VISION PLUS
5G MI-FI ROUTER

23-2740/5G

This Modem Uses a Micro SIM card

Introducing the VisionPlus 5G router with Qualcomm Snapdragon X62 5G chipset: A Powerhouse of Connectivity. This top-tier 5 G chipset, equipped with cutting-edge capabilities and a 4nm process chip, delivers lightning-fast download speeds and rock-solid connections.

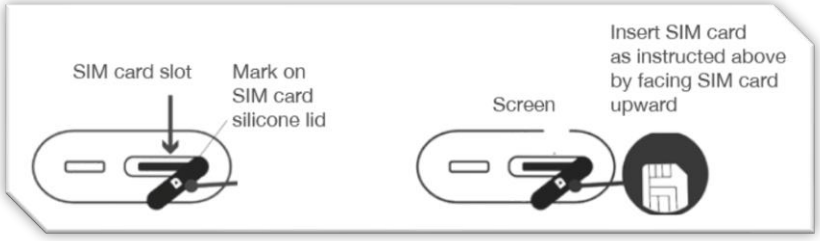
Improved privacy and Security with Advanced DNS Protection.
This system prioritises your online security and privacy in several ways:

- **DNS Choice:** You can select your preferred DNS service or use the secure, built-in default option, "Cloudflare for Families," which provides robust protection against known malware websites and increased privacy.
- **Cloudflare's Advanced DNS Security:** Benefit from Cloudflare's renowned speed, reliability, and security features, including advanced DNS security that safeguards your online privacy by preventing eavesdropping and data manipulation by malicious actors.
- **Latest Wi-**Fi encryption standards WPA3-SAE (Simultaneous Authentication of Equals) is a Wi-Fi security protocol that enhances password protection by using strong cryptographic key exchange, even with weak passwords. It also prevents eavesdropping and offline dictionary attacks.
- **Time Synchronization with Cloudflare NTP:** For added reliability and security, the system also utilises Cloudflare's NTP service for accurate time synchronization.

Next-Gen Wi-Fi 6 for Optimal Performance
Experience the future of Wi-Fi with the latest standards. Equipped with Wi-Fi 6 AX and robust WPA3-SAE encryption, this router ensures the fastest speeds and unparalleled security. WPA3-SAE's password-based authentication method is highly resistant to dictionary and brute force attacks, while additional security features safeguard against vulnerabilities like KRACK and EAP attacks.
Versatile Power Options
Enjoy the flexibility of multiple power options. The USB connection is compatible with standard 5V USB supplies, while the built-in battery pack provides up to 2.5 hours of uninterrupted usage for on-the-go connectivity.
Category 22 Class High-Speed Mi-Fi Router with Battery Backup
This powerful Mi-Fi router, designed for high-speed performance, features battery backup for extended usage and two external TS9-type connectors for enhanced antenna compatibility.
Carrier Aggregation: Combining Carriers for Faster Speeds
Carrier aggregation allows multiple wireless carriers to be combined into a wider channel, providing faster data speeds and improved network capacity. Consider combining multiple highway lanes into one wider lane, allowing more cars to pass through simultaneously.

Before connecting your mobile router, get to know its features. This includes understanding its LCD screen, the icons displayed, the buttons you can use, and the available ports.
The router comes with a USB-C charging cable. It also has a USB-C port for power that can also be used for CDC Ethernet connection on Windows or Linux platforms, so you can connect your computer directly to the router using a USB-C cable instead of Wi-Fi. This direct connection is called tethering. It also has two TS-9 connectors for an external antenna.

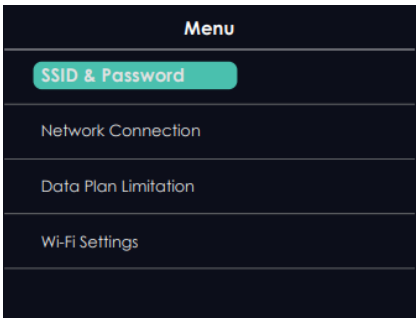
The power button is on the right side of the router labelled. 
Hold for 5 seconds to turn on or off.
Before inserting a Nano-SIM card, ensure the device is turned off.
Open the cover on the right side of the micro-SIM card slot.
Gently push the Nano-SIM card into the SIM card slot. Put the cover back in place.



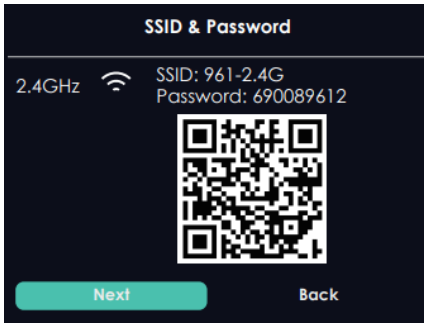
LCD SCREEN

The LCD screen shows basic functional information like speed, SMS received, battery, signal, and data used. It has an uncomplicated menu system that can be navigated using the down and select buttons on the side, just above the power button. The ▼ key scrolls between each menu and using the select key to choose that menu or option, the screen scrolls to the bottom and back to the start.\

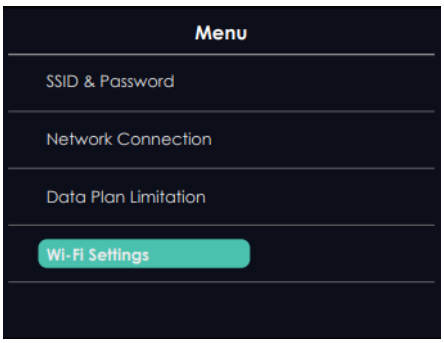
SSID & password



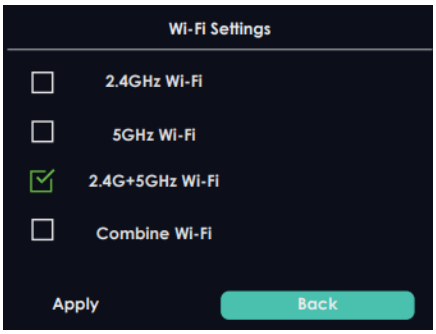
From here, you can see the SSID and password of the wi-fi; this also shows a QR code that you can scan using your phone, connecting you to the Wi-Fi. If there are two SSID (2.4G and 5G), selecting next will display the other Wi-Fi details. You can also scan the QR code to connect to the Wi-Fi automatically.



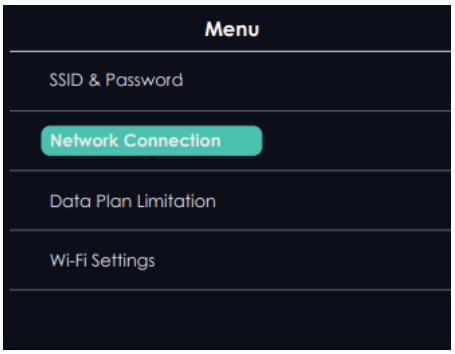
Wi-Fi Settings.



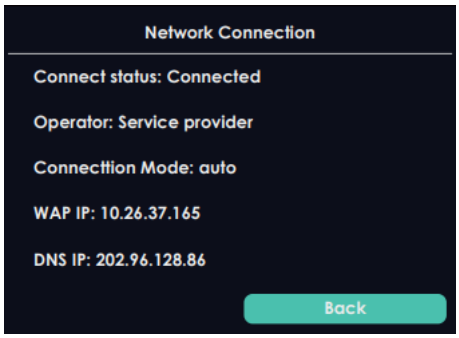
You can activate or deactivate and combine 2.4GHz and 5GHz Wi-Fi from here.



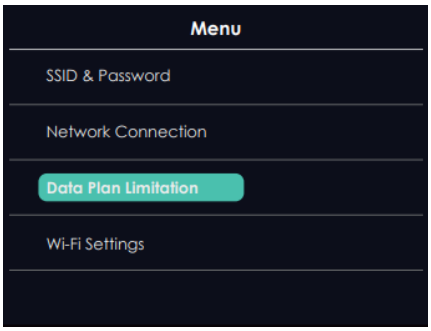
Network connection.



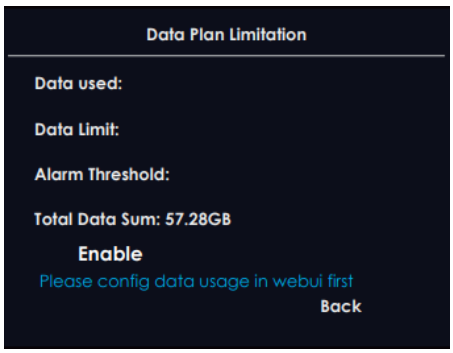
Displays the connection status, the SIM operator, the selected connection mode, and the IP numbers for WAP and the DNS in use.



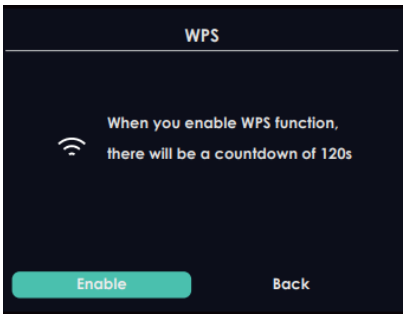
Data Plan Limitations



This shows the approximate amount of data used and if you are currently roaming.



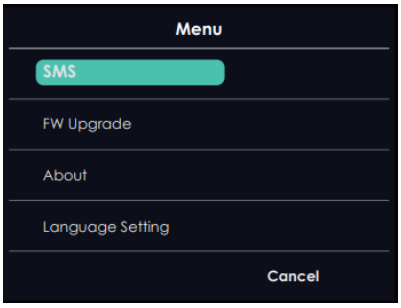
WPS



If you have set the WPS option in settings, you can use this section to activate WPS mode to connect your devices using the WPS functionality.

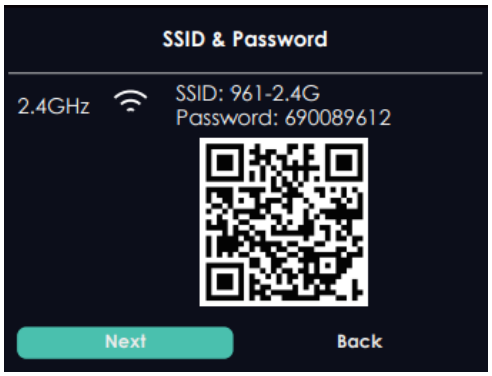
SMS

Allows you to read but not reply to text messages.
After logging in to the interface, you can reply to messages within the User Interface.



