



User Guide

Enterprise Wi-Fi 7 Tri-Band Access Point

LITEON Model: WPB8326

Version: v1.1

Date: 2025-08-05

Table of Contents

Chapter 1	Overview of WPB8326 Access Point.....	3
Chapter 2	Interface Definition	4
	WPB8326 Interface Definition	4
Chapter 3	How to connect to WPB8326	5
3.1.	Connect to WPB8326	5
3.2.	Configure IP	5
Chapter 4	Configuration and Management	6
4.1.	First Login	6
4.2.	Status C Tools.....	7
4.3.	System Config.....	9
4.4.	Network Config	13
4.5.	Wi-Fi Config	17
4.6.	System Log	25
4.7.	Statistic Status	28
4.8.	Client List.....	29
4.9.	VLAN Config.....	29
4.10.	QoS Config	31
4.11.	Bandwidth Control	33
4.12.	Scan Radio	38
Chapter 5	FAQ	45

Chapter 1 Overview of WPB8326 Access Point

The WPB8326 supports 2.4G/5G/6GHz wireless access and one 5G Ethernet Port and one 1G Ethernet Port.

➤ **Wireless Access:**

- **2.4 GHz radio:**

Supports IEEE 802.11b/g with 4096-QAM and two spatial streams for a data rate of 688 Mbps.

- **5 GHz radio:**

Supports IEEE 802.11b/g with 4096-QAM and two spatial streams for a data rate of 4324 Mbps.

- **6 GHz radio:**

Supports IEEE 802.11b/g with 4096-QAM and two spatial streams for a data rate of 5765 Mbps.

➤ **Wired Access:**

- The E0 / 5G PoE port is used for connecting to uplink switch with power supply.
- The E1 / 1G port is used for connecting Ethernet devices as a LAN port.

➤ **Scan Radio:**

Dedicated tri-band scan radio is for RF environment scan and packet capturing.

The WPB8326 supports power supply by using PoE 802.3at (default) or 12V/2.5A DC external power adapter.

Chapter 2 Interface Definition

WPB8326 Interface Definition

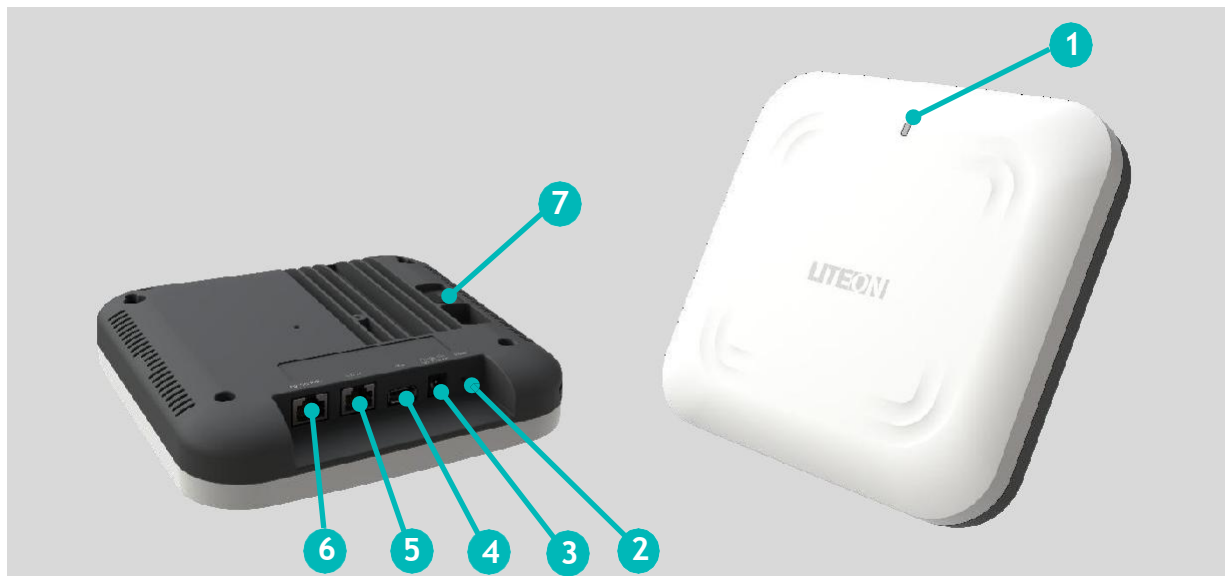


Table 1. AP front and back views

1	LED Indicator	Use the LED on the front of the AP to determine its status. For more information about LED behavior, see Table 2.
2	Reset Button	Factory default reset: hold ≥ 10 seconds
3	Power Input	12V/2.5A DC
4	USB Type-A Port	Reserved
5	E1 / 1G	10/100/1000Mbps RJ-45 Ethernet Port as a LAN port
6	E0 / 5G PoE	10/100/1000/5000Mbps RJ-45 Ethernet Port with PoE as uplink
7	Console Port	4-pin UART console port for debugging purpose VCC (3.3V) pin could be floating, or the voltage should be 3.3V.

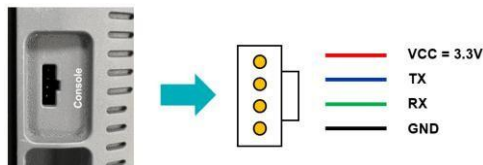


Table 2. LED behavior

Solid Red	The device is powered before initializing
Flashing Red	The device is initializing and booting up
Flashing Green	System is ready, uplink is not connected
Solid Green	Uplink is connected, no client is connected
Solid Blue	Uplink is connected, and client is connected
Flashing Green and Red	Factory reset is triggered
Flashing Green and Blue	System is updating firmware

Note: If the LED is **White**, the status is incorrect, MUST immediately remove the power supply and check the UART pins whether it has connected error.

Chapter 3 How to connect to WPB8326

Before using WPB8326, consider changing its settings to fit the network. Use a laptop or desktop PC to connect to the E1 port or wireless SSID of WPB8326. After the computer is connected to WPB8326, use a web browser to configure and manage the AP device, which will be described in the next chapter.

3.1. Connect to WPB8326

Connect computer to WPB8326:

- Connect by Wi-Fi

The default Wi-Fi SSID and password are listed as follows:

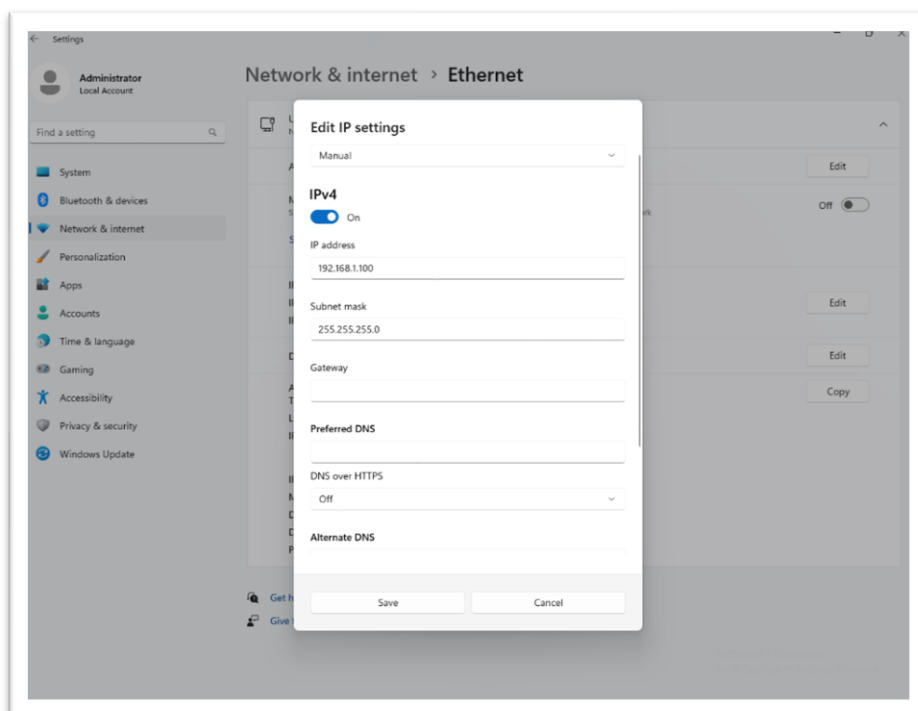
 - WPB8326-2.4G / 1234567890
 - WPB8326-5G / 1234567890
 - WPB8326-6G / 1234567890
- Connect by Ethernet

Connect one end of an Ethernet cable to E1 port of WPB8326.

3.2. Configure IP

- **Default IP**

If WPB8326 is not connected to existing network, the default IP will be 192.168.1.20. In this case, manually configure the IP address of computer to the same subnet as that of WPB8326. e.g., Set computer to 192.168.1.100/255.255.255.0



Dynamic IP

If WPB8326 is connected to existing network via E0 / 5G PoE port, the IP will be assigned by the DHCP server.

Chapter 4 Configuration and Management

WPB8326 provides local web for configuration and management.

4.1. First Login

Open the URL with the web browser and log in with the default password.

- URL with default IP: <https://1G2.168.1.20>
- Default password: 12345678

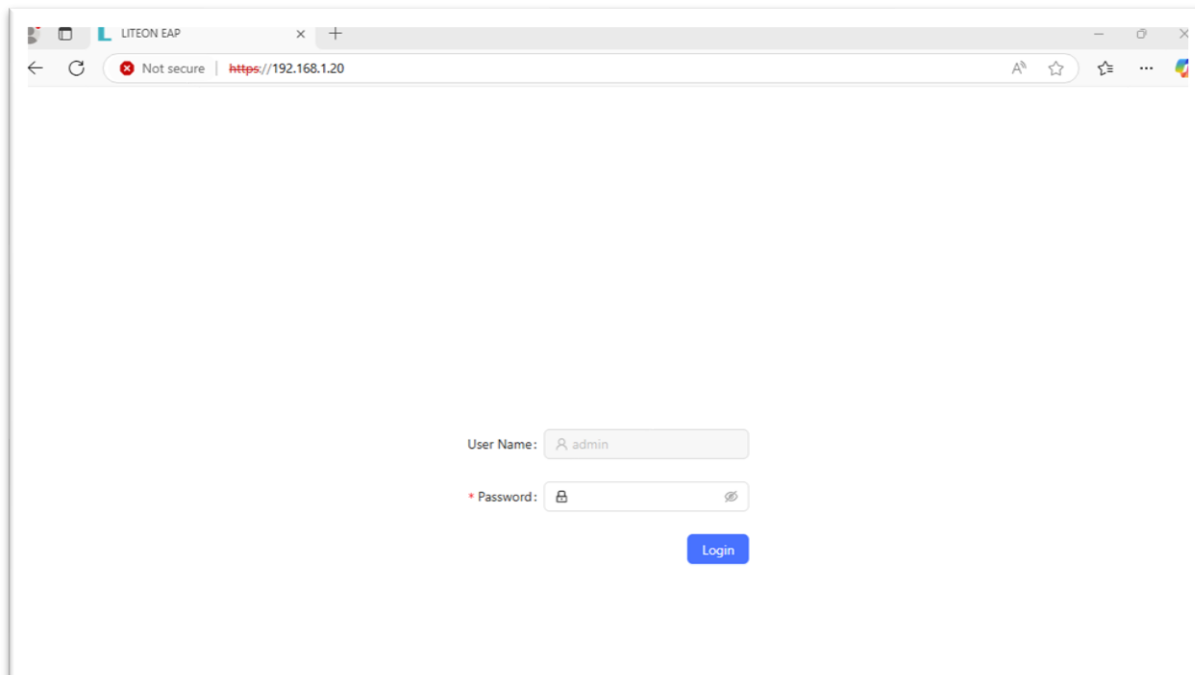


Figure 1. Web Login

NOTE:

- Please use Chrome, Edge, Firefox, or Safari to open web. IE is not supported.

After logging in, the system will prompt you to change login password.

