ATEL WB550 5G FWA Indoor Router

User Manual

Powering Change

missiontelecom.org

Click Here for Customer Support

Table of Contents

1. About this Manual 3
2. Router Interfaces 3
3. Configuring the Router 6
   - 3.1 Login 6
   - 3.2 Dashboard 6
   - 3.3 Status 7
     - 3.3.1 WAN Status 7
     - 3.3.2 WiFi LAN Status 8
     - 3.3.3 Cellular Status 8
     - 3.3.4 Network Status CA 9
     - 3.3.5 Software 9
     - 3.3.6 Device List 10
     - 3.3.6 WLAN Device List 10
     - 3.3.7 Statistics 11
   - 3.4 Settings 11
     - 3.4.1 Basic 12
     - 3.4.2 WiFi 17
     - 3.4.3 VPN 26
     - 3.4.4 Security 27
     - 3.4.5 Advanced 35
     - 3.4.6 Cellular Settings 39
   - 3.5 SMS 42
4. ATRACS Cloud Connect Remote Management 43
   - Common Problems, FAQ's and Solutions 43

Regulatory Statements 44

Safety Hazards 45

Limited Warranty: 46

1. About this Manual

The contents of this User Manual have been made as accurate as possible. However, due to continual product improvements, specifications and other information are subject to change without notice. Please visit www.ATEL-USA.com or contact ATEL USA for additional information and the latest version of this User Manual.

2. Router Interfaces

- **LEDs**

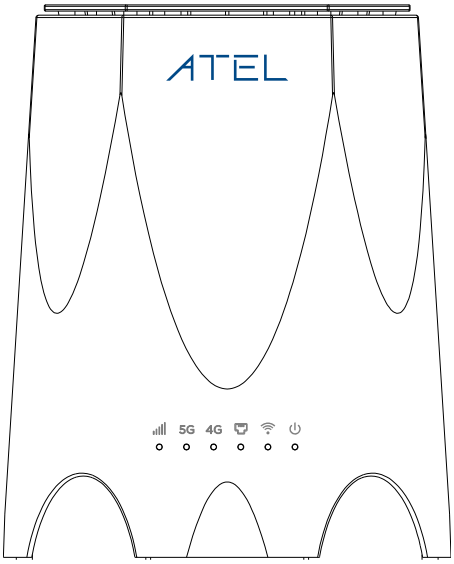


Figure 1 Front Panel

LED	Color	Status	Description
Power	Green	On	Indicates AC/DC Adaptor is ON and plugged in.
		Off	No AC/DC Adaptor.
WiFi	Green	On	WiFi feature is enabled.
		Off	WiFi feature is turned off/Disabled.

LED	Color	Status	Description
Ethernet	Green	On	A wired user is connected over LAN Port.
		Off	No Wired user is connected over LAN Port.
4G	Green	On	Router connected with 4G network.
		Off	No 4G data connection.
5G	Green	On	Router connected with 5G network.
		Off	No 5G data connection.
Signal	Green	On	Good 4G/5G Signal. RSRP>=-95dBm
	Blue	On	Normal 4G/5G Signal. -95dBm>RSRP>=-115dBm
	Red	On	Weak 4G/5G Signal. -115dBm>RSRP>=-125dBm
	Red	Blinking	Error, no SIM.
		Off	RSRP<-125dBm
Notes	1. All LEDs except Power blink while software is updating. 2. WiFi LEDs blink while WPS function is activated.		

- **Ports**

  - **RJ45** – These ports allow the WB550 to connect with your computer via Ethernet cable.
  - **SIM** – A 4FF SIM card can be installed via this slot.
  - **DC** – Power (12V DC) jack to input power supply from the Power Adaptor provided with the device's accessories. Note: Please only use accessories provided by ATEL USA. The use of other accessories may damage the device and/or void the warranty.

Note: The adapter should be installed near the equipment and should be easily accessible.

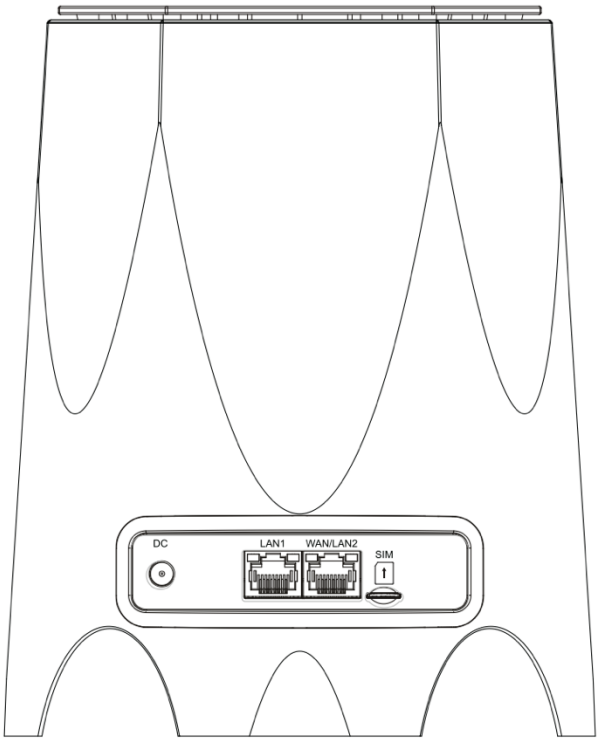


Figure 2 Rear Panel

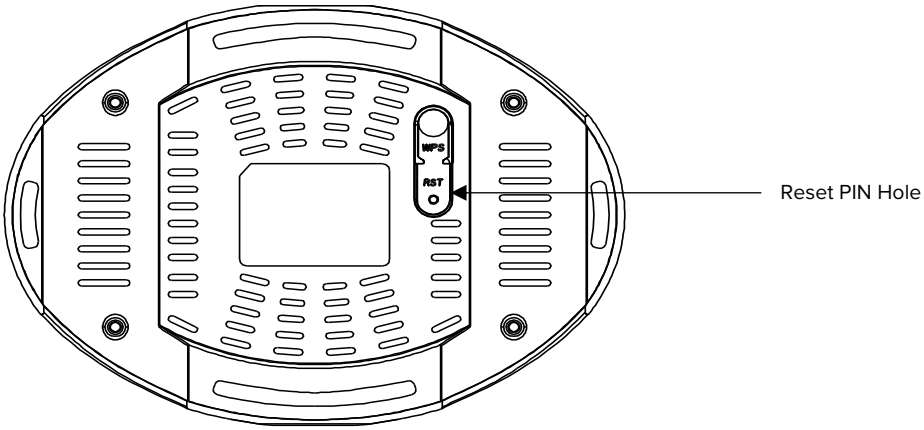


Figure 3 Bottom Panel

- **WPS –** Press this button to activate the WPS feature.
- **RST –** Press this keyhole for up to 10 seconds to reset the router to factory defaults.

3. Configuring the Router

You can login to the WebGUI by following the instructions below. Once logged in, you can configure the device settings according to your requirements.

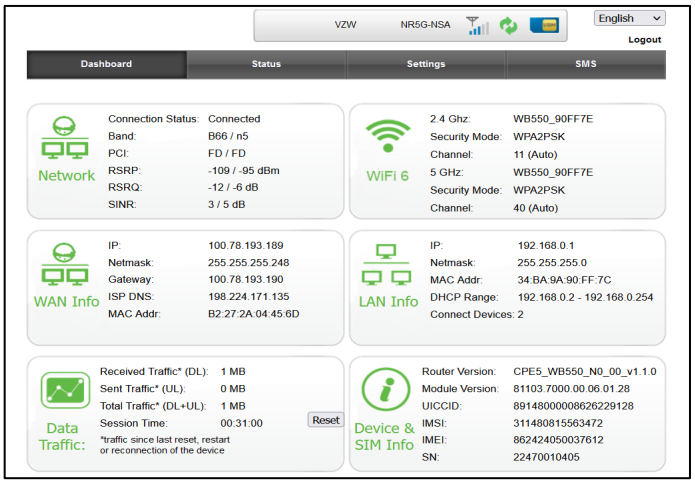
1. Connect your PC to the WB550 Router using the Ethernet cable. Use either of the two Ethernet ports on the router.
2. Power on the Router and wait for about 40 seconds (until it finishes initializing).
3. Please ensure that a USIM card has been inserted into the USIM slot in the device and login to the WebGUI as instructed in section 3.1 Login (below).
4. Note: You can also connect your PC to the router via WiFi. Connect to the WB550 WiFi (as you would any WiFi) and input the WiFi SSID and the accurate password as shown on the device label to connect.

3.1 Login

1. Open your Web browser and enter 192.168.0.1 in the address bar. The login window will popup.
2. When prompted for the Username and password, enter the following:
    a. Username: admin
    b. Password: Unique to your device, check the device label for your password.

3.2 Dashboard

After successfully logging in, the screen below will appear and you will see four main menus on the top bar of the WebGUI.



The bars in the middle indicate the signal level received and the USIM icon displays the status of the USIM. Click “Logout” and the WebGUI will log you out and return you to the login window.

From this dashboard page, you can also view Network status, Wi-Fi, WAN Information, LAN Information, Data Traffic and Device & SIM Information.

3.3 Status

On this page, you can view WAN Status, WiFi LAN Status, Cellular Status, Software, Device List, WLAN Device List and Statistics.

3.3.1 WAN Status

From the WAN Status page, you can view the WAN IP Address, WAN Primary DNS and WAN Secondary DNS information.

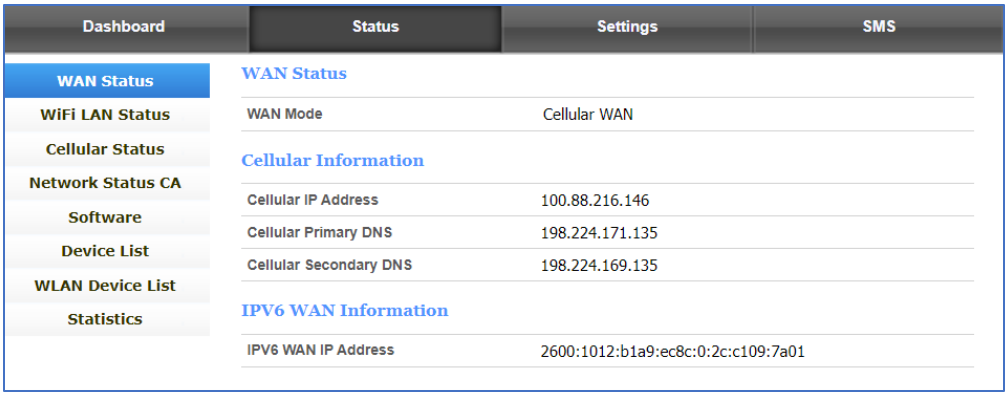


Figure 5 WAN Status

3.3.2 WiFi LAN Status

From this page, you can view the WiFi LAN Status and information such as SSID, Channel, Security, Key, LAN IP and DHCP Server.

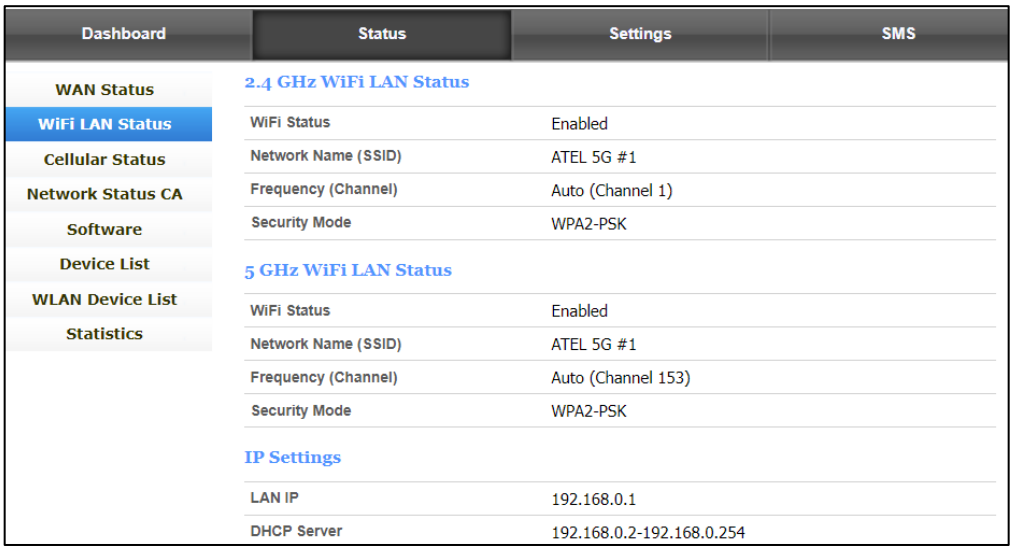


Figure 6 WLAN Status

3.3.3 Cellular Status

From this page, you can view the Cellular information, such as, Connection Status, USIM Status, IMEI, IMSI, RSRP, RSRQ, RSSI, SINR, PCI, Cell ID and Band.