You can set up your VisionPlus 5G router using a computer, Laptop (Windows, MAC or Linux), Tablet, or Mobile phone (Android or Apple).

1. **Connect to the 5G router's Wi-Fi on your device.**
   To display the QRCode, use the select and down buttons on the side of the router, select the SSID & Password option, and scan the QRCode on the router's front screen. Ensure there are no reflections on the screen; you may need to move to somewhere darker and move the camera around before the QRCode reader scans it.



If you can't use the QR code you can connect to the router in the usual way, select the SSID (Name of Wi-Fi) which will begin VisionPlus2.4G-xxxx on your device. enter the password 12345678, which is the setup password.

1. Launch a web browser from your device that is connected to the mobile router via USB or WiFi.
2. Enter http://192.168.8.1 or type http://my.5g.device or scan this QR code.

Scan for Setup Interface

The mobile router web page displays.

3. Enter the administrator login password. The default password is printed on the product label.

If you are struggling to connect to the setup interface,
Turn the mobile data option on your phone off while setting the router up.

APPLE


ANDROID

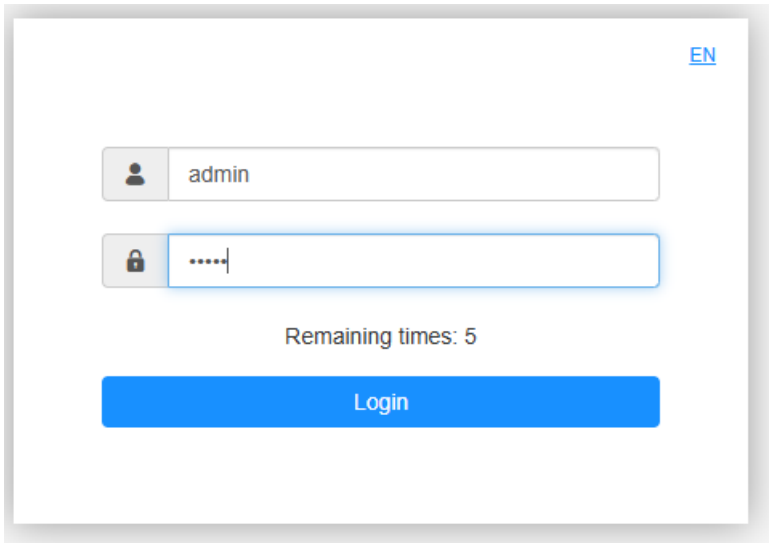
The password is case-sensitive. If this is the first time you have logged into the screen, you will be forced to create a personal password for both Wi-Fi and the admin Login password. For security we suggest a mixture of:

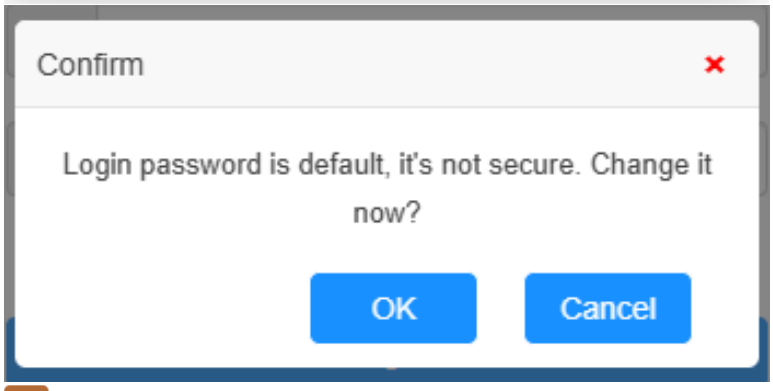
- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Symbols (e.g., !@#$%^&*)
- No spaces
- 8 minimum and 16 maximum characters"
- If you forget the password, you must factory reset the router.

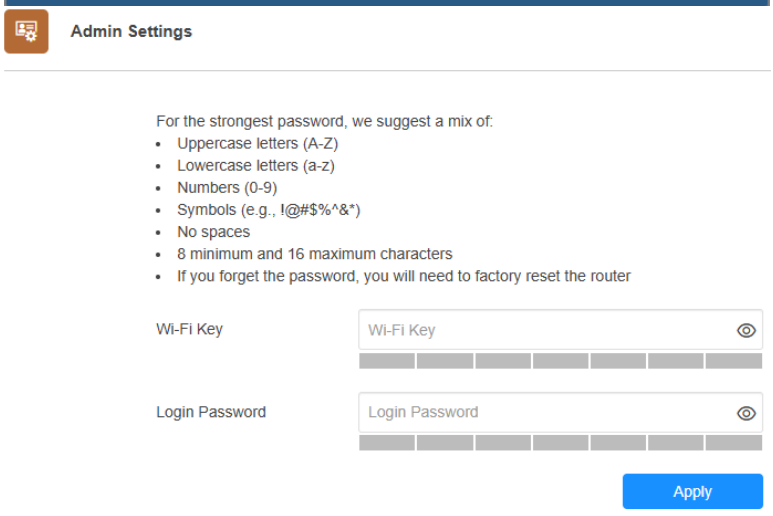
For initial setup the username and password are admin for both (admin admin).

Login Screen

Do not lose the password, or you will have to factory reset the router, which will cause all your settings to be lost.

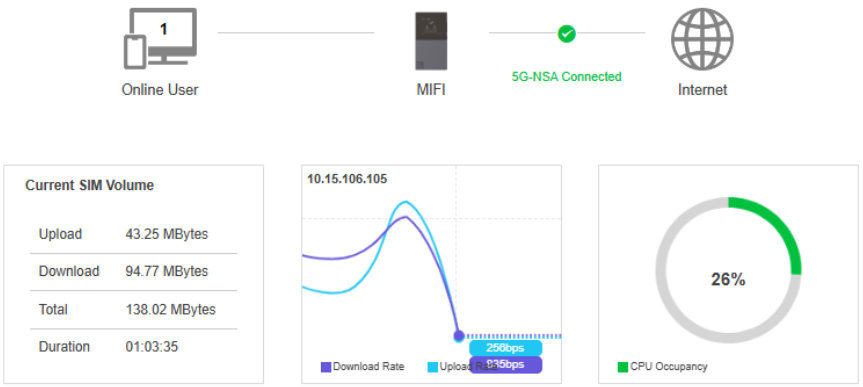




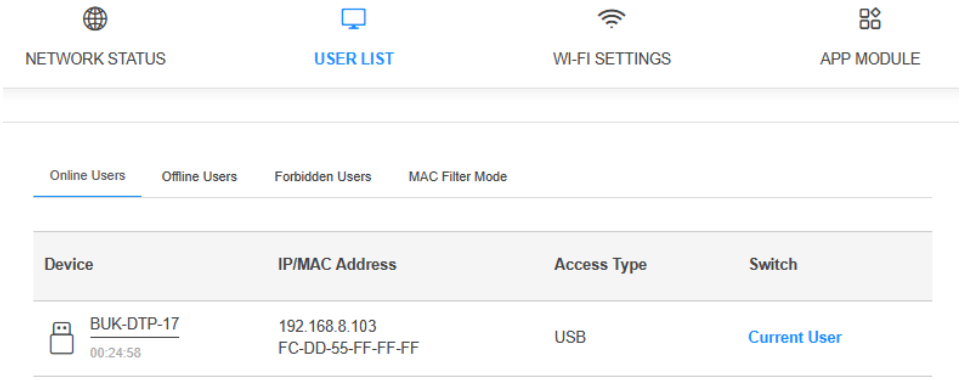


Information Screen

This is the default screen once you have logged in. It shows the connection status and how you are connected. In the image below, we are connected using the Wi-Fi repeater mode, and one person is connected to the router.

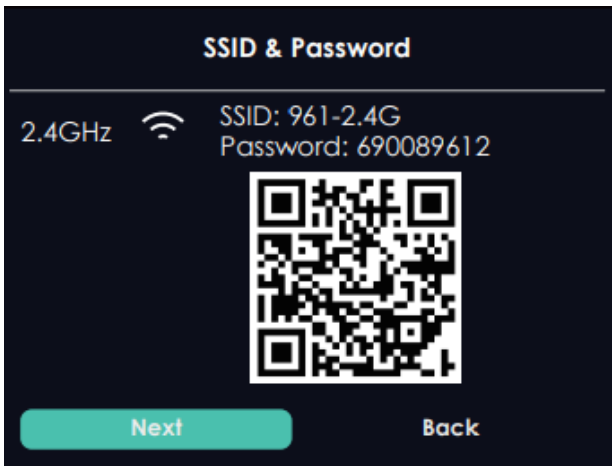


Selecting the next tab to the right, called User List, shows the ID of the devices connected.
In this example, you can see one PC, its allocated IP address and MAC address, and how they are connected—in this case, via a USB cable.
The smaller tabs give information on:
Offline Users: Devices that were previously connected.
Forbidden Users: The ability to ban users by MAC address.
MAC filter Mode: The ability to blacklist (ban) or whitelist (approve) users by MAC address.



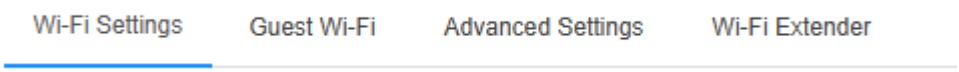
The next main tab is called **Wi-Fi Settings.**

The default SSID (Name of the Wi-Fi) is VisionPlus2.4G-XXXX and VisionPlus5G-XXXX
The Wi-Fi password will be the password you set initially.
It can also be found on the front screen by selecting the SSID & Password option.