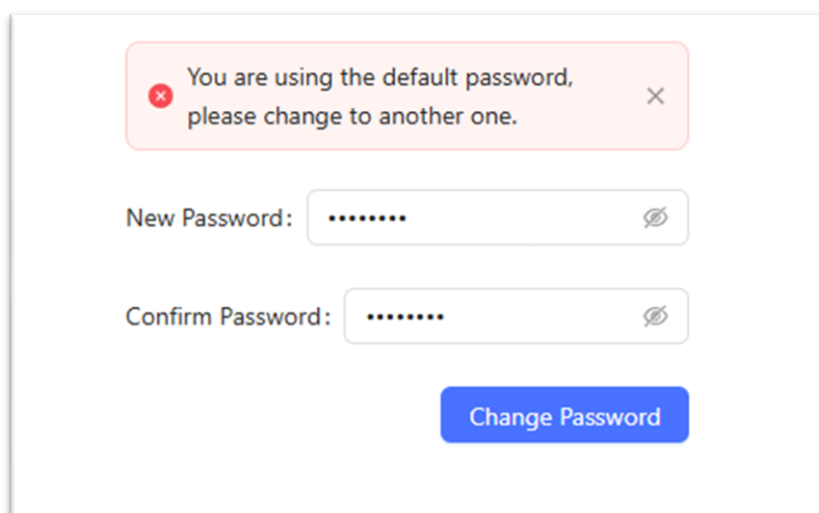


Figure 2. Change default password

After changing the login password, the web will be redirected to the **Status s Tools** page.

4.2. Status s Tools

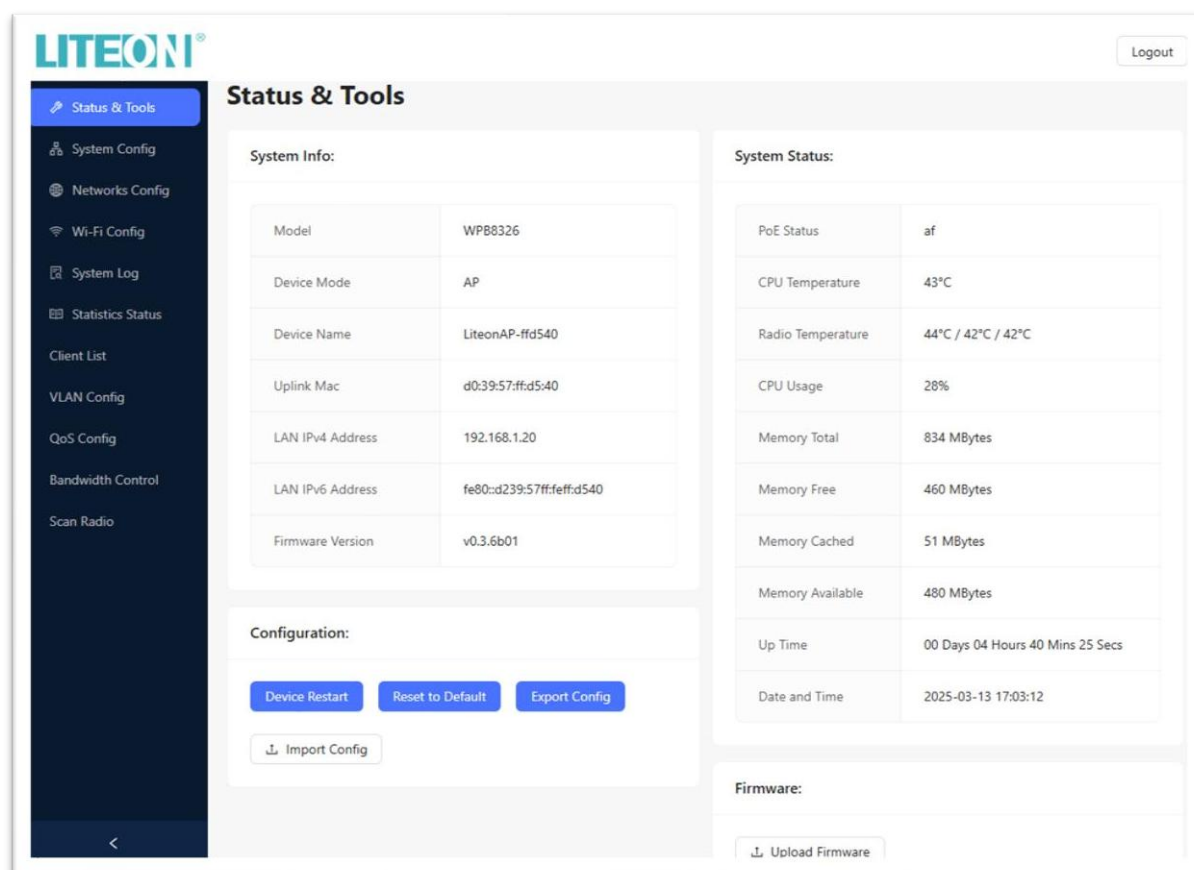


Figure 3. Status C Tools

- **System Info** - Show the information of the System, including Model name, Device Mode, Device Name, Uplink Mac, LAN IPv4 Address, LAN IPv6 Address, and Firmware Version.
- **System Status** - Show the status of the System, including PoE Status, CPU Temperature, Radio Temperature, CPU Usage, Memory Total, Memory Free, Memory Cached, Memory Available, Up Time, Date and Time.
- **Configuration**
 - **Device Restart** - Reboot the WPB8326.
 - **Reset to Default** - Reset the WPB8326 to factory default settings.
 - **Export Config** - Backup and download the current config from the WPB8326. The file name format is Backup-WPB8326-<backup-date>_<firmware-version>.config. e.g., “Backup-WPB8326-2025-03-17_v0.3.6b01.config”.
 - **Import Config** - Upload and restore a configuration to the WPB8326. The config is specific to the WPB8326 model and must be exported from WPB8326 device.

➤ Firmware

- Upload Firmware** - Click "Upload Firmware" to select the firmware file. Once the upload is complete, a confirmation window will pop up, then click "OK" to confirm. The firmware upgrade takes 4-6 minutes depending on the number of SSIDs. When the LED is flashing **Green** and **Blue**, it means the firmware upgrade has begun.
 When the LED turns **Green**, it indicates that the firmware upgrade is complete.

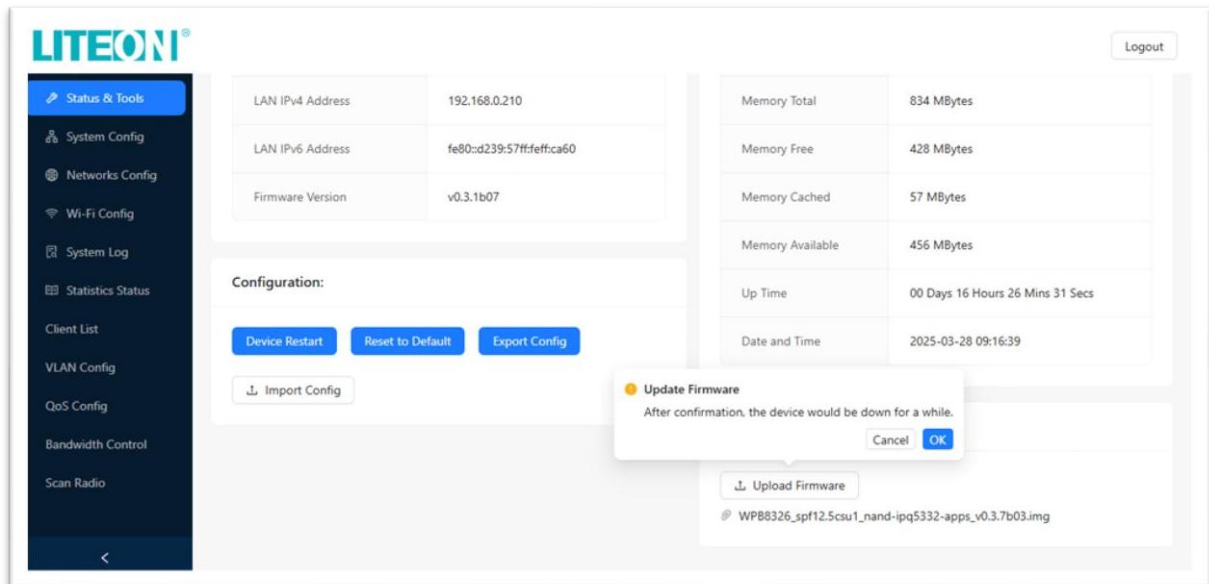


Figure 4. Update Firmware

4.3. System Config

Figure 5. System Config

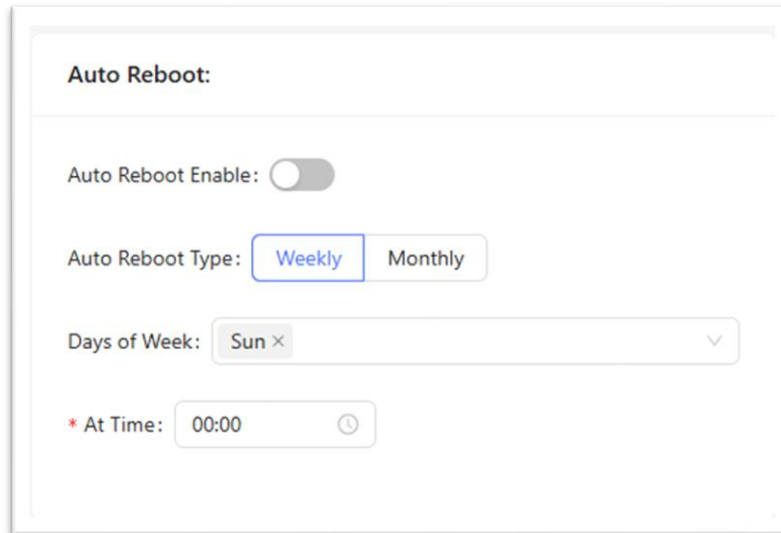
➤ System Settings

- **Device Name** - Hostname of the device.
- **Bonjour Client** - The device can be discovered by Bonjour on local area network when this feature is enabled.
- **Led Enable** - The LED indicator can be turned on/off.

Figure 6. System Settings

➤ Auto Reboot

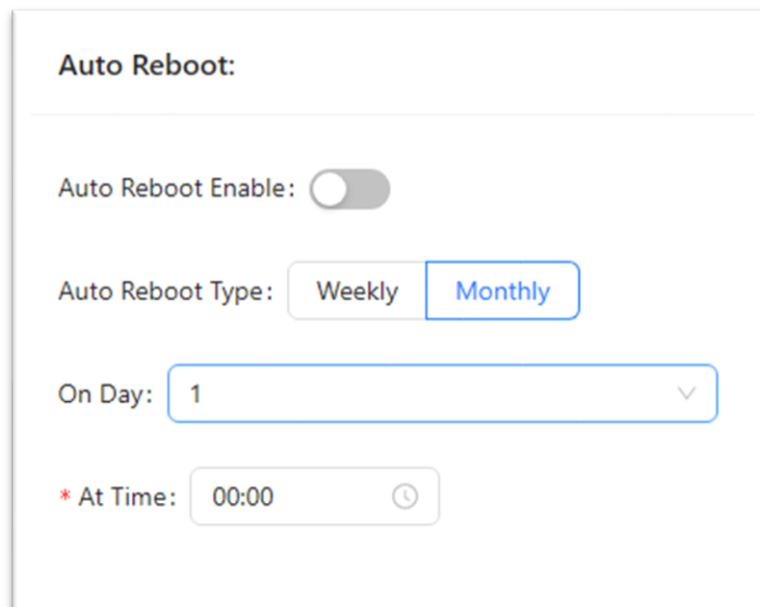
- **Auto Reboot Enable** - Schedule to reboot WPB8326 at specified time.
- **Auto Reboot Type** - The scheduled period (weekly/monthly) for auto reboot.
- **Days of Week** - Select multiple days, including Sun, Mon, Tue, Wed, Thu, Fri and Sat, when Auto Reboot Type is “Weekly”.
- **At Time** - Select the time at which you want WPB8326 to reboot.