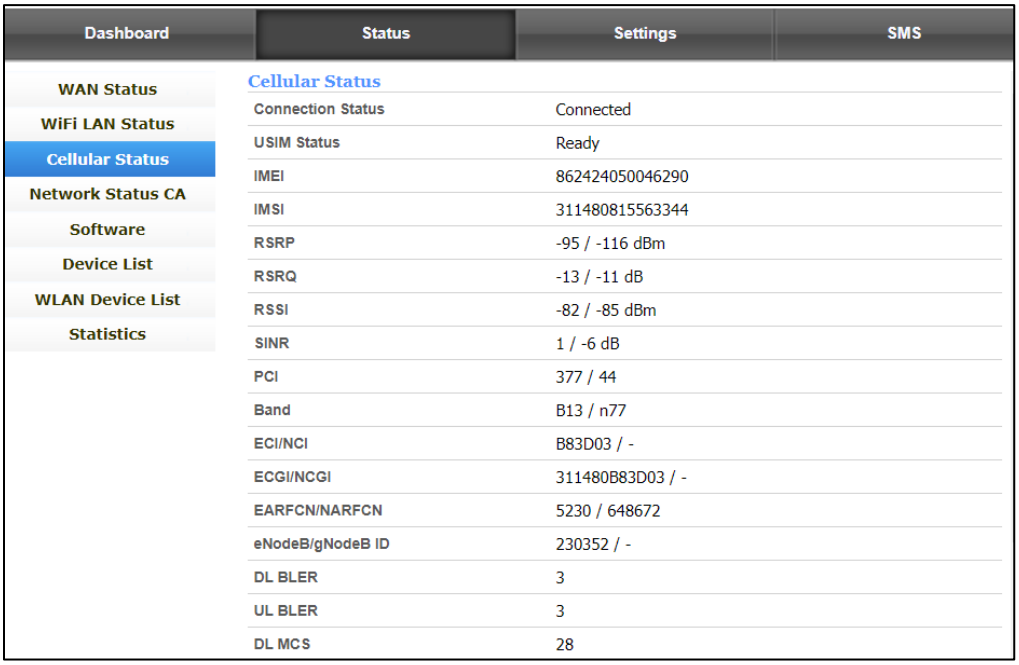
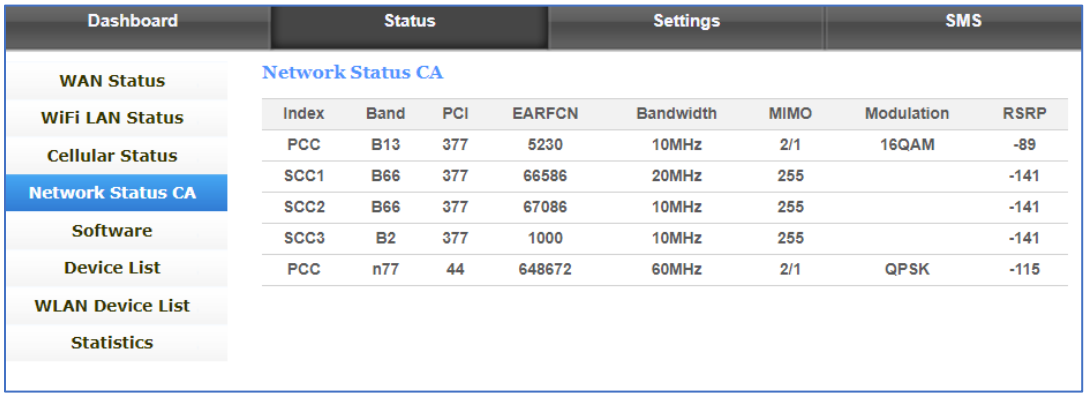


Figure 7 Cellular Status

3.3.4 Network Status CA

On this page, you can view network status CA information, such as, Index, Band, PCI, EARFCN, Bandwidth, MIMO, Modulation and RSRP.



Index	Band	PCI	EARFCN	Bandwidth	MIMO	Modulation	RSRP
PCC	B13	377	5230	10MHz	2/1	16QAM	-89
SCC1	B66	377	66586	20MHz	255		-141
SCC2	B66	377	67086	10MHz	255		-141
SCC3	B2	377	1000	10MHz	255		-141
PCC	n77	44	648672	60MHz	2/1	QPSK	-115

Figure 8 Cellular Network Status CA

3.3.5 Software

From this page, you can view the software version and the Module software version for the WB550 5G Router.

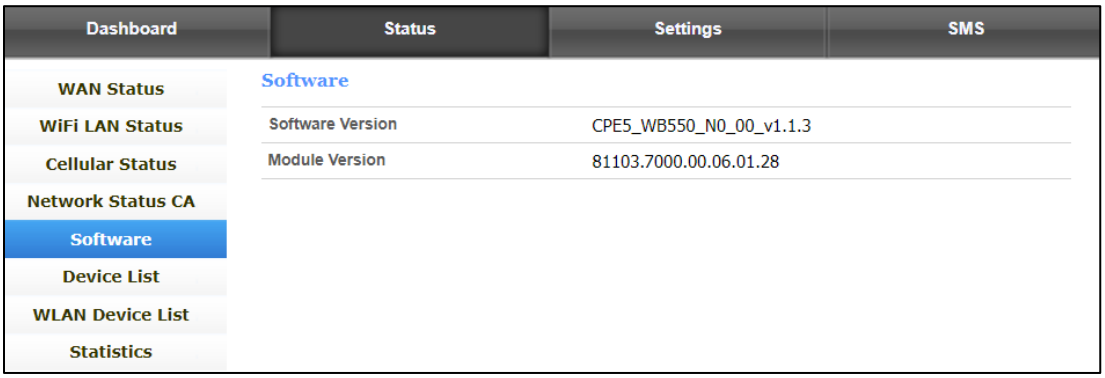


Figure 4 Software

3.3.6 Device List

From the device list page, you can view the connected users' information, including Hostname, MAC address, IP address and expiration time for assigned IP address.

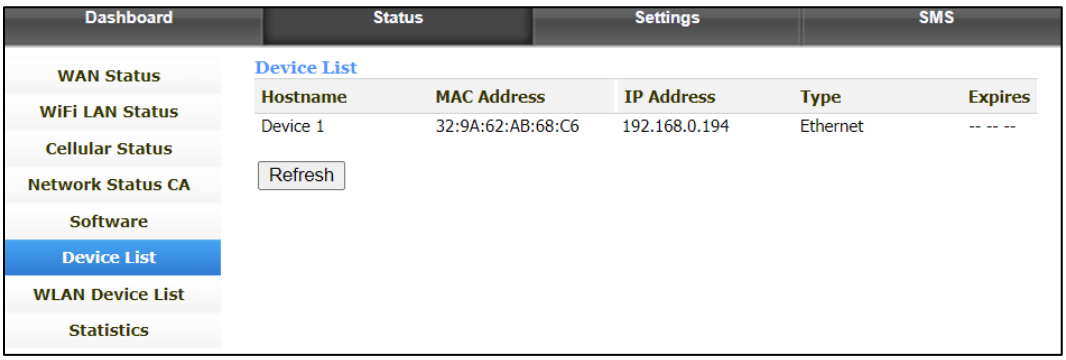


Figure 5 Device List

3.3.6 WLAN Device List

On this page, you can view the connected wireless users' information, including Hostname, MAC address, IP address, MCS, and receiving signal information for each user.

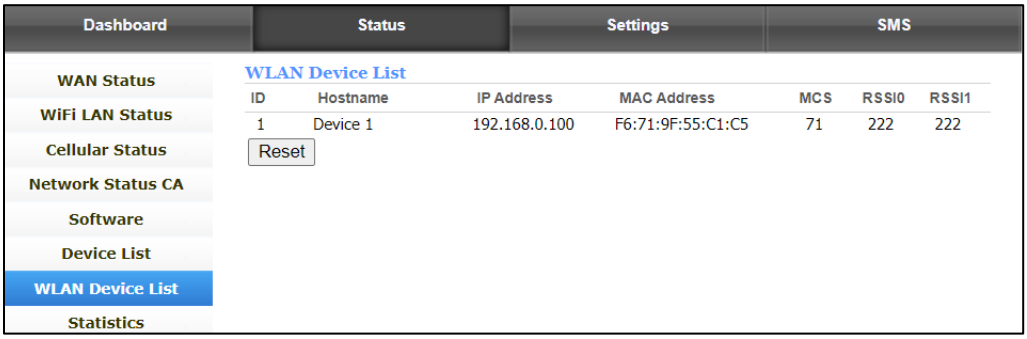


Figure 6 WLAN Device List

3.3.7 Statistics

From the Statistics page, you can view the speed and data used traffic statistics. Click on “Clear” button to reset available traffic statistics.

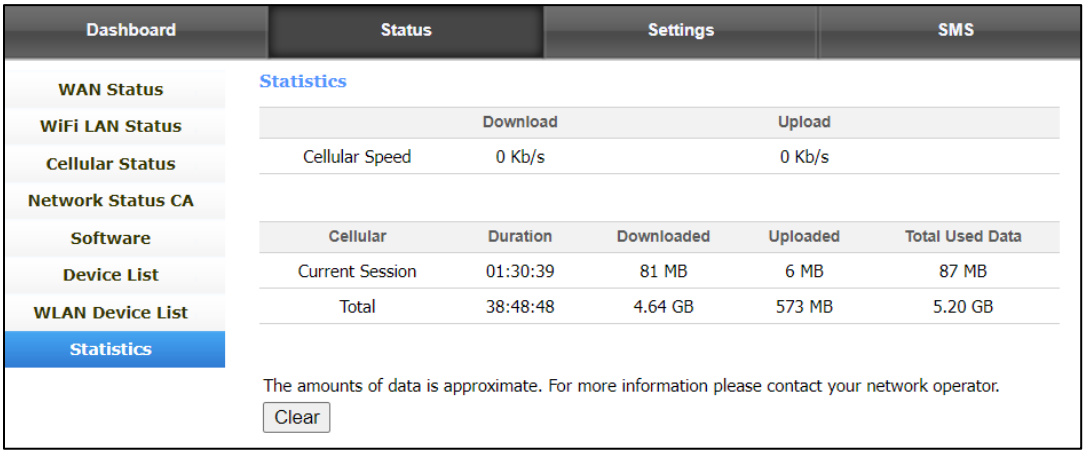


Figure 7 Statistics

Note: Statistics data might differ from the data consumed on the ISP side.

3.4 Settings

On this page, you will find some Basic & Advanced configuration options, such as, Basic, WiFi, VPN, Security, Advanced & Cellular Settings.

Figure 8 Settings

3.4.1 Basic

3.4.1.1 Management

On this page, you can modify the default password for the WebGUI login. You need to input the new password 2 times and click the “Apply” button for changes to take effect. Next you would logout automatically and you should login to the system with the new password.

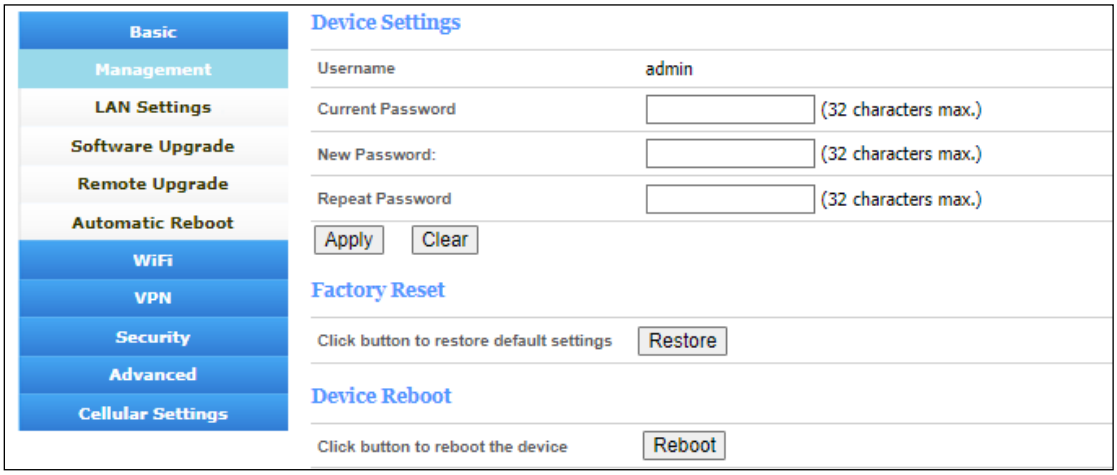


Figure 9 Basic > Management

On the same page, you can click the “Restore” button to load to the default factory settings and click the “Reboot” button to reboot the router.

Note: After factory reset, all the configuration or data on the router will be replaced with factory default settings.

3.4.1.2 LAN Settings

On this page, you can view the existing settings for the LAN (Local Area Network) and modify them as per your requirements.

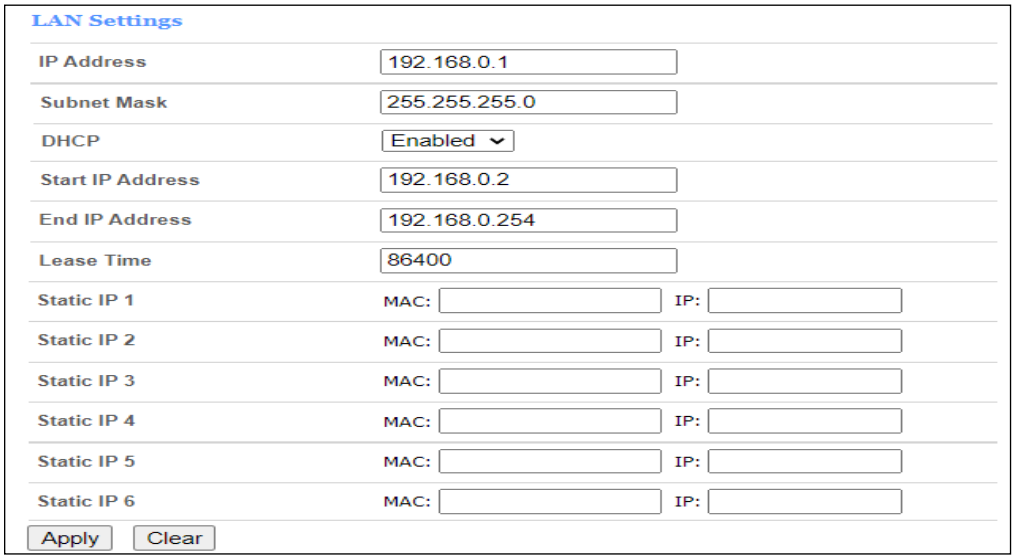


Figure 10 Basic > LAN Settings

- **IP Address -** Displays the IP address of your router (default: 192.168.0.1).
- **Subnet Mask** - An address code that determines the size of the network. Generally, use 255.255.255.0 as the subnet mask.
- **DHCP** - Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server within your network, otherwise, you must configure the address of your PC manually.
- **Start IP Address** - Specify an IP address for the DHCP server to start with when assigning IP addresses. The default start address is 192.168.0.2.
- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP addresses. The default end address is 192.168.0.254.
- **Lease Time** - The Lease Time is the amount of time a user will be allowed connection to the router with their current assigned IP address. Enter the amount of time in minutes and the user will be "leased" the IP address for that time. After the time is up, the user will be assigned a new IP address automatically.
- **Static IP** - IP/MAC binding function, the router will assign a fixed IP address to a specific user using its MAC address according to the rules.