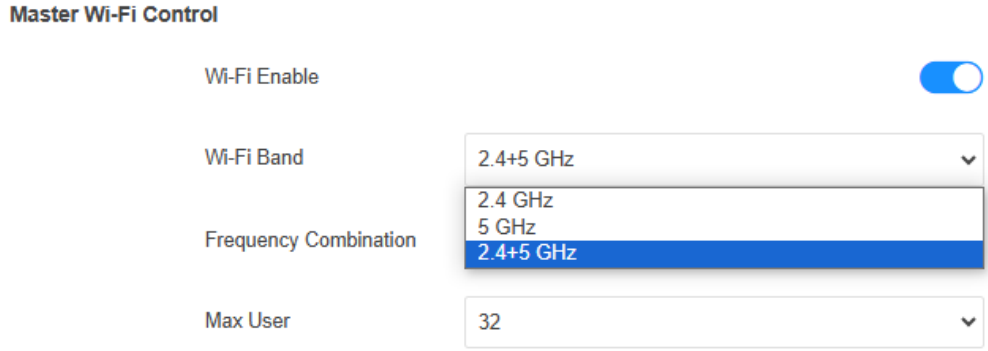


You can change both the SSID (Name of Wi-Fi) and password (Wi-Fi Key).
For the strongest password, we suggest a mix of:

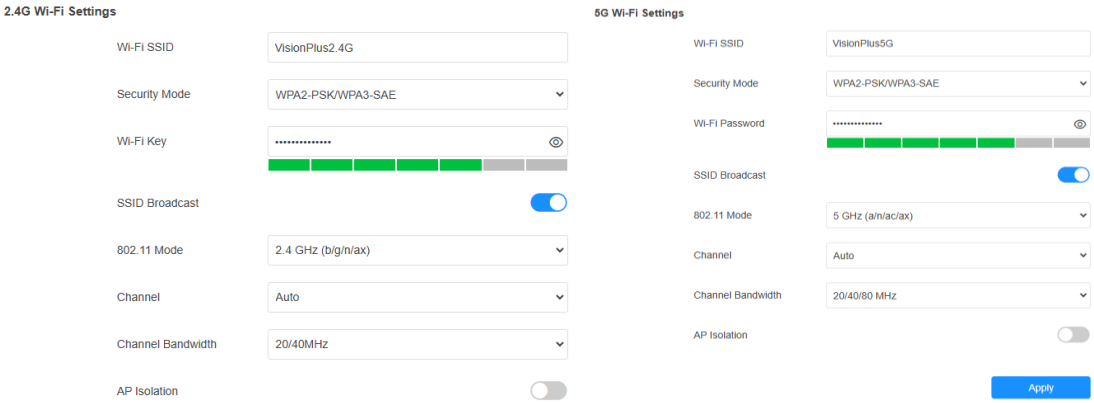
- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Try **not** to use special character symbols (e.g., !@#$%^&*)
- No spaces
- 8 minimum and 16 maximum characters”
- If you forget the password, you must factory reset the router.



Master Wi-Fi control.
Here, you can turn the Wi-Fi signal on or off and independently for each band.
For example, if you do not need both the 2.4G and 5G Wi-Fi bands, you can switch one off independently of the other.
You can also limit the number of connections to the Wi-Fi (Max Users).



Wi-Fi Enable: Switch the Wi-Fi signal for 2.4G and 5G off.
Wi-Fi band: You can select only 2.4G, only 5G or both.
Frequency combination: This combines the 2.4G and 5G with the identical SSID and Password, making it appear as just one signal. Your device will be offered the best band depending on signal strength.
Some devices only work on 2.4G and cannot distinguish between the 2.4G and 5G SSID, so they won't work with this function switched on.



2.4G & 5G Wi-Fi Settings See pages 22 and 23 for details and tips for this section
Wi-Fi SSID: name (SSID, Service Set Identifier) of the Wi-Fi.
Security Mode. WPA3 is the most secure, but not all devices are compatible.
Check with the manufacturer of the device you wish to connect to.
The Wi-Fi key: This is the Wi-Fi password. It must be at least 8 characters long and try not to use special characters such as # % and " $ ₷ as these can prevent devices from connecting to the Wi-Fi.
A green bar indicates how good your password is.
SSID Broadcast: This feature hides the Wi-Fi SSID and can be used for security. However, you must manually enter the

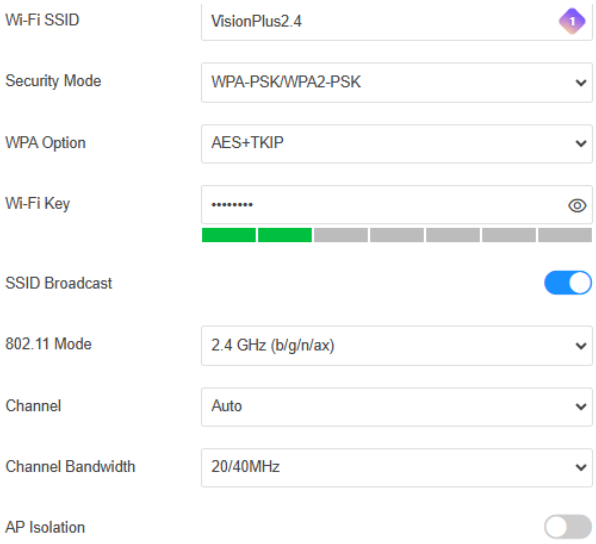
802.11 Mode: See **page 22** for more details on this
2.4b offers the slowest speeds, with a maximum theoretical speed of 11 Mbps.
2.4g is essentially the same as 2.4b but 54 Mbps maximum speeds.
2.4n offers a significant speed improvement, with a maximum theoretical speed of up to 300 Mbps.
2.4ax Wi-Fi 6 offers the fastest speeds. Note that real-world speeds will typically be much lower than the theoretical maximum of 573 Mbps
Channel: Use a Wi-Fi scanner app on your phone or computer to find the least crowded Wi-Fi channel. These apps show nearby networks and their channels. Choose a channel with the fewest neighbouring networks. See **page 23** for best practice on selecting the best channels.
Channel Bandwidth: In crowded areas with a lot of frequency noise and interference, a single 20MHz channel will be more stable. 40MHz channel width allows for greater speed and faster transfer rates, but it does not perform as well in crowded areas
AP Isolation: AP Isolation protects the device against attacks from another device in the same network.

5GHz **a** (802.11a): This is the oldest standard for 5 GHz Wi-Fi,
However, due to its limitations, it's rarely used today.

5GHz **n** (802.11n): This standard allows routers that support it to use the 5 GHz and 2.4 GHz bands. It offers significant speed improvements over 5GHz a, reaching up to 300 Mbps.

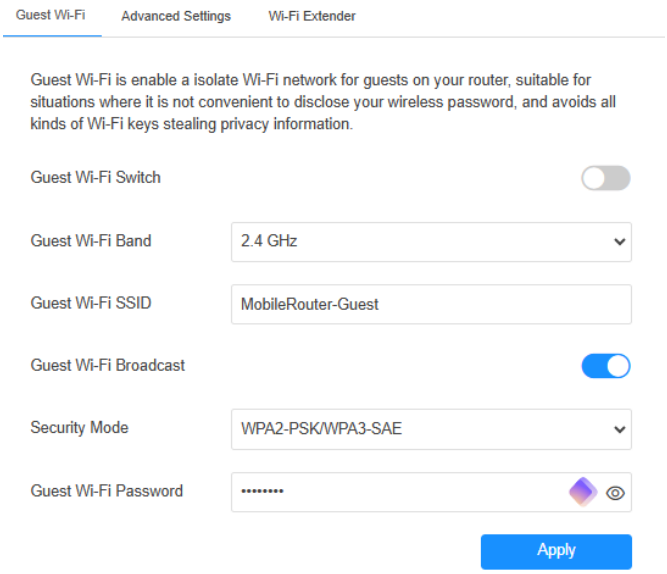
5GHz **ac** (802.11ac) uses wider channels and improved modulation techniques for faster data transfer. Most modern routers support 5GHz ac.

5GHz **ax** (802.11ax) is the latest standard. It improves AC by better handling multiple devices simultaneously and increasing network efficiency.



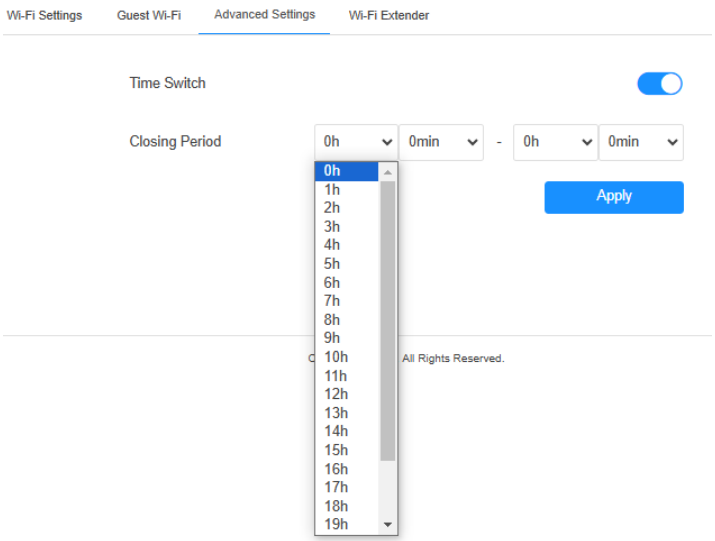
Guest Wi-Fi

A guest Wi-Fi network allows you to create a separate wireless signal with its own password, distinct from your primary Wi-Fi. This is particularly useful for occasions like parties or gatherings, where you want to provide internet access to guests without sharing your main Wi-Fi password. Once the event is over, you can simply turn off the guest network to revoke access. Setting up a guest Wi-Fi is as straightforward as configuring a regular Wi-Fi network, typically done through your router's settings. This feature enhances security, keeps your main network private, and offers convenient control over guest access.



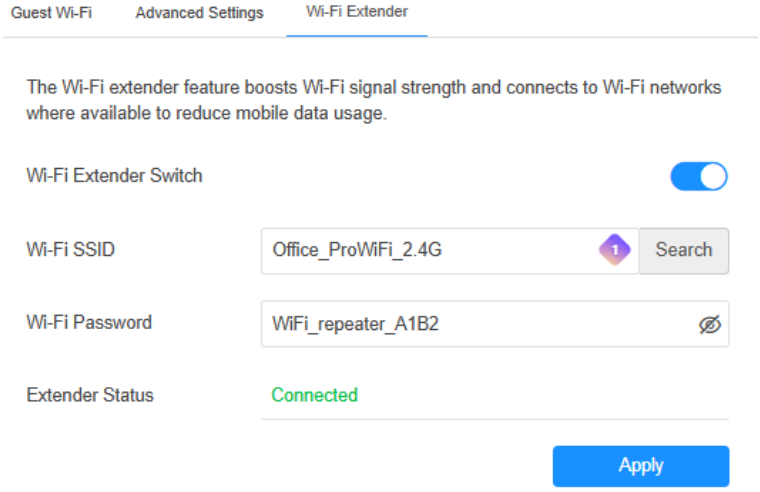
Advanced Settings

This lets you switch Wi-Fi on and off, automatically, at a preset time.
Before using, ensure you have selected the correct time and zone in N.T.P.
First, set the Wi-Fi off time, then choose the Wi-Fi on time.



Wi-Fi Extender.