The screenshot shows the 'Auto Reboot' configuration window. At the top, the title 'Auto Reboot:' is displayed. Below it, there is a toggle switch for 'Auto Reboot Enable' which is currently turned off. Underneath, the 'Auto Reboot Type' is set to 'Weekly' (highlighted with a blue border) and 'Monthly' is also visible. The 'Days of Week' section shows a dropdown menu with 'Sun' selected and a close icon (X). At the bottom, the '* At Time:' is set to '00:00' with a clock icon for selection.

Figure 7. Auto Reboot - Weekly

- **On Day** - When “Monthly” is selected, choose one day (1 ~ 31) for auto reboot.
NOTE: If the specified day does not exist in a month, the reboot action will not be triggered.

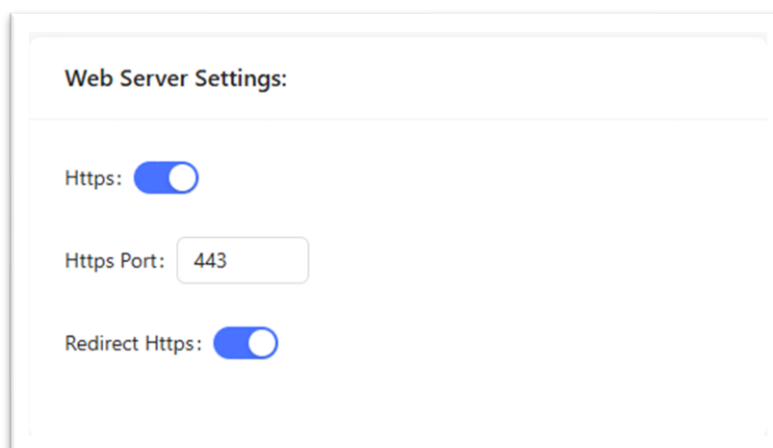


The screenshot shows the 'Auto Reboot' configuration window with 'Monthly' selected for the 'Auto Reboot Type' (highlighted with a blue border). The 'Auto Reboot Enable' toggle is still off. The 'On Day' dropdown menu is set to '1'. The '* At Time:' remains at '00:00' with a clock icon.

Figure 8. Auto Reboot - Monthly

➤ Web Server Settings

- **Https** - When toggled on, HTTPs is used for secure web access; when toggled off, HTTP is used for web access.
- **Https Port** - The HTTPs port used for local web access. By default, the HTTPs port number is 443.
- **Http Port** - When “Https” is toggled off, HTTP port is configurable. The default HTTP port number is 80.
- **Redirect Https** - When HTTPs is enabled, enable “Redirect Https” to redirect HTTP to HTTPS.

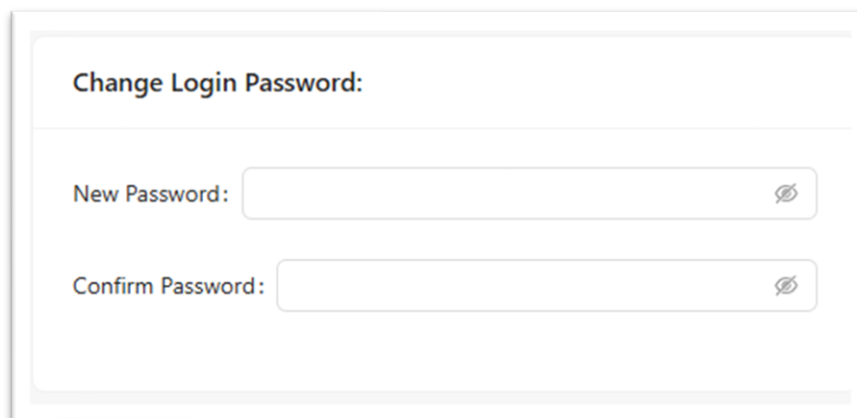


The image shows a 'Web Server Settings' dialog box. It contains three settings: 'Https' is a toggle switch that is turned on (blue); 'Https Port' is a text input field containing the value '443'; and 'Redirect Https' is a toggle switch that is also turned on (blue).

Figure 9. Web Server Settings

➤ Change Login Password - Change the password of local web login.

- **New Password** - The length of the new password must be 8 ~ 64 ASCII characters.
- **Confirm Password** - Must be the same as the new password.



The image shows a 'Change Login Password' dialog box. It contains two text input fields: 'New Password' and 'Confirm Password'. Each input field has a small eye icon to its right, likely for toggling password visibility.

Figure 10. Change Login Password

➤ Time Settings

- **NTP Enable** - The system time of WPB8326 will be synchronized by the NTP server when NTP is enabled.
- **Time Zone** - Choose the time zone where the device is located.
- **NTP Server 1** - The primary NTP server which provides time synchronizing service for the device.
- **NTP Server 2** - The secondary NTP server which provides time synchronizing

service for the device.

- **Date and Time** - Set the system time manually when NTP is disabled.
- **Day Light Saving** - Enable this option if the time zone has Daylight savings.
- **Start Month** - Select the start month of Daylight saving.
- **Start Week** - Select the start week of Daylight saving.
- **Start Time** - Select the start time for Daylight saving.
- **End Month** - Select the end month of Daylight saving.
- **End Week** - Select the end week of Daylight saving.
- **End Time** - Select the end time for daylight saving.

Time Settings:

NTP Enable: ☒

Time Zone: UTC+08:00,Taiwan,China,Hong_Kong,Western_Australia,Singap... ▼

NTP Server 1: pool.ntp.org

NTP Server 2: time.nist.gov

* Date and Time: 1970-01-01 12:00

Day Light Saving: ☐

Start Month: March ▼

Start Week: 2nd ▼

Start Day: Sunday ▼

* Start Time: 02:00

End Month: November ▼

End Week: 1st ▼

End Day: Sunday ▼

* End Time: 02:00

Figure 11. Time Settings

➤ SSH Server Settings

- **SSH Enable** - Allow to access WPB8326 via SSH. The username is “root” and password is “<login password for local web>”.

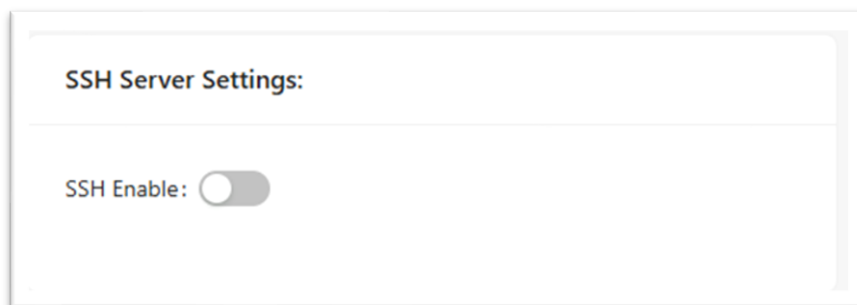


Figure 12. SSH Server Settings

4.4. Network Config

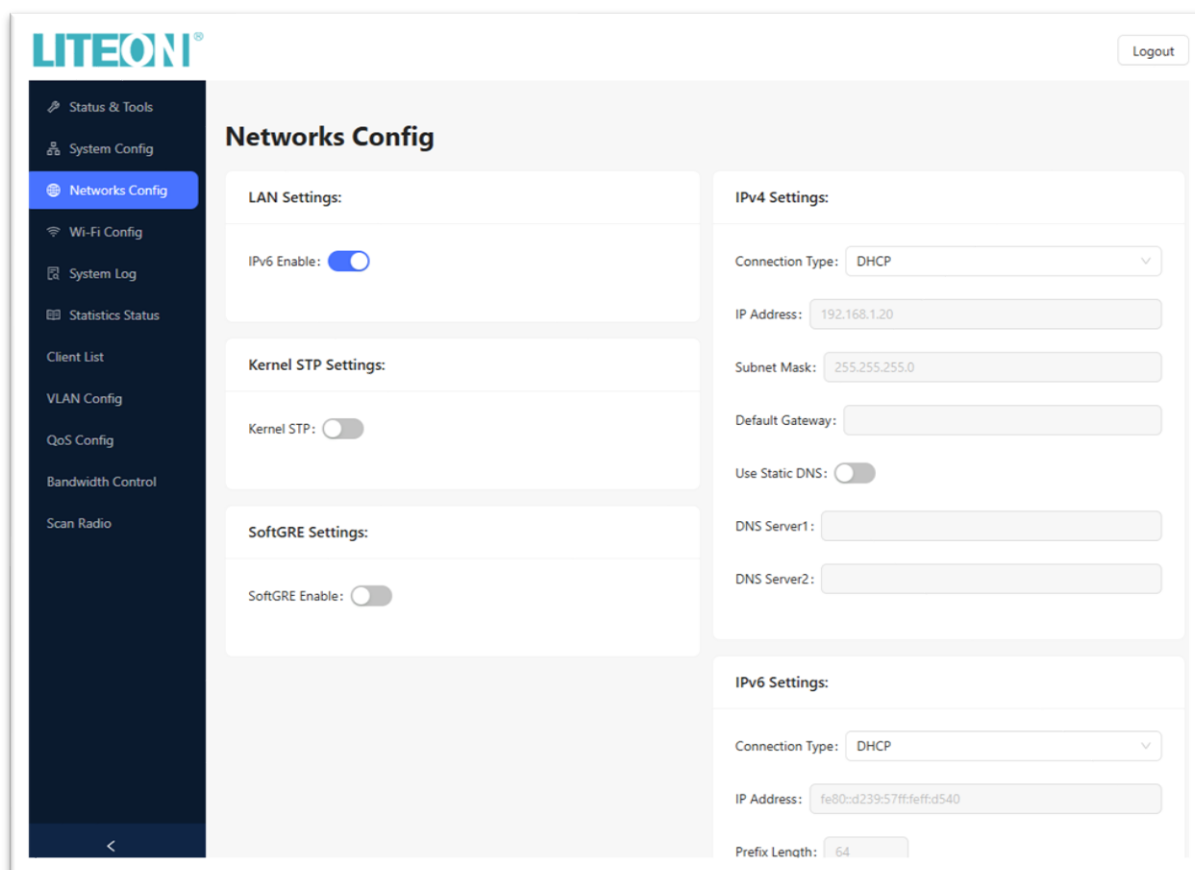


Figure 13. Networks Config

➤ LAN Settings

- **IPv6 Enable** - Allow WPB8326 to obtain IPv6 address.

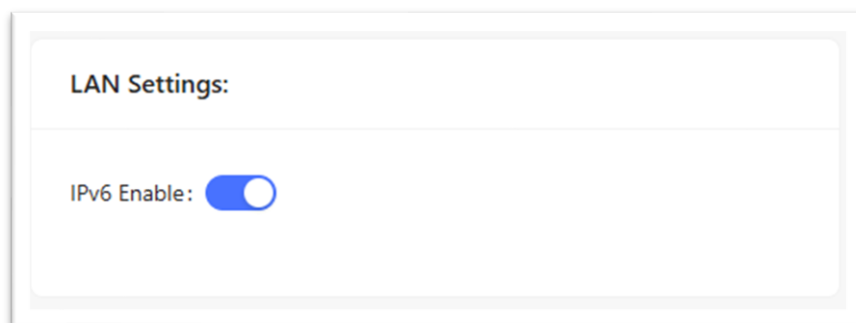


Figure 14. LAN Settings

➤ IPv4 Settings

- **Connect Type** - Obtains IPv4 address, including DHCP and static.
- **IP Address** - Specify a fixed IPv4 address, when "Connect Type" is "static".
- **Subnet mask** - Specify a fixed IPv4 subnet mask, when "Connect Type" is "static".
- **Default Gateway** - Specify the default IPv4 gateway, when "Connect Type" is "static".
- **Use Static DNS** - Allow setting the DNS Server manually.
- **DNS Server1** - Specify the primary DNS Server manually.
- **DNS Server2** - (Optional) Specify the secondary DNS server manually.

