>
<td>Enter a secondary DNS address.</td>
</tr>
</tbody>
</table>
This wireless router supports IPv6 addressing: a system that supports more IP addresses. This standard is not yet widely available. Contact your ISP to setup IPv6 if your Internet service supports it.

### IPv6 Settings

<table>
<thead>
<tr>
<th>IPv6</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN</td>
<td></td>
</tr>
<tr>
<td>Profile Name</td>
<td></td>
</tr>
</tbody>
</table>

**WAN DHCP Settings**

- **DNS Address**
  - Dynamically from ISP
  - Use the following DNS Addresses

**Primary DNS**

**Secondary DNS**

**LAN Settings**

- **IPv6 Delegation**
  - On

- **IPv6 Address**

- **IPv6 Prefix Length**

- **IPv6 Address Type**
  - SLAAC+DHCPv6
  - SLAAC+DHCPv4
  - DHCPv6

- **Life Time (Weeks)**
  - 600
5.4.8 Client List

> Network > Client List

Displays all devices (clients) connected to your router, by Ethernet (LAN) or Wi-Fi (wireless) e.g. laptops, smartphones. The device name, MAC address and IP address is listed for each device.

**Client List**

<table>
<thead>
<tr>
<th>LAN</th>
<th>Wi-Fi</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**KD**

MAC Address: 80:1F:02:9C:8F:FF
IP Address: 192.168.1.121
Various administrative functions of your router can be configured from the Device Settings menu, including the Web UI login password, router date & time settings, backup, router firmware and system logs.
5.5.1 Admin Settings
> Device Settings > Admin Settings

The **administration** function allows you to change the login password for the router’s Web UI. It’s essential to change this password for the security of your router. Use hard-to-guess password which include combinations of numbers, letters and symbols, and change your password regularly.

1. Enter the current password for authentication.

2. Enter your name password in the New Password field and again to confirm, and choose **Save** to save the new settings.
5.5.2 Date & Time

Set the **date and time** for your router. You can use a Simple Network Time Protocol (SNTP) which synchronizes the date and time with public time servers, or the router can get the date and time automatically based on your selected time zone.

### Date / Time Settings

<table>
<thead>
<tr>
<th>Mode</th>
<th>Automatically</th>
<th>SNTP</th>
</tr>
</thead>
</table>

**Gateway Current Time**: 2020 May 04 21:28

1. Select Automatically or SNTP for the mode.
2. For automatic, select your time zone from the drop-down menu.
3. For SNTP, to synchronize date and time with public time servers, enter the NTP Servers.

Examples of commonly used NTP Servers include time.microsoft.com or time.google.com.
5.5.3 Backup / Restore

Device Settings > Backup / Restore

The Backup / Restore page enables you to save/backup the router’s current settings as a file to your local computer, or restore your router to previously saved settings by loading a backed up file. You can also reset the router back to factory default settings. If the router malfunctions or is not responding, then it is recommended that you first reboot the device, and if still experiencing problems reset the device back to its factory default settings. You can reset the router back to its default settings using the Reset button on the back of the router (press and hold for 4-7 seconds).

---

**Backup**

Save A Copy Of Your Current Settings.

---

**Restore**

Restore saved settings from a file

---

**Factory Default Restore**

Revert All The Settings To Their Default Values.
### Backup

Save a copy of your current settings  Displays the MAC address of your router. A MAC address is a unique fixed identifier for every device on a network.

### Restore

Restore saved settings from a file  Choose Select File to locate a previously saved settings file on your computer and select it to load the file to your router.

### Factory Default Restore

Revert all the settings to their default values.  Select Factory Restore to revert your router to it's original factory default state. This resets all settings.
5.5.4 Firmware

> Device Settings > Firmware

The Firmware page displays your router’s firmware version information. Firmware is the software that your router runs on. You can click Check For New Version to manually initiate a check to see if new firmware is available.

<table>
<thead>
<tr>
<th>Software Version</th>
<th>201824</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applied On</td>
<td>04/28/2020 00:45:01 UTC</td>
</tr>
</tbody>
</table>

Check For New Version
5.6 Diagnostic

You can run Ping & Traceroute diagnostic tests with the router. Enter the IP address to use for the test and click Start, results are displayed in the box.
Use the **Security** menu to configure various security functions if needed, including Firewall, IP/MAC Binding and Access Control.
5.7.1 Firewall
> Security > Firewall

The router features a built-in firewall that provides protection to your network from unauthorized intrusions from the Internet. The firewall features four modules which can be enabled or disabled using the switches.