A Wi-Fi extender receives a Wi-Fi signal (2.4GHz or 5GHz) from a router and rebroadcasts it within the router's coverage area. This is particularly useful for sites with existing Wi-Fi, helping to strengthen and stabilise the connection. The extended network will retain your SSID and password for seamless access..

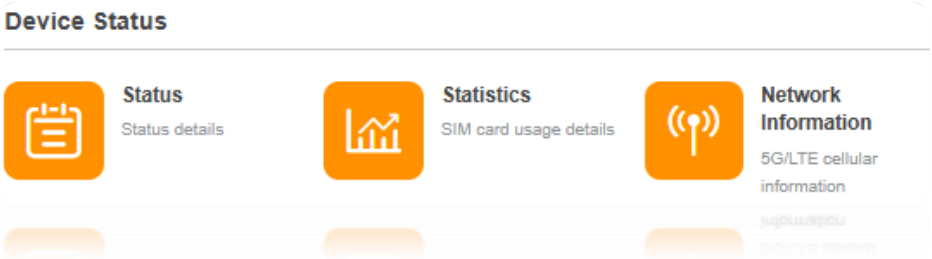


Please note this works with Wi-Fi that uses a simple username and password.

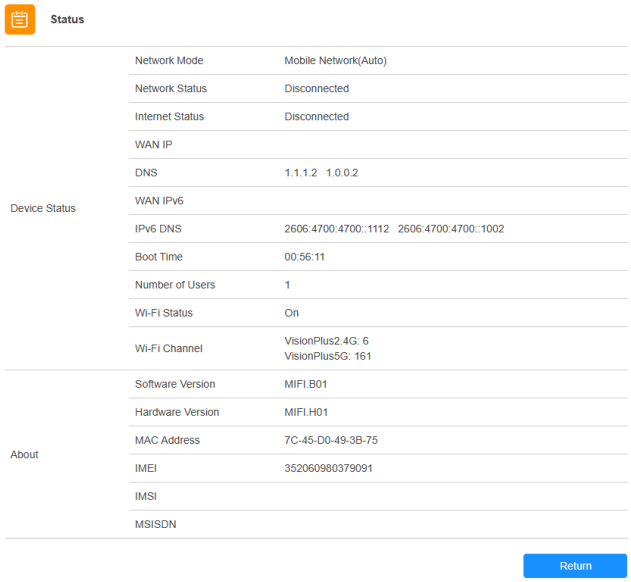
If the Wi-Fi has a customised login page (captive portal), this may not function as expected.
When using a Wi-Fi repeater, you may find that you cannot enter the captive portal, so you cannot connect to the hotspot or access the Internet. In this case, please try the following solutions.

1. Use Auto DNS (Found in the DHCP & DNS section)
2. Do not use VPN
3. Do not use AdGuard or similar
4. Use your web browser to visit a webpage; you should be redirected to the captive portal automatically.
5. Connecting to a captive portal using a Wi-Fi repeater can sometimes be tricky due to how captive portals work. Here are some tips to make the process smoother:
6. Place the repeater within a strong signal range of the Wi-Fi source with the captive portal to ensure reliable communication.
7. Connect to the Captive Portal Network Directly
   Before setting up the repeater, connect a device (e.g., your phone or laptop) directly to the captive portal network.
8. Log in or accept the terms to authenticate your access.
9. Once authenticated, the repeater should be able to connect without further authentication.
10. Access the Repeater's Settings
11. Open the configuration page for the repeater (usually accessible via its IP address, such as 192.168.x.x).
12. Log in using the admin credentials.
13. Scan and Select the Captive Portal Network
    Use the repeater’s Wi-Fi scan feature to find the captive portal network.
14. Select it and connect using any necessary credentials, if prompted by the repeater’s interface.
15. 5. Test Device Authentication
16. If the captive portal prompts for individual device authentication, connect one device to the repeater's extended network.
17. Open a browser and complete the login or agreement process.

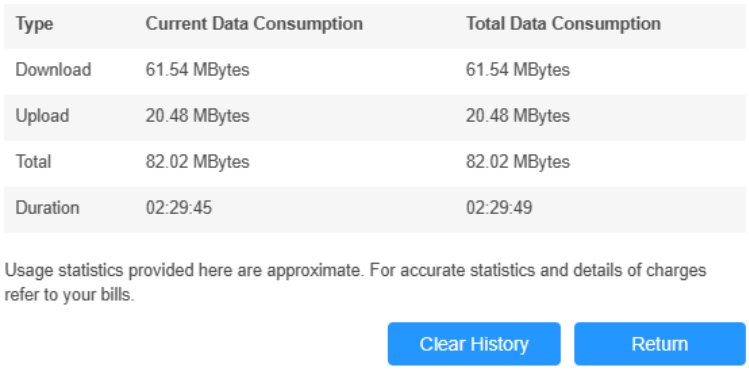
If you are using a smartphone but your web browser doesn't redirect you to the captive portal, please turn off your smartphone's Wi-Fi and mobile data, turn the Wi-Fi back on, and reconnect to your router's Wi-Fi again.
The captive portal should pop up directly after you enter the Wi-Fi password.
Some Wi-Fi networks may have a stringent verification policy. If the solution does not work, you should consult with the Wi-Fi provider's staff to see if they can add the router's MAC address to their "Whitelist" directly.



This section is for operational information only

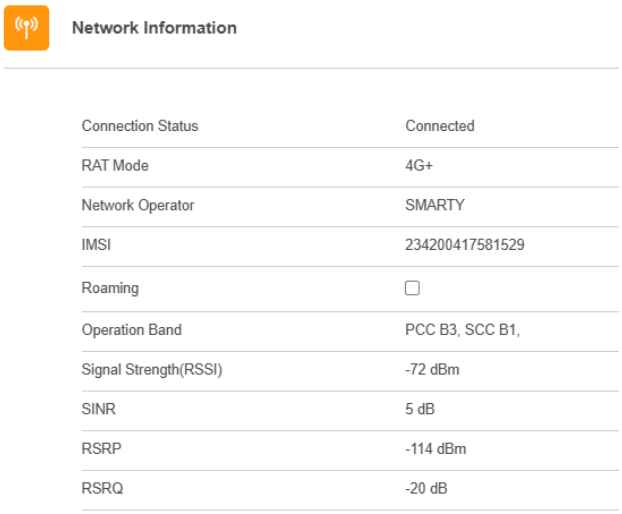


Details of how the router is connected and setup (information only)



Details on the approximate data consumption of the cellular data.

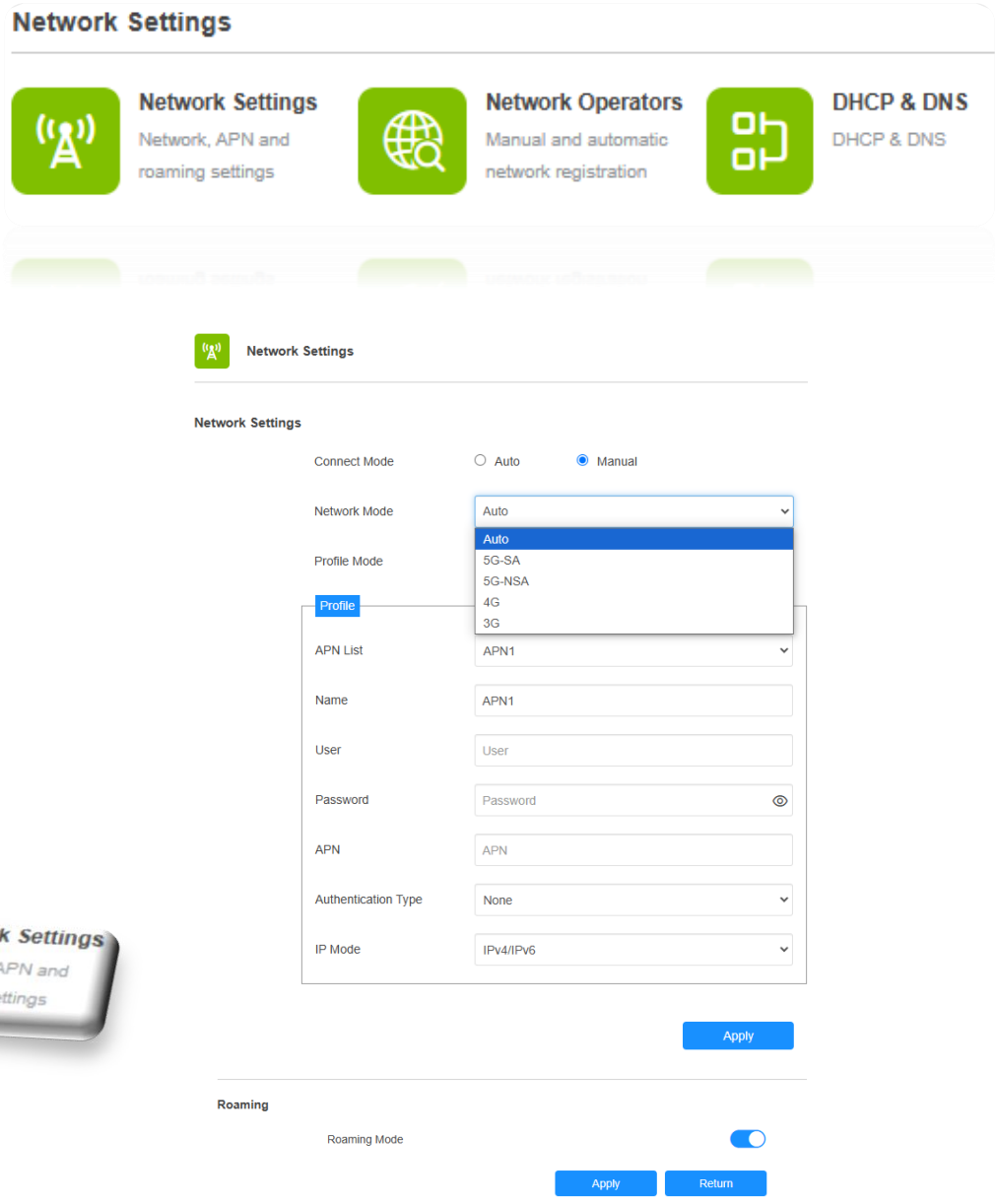
Showing the approximate upload, download totals and duration that the router has been switched on.
for more accurate details of data consumption please refer to your bill or if available your providers app.