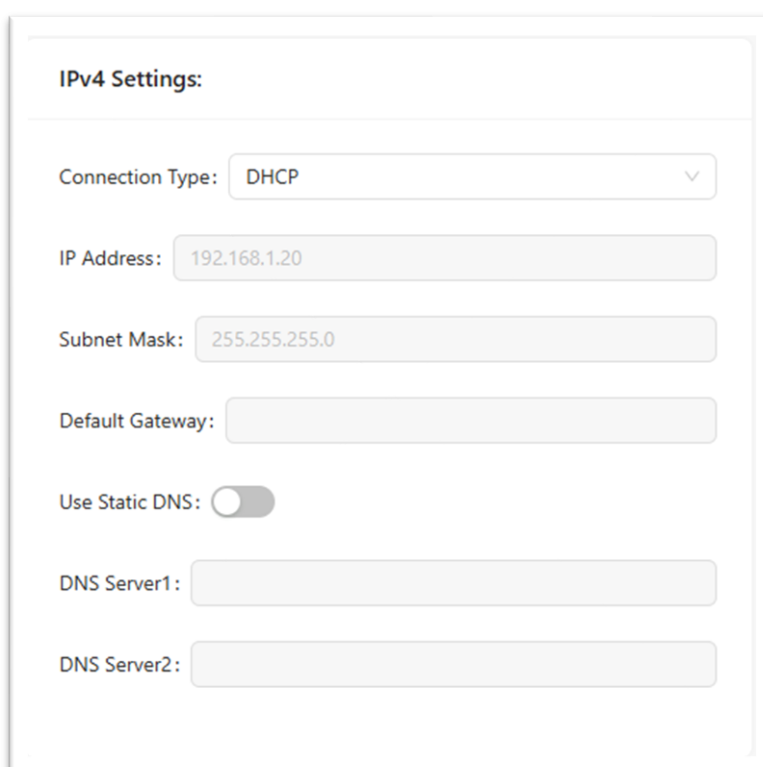
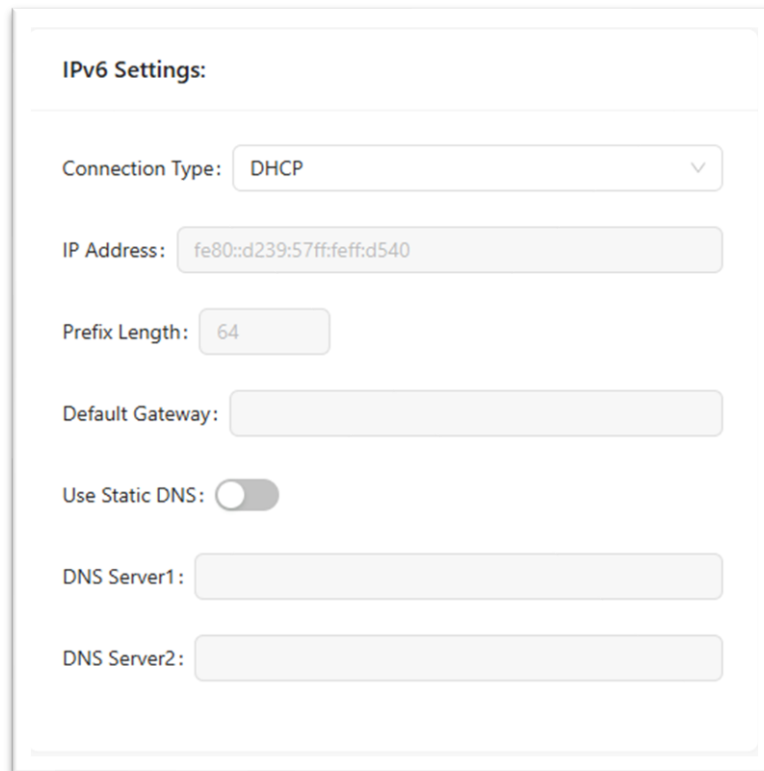


Figure 15. IPv4 Settings

➤ **IPv6 Settings**

- **Connection Type** - Obtains IPv6 address, including DHCP and static.
- **IP Address** - Specify a fixed IPv6 address, when “Connect Type” is “static”.
- **Prefix Length** - Specify a fixed IPv6 prefix length, when “Connect Type” is “static”.
- **Default Gateway** - Specify the default IPv6 gateway.
- **Use Static DNS** - Allow setting the DNS Server manually.
- **DNS Server1** - Specify primary DNS Server manually.
- **DNS Server2** - (Optional) Specify secondary DNS server manually.



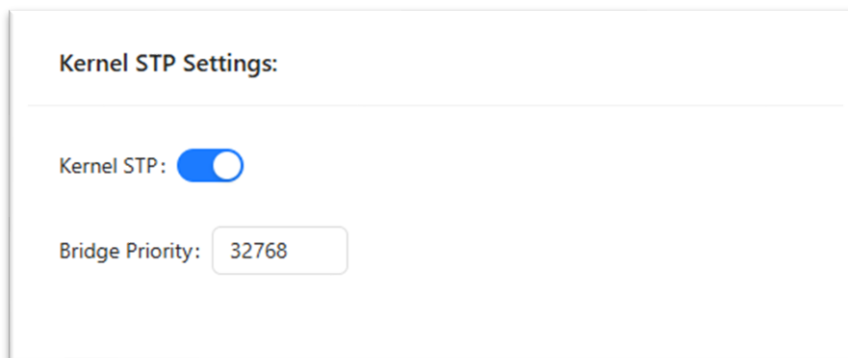
The screenshot shows a configuration window titled "IPv6 Settings:". It contains several input fields and a toggle switch. The "Connection Type" is set to "DHCP" in a dropdown menu. The "IP Address" field contains the value "fe80::d239:57ff:feff:d540". The "Prefix Length" field contains the value "64". The "Default Gateway" field is empty. The "Use Static DNS" toggle switch is turned off. The "DNS Server1" and "DNS Server2" fields are also empty.

Field	Value
Connection Type	DHCP
IP Address	fe80::d239:57ff:feff:d540
Prefix Length	64
Default Gateway	
Use Static DNS	Off
DNS Server1	
DNS Server2	

Figure 16. IPv6 Settings

➤ Kernel STP Settings

- **Kernel STP** - It works by creating network paths without loops, which could be harmful in cases such as flooding broadcast messages, by disabling (blocking) ports in the configured bridges.
- **Bridge Priority** - Determines the root bridge in the network, Bridge Priority only accepts values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440.



Kernel STP Settings:

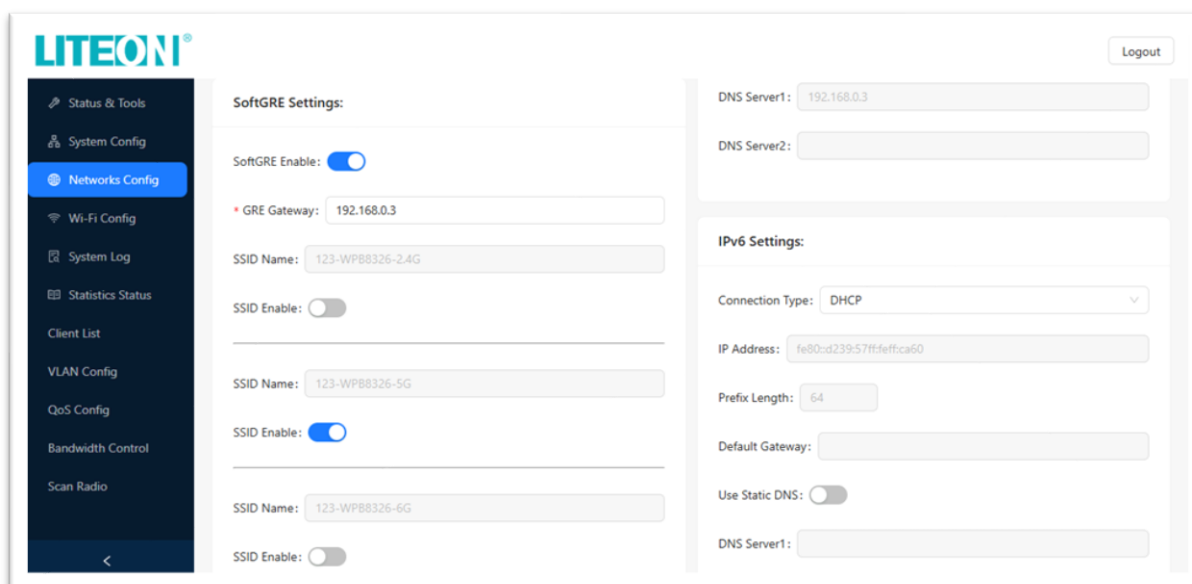
Kernel STP: ☒

Bridge Priority:

Figure 17. Kernel STP Settings

➤ SoftGRE Settings

- **SoftGRE Enable** - Enable SoftGRE on the device.
- **GRE Gateway** - Specify IPv4 address of the SoftGRE gateway.
- **SSID Enable** - Specify which SSID the SoftGRE function will work on. When enabled for a designated SSID, the traffic of that SSID will be tunneled into the GRE gateway.



SoftGRE Settings:

SoftGRE Enable: ☒

* GRE Gateway:

SSID Name:

SSID Enable: ☐

SSID Name:

SSID Enable: ☒

SSID Name:

SSID Enable: ☐

DNS Settings:

DNS Server1:

DNS Server2:

IPv6 Settings:

Connection Type:

IP Address:

Prefix Length:

Default Gateway:

Use Static DNS: ☐

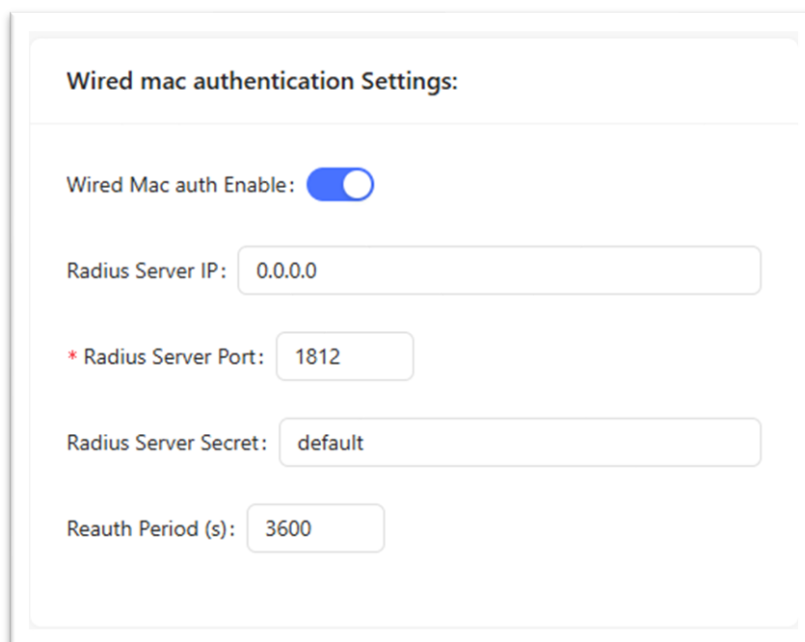
DNS Server1:

Figure 18. SoftGRE Settings

➤ Wired mac authentication Settings

- **Wired Mac auth Enable** - Enable wired MAC authentication.
- **Radius Server IP** - Specify the RADIUS server IP.
- **Radius Server Port** - Specify the RADIUS server port.

- **Radius Server Seret** - Specify the RADIUS server secret.
- **Radius Server Port** - Specify the re-auth period (seconds).