Note:

1. If you change the IP Address of LAN, you must use the new IP address to login to the router.
2. If the new LAN IP address you set is not in the same subnet, the IP address pool of the DHCP server will change at the same time, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

3.4.1.3 Software Upgrade

On this page, you can upgrade the SW version of the router manually from the connected PC. It will take several seconds (~120) to complete the whole upgrade process, and then the router will reboot automatically.

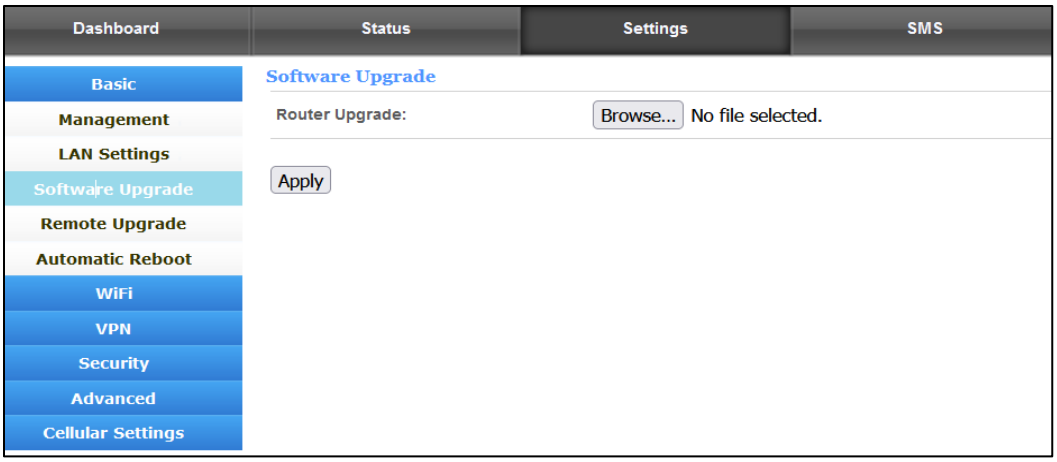


Figure 11 Basic > Software Upgrade

3.4.1.4 Remote Upgrade

On this page, you can view the default configuration for the remote upgrade function. After the router detects the new router and LTE version on the remote FOTA server, it will upgrade the new version automatically. It can also check if a new version is available when you click the “Check” button and upgrade the new version after you click the “Upgrade” button.

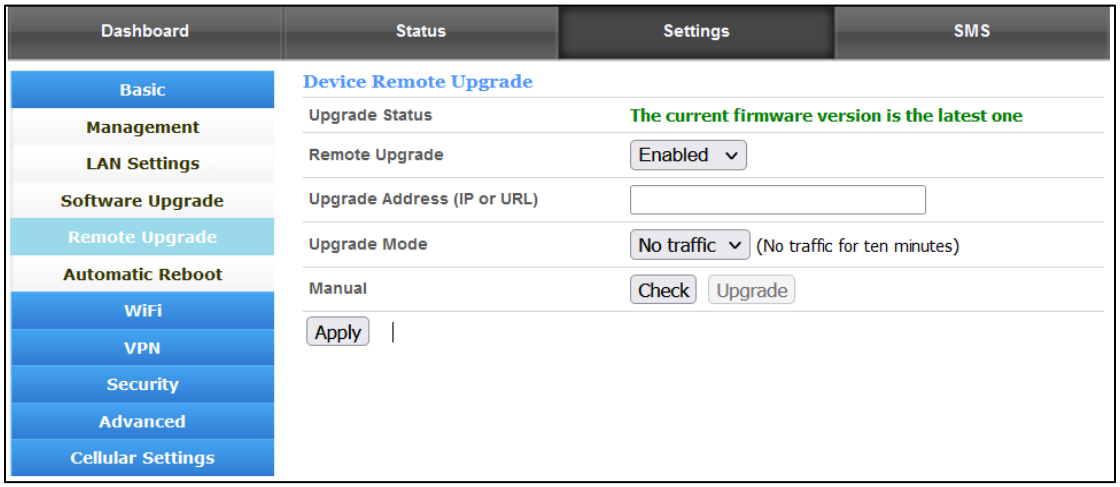


Figure 12 Basic > Remote Upgrade

3.4.1.5 Automatic Reboot

On this page, you can set up the Automatic Reboot feature. By default, it is Disabled.

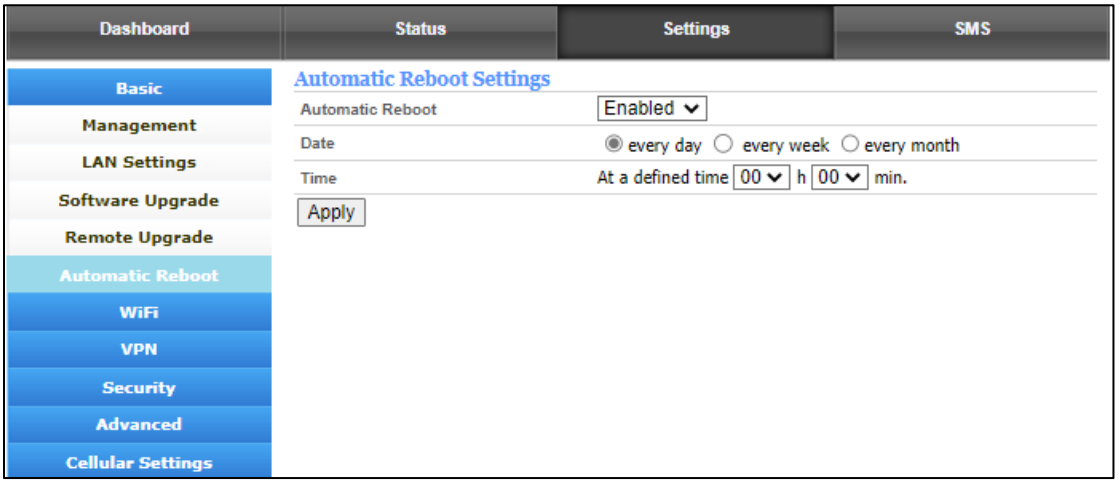


Figure 13 Basic > Automatic Reboot

You can define the rule for this router to reboot itself automatically on a defined day and time. For the settings to take effect, make sure to click on the “Apply” button.

3.4.2 WiFi

3.4.2.1 WiFi Settings

On this page, you can view and modify the existing settings related to WiFi.

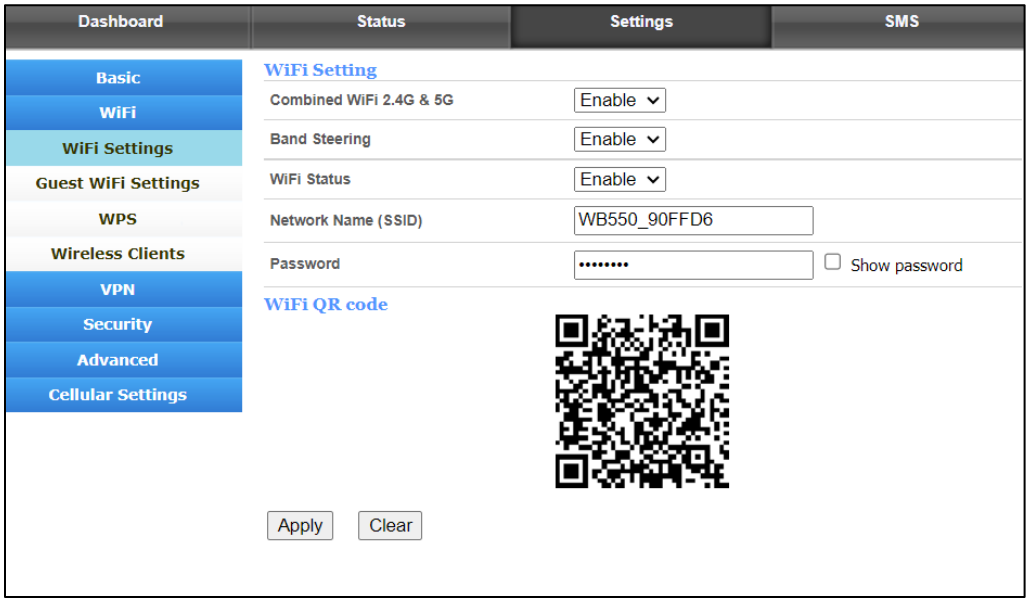


Figure 14 WiFi > WiFi Settings

By default, the combined “WiFi 2.4G & 5G” feature is enabled, which means both 2.4GHz and 5GHz are active and use same SSID Name & Password.

Any 5GHz WiFi capable Wireless user will have preference to connect over 5GHz WiFi radio with their router for the best performance (in terms of speed). 2.4GHz WiFi radio is suitable for good coverage but offers low throughput compared to 5GHz WiFi.

Band Steering: When this feature is enabled, the router will connect to the user equipment by 5GHz when the user equipment is near the router, and by 2.4GHz when the user equipment is far from the router. When this feature is disabled, it is the user equipment instead of the router that decides which frequency WiFi to connect to. By default, this feature is disabled.

You can disable the combined WiFi feature and configure 2.4GHz & 5GHz WiFi radio as required.

2.4GHz WiFi Settings

If you disable the combined WiFi Feature, you can select the WiFi 2.4GHz option and setup the configuration as required.

Figure 15 WiFi > 2.4GHz WiFi

- **WiFi Status:** Enabled (default)/Disabled

The WiFi status is enabled by default. If disabled, you can only connect to the router by Ethernet cable.

- **WiFi Standard:**

This router can be operated in six different wireless modes: “11b/g/n/ax mixed mode”, “11b/g/n mixed mode”, ”11b/g mixed mode”, “11n only”, “11g only”, “11b only”. You can set your preferred mode as shown in the image below.

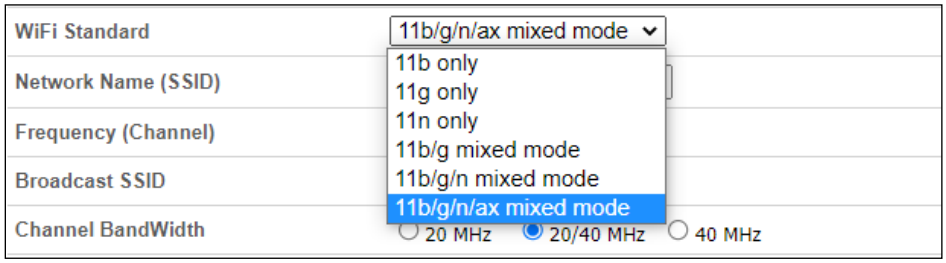


Figure 16 2.4GHz > WiFi Standard

- **Network Name (SSID)**

To identify your wireless network, the SSID (Service Set Identifier) is used. You can set it to anything you'd prefer. You should make sure that your SSID is unique if there are other wireless networks operating in your area.

- **Frequency (Channel)**

This field determines which operating frequency will be used for WiFi. It is not necessary to change the wireless channel unless you noticed interference problems with other access points nearby.

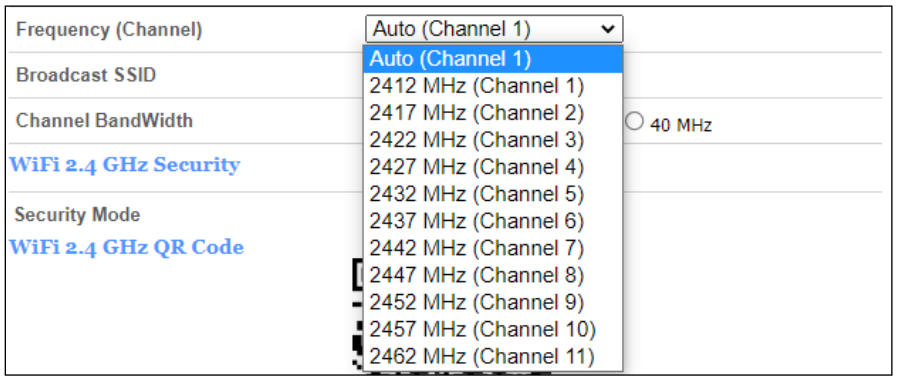


Figure 17 2.4GHz > Channel

- **Broadcast SSID:** Enabled (default)/Disabled

When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast of the router. If you disable this feature, the WiFi SSID of the router is invisible.

- **Channel Bandwidth:** 20MHz, 20/40MHz,40MHz

- **2.4GHz WiFi Security**

Setup the wireless security and encryption to prevent the router from unauthorized access and monitoring. The default security mode is WPA2-PSK and the default password is unique. You can modify the security mode and password from this page.

- **Security Mode:** Disabled, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK, WPA2-PSK/WPA3-SAE
- **WPA Algorithms:** TKIP, AES, TKIP/AES
- **Password:** 1~32 characters
- **Key Renewal Interval:** 0~4194302s

- **2.4GHz WiFi QR Code:** You can use this QR code to connect with this router wirelessly.

Make sure to click the "Apply" button to apply any settings.

5GHz WiFi Settings

Figure 18 WiFi > 5GHz WiFi

➢ **WiFi Status:** Enabled (default)/Disabled

The WiFi status is enabled by default. If disabled, you can only connect to this router by Ethernet cable.

➢ **WiFi Standard:**

This router can be operated in four different wireless modes: “11a/n/ac/ax mixed mode”, “11n only”, “11n/ac mixed mode”, and “11a/n/ac mixed mode”.

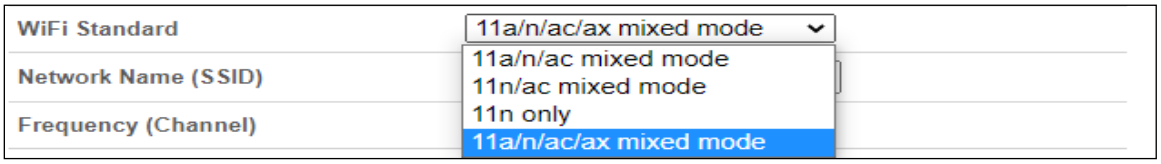


Figure 19 5GHz > WiFi Standards

➢ **Network Name (SSID)**

To identify your wireless network, the SSID (Service Set Identifier) is used. You can set it to anything you’d prefer. Make sure that your SSID is unique if there are other wireless networks operating in your area.