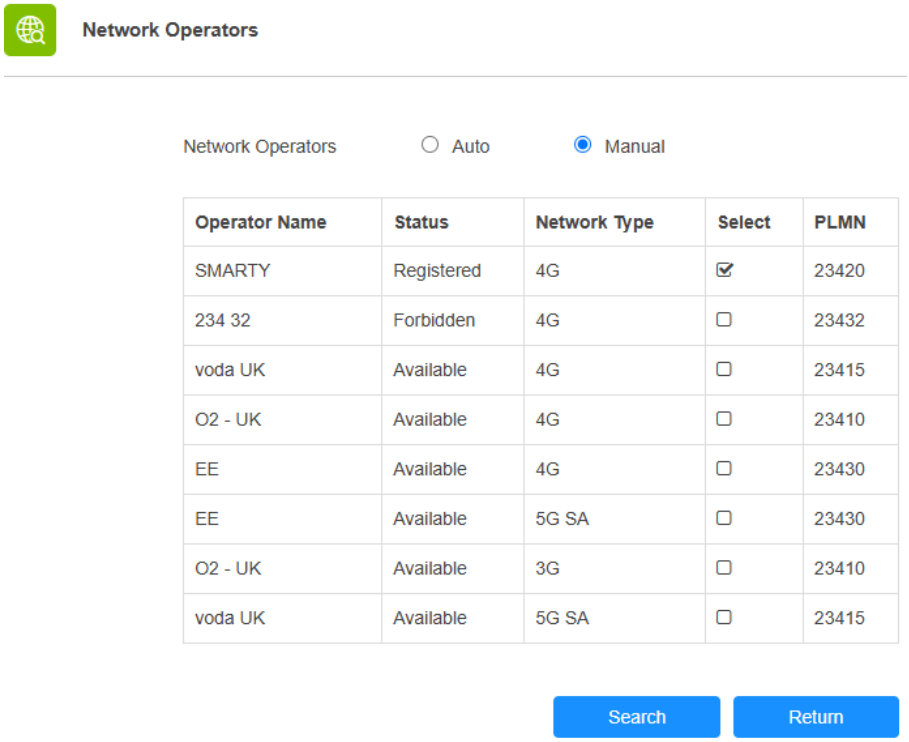
Shows the connection status and signal levels.
The network mode (RAT): Unique ID for network mode.
There are various RATs, each with its characteristics and capabilities. Common examples include:

- **GSM**: Global System for Mobile Communications (2G)
- **3G**: Universal Mobile Telecommunications System (3G)
- **4G**: Fourth generation of mobile technology, fast speeds and smooth online experiences
- **4G+**: combines multiple 4G signals to increase data speeds when 5G isn't available.
- **5G**: a fifth generation of cellular network technology, offering faster speeds, lower latency

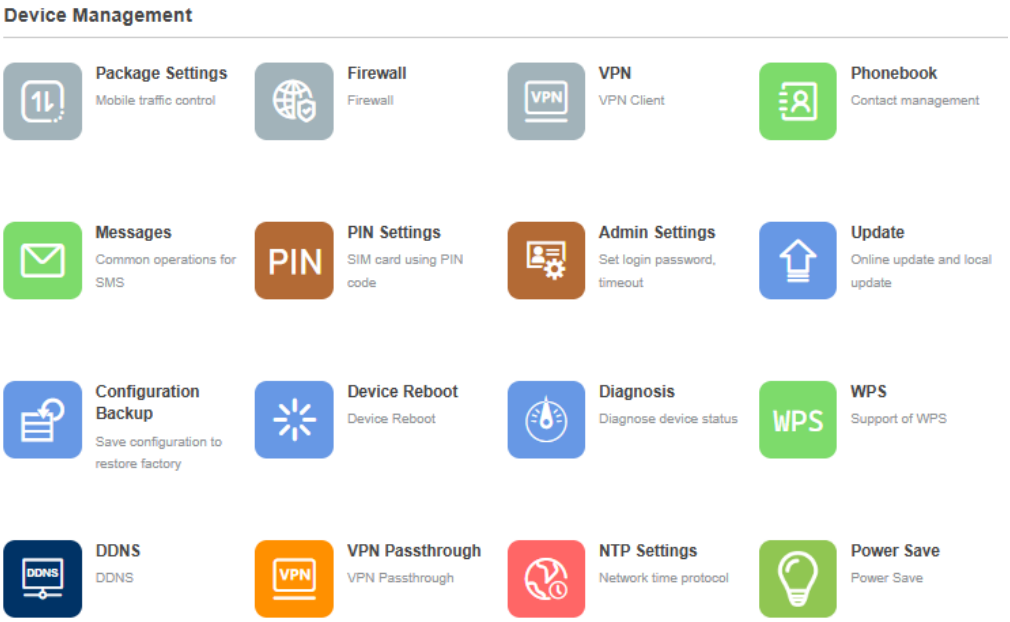
The Network operator: Name for the network operator.
IMSI number: Unique ID for mobile device
Roaming: SIM card access to a network outside the home area (Check with the operator for added charges!).
Operation band: The band in which the router is operating.
Signal levels: (RSSI, SINR, RSRP and RSRQ) See page 21 for details on Signal levels



Network mode: Auto /Manual to lock to either 3G, 4G or 5G network signals.
Most UK cellular networks are included within the 5G router.
If your SIM is not identified, you can set up the APN manually by selecting Manual in profile mode and entering the APN. These details can usually be found on the SIM provider's website or by contacting the provider directly.
Roaming Mode: Tick roaming and ensure your SIM is enabled for roaming. Check with the SIM provider regarding extra charges associated with roaming in other countries.



This scans for other mobile operators within the area.
It helps detect other networks available in the area which may be useful when choosing a SIM for the area.



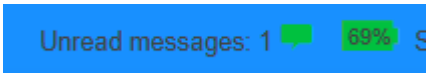
We recommend leaving the IP allocation method as the default (DHCP) unless you have specific requirements for manual IP assignment. The default IP address range is 192.168.8.*, and the router's IP is 192.168.8.1.
You can change the DNS settings from default (Cloudflare, for families) to manual and choose your preferred DNS service. Example, you could use Google DNS (8.8.8.8), OpenDNS (208.67.222.222) or Quad9 (9.9.9.9)
See https://www.cloudflare.com , https://www.opendns.com or https://quad9.net for details.

It can help you watch the amount of data your SIM provider allocates.
Select how often your contract is renewed, set the Data you have already used, and then click synchronise.

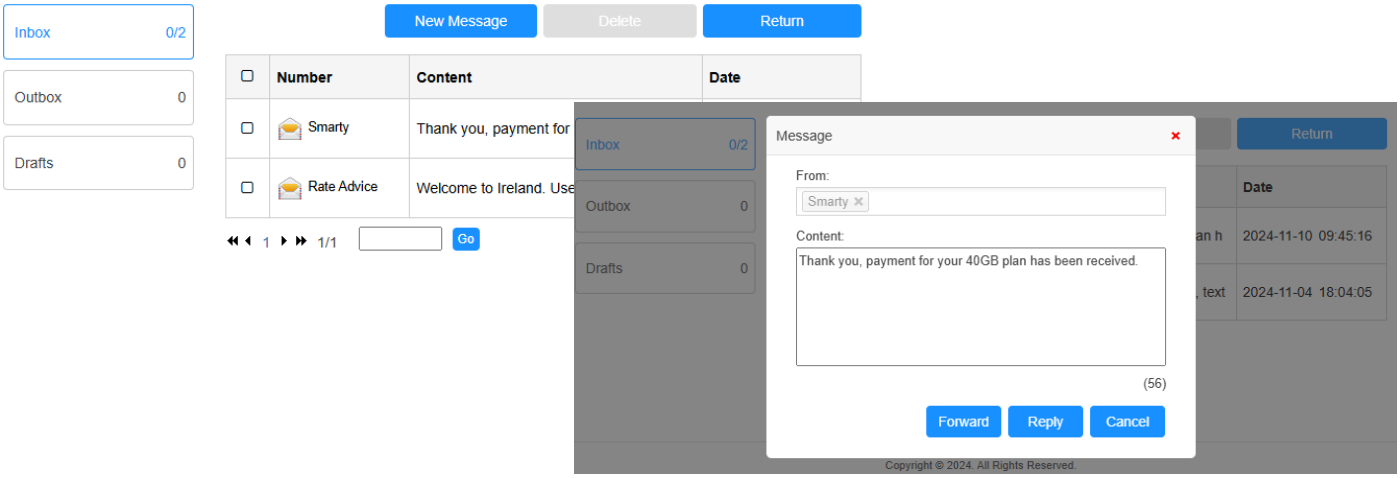
For advanced users, please leave this setting at default unless you are a network specialist.
In a demilitarized zone (DMZ) network configuration, a computer runs outside the firewall and intercepts incoming Internet traffic. Be fully aware of using DMZ and its security implications.

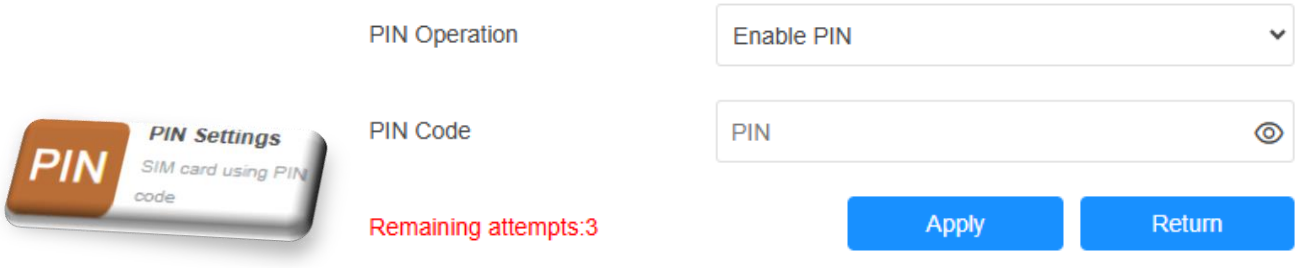
VPN client is a software application that allows users to securely connect to a VPN server over the internet. Your VPN provider will need to provide the details for this function. Check compatibility with the provider before purchasing the service. Please note: This function may only work when the cellular signal is strong enough to provide the service.

Allows the storage of valuable numbers and the use of the router to send text messages.
Please also see **Messages** for related functions. Once a number has been stored in the phonebook, you can recall this contact within **Messages** and send/receive SMS messages.