Wired mac authentication Settings:

Wired Mac auth Enable: ☒

Radius Server IP:

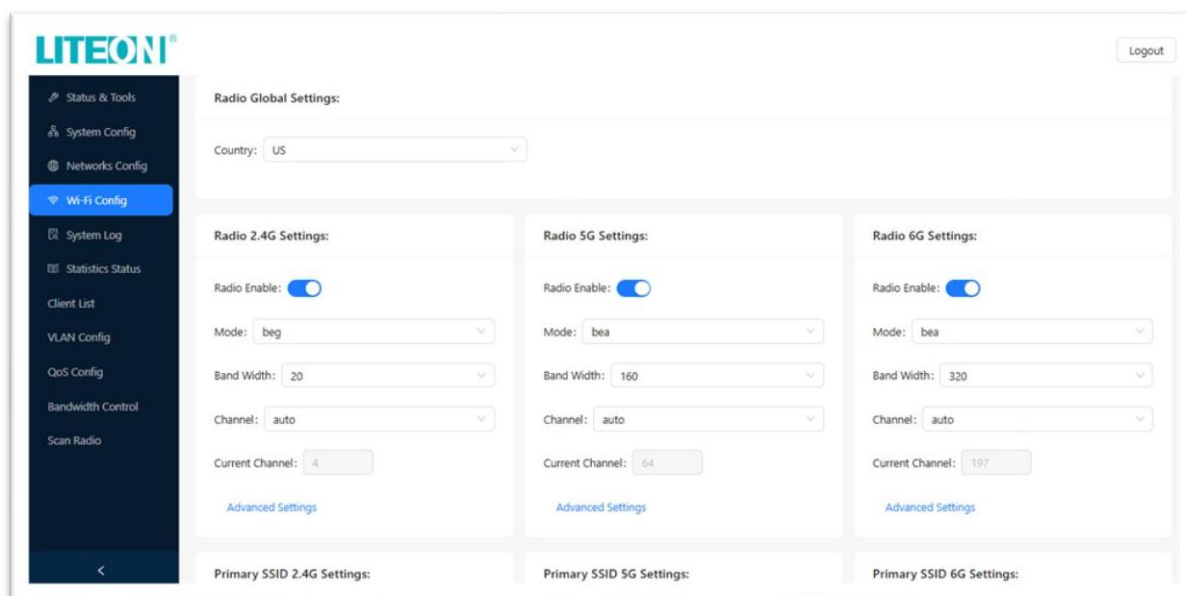
* Radius Server Port:

Radius Server Secret:

Reauth Period (s):

Figure 19. Wired MAC Authentication Settings

4.5. Wi-Fi Config



LITEON[®] Logout

Radio Global Settings:

Country:

Radio 2.4G Settings:

Radio Enable: ☒

Mode:

Band Width:

Channel:

Current Channel:

[Advanced Settings](#)

Radio 5G Settings:

Radio Enable: ☒

Mode:

Band Width:

Channel:

Current Channel:

[Advanced Settings](#)

Radio 6G Settings:

Radio Enable: ☒

Mode:

Band Width:

Channel:

Current Channel:

[Advanced Settings](#)

Primary SSID 2.4G Settings: Primary SSID 5G Settings: Primary SSID 6G Settings:

Figure 20. Wi-Fi Settings

➤ Radio Global Settings

- **Country** - Select the country code where the device is located.

➤ Radio 2.4G/5G/6G Settings

- **Radio Enable** - Enable/disable the radio.
- **Mode** - Select the Wi-Fi mode.
 - **2.4G:** bgn (Wi-Fi 4), axg (Wi-Fi 6), beg (Wi-Fi 7)
 - **5G:** anac (Wi-Fi 5), axa (Wi-Fi 6), bea (Wi-Fi 7)
 - **6G:** axa (Wi-Fi 6), bea (Wi-Fi 7)
- **Band Width** - Select bandwidth (MHz) for the radio.
 - **2.4G:** 20, mixed40 (enable coexistence), only40 (disable coexistence)
 - **5G:** 20, 40, 80, 160, 240
 - **6G:** 20, 40, 80, 160, 320
- **Channel** - Select “auto” or a fixed channel for the radio.
- **Current Channel** - Show the channel that the radio is current operating on.

➤ Radio 2.4G/5G/6G Advanced Settings

- **Radio Enable** - The same as that in Radio 2.4G/5G/6G Settings.
- **Mode** - The same as that in Radio 2.4G/5G/6G Settings.
- **Band Width** - The same as that in Radio 2.4G/5G/6G Settings.
- **Channel** - The same as that in Radio 2.4G/5G/6G Settings.
- **Current Channel** - The same as that in Radio 2.4G/5G/6G Settings.
- **Beacon Interval (ms)** - Configure the interval that SSIDs are broadcasting. The default value is 100ms, and lowering the Beacon Interval can speed up wireless client connections, but it will downgrade the wireless network performance.
- **DTIM period** - The DTIM (Delivery Traffic Indication Message) period determines how often a beacon frame includes a DTIM. The default value is 10, increasing the DTIM period will help the wireless client sleep longer and save more power, but the disadvantage is that latency may deteriorate.
- **Max Station** - Limit the number of concurrent wireless client connections. 0 means not limiting the number of wireless client connections. The max station of each radio is 128.
- **Power** - Configure the Wi-Fi transmit power (3 ~ 30 dBm). The actual transmitted power will be the minimal value of this value and the regulatory power.
- **Min RSSI Enable** - Enable/disable Min RSSI feature.
- **Min RSSI Value** - The wireless client with RSSI lower than this threshold (dBm) will be rejected by the radio.
- **DFS Puncturing** - The device will first try to puncture the radar affected channels instead of jump to a different channel when DFS radar is detected.
- **Dynamic Channel Selection** - The radio will perform dynamic channel selection when the working channel is busy, but it is not recommended to enable on 2.4G radio, which is usually crowded. It might cause frequent channel selection on 2.4G.

Radio 5G Advanced Settings ✕

Radio Enable: ☒

Mode: ▼

Band Width: ▼

Channel: ▼

Current Channel:

Beacon Interval (ms):

DTIM period:

Max Station:

Power:

MIN RSSI Enable: ☒

MIN RSSI Value:

DFS Puncturing: ☒

Dynamic Channel Selection: ☒

Figure 21. Wi-Fi Settings - Radio Advanced Settings

➤ Primary SSID 2.4G/5G/6G Settings

- **MLO Enable** - Enable Wi-Fi 7 MLO (Multi-Link Operation) feature on the radio.
- **SSID Enable** - Enable/disable primary SSID on this radio.
- **SSID** - Configure the SSID name.
- **Security** - Wi-Fi encryption mode, including OPEN, WPA2 PSK, WPA2 ENTERPRISE, WPA3 SAE, WPA3 SAE + WPA2 PSK, WPA3 ENTERPRISE 192-BIT, WPA3 ENTERPRISE ONLY and WPA3 OWE.
- **Key** - Configure the Wi-Fi password for the SSID.

Primary SSID 2.4G Settings:	Primary SSID 5G Settings:	Primary SSID 6G Settings:
MLO Enable: ☐	MLO Enable: ☐	MLO Enable: ☐
SSID Enable: ☒	SSID Enable: ☒	SSID Enable: ☒
* SSID: WPB8326-2.4G	* SSID: WPB8326-5G	* SSID: WPB8326-6G
Security: WPA2 PSK	Security: WPA2 PSK	Security: WPA3 SAE
Key: 1234567890	Key: 1234567890	Key: 1234567890
Advanced Settings	Advanced Settings	Advanced Settings

Figure 22. Wi-Fi Settings - SSID Settings

➤ Primary SSID 2.4G/5G/6G Advanced Settings

- **MLO Enable** - The same as that in Primary SSID 2.4G/5G/6G Settings.
- **SSID Enable** - The same as that in Primary SSID 2.4G/5G/6G Settings.
- **SSID** - The same as that in Primary SSID 2.4G/5G/6G Settings.
- **Security** - The same as that in Primary SSID 2.4G/5G/6G Settings.
- **Key** - The same as that in Primary SSID 2.4G/5G/6G Settings.
- **Hide SSID** - The SSID name will not be broadcasted.
- **VLAN Mode** - Clients connected to the SSID are in the same VLAN group. A fixed VLAN ID is used in access mode.
- **VLAN ID** - VLAN ID assigned to this SSID.
- **Radius MAC Enable** - Enable Radius MAC authentication for wireless clients using Open security connected to this SSID.
NOTE: The Radius MAC feature can only be activated when the security is set to "OPEN" for 2G and 5G SSIDs. This function is disabled for the 6G SSID for now.
- **Max Station** - Limit the number of concurrent wireless clients connect to this SSID. "0" means not limiting the number of wireless client connections.

Primary SSID 2.4G Advanced Settings ×

MLO Enable: ☐

SSID Enable: ☒

* SSID:

Security: ▼

Key:

Hide SSID: ☐

VLAN Mode: ▼

VLAN ID:

Radius MAC Enable: ☐

Radius Server 1 Address:

Radius Server 1 Port:

Radius Server 1 Key:

Radius Server 2 Address:

Radius Server 2 Port:

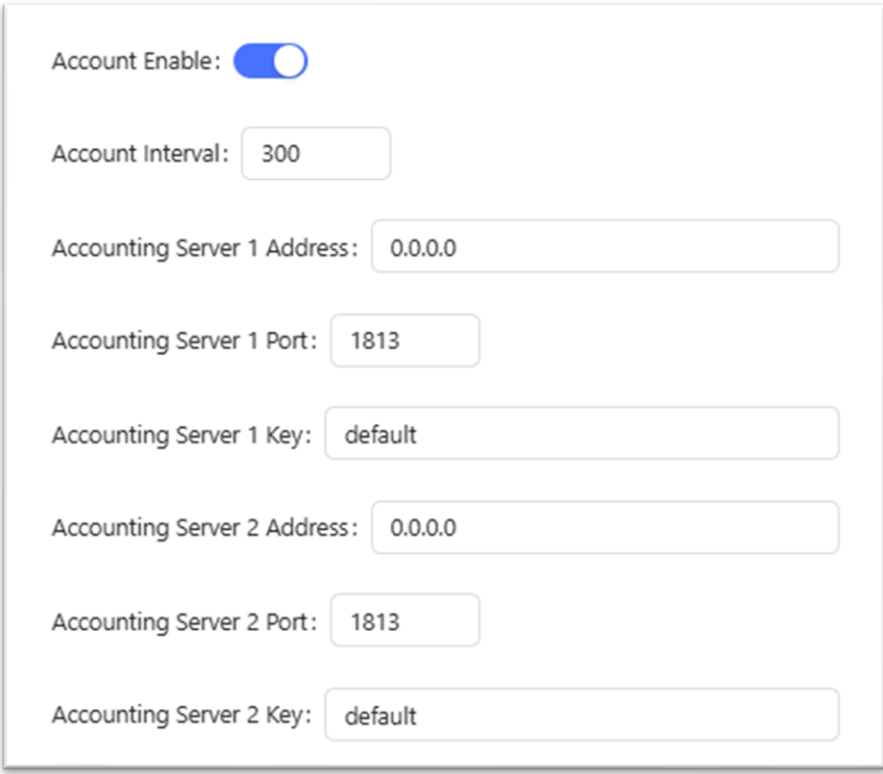
Radius Server 2 Key:

Account Enable: ☐

Max Station:

Figure 23. Wi-Fi Settings - SSID Advanced Settings

- **Account Enable** - Enable RADIUS accounting on this SSID.
- **Account Interval** - Configure the accounting interval (seconds)
- **Account Server 1 Address** - Configure the IP address of primary accounting server.
- **Account Server 1 Port** - Configure the port of primary accounting server.
- **Account Server 1 Key** - Configure the key of primary accounting server.
- **Account Server 2 Address** - Configure the IP address of secondary accounting server.
- **Account Server 2 Port** - Configure the port of secondary accounting server.
- **Account Server 2 Key** - Configure the key of secondary accounting server.



The screenshot displays the 'SSID Advanced Settings - RADIUS Accounting Settings' interface. It features a toggle switch for 'Account Enable' which is turned on. Below this, there are input fields for 'Account Interval' (set to 300), 'Accounting Server 1 Address' (set to 0.0.0.0), 'Accounting Server 1 Port' (set to 1813), 'Accounting Server 1 Key' (set to default), 'Accounting Server 2 Address' (set to 0.0.0.0), 'Accounting Server 2 Port' (set to 1813), and 'Accounting Server 2 Key' (set to default).