**Firewall Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPI Firewall</td>
<td>On</td>
</tr>
<tr>
<td>DoS Protection</td>
<td>Off</td>
</tr>
<tr>
<td>WAN Block Ping</td>
<td>On</td>
</tr>
<tr>
<td>LAN Block Ping</td>
<td>Off</td>
</tr>
</tbody>
</table>

**SPI Firewall**
Stateful Packet Inspection (SPI) firewall protection means only packets matching a known active connection will be allowed by the firewall, and others will be rejected. An SPI firewall goes beyond stateless filtering and checks an entire packet’s content rather than only packet headers. This is a security feature to help distinguish between legitimate packets of information and potentially harmful packets, and provides greater security for your network.

**DoS Protection**
Denial-of-Service (DoS) is a common form of malicious attack against a network. The router’s firewall can protect against such attacks.
by filtering unreasonable packets that could flood and disable network with large amounts of traffic.

**WAN Block Ping**
When active the router will not answer ping requests from the Internet. This can increase security as pinging is a common method used by hackers to test networks.

**LAN Block Ping**
When active the router will not answer ping requests from the local network. This can increase security as pinging is a common method used by hackers to test networks.
5.7.2 IP / MAC Binding

> Security > IP / MAC Binding

IP/MAC Binding allows you to reserve a static IP address for a device on the network, rather than being assigned a new (dynamic) IP address by the router’s DHCP Server every time the device connects to the router. Static IP addresses can be useful for using various services on the local network. Every device is identified by a unique MAC address, and the IP address can be bound to the MAC address.

**IP/MAC Binding Settings**

1. Switch IP/MAC Binding on using the toggle switch.
2. Click **Add New** to setup a new client for IP/MAC Binding.
3. Select a device from the Client menu or enter the MAC address manually.

4. Specify the IP Address the client will use, and enter a Description of the device for easy reference.

Add New

Enable This Entry

Client

MAC Address
AA:BB:CC:DD:EE:FF

IP Address
192.168.1.254

Description

You will need to disconnect and reconnect the device to the router for the IP binding settings to take effect.

Cancel Save
5.7.3 Access Control
> Security > Access Control

Access Control is a security feature that can help to prevent unauthorized users from connecting to your router. You can define a list of network devices permitted (whitelist) or denied (blacklist) to connect to the router. Devices are each identified by their unique MAC address or IP address.

### Access Control Settings

- **Access Control**: [ ]

- **Access Mode**
  - [ ] Blacklist
  - [ ] Whitelist

- **Binding List**
  - [ ] Add New
  - [ ] Delete All

**Smartphone**

MAC Address: F4:F5:DB:D9:81:F9
IP Address: undefined

1. Switch Access Control on using the switch.
2. Select Blacklist (not permitted) or Whitelist (permitted), and click Add New.
3. Select a device from the Client menu or enter the MAC address manually.
4. Enter the Name of the device for easy reference.
Functions in the **Network Address Translation (NAT) Forwarding** menu can improve network performance and security.
5.8.1 DMZ

> NAT Forwarding > DMZ

A Demilitarized Zone (DMZ) is an isolated area in your local network where a computer runs outside the firewall and receives/intercepts all incoming Internet traffic. This can provide an extra layer of security to the rest of the network, or can be useful if a network client PC cannot run an application properly from behind an NAT firewall. However since it opens the client up to unrestricted two-way access this computer is vulnerable. DMZ should be configured only by expert network users aware of the security risks.

**DMZ Settings**

1. Use the switch to set DMZ to **active**.

2. Enter the IP Address of the computer to provide the DMZ service (ensure this computer is using a Static IP Address).
5.8.2 UPnP

Universal plug-and-play (UPnP) is a set of networking protocols which enables network devices to communicate and automatically establish working configurations with each other, such as computers, printers, mobile devices etc.

It's typically used for data sharing, communications and entertainment purposes, although sometimes not preferred due to security concerns. Some devices may require UPnP to be enabled to function properly. Use the switch to set UPnP to active or inactive, according to your requirements.

UPnP Settings
5.8.3 ALG
> NAT Forwarding > ALG

**Application Level Gateway (ALG)** settings are advanced functions that can resolve issues where services are disrupted by the firewall. Each ALG module is a security component that augments the firewall. Services such as VPNs or Virtual Servers may require ALG modules enabled. By default all ALG modules are active. Use the switches to disable any ALG module required. ALG Settings are recommended for expert users only.

SIP ALG may disrupt Wi-Fi calling for cellphones connected to the network.

**ALG Settings**

- **PPTP Pass-through**
- **L2TP Pass-through**
- **IPSec Pass-through**
- **FTP ALG**
- **TFTP ALG**
- **RTSP ALG**
- **SIP ALG**

**Manage ALG Settings**

- **PPTP Passthrough**
  - Point-to-Point Tunneling Protocol (PPTP) is a module for implementing virtual private networks.