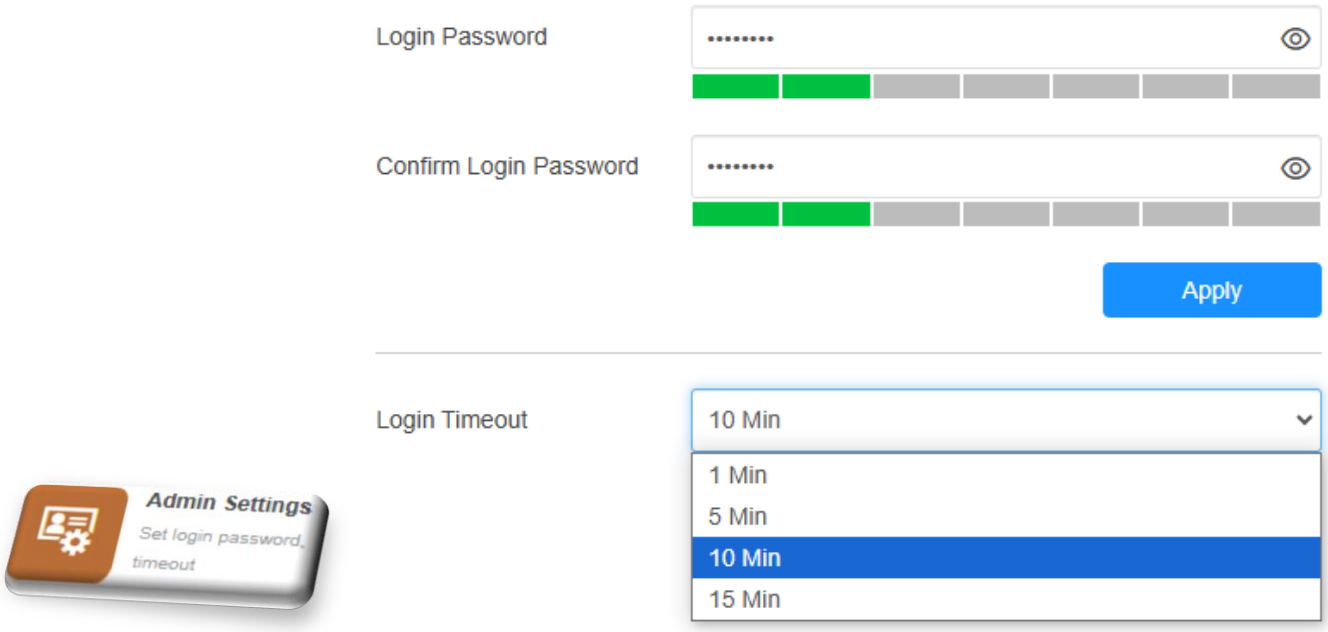


When you receive an SMS message, the chat icon flashes green.
Click the icon to read and reply to messages directly in the messages section.

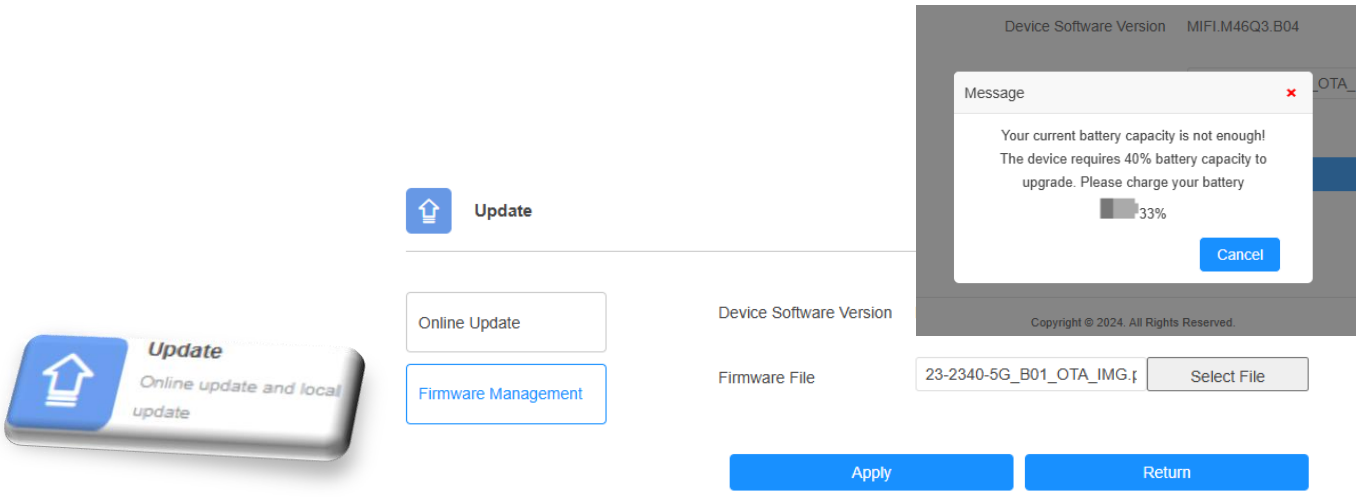




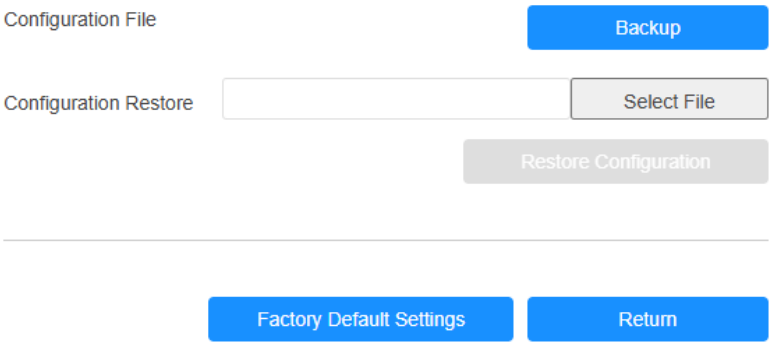
Enables SIM lock PIN functionality.
Please note that if you forget this PIN, your SIM card will be locked and rendered unusable.



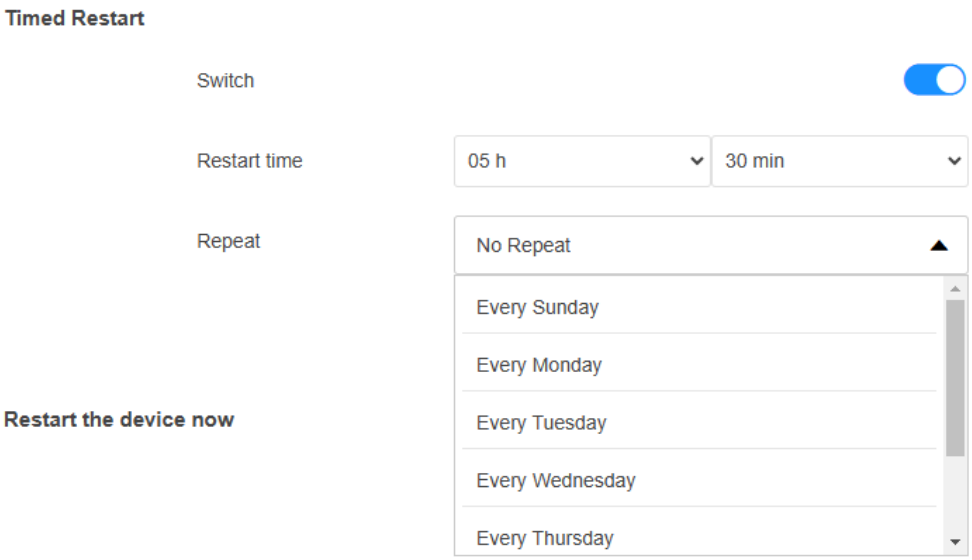
Change the login password and adjust the auto-logout timeout.
We strongly recommend using a secure, memorable password for enhanced security.
You'll be automatically logged out if inactive for a certain period. This is called a timeout



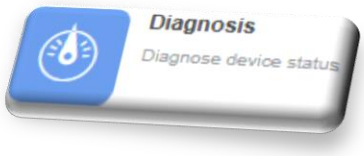
Here, you can manually check for firmware updates or set the updates to check automatically.
Please be aware that the downloaded file will use your data allowance.
This feature is intended for technical support only. Only use this feature if requested by technical support.



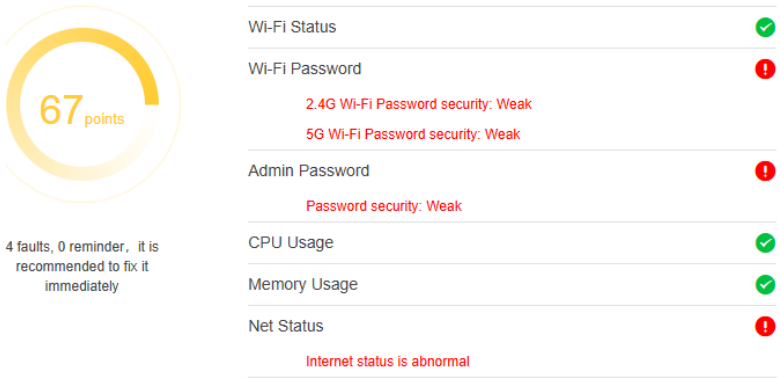
Create a backup of your router's current settings.
This is helpful if you plan to perform a factory reset.
Select Backup to backup your router configuration (BIN File) to your PC
Restore your backup by selecting the file and choosing restore configuration.