➢ **Frequency (Channel)**

This field determines which operating frequency will be used for WiFi. It is not necessary to change the wireless channel unless you noticed interference problems with other access points nearby.

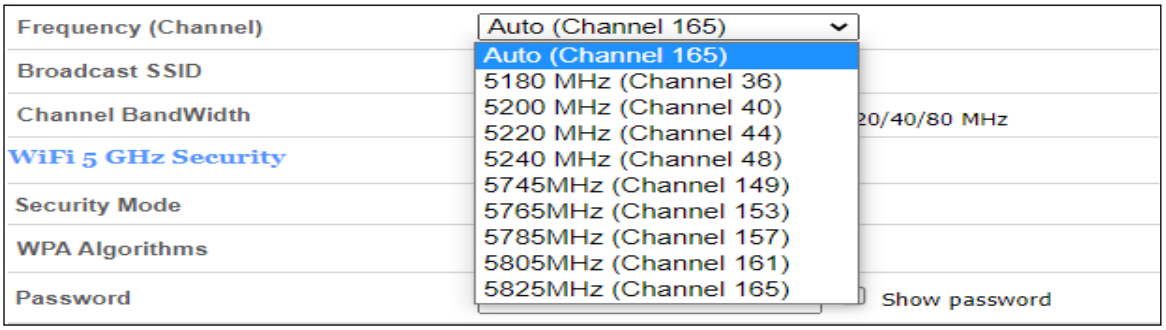


Figure 20 5GHz > Channel

➢ **Broadcast SSID:** Enabled (default)/Disabled

When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast of the router. If you disable this feature, the WiFi SSID of the router is invisible.

Channel Bandwidth: 20MHz, 20/40MHz, 20/40MHz/80MHz

- **5GHz WiFi Security**

The wireless security and encryption setting(s), which prevent the router from unauthorized access and monitoring. Default security mode is WPA2-PSK, and the default password is unique. You can modify the security mode and password from this page.

- **Security Mode:** Disabled, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK, WPA2-PSK/WPA3-SAE
- **WPA Algorithms:** TKIP, AES, TKIPAES
- **Password:** 1~32 characters
- **Key Renewal Interval:** 0~4194302s

- **5GHz WiFi QR Code:** You can use this QR code to connect with this router over 5GHz radio wirelessly.

Make sure to click the "Apply" button to apply any settings.

3.4.2.2 Guest WiFi Settings

On this page, you can set the configuration for Guest WiFi as 2.4GHz or 5GHz (as required). By default, Guest WiFi is disabled.

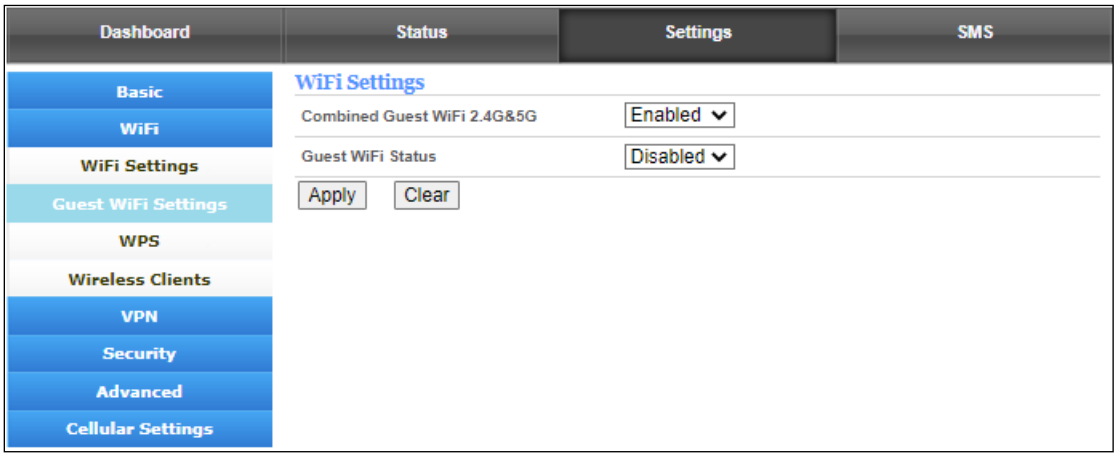


Figure 21 WiFi > Guest WiFi

- 2.4GHz Guest WiFi Settings

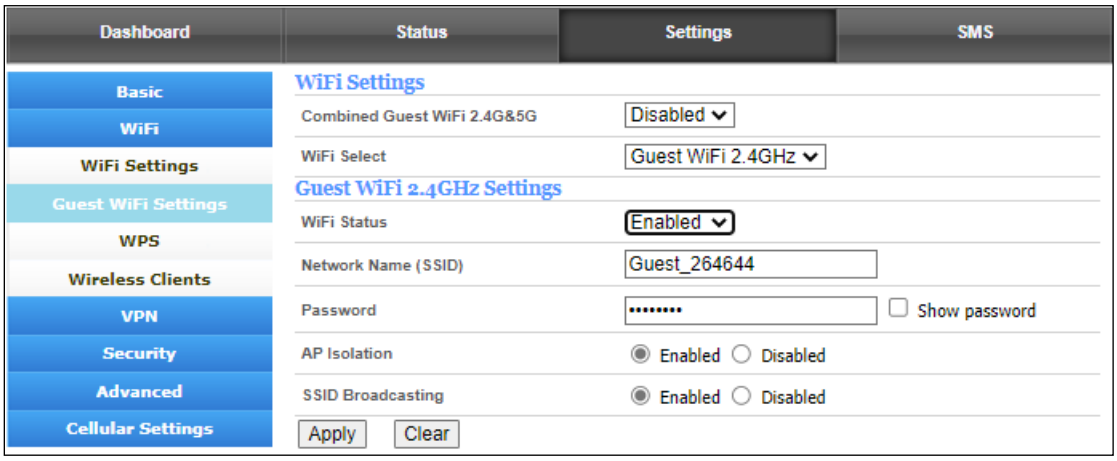


Figure 22 WiFi > Guest 2.4GHz WiFi Settings

- **WiFi Status:** Enabled (default)/Disabled

The WiFi status is enabled by default. If disabled, you can only connect to this router via Ethernet cable.

- **Network Name (SSID)**

To identify your wireless network, the SSID (Service Set Identifier) is used. You can set it to anything you prefer. Make sure that your SSID is unique if there are other wireless networks operating in your area.

- **AP Isolation:** Enabled/Disabled (default)

This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the router but not with each other.

- **Broadcast SSID:** Enabled (default)/Disabled

When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast of the router. If you disable this feature, the WiFi SSID of the router is invisible.

- 5GHz Guest WiFi Settings

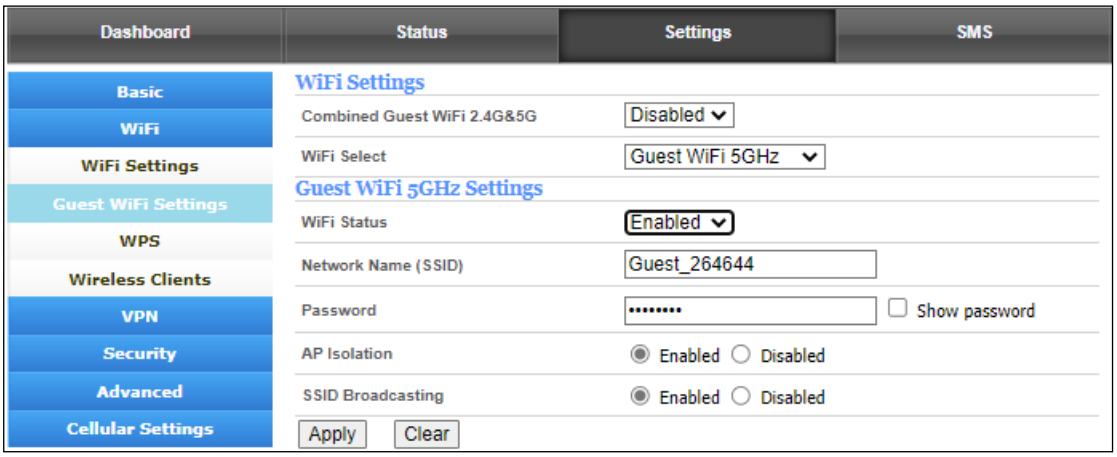


Figure 23 WiFi > Guest 5GHz WiFi Settings

- **WiFi Status:** Enabled (default)/Disabled

The WiFi status is enabled by default. If disabled, you can only connect to this router via Ethernet cable.

- **Network Name (SSID)**

To identify your wireless network, the SSID (Service Set Identifier) is used. You can set it to anything you prefer. Make sure that your SSID is unique if there are other wireless networks operating in your area.

- **AP Isolation:** Enabled/Disabled (default)

This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the router but not with each other.

- **Broadcast SSID:** Enabled (default)/Disabled

When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast of the router. If you disable this feature, the WiFi SSID of the router is invisible.

Make sure to click the “Apply” button to apply any settings.

3.4.2.3 WPS

On this page, you can setup the WPS (WiFi Protected Setup) feature which allows your wireless client/device to connect with the WB550 router over WiFi with ease.

You need to scan the WiFi network from your wireless device/client and select the available WIFI SSID from your WB550. Then simply either press the WPS button for 10 seconds or click on the **Start PBC** button available on WebGUI.

Your wireless client/device will connect with WB500 over WiFi without any password input.

- **WPS Status –** Displays the WPS status. When you push the WPS button, **the** WPS status changes from "Idle" change to "Processing...". After the connection process is completed, the WPS status change to “Successfully Connected”. You can click on the **Disable** button to disable the WPS feature, if required.

- **Frequency** – Select the WPS connection as either 2.4G WiFi or 5G WiFi.

- **Start PBC -** Click on this button to turn on the WPS feature. You can also use the WPS button available on the bottom panel of your WB550.

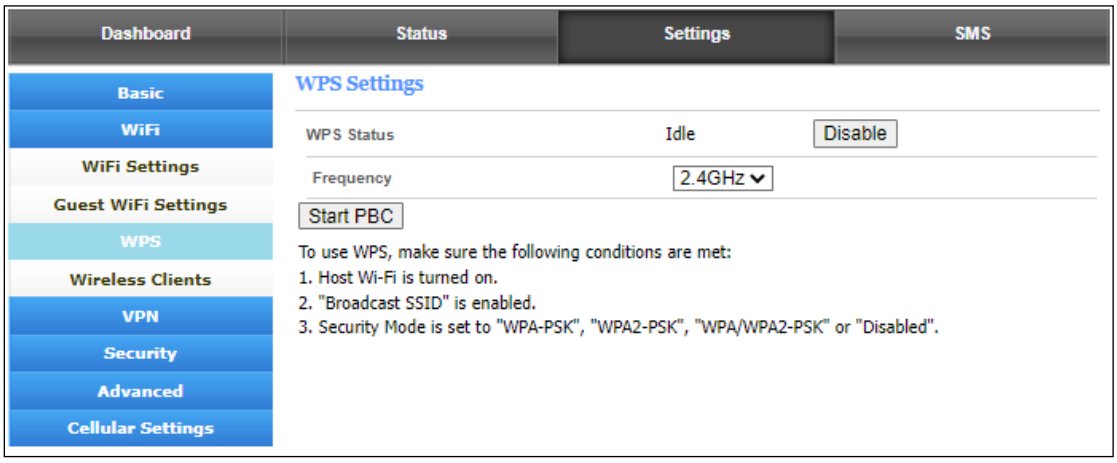
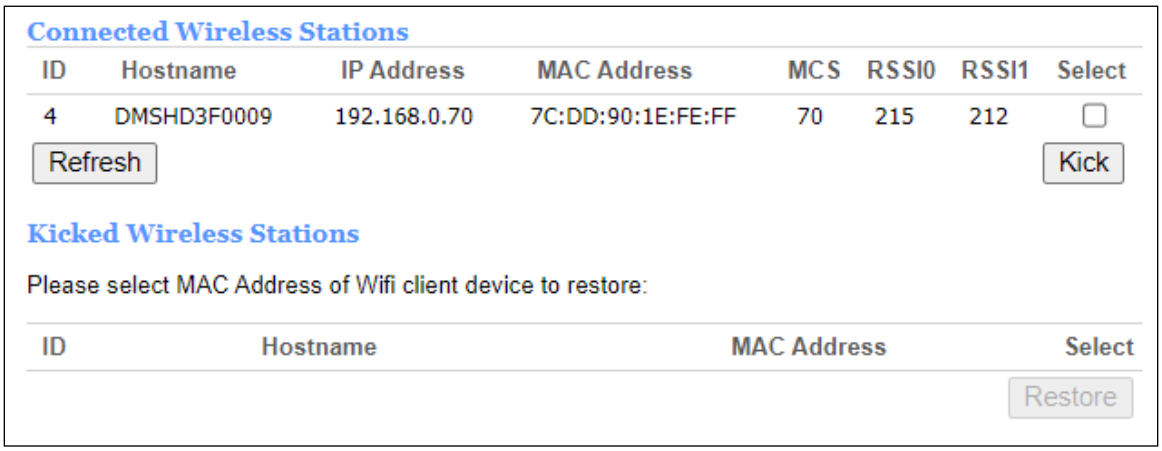


Figure 30 WiFi > WPS Settings

3.4.2.4 Wireless Clients

From this page, you can view the connected wireless devices' information, such as, IP address, MAC address, MCS, RSSI and so on. You can also kick/block the selected users by clicking the "Block" button, then the connection between the wireless clients and the router will be disconnect immediately.
The users that you kicked will be shown on the "Kicked Wireless Stations" list. You can restore them to allowed, if needed.