Setting	Value
Account Enable	Enabled
Account Interval	300
Accounting Server 1 Address	0.0.0.0
Accounting Server 1 Port	1813
Accounting Server 1 Key	default
Accounting Server 2 Address	0.0.0.0
Accounting Server 2 Port	1813
Accounting Server 2 Key	default

Figure 24. SSID Advanced Settings - RADIUS Accounting Settings

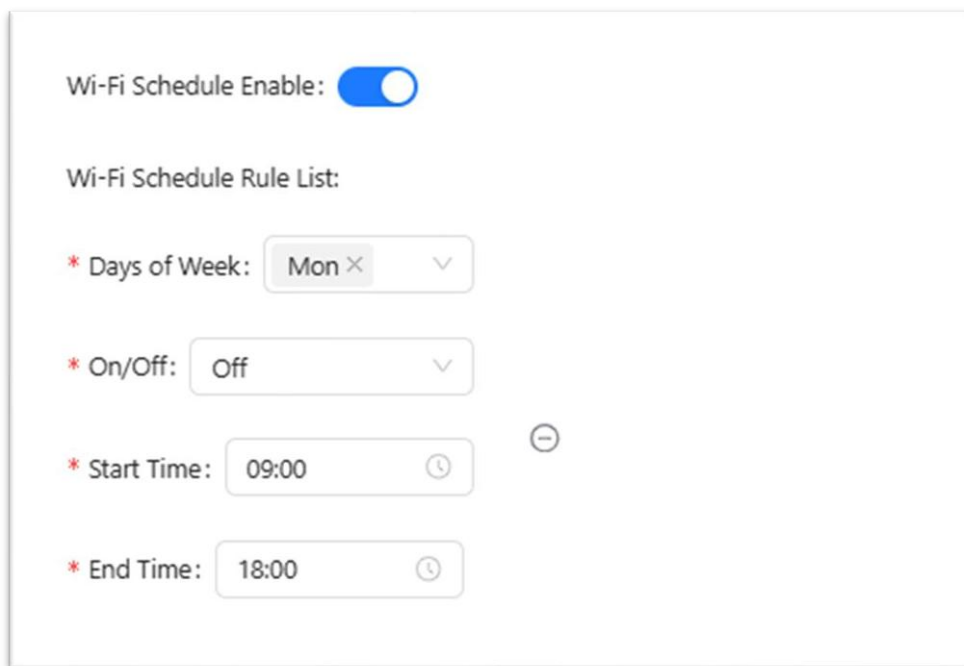
- **ACL Enable** - Enable ACL (Access Control List) on the SSID.
- **ACL Policy** - Select the ACL policy (deny/allow).
- **ACL MAC List** - Add the MAC address to the ACL MAC List.

Figure 25. SSID Advanced Settings - ACL Settings

- **Multicast Enhancement** - Enable multicast to unicast conversion.
NOTE: When enabled, IGMP Snooping and MLD Snooping will be enabled.
- **Station Isolation** - When enabled, the traffic of different clients connected to this SSID is isolated.
- **Band Steering** - Select “load balance” to enable band steering of 2.4G/5G band.
NOTE: 2.4G and 5G SSID names must be identical, otherwise band steering will not work.
- **11r Enable** - Enable 11r Fast BSS Transition reduces latency during client roaming.
NOTE: Some legacy clients not supporting 11r might not connect to the SSID.

Figure 26. SSID Advanced Settings - Multicast/Isolation/Steering/11r Settings

- **Wi-Fi Schedule Enable** - Schedule to enable/disable the wireless access of this Wi-Fi SSID.
- **Days of Week** - Choose single or multiple days of a week.
- **On/Off** - Turn on/off the SSID.
- **Start Time** - Specify the start time of the scheduling.
- **End Time** - Specify the end time of the scheduling.



The image shows a web-based configuration interface for Wi-Fi scheduling. At the top, there is a toggle switch for 'Wi-Fi Schedule Enable', which is currently turned on (blue). Below this is a section titled 'Wi-Fi Schedule Rule List'. This section contains four rows of settings, each marked with a red asterisk: 'Days of Week' is set to 'Mon' with a dropdown arrow; 'On/Off' is set to 'Off' with a dropdown arrow; 'Start Time' is set to '09:00' with a clock icon; and 'End Time' is set to '18:00' with a clock icon. A minus sign icon is positioned to the right of the 'Start Time' field.

Figure 27. SSID Advanced Settings - Wi-Fi Scheduling Settings

4.6. System Log

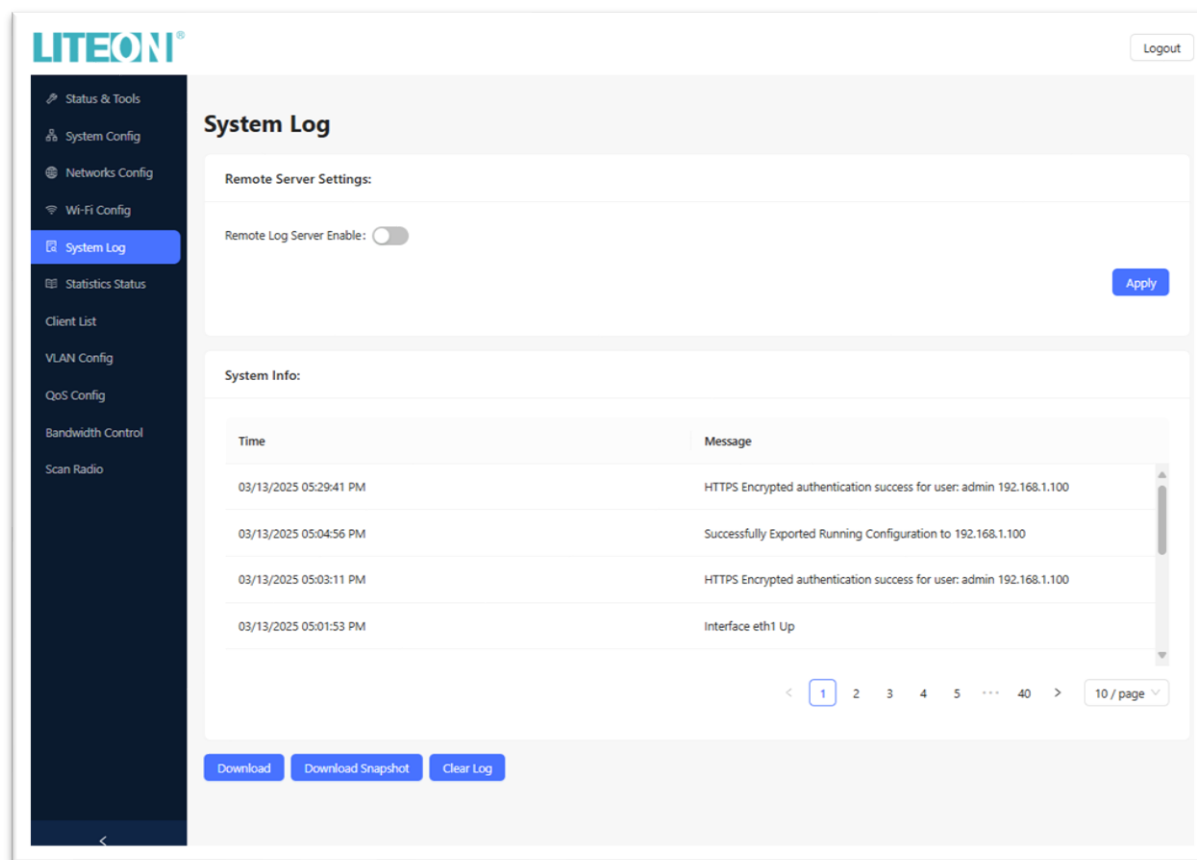


Figure 28. System Log

➤ Remote Server Settings

- **Remote Log Server Enable** - After enabled, the system logs will be sent to below remote log servers.
- **Server 1 Address** - Configure the IP address of Log Server 1.
- **Server 1 Port** - Configure the TCP/UDP port of Log Server 1.
- **Server 1 Level** - Logs with level above this configured level are sent to Log Server 1. Available levels include debug, info, notice, warning, error, critical, alert, and emergency.
- **Server 2 Address** - Configure the IP address of Log Server 2.
- **Server 2 Port** - Configure the TCP/UDP port of Log Server 2.
- **Server 2 Level** - Logs with level above this configured level are sent to Log Server 2. Available levels include debug, info, notice, warning, error, critical, alert, and emergency.
- **Server 3 Address** - Configure the IP address of Log Server 3.
- **Server 3 Port** - Configure the TCP/UDP port of Log Server 3.
- **Server 3 Level** - Logs with level above this configured level are sent to Log Server 3. Available levels include debug, info, notice, warning, error, critical, alert, and emergency.

Remote Server Settings:

Remote Log Server Enable: ☒

Server 1 Address:

* Server 1 Port:

Server 1 Level:

Server 2 Address:

Server 2 Port:

Server 2 Level:

Server 3 Address:

Server 3 Port:

Server 3 Level:

Apply

Figure 29. System Log - Remote Log Server Settings

➤ System Info

- **Time** - The time the event occurred on the system.
- **Message** - Event description.
- **Download** - Download the log. The file name format is Log-WPB8326-<backup-date>.txt.
e.g., "Log-WPB8326-2025-03-17.txt"
- **Download Snapshot** - Download the system snapshot for troubleshooting. The file name format is Snapshot-WPB8326-<backup-date>.tar.gz.
e.g., "Snapshot-WPB8326-2025-03-17.tar.gz"
- **Clear Log** - Clear all logs.

System Info:

Time	Message
03/13/2025 05:29:41 PM	HTTPS Encrypted authentication success for user: admin 192.168.1.100
03/13/2025 05:04:56 PM	Successfully Exported Running Configuration to 192.168.1.100
03/13/2025 05:03:11 PM	HTTPS Encrypted authentication success for user: admin 192.168.1.100
03/13/2025 05:01:53 PM	Interface eth1 Up