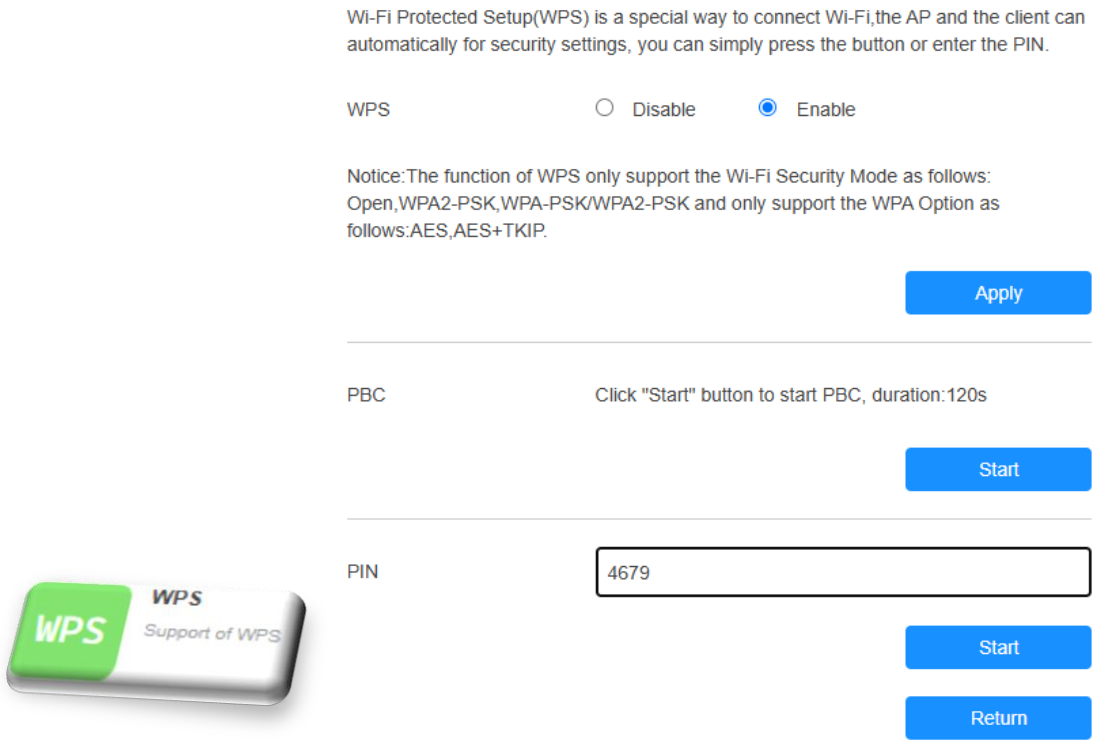


Enables the router to reboot automatically at a specified time and date.
Hold down the CTRL key to select multiple days.
You can also perform a software restart of the router from this menu.

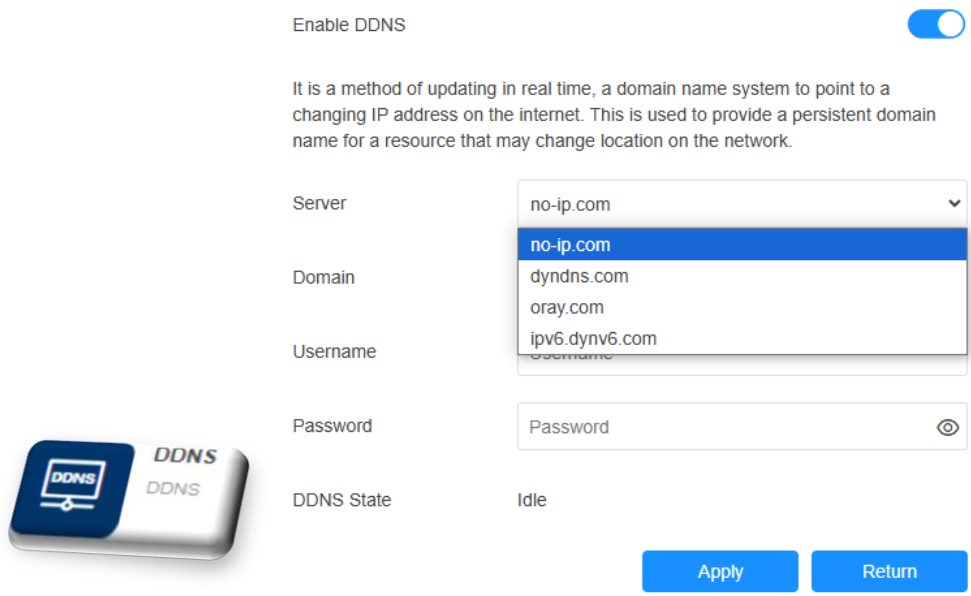


You can conduct a security scan after the router is fully set up. Any critical vulnerabilities, such as weak login credentials or an open Wi-Fi network, will be highlighted in red. Potential areas for improvement will be indicated in

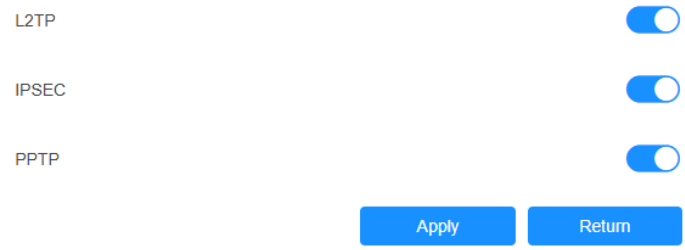




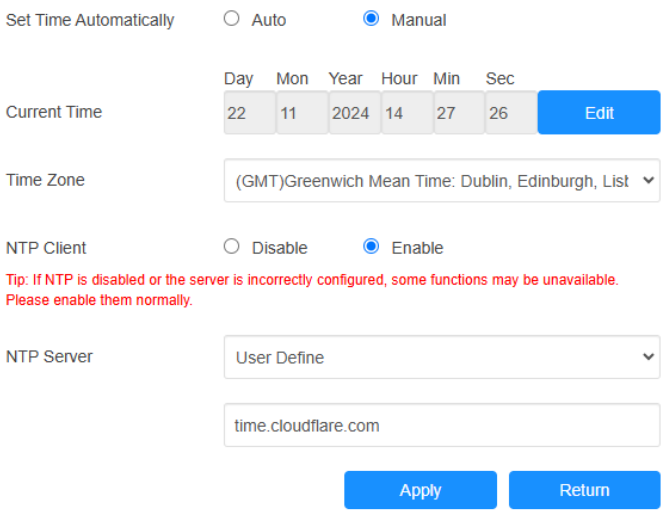
WPS stands for Wi-Fi Protected Setup. This simplifies the process of connecting devices to your Wi-Fi network. Instead of manually entering the network name (SSID) and password, you can use WPS to establish a secure connection with a few clicks.



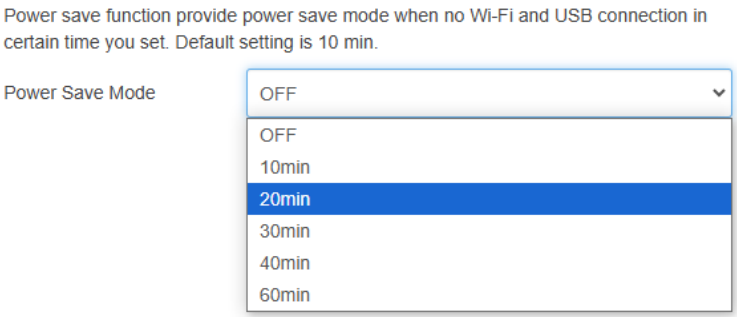
This feature is only supported on special SIM cards, with external-facing IPs.
It requires the router not to be behind the provider's Carrier-Grade NAT (CGNAT)\



This router supports L2TP, IPSEC, and PPTP VPN protocols.
It lets you establish a secure VPN connection from your PC or laptop to your network.



While your router automatically retrieves the time, you can choose a preferred Network Time Protocol (NTP) server for improved accuracy. Popular options include time.cloudflare.com, time.google.com, or pool.ntp.org.



Wi-Fi can automatically be turned off when no devices are detected. To reactivate Wi-Fi, give the power button on the router a light push. This feature is **disabled** by default.

User list (Whitelist/blacklist banning)
· From Apple iOS 14 and Android 10, MAC randomization is done in their devices to improve privacy. This will have the effect of not being able to identify or block devices using ACL, as this relies on MAC addresses
This MAC feature is expected to be a default on devices starting with the release of iOS 14 and Android 10. However, you can deactivate this function on your mobile device.

Specifications

Device Power Consumption: is between 1.16w to 2.85w
This means an approximate battery discharging time between 5.84 and 14.35 hours, depending on the usage.

- LCD: 2.4inch TFT 320*240
- USB-Port: Type-C, USB3.1, support data transfer
- Button: Power Key, Menu Select Key, Menu Confirm Key, Reset (Hidden)
- External Antenna: 1 x TS-9 connector for Tx/RX 1 x TS-9 connector for Rx
- Card slot One 4FF (Nano) UICC push slot.
- Battery 4500mAh Li-ion none-removable
- Charger Power 15W(5V/3A)/18W(9V/2A@PD) quick charging
- Wi-Fi QCA2064 Standard compliant: IEEE 802.11 a/b/g/n/ac/11ax 2.4 GHz (2x2 MIMO) and Wi-Fi 5G band (2x2 MIMO) AX1800

Cellular 5G/LTE

Qualcomm Snapdragon X62

Standard compliant: 3GPP Release 16 (both LTE and 5G)

Supported:

- NR Sub-6: n1/3/5/7/8/20/28/38/40/41/71/75/76/77/78

- LTE: B1/3/5/7/8/20/28/32/71/38/40/41/42/43

Modulation:

- Sub-6 UL: 256QAM, DL: 256QAM

- LTE DL: 256QAM, UL: 256QAM

MIMO:

Antenna (both LTE and 5G): 4 internal antennas
- Sub-6 DL: 4×4, UL: 2×2

- LTE DL: 4X4, UL: 1X1

Peak data rate:

- NSA: 3.4Gbps@DL, 550Mbps@UL

Output Power Class

WCDMA Class 3 (23 dBm ±2 dB)

LTE-FDD Class 3 (23 dBm ±2 dB)

LTE-TDD Class 3 (23 dBm ±2 dB)

LTE B38/B41/B42/B43 HPUE Class 2 (26 dBm ±2 dB)

5G NR Class 3 (23 dBm ±2 dB)

5G NR n38/n41/n77/n78 HPUE Class 2 (26 dBm +2/-3 dB)

Wi-Fi

QCA2064

Standard compliant: IEEE 802.11 a/b/g/n/ac/11ax

2.4 GHz (2×2 MIMO) + 5G band (2x2 MIMO) Wi-Fi Enabled Device: up to 32

Security Modes: Open, WPA2-PSK, WPA-PSK/WPA2-PSK, WPA3-SAE, WPA2-PSK/WPA3-SAE
AES

Environment Temperature

Operating 0°C to 40°C

Storage -20°C to 60°C

Understanding Signal Strength Metrics for 5G/4G Routers

Here's a breakdown of the key signal strength metrics you'll encounter, along with what constitutes a good or bad signal level:

RSSI (Received Signal Strength Indicator)

- **Simple Explanation:** This measures the overall strength of the signal received by your router from the cell tower. It's like measuring the volume of a radio broadcast.
- **Good Signal:** A higher RSSI value (typically less negative, like -70 dBm or higher) indicates a strong signal.
- **Bad Signal:** A lower RSSI value (more negative, like -100 dBm or lower) means a weak signal.