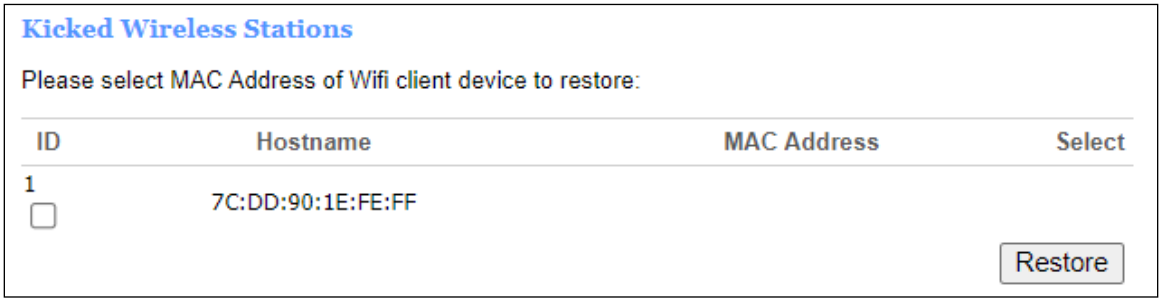


Figure 31 WiFi > Wireless Clients

3.4.3 VPN

From this page, you can use the VPN feature, as required. By default, this feature is disabled.
You can find different VPN types (i.e., PPTP, IPsec, L2TP and GRE). You must know how to use them, otherwise check with your ISP or VPN provider.

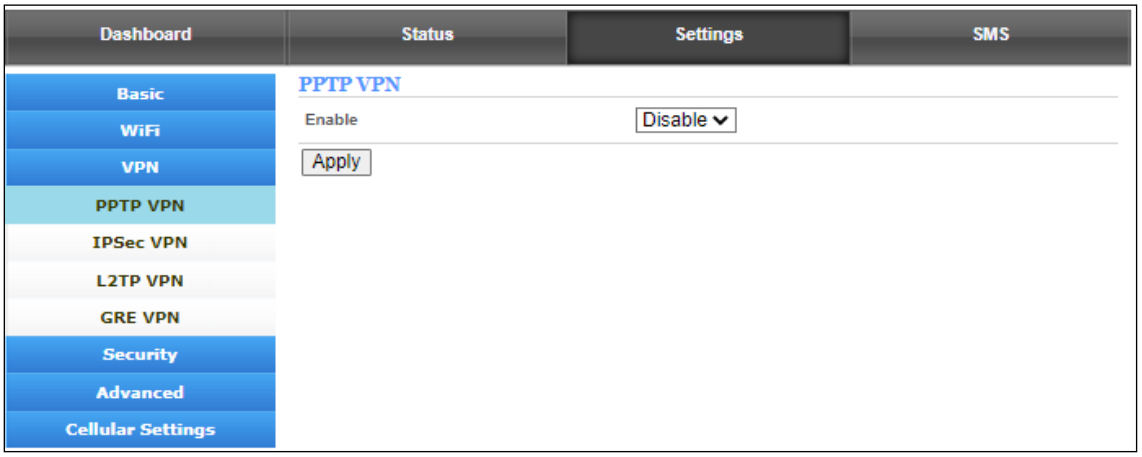


Figure 32 VPN

3.4.4 Security

On this page, you can find basic security/firewall features supported by this router. You can define them as per your requirements.

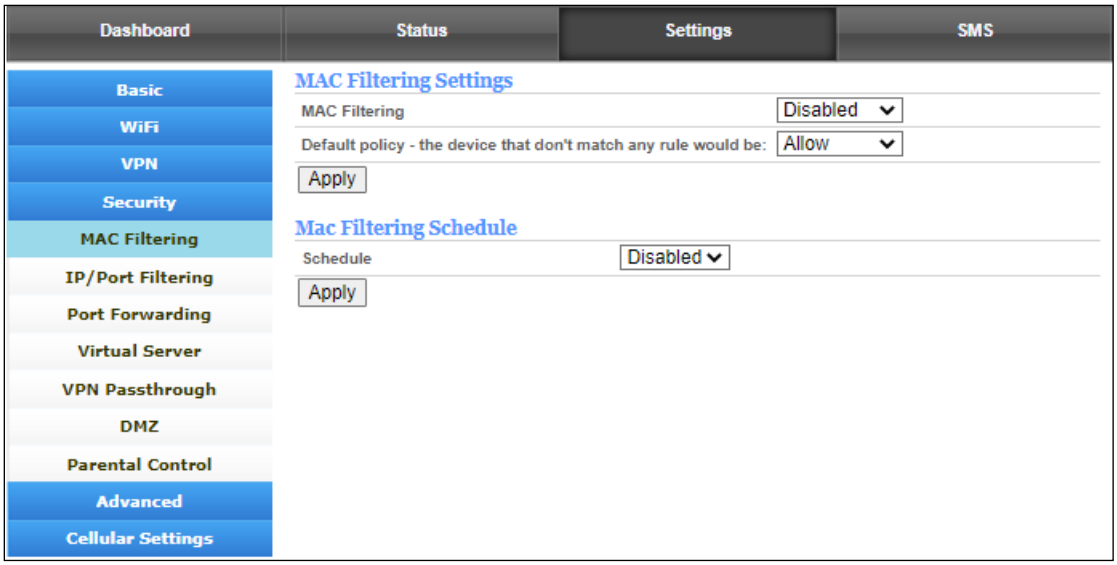


Figure 33 Security

3.4.4.1 MAC Filtering

This function is a powerful security feature that allows you to specify which user(s) are not allowed to connect with this router and surf the Internet.

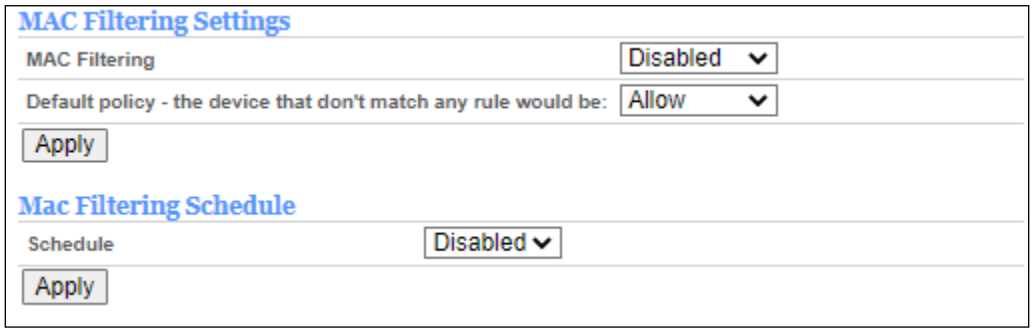


Figure 34 MAC Filtering

The default MAC filtering setting is disabled, so you should enable it before you begin to configure the filter. Then click the “Add New” button and you can configure the rules you like.

Default Policy: The packets that don’t match with any rules would be “Allow/Deny”. If you choose the “Allow” button here, the MAC address that you add would be dropped. Otherwise, only the MAC addresses on the rule table can be accepted.

The new rules will be shown on the rule table, here you can delete the rules that you have selected and add new rules sequentially. The maximum rule count is 10.

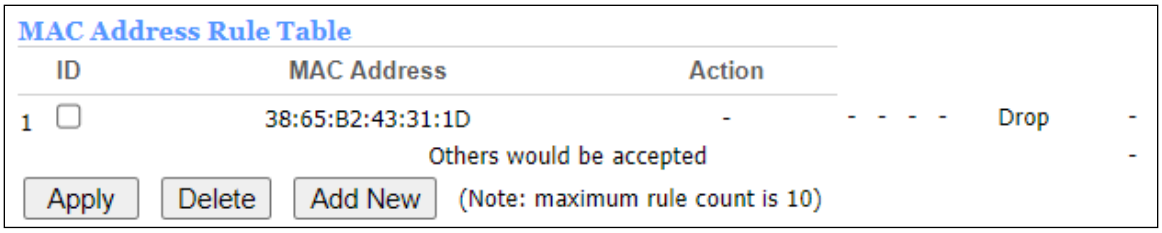


Figure 35 MAC Filtering Rule Table

The MAC Filtering Schedule gives you the option to set up a schedule for the filtering policy.

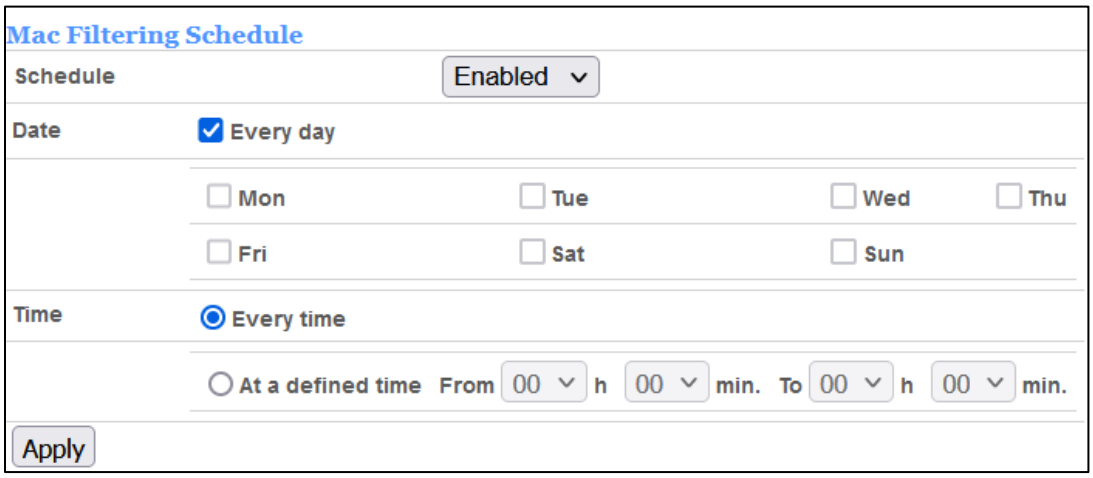


Figure 36 MAC Filtering Schedule

3.4.4.2 IP/Port Filtering

From this page, you can configure the IP/Port filter to forbid relevant users from accessing it via the router.

The default IP/Port filter setting is disabled, so you should enable it before you begin to configure the filter. Click the “Add New” button to configure settings, as needed.

Default Policy: The packets that don’t match with any rules would be “Dropped/Accepted”. If you choose “Dropped” here, the action of the new rule would be “Accept”. Otherwise, the action is “Drop” by default, and the packet that doesn’t match with any rules would be accepted.

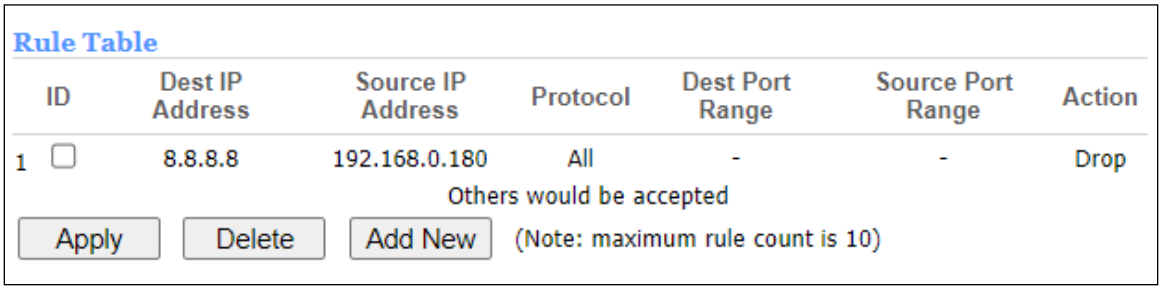


Figure 37 IP/Port Filtering Settings

- **Dest IP Address –** The IP address of a website that you want to filter (such as Google 74.125.128.106).
- **Source IP Address -** The IP address of a PC (such as 192.168.0.2).
- **Protocol -** TCP, UDP, ICMP
- **Dest Port Range –** Set a fixed value (such as 21-21) to restrict Internet access to a single user.
- **Source Port Range -** 1~65535
- **Action -** Accept, Drop

The new rules will be shown on the rule table, you can delete the rules that you have selected or add new rules. The maximum rule count is 10.

3.4.4.3 Port Forwarding

Clicking on the header of the "Port Forwarding" button will take you to the "Port Forwarding" page. By clicking on the "Add New" button, you can configure IP addresses and set a port range to achieve the port forwarding purpose.

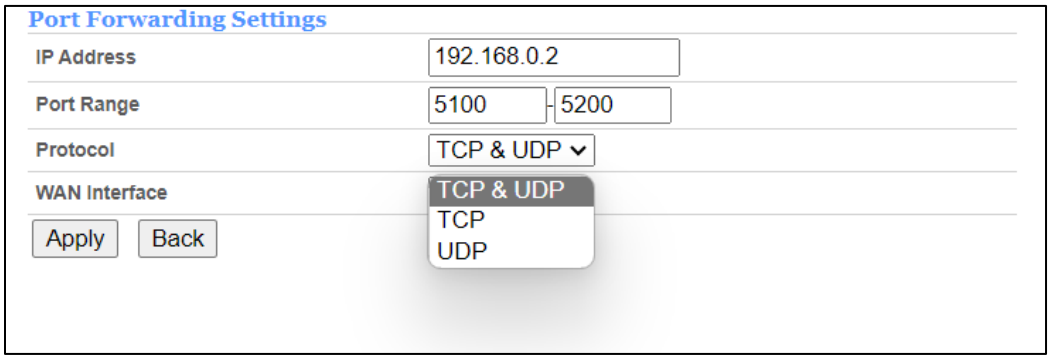


Figure 38 Port Forwarding Settings

- **IP Address -** The IP address of the PC running the service application.
- **Port Range -** You can enter a range of the service port or set a fixed value.
- **Protocol -** UDP, TCP, TCP & UDP.
- **WAN Interface –** BOTH, LTE and ETH WAN. Choose on which interface to do the port forwarding.

The new rules will be shown on the Rule Table. You can delete the items that you have selected or add new rules by clicking the "Add New" button. The maximum rule count is 20.