< 1 2 3 4 5 ... 40 >

10 / page

Download

Download Snapshot

Clear Log

Figure 30. System Log - Log List

4.7. Statistic Status

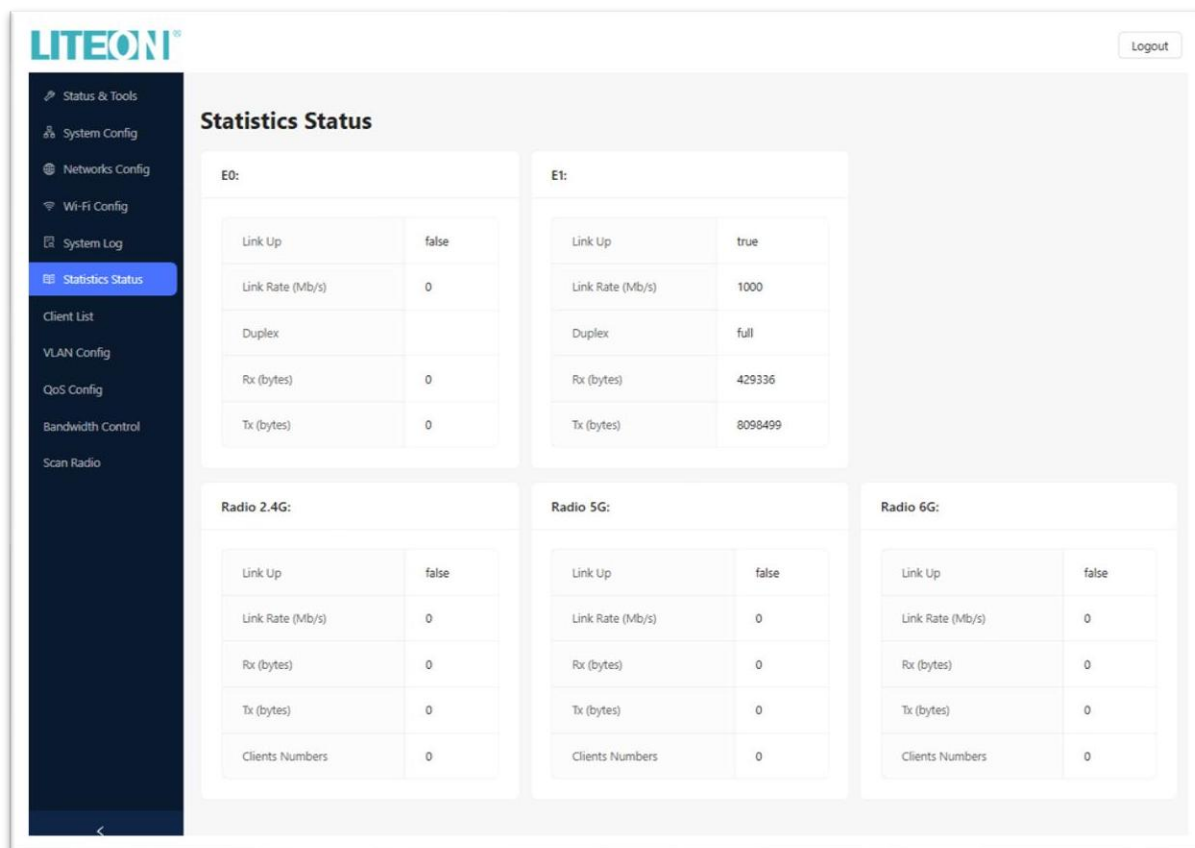


Figure 31. Statistic Status

- **E0** - Show the status of Ethernet port E0 / 5G PoE, including Link Up State, Link Rate(Mb/s), and Duplex mode (full/half), Rx(bytes), Tx(bytes).
- **E1** - Show the status of Ethernet port E1 / 1G, including Link Up State, Link Rate(Mb/s), and Duplex mode (full/half), Rx(bytes), Tx(bytes).
- **Radio 2.4G** - Show the status of Radio 2.4G, including Link Up State, Link Rate(Mb/s), and Rx(bytes), Tx(bytes), Clients Numbers.
- **Radio 5G** - Shows the status of Radio 5G, including Link Up State, Link Rate(Mb/s), and Rx(bytes), Tx(bytes), Clients Numbers.
- **Radio 6G** - Shows the status of Radio 6G, including Link Up State, Link Rate(Mb/s), and Rx(bytes), Tx(bytes), Client numbers.

4.8. Client List

- **Total Clients** - The number of total connected clients including wired client and wireless clients.
- **Client Info**
 - **Interface** - The Wi-Fi radio or Ethernet port which client connects to.
 - **Client Host Name** - Client hostname.
 - **IP Address** - Client IPv4 address.
 - **MAC Address** - Client MAC Address.
 - **Manufacturer** - Manufacturer of the client.
 - **RSSI** - Received Signal Strength Indicator of the wireless client. Not applicable for wired clients.
 - **Tx Bytes** - The amount of transmission data of the wireless client.
 - **Rx Bytes** - The amount of receiving data of the wireless client.

Interface	SSID	Client Host Name	IP Address	MAC Address	Manufacturer	RSSI	Tx Bytes	Rx Bytes
5G	123-WPB8326-5G	NCNL0195	192.168.0.68	84:7b:57:6cfd:45	Intel Corporate	-33	68,246 KB	60,809
6G	123-WPB8326-6G	NCNL0246	192.168.0.210	54:07:7d:9b:6c:1f	NETGEAR	-33	51,915 KB	251,111
MLO	123-WPB8326-MLO	NCNL0246	192.168.0.60	a0:b3:39:36:af:92	Intel Corporate	6G:-94.5G:-38	668,343 KB	623,351
5G	123-WPB8326-MLO	Host-b2:e0:f9:58:d6:91	192.168.0.121	b2:e0:f9:58:d6:91	*	-59	374,521 KB	279,621
5G	123-WPB8326-MLO	Host-62:c3:1d:75:2a:d3	192.168.0.103	62:c3:1d:75:2a:d3	*	-56	271,526 KB	121,421
E1		Host-10:65:30:ed:ff:c4	192.168.0.188	10:65:30:ed:ff:c4		0	-	-

Figure 32. Client List

4.G. VLAN Config

By default, there is only one management VLAN enabled for E0 and E1 ports. Add more VLANs by selecting “Add” from the “Options” dropdown list. Edit or delete an existing VLAN from the VLAN table by selecting the “Edit” or “Delete”.

- **Options**
 - **Add** - Add a new VLAN when selecting the “Add” option.
 - **Edit** - Select one VLAN rule from the VLAN table, then click the “Edit” option”. A page will display the VLAN settings of VLAN rule for editing.
 - **Delete** - Select at least one VLAN rule from the VLAN table, then click the “Delete” option. The VLAN rules will be deleted.

NOTE: The VLAN to be deleted must not be in use by any SSID.

➤ VLAN Table

- **VLAN ID** - VLAN ID of this rule.
- **Name** - A name for describing this VLAN.
- **Device Management** - Allow access WPB8326 web via this VLAN.
- **E0** - Allow E0 / 5G PoE port to tag or untag the VLAN ID.
- **E1** - Allow E1 / 1G port to tag or untag the VLAN ID.

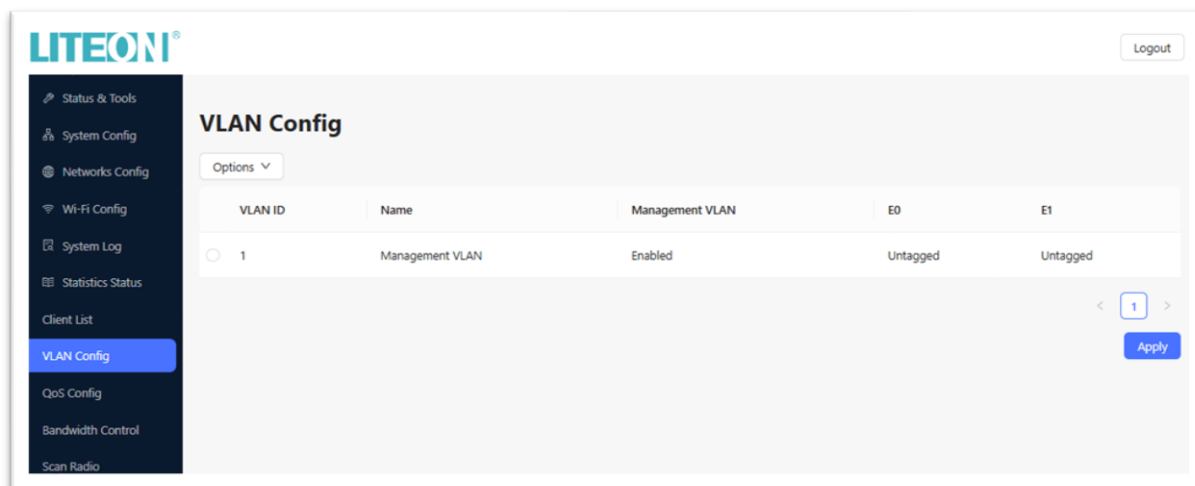


Figure 33. VLAN Config

Below is the page of adding a VLAN.

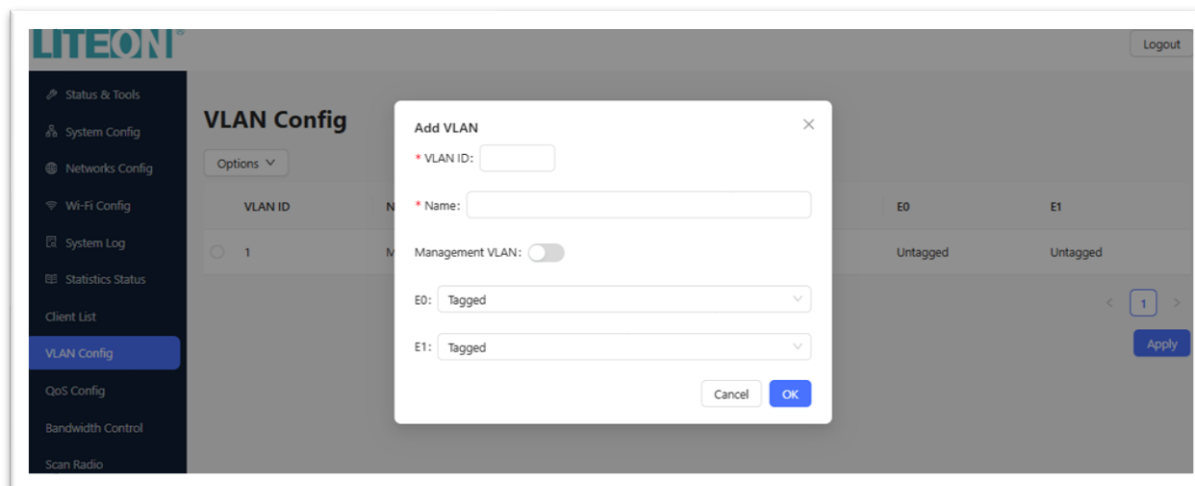


Figure 34. VLAN Config - Add VLAN

4.10. QoS Config

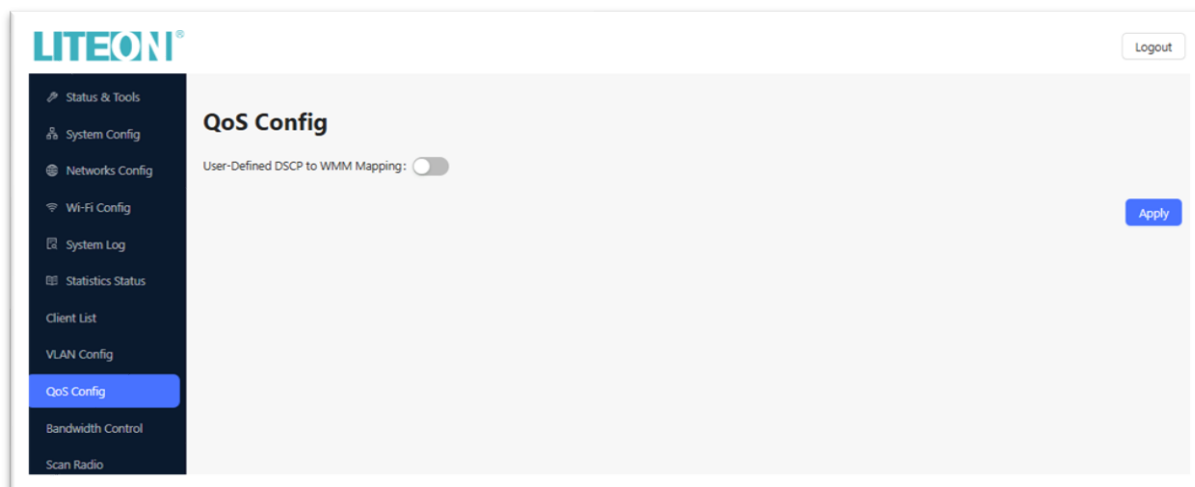


Figure 35. QoS Config

Enable “User-Defined DSCP to WMM Mapping” for configure user-defined DSCP-to-WMM mapping.