RSRP (Reference Signal Received Power)

- **Simple Explanation:** This focuses on the strength of the specific signal used for initial connection and data transmission.
- **Good Signal:** A higher RSRP value (less negative) is better, generally above -110 dBm.
- **Bad Signal:** A lower RSRP value (more negative) indicates a weaker signal, below -110 dBm.

RSRQ (Reference Signal Received Quality)

- **Simple Explanation:** This measures the quality of the reference signal, considering factors like interference and noise.
- **Good Signal:** A higher RSRQ value (less negative, closer to 0) means a better signal quality.
- **Bad Signal:** A lower RSRQ value (more negative) indicates a poorer signal quality, potentially leading to slower speeds or dropped connections.

SINR (Signal-to-Interference-plus-Noise Ratio)

- **Simple Explanation:** This compares the strength of the desired signal to the combined strength of interference and noise.
- **Good Signal:** A higher SINR value (typically expressed in decibels, like 10 dB or higher) means a strong signal relative to interference.
- **Bad Signal:** A lower SINR value indicates significant interference, potentially leading to slower speeds and unreliable connections.

In Summary:

- **Stronger signals (higher RSSI, RSRP, and SINR) generally result in faster speeds and more reliable connections.**
- **Weaker signals (lower values) can lead to slower speeds, dropped connections, and increased latency.**

Note: The specific values considered "good" or "bad" can vary depending on the network operator and specific conditions. However, these general guidelines should help you interpret your router's signal strength readings.

Benefits and Differences of 802.11 Standards (5 GHz Band)

Standard	Benefits	Differences
802.11a	- First 5 GHz Wi-Fi standard - Higher speeds than 802.11b/g	- Limited range - Less compatible devices
802.11n	- Significant speed improvement over 802.11a/g - MIMO technology for better performance	- Can be susceptible to interference
802.11ac	- Much faster speeds than 802.11n - Wider channels for increased bandwidth	- Shorter range than 802.11n
802.11ax (Wi-Fi 6)	- Even faster speeds and greater capacity than 802.11ac - Improved efficiency and reduced latency	- Requires compatible devices

Benefits and Differences of 802.11 Standards (2.4 GHz Band)

Standard	Benefits	Differences
802.11b	- First widely adopted Wi-Fi standard	- Slower speeds - Shorter range
802.11g	- Faster speeds than 802.11b - Better compatibility	- Can be susceptible to interference
802.11n	- Significant speed improvement over 802.11g - MIMO technology for better performance	- Can be susceptible to interference
802.11ax (Wi-Fi 6)	- Improved efficiency and reduced latency compared to 802.11n - Better performance in crowded environments	- Requires compatible devices

Wi-Fi security is like the lock on your front door, but for your wireless network. It uses different methods to scramble your internet traffic, making it difficult for snoopers to steal your data or hijack your connection. Here's a breakdown of common Wi-Fi security standards:

WEP (Wired Equivalent Privacy)

- **Benefits:** It was one of the first Wi-Fi security standards. That's about it for benefits...
- **Downside:** WEP is outdated and very easy to crack. It's like using a flimsy padlock on your door. **Avoid using WEP if at all possible.**

WPA/PSK (Wi-Fi Protected Access with Pre-Shared Key)

- **Benefits:** A step up from WEP, WPA offered improved encryption and better protection.
- **Downside:** While better than WEP, WPA is still vulnerable to determined hackers. Think of it as a sturdier door lock, but not the most secure.

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

- **Benefits:** For a long time, WPA2-PSK was the gold standard for home Wi-Fi security. It uses strong encryption and is widely supported by devices.
- **Downside:** While generally secure, vulnerabilities have been found over time. It's crucial to keep your router's firmware updated to patch these weaknesses.

WPA3-SAE (Wi-Fi Protected Access 3 with Simultaneous Authentication of Equals)

- **Benefits:** The latest and most secure Wi-Fi standard. It offers even stronger encryption and better protection against password guessing attacks.
- **Downside:** Not all devices support WPA3 yet, but adoption is increasing. Think of this as the most advanced lock with extra security features.

In Summary

Always aim for the highest Wi-Fi security standard your devices support. WPA3-SAE is ideal, but WPA2-PSK is still a decent option if WPA3 isn't available. Just remember to never use WEP, as it offers very little protection.

Wi-Fi Channel Allocation

Wi-Fi networks operate on specific radio frequencies, or channels. These channels are divided into two primary bands: 2.4 GHz and 5 GHz. Each band has a limited number of channels, and devices must be configured to use non-overlapping channels to avoid interference.

Channel Overlap and Interference

The 2.4 GHz band is particularly susceptible to interference because it is a crowded band shared by various devices, including cordless phones, microwaves, and Bluetooth devices. Even though there are 11 channels in the 2.4 GHz band, only three channels (1, 6, and 11) are non-overlapping. This means that if multiple Wi-Fi networks are using overlapping channels, they can experience significant interference, leading to slow speeds and dropped connections.

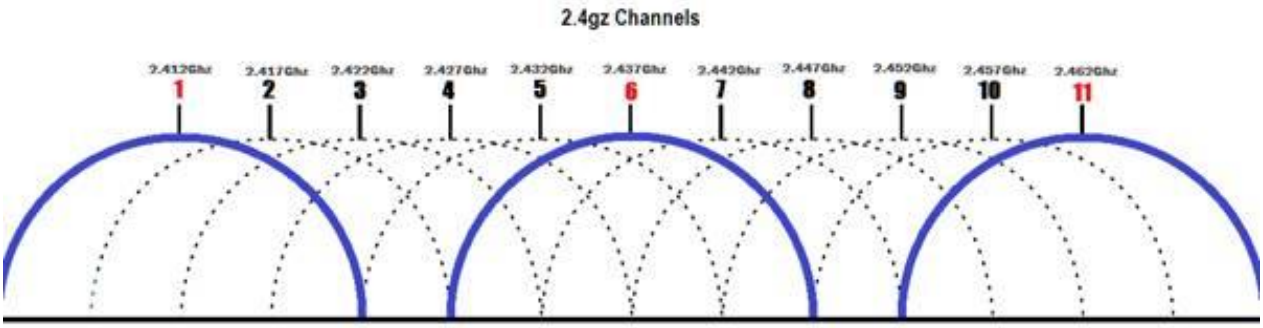
Wide Bandwidth and Interference

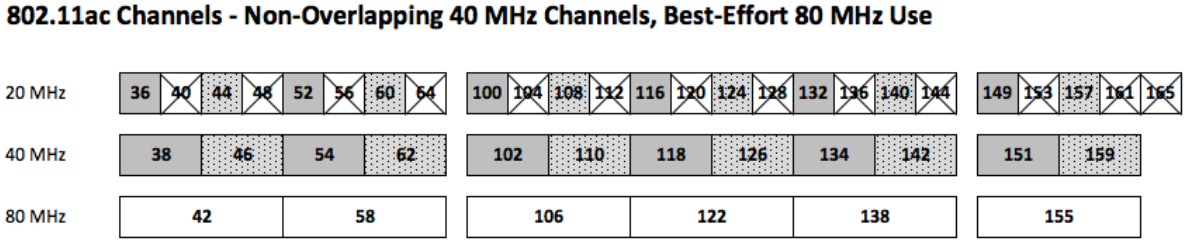
Modern Wi-Fi standards, such as 802.11ac and 802.11ax (Wi-Fi 6), support wider channel widths, such as 20, 40 MHz and 80 MHz While wider channels can significantly increase data transfer speeds, they also increase the potential for interference. This is because wider channels occupy a larger portion of the spectrum, making it more likely to overlap with other devices or networks.

Mitigating Interference with Wide Channels

To mitigate interference with wide channels, several strategies can be employed:

1. **Channel Selection:** Choose channels with minimal interference. Tools like Wi-Fi analysers can help identify the least congested channels in your area.
2. **Channel Bonding:** Combine multiple smaller channels to create a wider channel. This can be done if there are adjacent channels available with minimal interference.
3. **Dynamic Frequency Selection (DFS):** Some 5 GHz channels are reserved for radar use. DFS-capable devices can automatically switch to a different channel if radar activity is detected.
4. **MU-MIMO:** This technology allows multiple devices to communicate simultaneously on the same channel, improving efficiency and reducing interference.





Troubleshooting Wi-Fi Interference

Wi-Fi interference can significantly impact your network's speed and reliability. Here's a breakdown of troubleshooting steps:

1. Identify the Source of Interference

- **Check for Overlapping Networks:** Use a Wi-Fi analyser app (like Wi-Fi Analyzer for Android or Acrylic Wi-Fi for Windows) to scan for nearby networks. Identify overlapping channels and choose a less congested one for your router. **Channel Selection:** Choose a less congested channel, especially in the 2.4 GHz band. Wi-Fi analysers can help you find the best channel.
- **Identify Potential Electronic Devices:** Common culprits include:
    - Microwaves
    - Cordless phones
    - Bluetooth devices
    - Baby monitors
    - Even other Wi-Fi networks
- **Physical Obstructions:** Walls, furniture, and even metal objects can block or weaken Wi-Fi signals.

2. Optimize Your Router's Placement

- **Clear Line of Sight:** Ensure there are no major obstructions between your router and devices.
- **Distance from the router:** Signal strength weakens with distance.
- **Physical obstacles:** Walls, floors, and furniture interfere with Wi-Fi signals.
- **Interference from other devices:** Other Wi-Fi networks, microwaves, and Bluetooth devices can all cause interference.

Selecting bandwidth on your router.

Theoretical **maximums are misleading:** While we can talk about theoretical maximum speeds, you'll almost never achieve them in practice and your Wi-Fi can't be faster than the internet speed provided by your ISP.

Frequency Band	Channel Width	Theoretical Maximum Speed	Realistic Average Speed
2.4 GHz	20 MHz	Up to 150 Mbps	47 Mbps
2.4 GHz	40 MHz	Up to 300 Mbps	100 Mbps
5 GHz	20 MHz	Up to 433 Mbps	135 Mbps
5 GHz	40 MHz	Up to 867 Mbps	275 Mbps
5 GHz	80 MHz	Up to 1733 Mbps	550 Mbps

5 GHz is generally faster:
5 GHz offers higher speeds and less interference than 2.4 GHz, but it has a shorter range.

Wider channels offer higher speeds:
40 MHz and 80 MHz channels can provide significantly faster speeds, but they are more susceptible to interference.