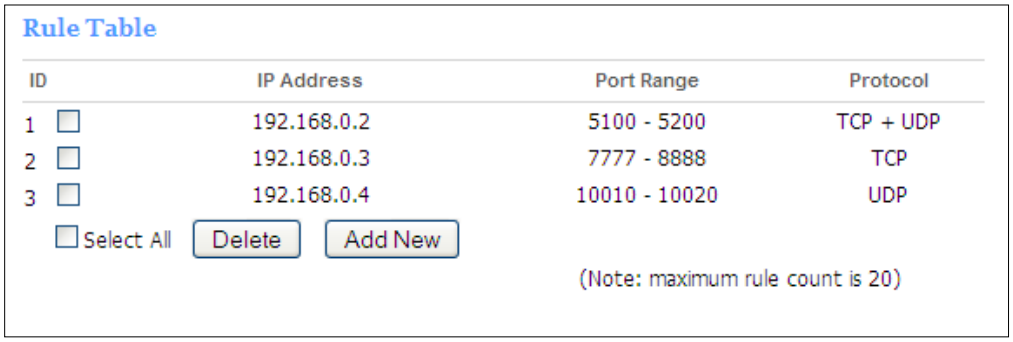
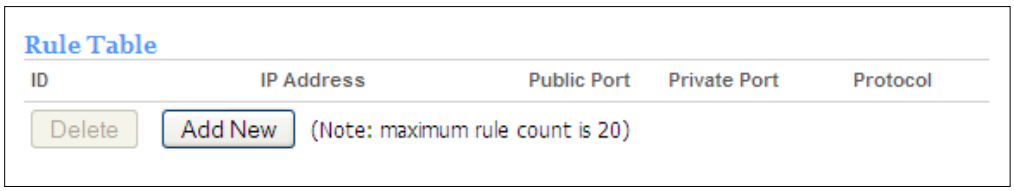


Figure 39 Port Forwarding Rule Table

3.4.4.4 Virtual Server

Clicking on the header of the "Virtual Server" button will take you to the "Virtual Server" page. It is a feature that is similar to port forwarding. Click on the "Add New" button to add a new rule. You can configure the IP Address, Public Port, Private Port and Protocol to achieve the virtual server function.



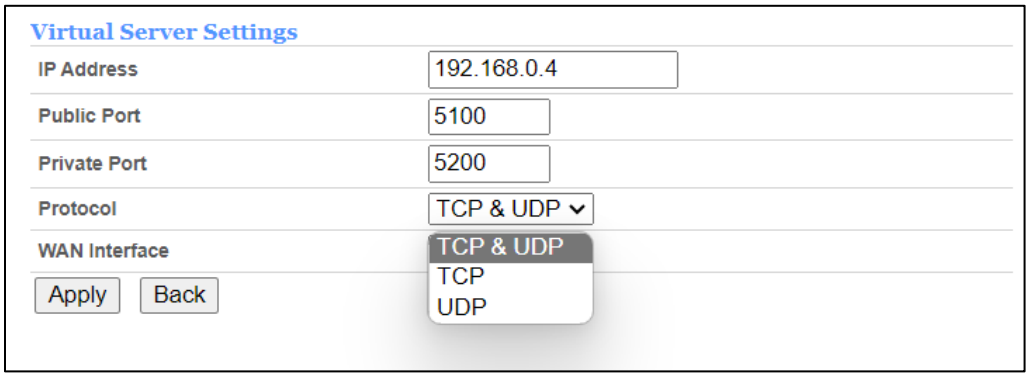


Figure 40 Virtual Server Settings

- **IP Address -** The IP address of the PC running the service application.
- **Public Port -** The server-side port.
- **Private Port -** The client-side port. It can be same as the public port.
- **Protocol -** UDP, TCP, TCP & UDP.
- **WAN Interface –** BOTH LTE and ETH WAN. Choose on which interface to deliver the Virtual Server function.

The new rules will be shown on the Rule Table. You can delete the items that you have selected or add new rules by clicking the "Add New" button. The maximum rule count is 20.

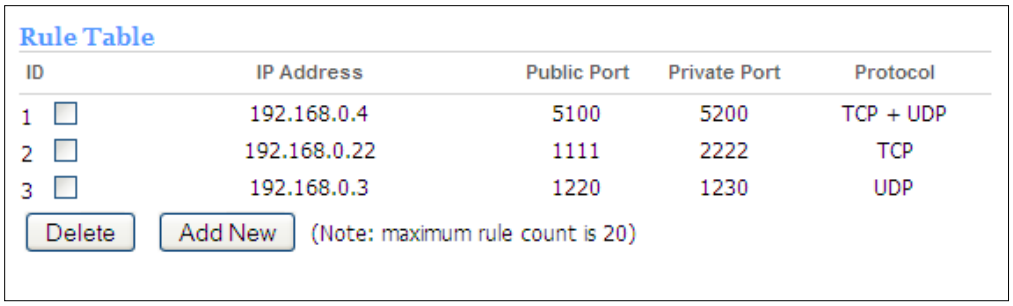


Figure 41 Virtual Server Rule Table

3.4.4.5 VPN Passthrough

A virtual private network (VPN) is a point-to-point connection across a private or public network (Internet).

VPN Passthrough allows the VPN traffic to pass through the router. Thereby we can establish VPN connections to a remote network. For example, VPNs allow you to securely access your company's intranet at home. There are three main kinds of the VPN tunneling protocol: PPTP, L2TP and IPSec.

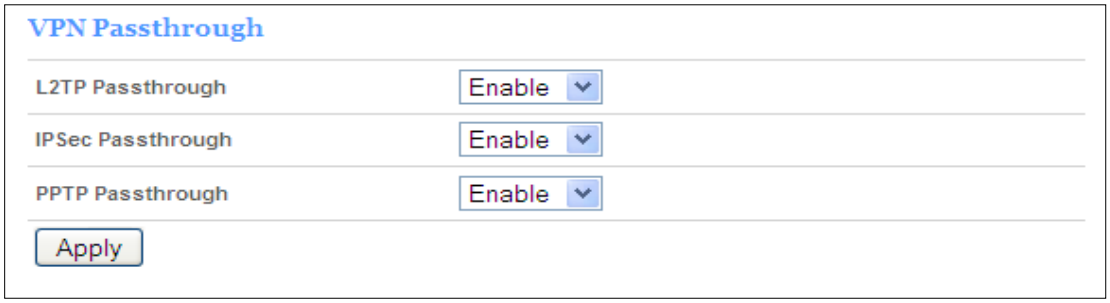


Figure 42 VPN Passthrough

Note: VPN Passthrough does not mean the router can create a VPN endpoint. VPN Passthrough is a feature that allows VPN traffic created by other endpoints to "pass through" the router.

3.4.4.6 Demilitarized Zone

From this page, you can configure a Demilitarized Zone (DMZ) to separate the internal network and the Internet.

- **WAN Interface -** You can select LTE/ETH WAN port.
- **DMZ IP Address -** The IP address of your PC (such as 192.168.0.3).

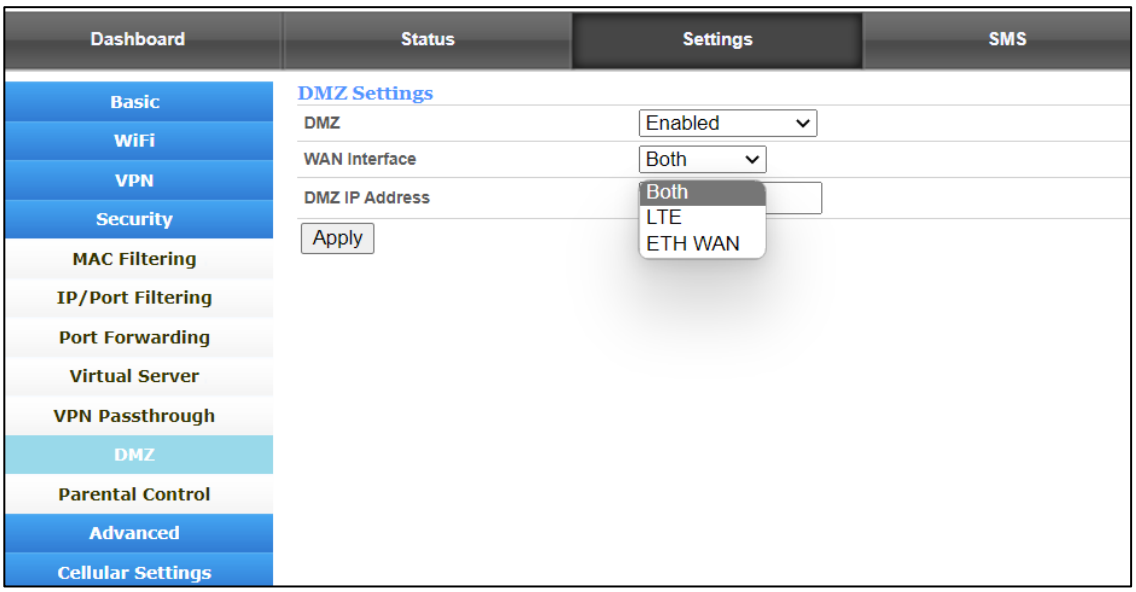


Figure 43 DMZ Settings

3.4.4.7 Parental Control

By default, it is disabled. If you enable the Parental Control feature, the rules added to the Rule Table will determine when access to the Internet or website will be denied. Internet or website access will be automatically blocked in the defined time.

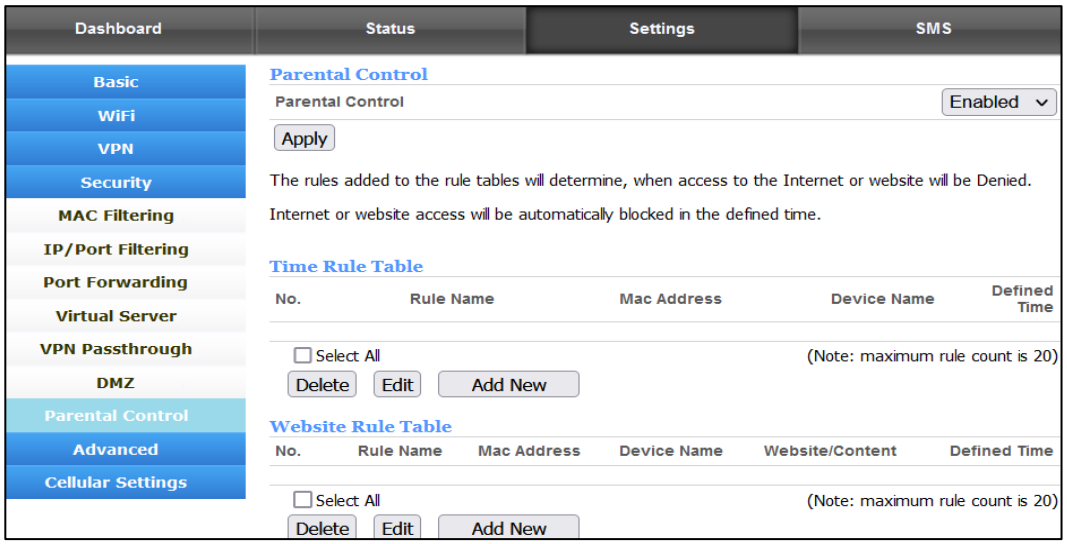


Figure 44 Parental Control

3.4.5 Advanced

3.4.5.1 Diagnostic

On this page, you will find "Ping" and “Traceroute” features.
Ping: allows you to check the reachability of an IP address/domain name.
Traceroute: allows you to check the host/route for an IP address/domain name.

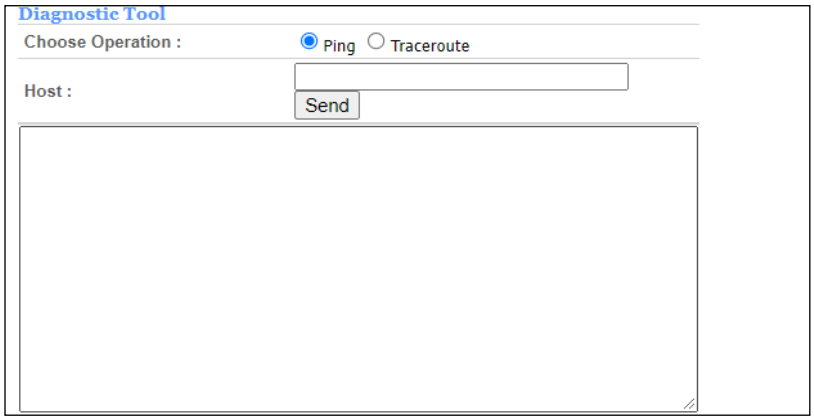


Figure 45 Advanced > Diagnostic

3.4.5.2 Dynamic DNS

On this page, you can set up the DDNS service.

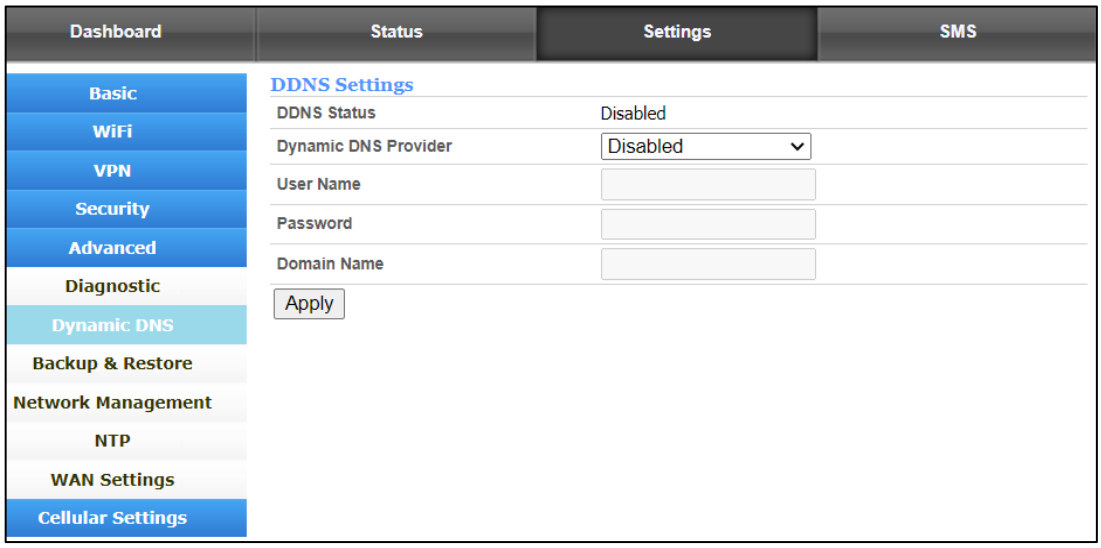


Figure 46 Advanced > Dynamic DNS

3.4.5.3 Backup & Restore

On this page, you can back up the existing configuration and restore it (if required). When you click on Backup button, a Configuration file will be saved as a data file to the local PC. You can restore this router configuration from the files that you saved.