- **L2TP Passthrough**
  - Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs.
<table>
<thead>
<tr>
<th>Protocol Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec Passthrough</td>
<td>Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.</td>
</tr>
<tr>
<td>FTP ALG</td>
<td>File Transfer Protocol is a widely and commonly used method of exchanging files over IP networks. The FTP ALG monitors PORT, PASV, and 227 commands. It performs NAT on the IP, port, or both in the message and gate opening on the device as necessary.</td>
</tr>
<tr>
<td>TFTP ALG</td>
<td>Trivial File Transfer Protocol (TFTP) is a simple protocol used for files transfer (RFC 1350). TFTP is implemented on top of UDP, with destination port 69 as the well-known port. The TFTP Application Layer Gateway (ALG) processes TFTP packets that initiate the request.</td>
</tr>
<tr>
<td>RTSP ALG</td>
<td>The Real Time Streaming Protocol (RTSP) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.</td>
</tr>
<tr>
<td>SIP ALG</td>
<td>The Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging all over Internet Protocol (IP) networks.</td>
</tr>
</tbody>
</table>
5.8.4 Virtual Servers
> NAT Forwarding > Virtual Servers

This function allows you to set up an internet service on a local computer, without exposing the local computer to the internet. Internet traffic is directed to a specific port or range of ports on a device or devices on your local network. You can also build various sets of port redirection, to provide various internet services on different local computers via a single internet IP address. It also allows PCs outside the network to access services provided by a computer in the local network.

Virtual Servers Settings

1. Click Add New and enter the parameters to setup a virtual server:
<table>
<thead>
<tr>
<th>Service Type</th>
<th>Specify the service type e.g. HTTP, FTP etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Port</td>
<td>Specify the external/public port to access the computer on your local network.</td>
</tr>
<tr>
<td>Client</td>
<td>Select whether to manually assign Internal (Private) IP &amp; Port.</td>
</tr>
<tr>
<td>Internal IP</td>
<td>Enter the IP address of the computer on your local network.</td>
</tr>
<tr>
<td>Internal Port</td>
<td>Specify the internal/private port you wish to use on the computer in your local network.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select the connection protocol: TCP, UDP or All.</td>
</tr>
</tbody>
</table>
6. Troubleshooting

If you are experiencing any trouble, try here first for some quick fixes to common problems.

Dropped Wi-Fi connection
Wi-Fi connections can occasionally drop for any number of reasons, such as interference or system updates. Try to ensure the space between your router and Wi-Fi devices is as clear as possible and make sure you’re not moving too far away from your router. Check that your router has a good LTE connection and that your Wi-Fi device isn’t trying to connect to any other saved Wi-Fi networks.

Can’t connect to Wi-Fi
If your router’s Wi-Fi doesn’t appear when scanning available networks on your device, or if you can’t make a connection, try switching both your router and Wi-Fi device off and back on again, and move closer to your router. If your router has a good LTE connection and you still can’t establish a Wi-Fi connection, try a factory reset. Press and hold the router’s reset button for 3-7 seconds and wait a few minutes to restart before trying again.

Can’t login to the Web UI
If you can’t access the Web UI, it might be an issue with your device or computer’s proxy or IP address settings. Make sure that proxy settings are disabled and that your device or computer can be allocated an IP address on the network by the gateway’s DHCP server. You’ll need to check the support for your device or computer’s operating system e.g. Windows, macOS, for detailed instructions how to do this.

Where can I get more help?
Visit https://www.verizonwireless.com/support/ to find your nearest Verizon store or for 24/7 help with live chat and device-specific support.
## 7. Technical Specification

### General

<table>
<thead>
<tr>
<th>Technical Standard</th>
<th>3GPP LTE, LTE Category 12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency band</td>
<td>LTE FDD: B2, B4, B5, B13, B48, B66</td>
</tr>
<tr>
<td>Wi-Fi Standard</td>
<td>802.11 a/b/g/n/ac</td>
</tr>
<tr>
<td>Dimensions (L x W x H)</td>
<td>170 mm x 124 mm x 43.4 mm</td>
</tr>
<tr>
<td>Operating temperature range</td>
<td>-20 – 45 °C</td>
</tr>
<tr>
<td>Storage temperature range</td>
<td>-40 – 85 °C</td>
</tr>
</tbody>
</table>

### Connections

<table>
<thead>
<tr>
<th>DC Input</th>
<th>12V / 2A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>RJ-45 LAN * 2, RJ-45 WAN * 1</td>
</tr>
</tbody>
</table>
Federal Communication Commission Interference Statement

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 equipment 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 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.

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

Radiation Exposure Statement

The product complies with the FCC portable RF exposure limit set forth for an uncontrolled environment and are safe for intended operation as described in this manual. The further RF exposure reduction can be achieved if the product can be kept as far as possible from the user body or set the device to lower output power if such function is available.