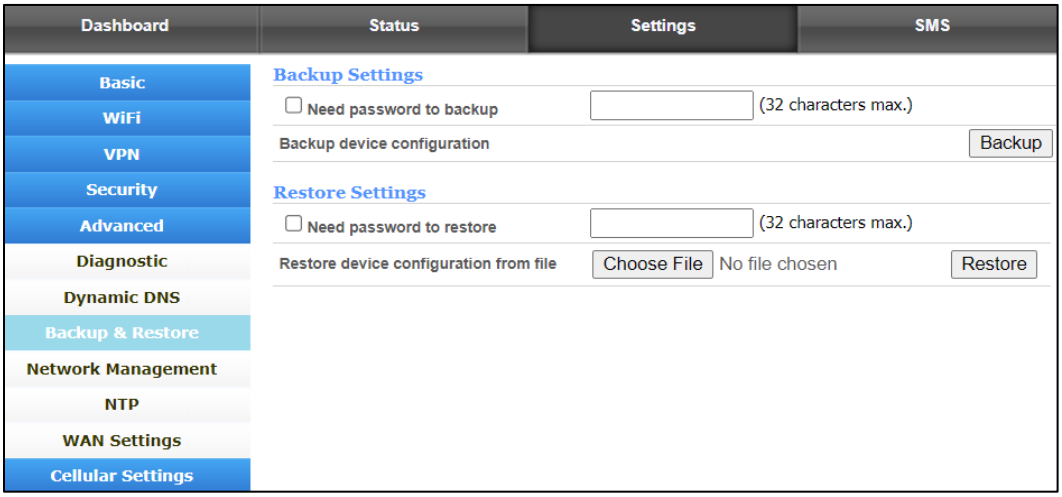


Figure 47 Advanced > Backup & Restore

3.4.5.4 Network Management

On this page, you can view and modify features related to the management of this router.

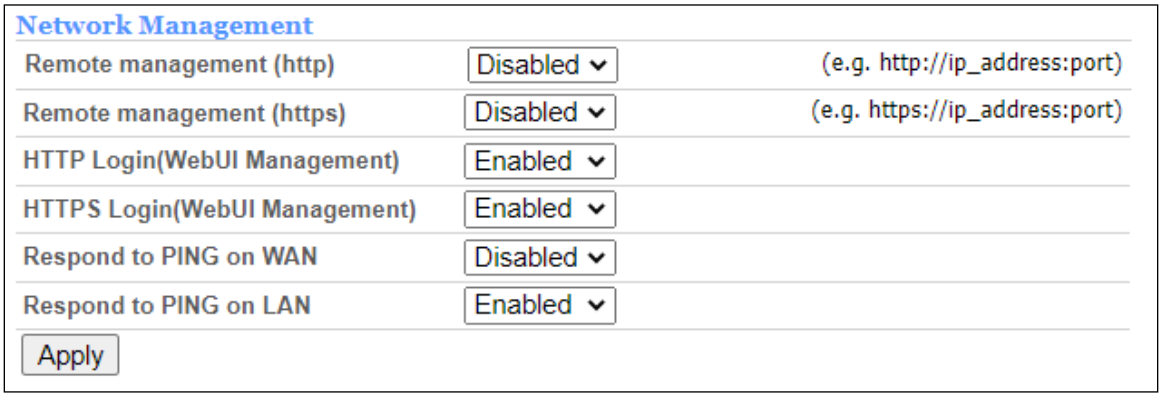


Figure 48 Advanced > Network Management

- **Remote Management (http)**

You can access the router's WebGUI remotely using its WAN IP HTTP protocol when the remote management feature is enabled.

- **Remote Management (https)**

You can access the router's WebGUI remotely using its WAN IP HTTPS protocol when the remote management feature is enabled.

- **Respond to PING on WAN**

By default, ping on WAN is not allowed. You can Enable it here.

- **Respond to PING on LAN**

By default, ping on LAN is allowed. You can disable it here.

- **HTTP Login (WebGUI Management)**

This function allows users to login to the WebGUI via the http protocol method.

- **HTTPS Login (WebGUI Management)**

This function allows users to login to the WebGUI via the https protocol method.

3.4.5.5 NTP

From this page, you can set the Current Time, Time Zone, NTP Server and NTP synchronization. When this router obtains the WAN IP, the current time will synchronize with the NTP server automatically.

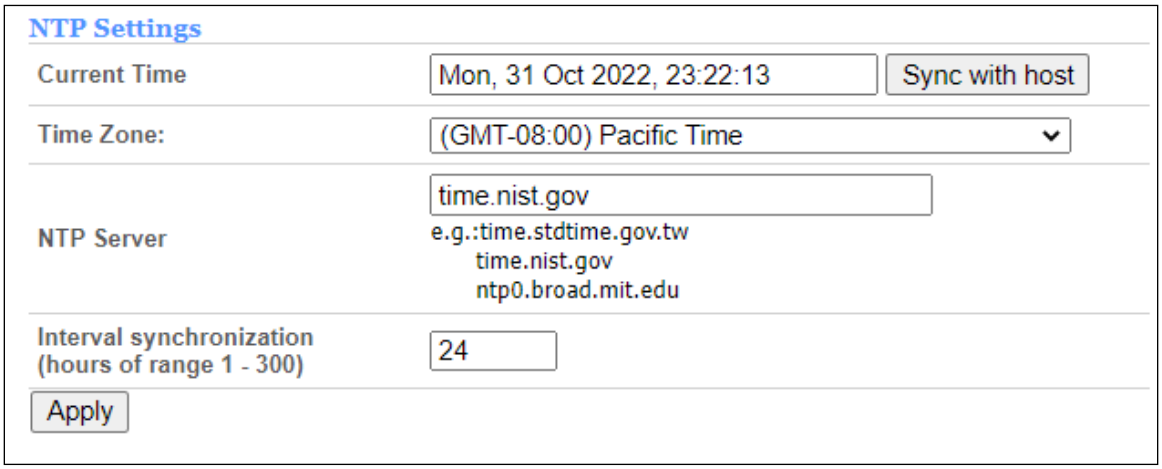


Figure 49 NTP

3.4.5.6 WAN Settings

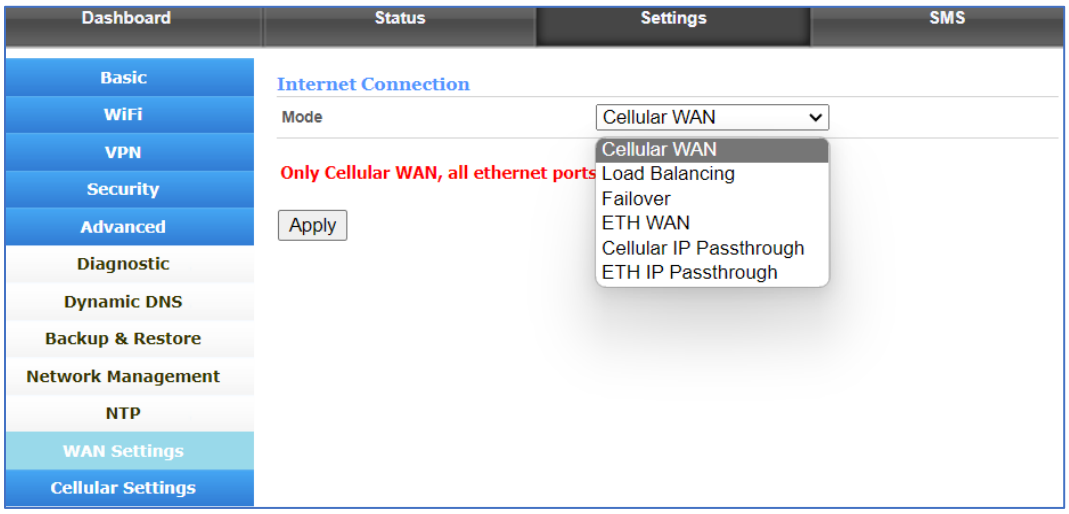


Figure 50 Advanced > WAN Settings

There are six options in WAN Settings:

1. Cellular WAN: LTE/5G Wireless connection is the only WAN connection.
2. Load Balancing: Both Cellular and Wired connection works at the same time using load balancing.
3. Failover: Wired connection as primary and Cellular connection as back up, vice versa.
4. ETH WAN: Wired connection is the only WAN connection.
5. Cellular IP Passthrough: After it is enabled, the Cellular WAN IP address will be assigned to the PC/Device connected to Ethernet port LAN1.
6. ETH IP Passthrough: After it is enabled, the Wired WAN IP address will be assinged to the PC/Device connected to Ethernet port LAN1.

3.4.6 Cellular Settings

3.4.6.1 Network

On this page, you can check and/or uncheck the network bands for 4G and 5G bands supported.

Auto: The router will automatically connect to the network with the best available signal/band.
4G Only: The router will use only 4G bands to connect with the network.
5G Only: The router will use only 5G bands to connect with the network.

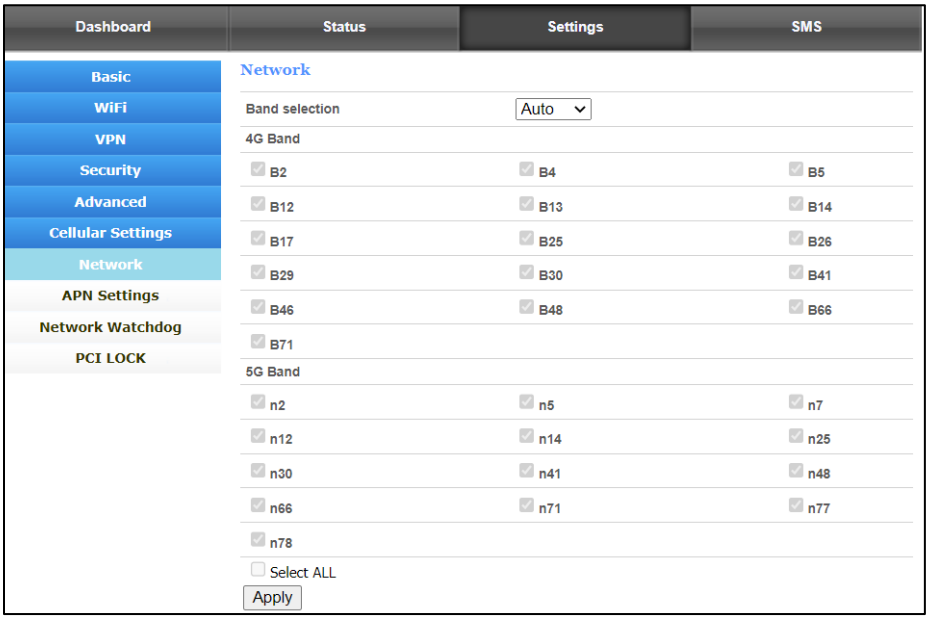


Figure 51 Cellular Settings > Network

3.4.6.2 APN Settings

On this page, you can find APN related settings. The default APN mode is set to “Auto”, if you want to configure the APN, you should choose the manual mode, then you can define the required APN settings by clicking on the “Add New” button.

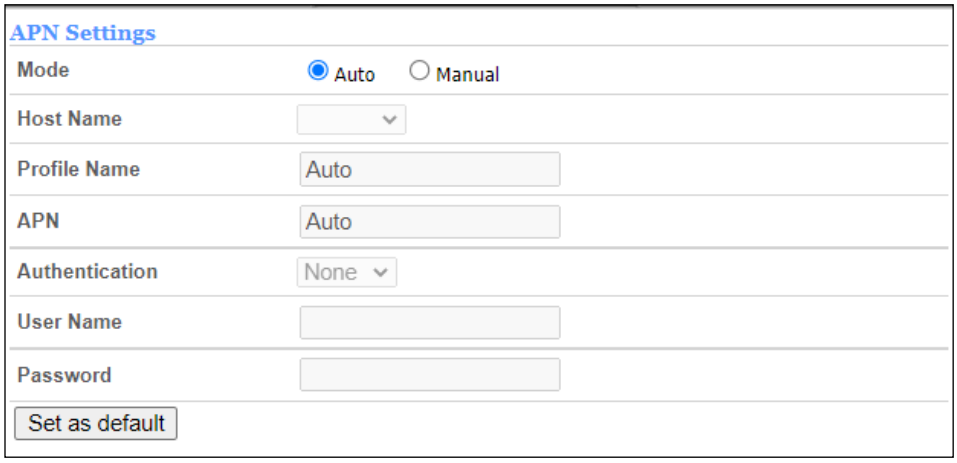


Figure 52 Cellular Settings > APN

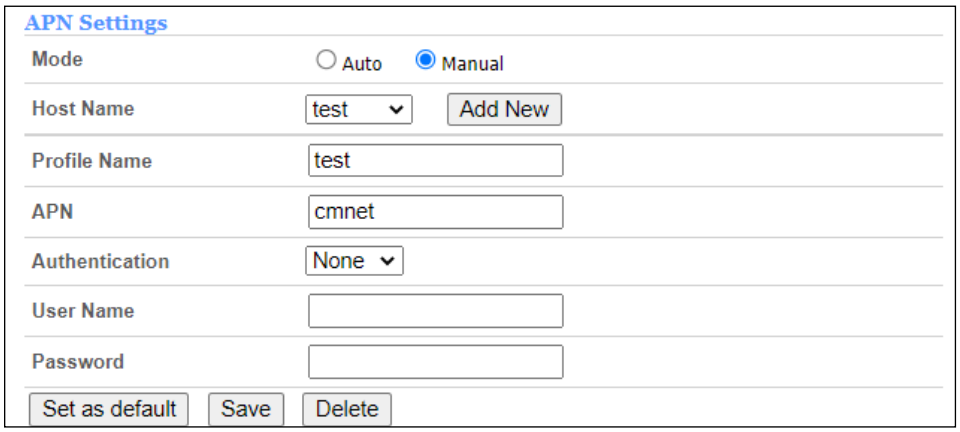


Figure 53 APN > Manual APN

From the “Host Name” option, you can choose the APN that you had configured, then click “Set as default” to take effect.

3.4.6.3 Network Watchdog

On this page, you can view the network watchdog feature which is designed to support uninterrupted data services defined by the ISP.
Sometimes the router finds connected and acquired WAN IP addresses from the network but no data/internet services. In that scenario, this feature can reboot/re attach to network.

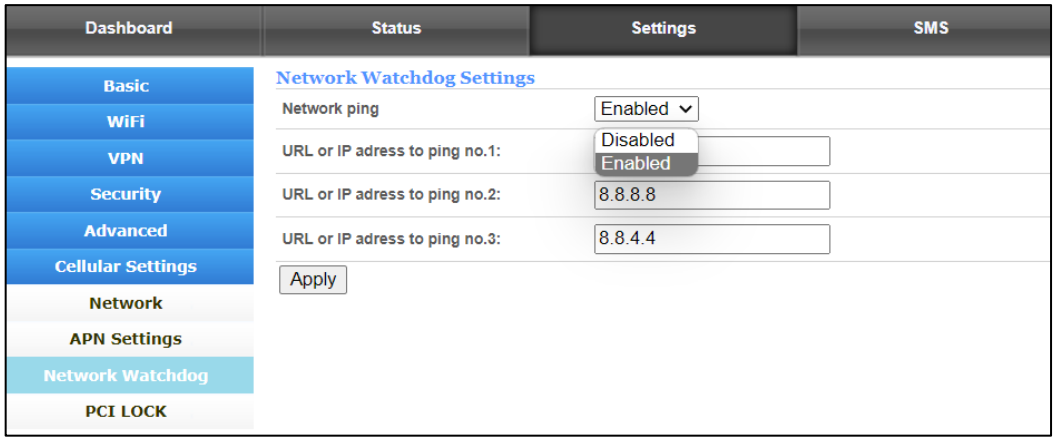


Figure 24 Cellular Settings > Network Watchdog

You can define the URL/IP address that the router will use to check the internet/data accessibility in regular intervals.

3.4.6.4 PCI LOCK

You can set up the PCI LOCK value to optimize device performance.

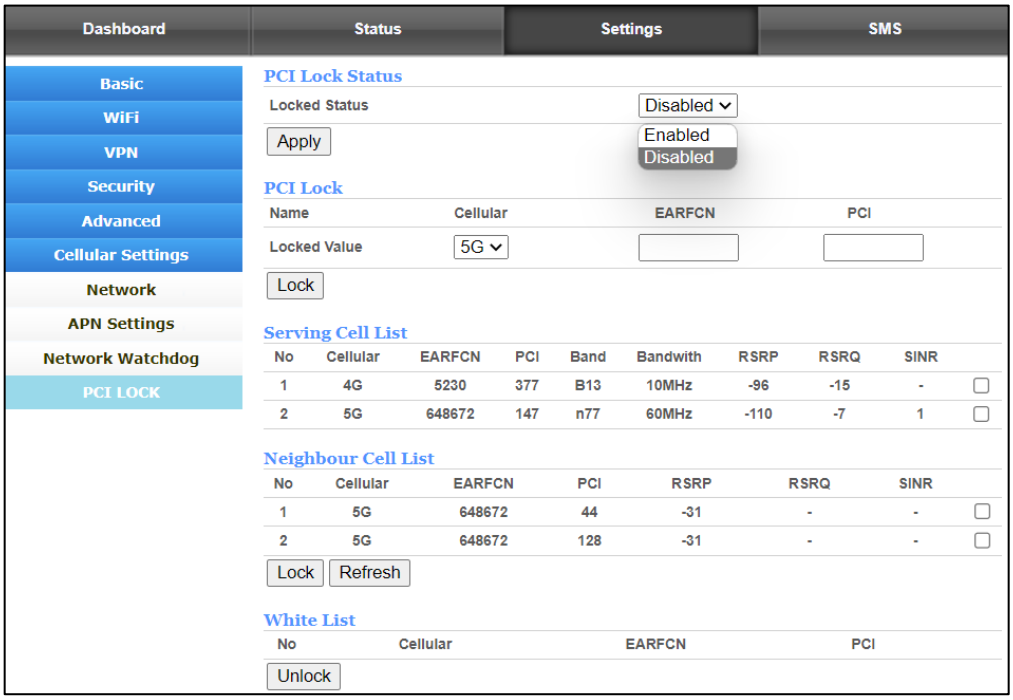


Figure 55 Cellular Settings > PCI LOCK

3.5 SMS

On this page, you will find the Inbox, Outbox and Drafts options related to SMS. You can send receive SMS on this page.

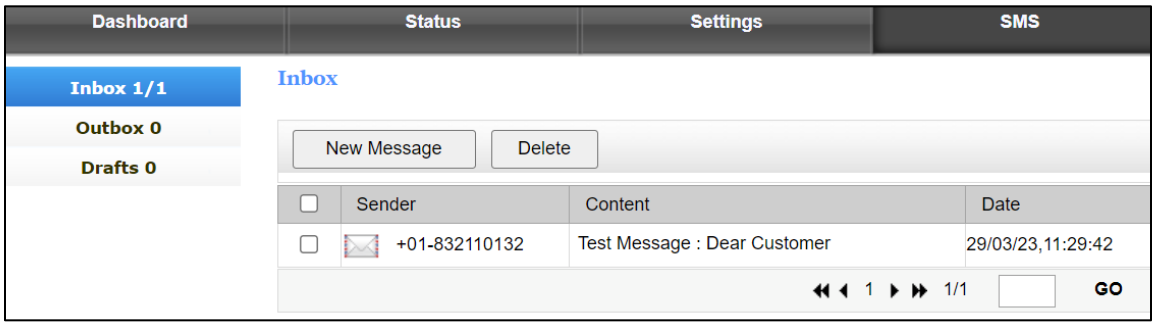


Figure 56 SMS

- **Inbox:** You can view/read all received messages.
- **Outbox:** You can view all sent messages.
- **Draft:** You can view draft messages.

To edit and send a text message, click the “New message” button.

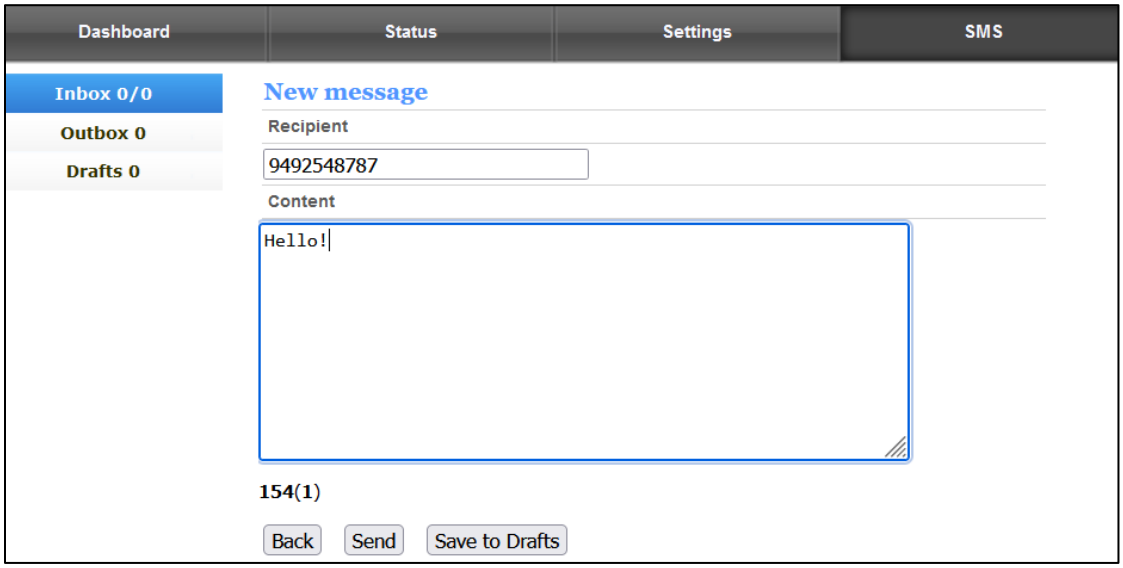


Figure 57 New message

Note: Please confirm with your service provider that SMS feature is provisioned by the network first.

4. ATRACS Cloud Connect Remote Management

You can manage the device using the ATEL Remote Management Platform ATRACS, by visiting http://aags.a-tracs.com or https://aags.a-tracs.com. Please refer to the ATRACS User Manual for details.

Common Problems, FAQ's and Solutions

1. **The Power LED indicator is not ON.**
    a. Confirm the power adapter is plugged properly into the AC socket.
    b. Confirm the power adapter is connected to the device properly.
    c. Note: Use only the Power Adaptor that is provided and comes packaged with the device.

2. **Web Based Utility (WebGUI) cannot be accessed.**
    a. Ensure that the WB550 is powered on.
    b. Ensure that your wireless client is connected and has acquired the IP address from the device over Wired or wireless connection.
    c. Check with another web browser or try to reset the browser cache memory.
    d. Try to Reboot or factory reset the device.

3. **Device cannot access the network.**
    a. Ensure your USIM card is valid and active.
    b. Check the 5G/4G LED, it should be On. If it is off, then login to WebGUI and check the Network details available on the home page.
    c. Network status should be showing Connected. If it is showing disconnected or connecting, check the network parameters RSRP, SINR values.
        i. SINR value (dB) should be Positive.
        ii. RSRP value must be greater than -115dBm. Preferred value should be around -90 dBm.
    d. Try to Reboot or factory reset the device.

4. **How do I optimize the device to maximize throughput?**
    a. You can move the device around to find the best location for data throughput. Generally, a higher location near windows and a place

with minimum obstruction to carrier cell towers will result in a better data throughput.

b. You can log into the WebGUI to check the RSRP/RSRQ/SINR to verify the changes to signal quality.
c. In the WebGUI, you can also go to “Settings” > “Cellular Settings” > “Network”, to specify the band you want to use. Please check and confirm band information with your carrier before you adjust the band you prefer. Please note that we don’t encourage customers to adjust these features by themselves if you are not familiar with mobile technology.

Regulatory Statements

FCC Equipment Authorization ID: XYO-WB550

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- 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.

FCC CAUTION: Any changes or modification not expressly approved by ATEL, the party responsible for compliance could void the user's authority to operate this equipment.
This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-- Reorient or relocate the receiving antenna.
-- Increase the separation between the equipment and receiver.
-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-- Consult the dealer or an experienced radio/TV technician for help.

RF Exposure Warning Statements:
The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons during the normal operations.

NOTE: The Radio Frequency (RF) emitter installed in your modem must not be located or operated in conjunction with any other antenna or transmitter, unless specifically authorized by ATEL.

Safety Hazards

Follow Safety Guidelines
Always follow the applicable rules and regulations in the area in which you are using your device. Turn your device off in areas where its use is not allowed or when its use may cause interference or other problems. Note that this type of device should be placed at least 10 ft from work area(s).

Electronic Devices
Most modern electronic equipment is shielded from radio frequency (RF) signals. However, inadequately shielded electronic equipment may be affected by the RF signals generated by your device.

Medical and Life Support Equipment
Do not use your device in healthcare facilities or where medical life support equipment is located as such equipment could be affected by your device's external RF signals.

Pacemakers

- It is recommended to maintain a minimum separation of six inches between a RF device and a pacemaker in order to avoid potential interference with the pacemaker.
- Persons with pacemakers should always follow these guidelines:
- Always keep the device at least six inches away from a pacemaker when the device is turned on.
- Place your device on the opposite side of your body where your pacemaker is implanted in order to add extra distance between the pacemaker and your device.
- Avoid placing a device that is on next to a pacemaker (e.g., do not carry your device in a shirt or jacket pocket that is located directly over the pacemaker).
- If you are concerned or suspect for any reason that interference is taking place with your pacemaker, turn your device OFF immediately.

Hearing Devices

When some wireless devices are used with certain hearing devices (including hearing aids and cochlear implants) users may detect a noise which may interfere with the effectiveness of the hearing device.

Use of Your Device while Operating a Vehicle

Please consult the manufacturer of any electronic equipment that has been installed in your vehicle as RF signals may affect electronic systems in motor vehicles. Please do not operate your device while driving a vehicle. This may cause a severe distraction, and, in some areas, it is against the law.

Use of Your Device on an Aircraft

Don't use your device during flight，it may violate FAA regulations. Because your device may interfere with onboard electronic equipment, always follow the instructions of the airline personnel and turn your device OFF.

Blasting Areas

In order to avoid interfering with blasting operations, your device should be turned OFF when in a blasting area or in an area with posted signs indicating that people in the area must turn off two-way radios. Please obey all signs and instructions when you are in and around a blasting area.

Disclaimer:

Certain variations may be present between the device and user manual description depending on software release or specific network services. ATEL shall not be held legally responsible for such deviations, if any, nor for their potential consequences.

Limited Warranty:

The full ATEL USA Warranty Policy can be found at www.atel-usa.com/warranty. On this page you can "Start a Warranty Claim", "Check on an Existing Claim" and read the Warranty Policy by clicking on "ATEL's Warranty Policy". Please follow all warranty instructions available and if you have any questions contact us at support@atel-usa.com. Note that some actions such as, but not limited to, using sharp objects to open the device, may void the warranty.

Trademark. ATEL & Axis are trademarks owned and protected by Asiatelco Technologies, Inc.
© 2023 Asiatelco Technologies, Inc. All rights reserved.

8310 S Valley Hwy Ste 300 Englewood, CO 80112

missiontelecom.org