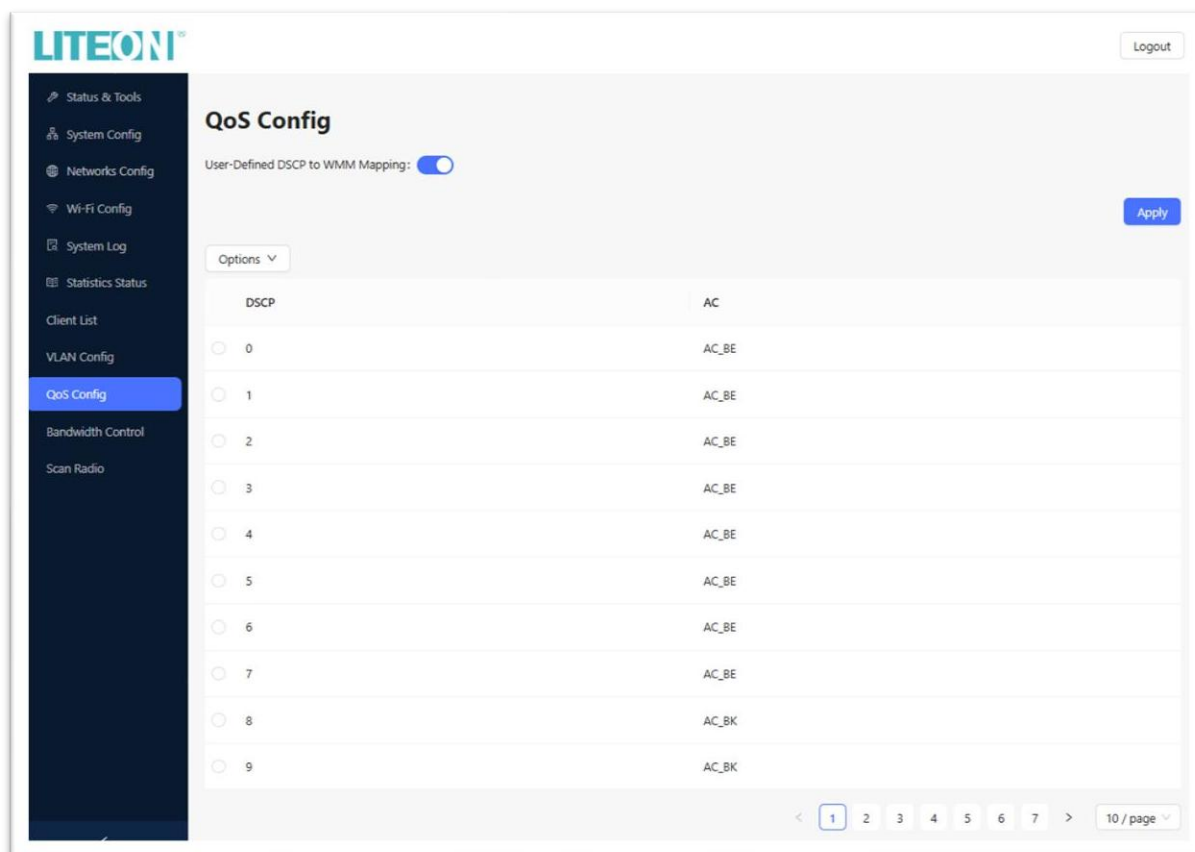


Figure 36. QoS Config - Enable User-defined DSCP-to-WMM Mapping

To edit the mapping, select a rule from the mapping table, and select “Edit” from “Options”.

➤ **Edit WMM AC Mapping**

- **DSCP** - DSCP value.
- **AC** - The WMM Access Categories: AC_VO (Voice), AC_VI (Video), AC_BE (Best Effort), and AC_BK (Background).

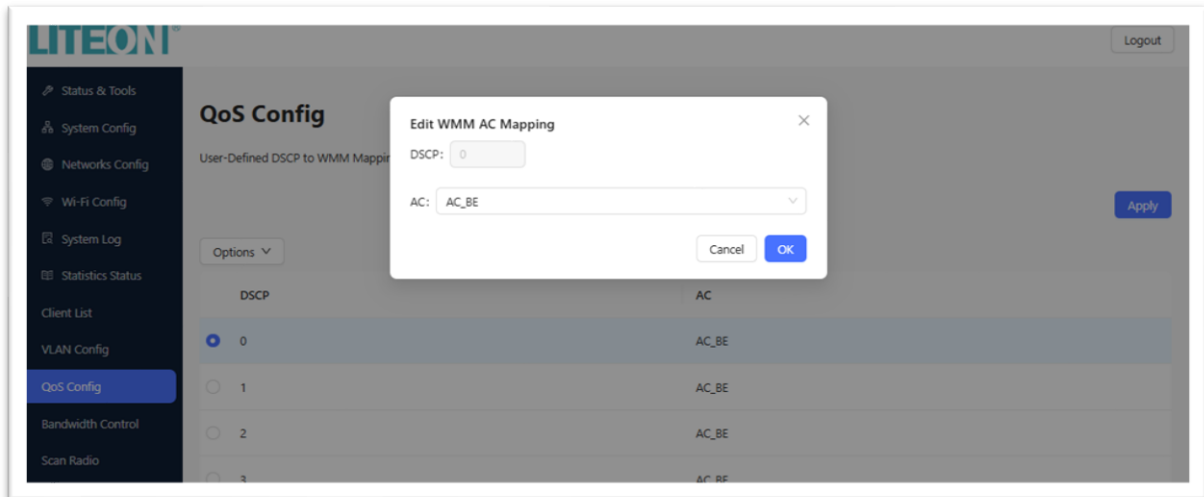


Figure 37. QoS Config - Edit WMM AC Mapping

4.11. Bandwidth Control

Bandwidth control is disabled by default. To configure bandwidth control, toggle on “Enable Bandwidth Control”.

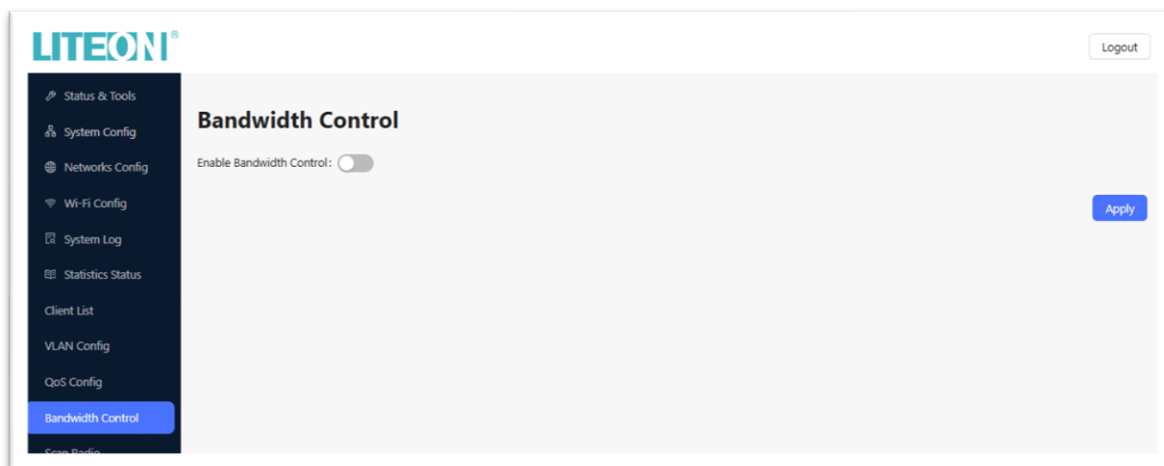


Figure 38. Bandwidth Control

(a) Service Management

Service Management already has some pre-defined services. To add more services by selecting “Add” from the “Options”. Also, edit or delete an existing service from the table by selecting “Edit” or “Delete” from the “Options”.

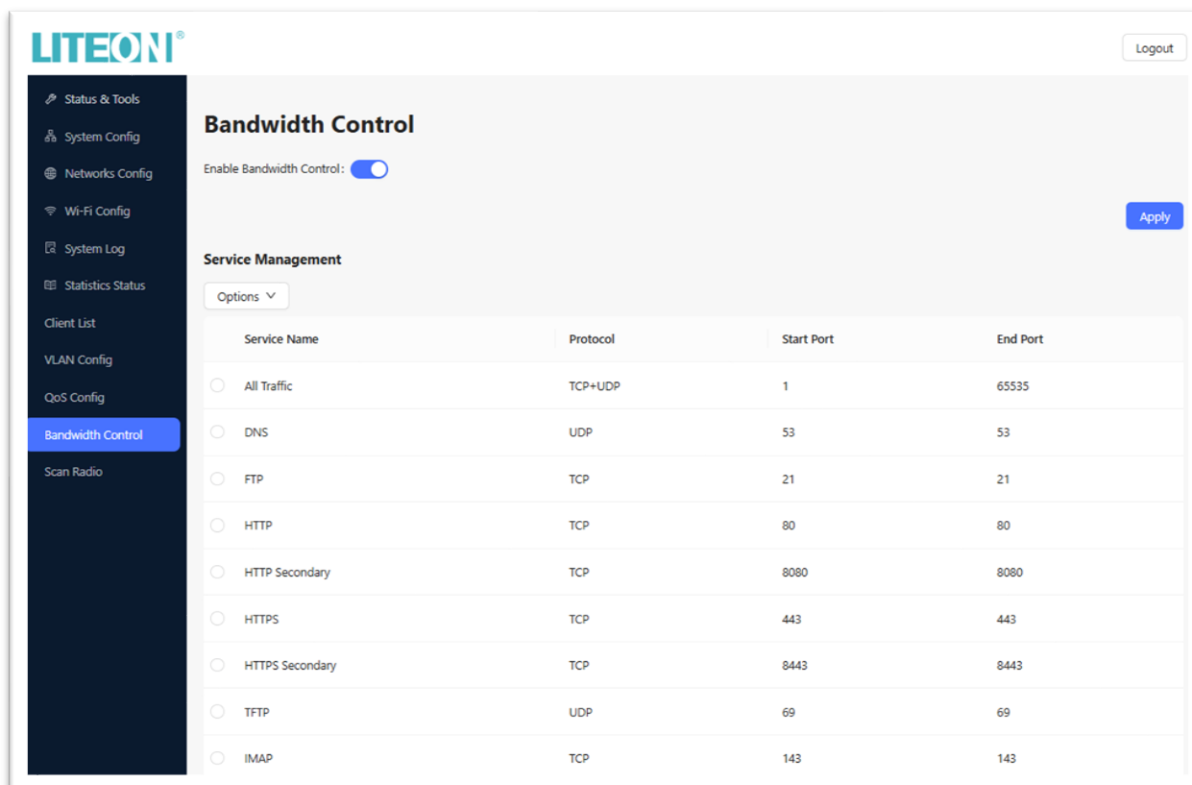


Figure 39. Bandwidth Control - Enable Bandwidth Control

➤ Add Service

- **Service Name** - Name for this service.
- **Protocol** - TCP+UDP, TCP, UDP.
- **Start Port** - Set TCP/UDP start port number for this service.
- **End Port** - Set TCP/UDP end port number for this service.

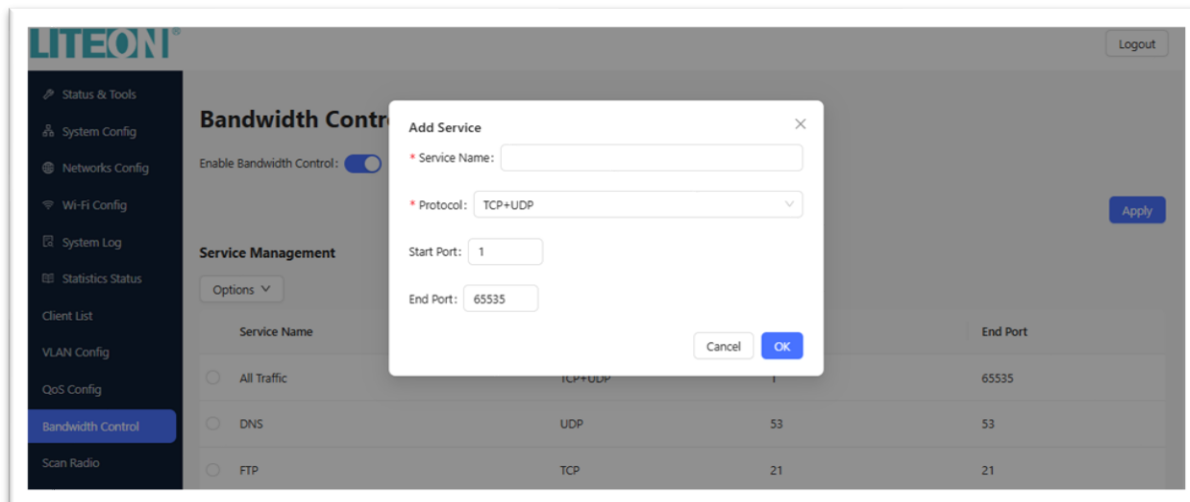


Figure 40. Bandwidth Control - Add Service

➤ Edit Service

To edit a service, choose the service from the service table, and select “Edit” from the “Options”. A page will be displayed for editing.

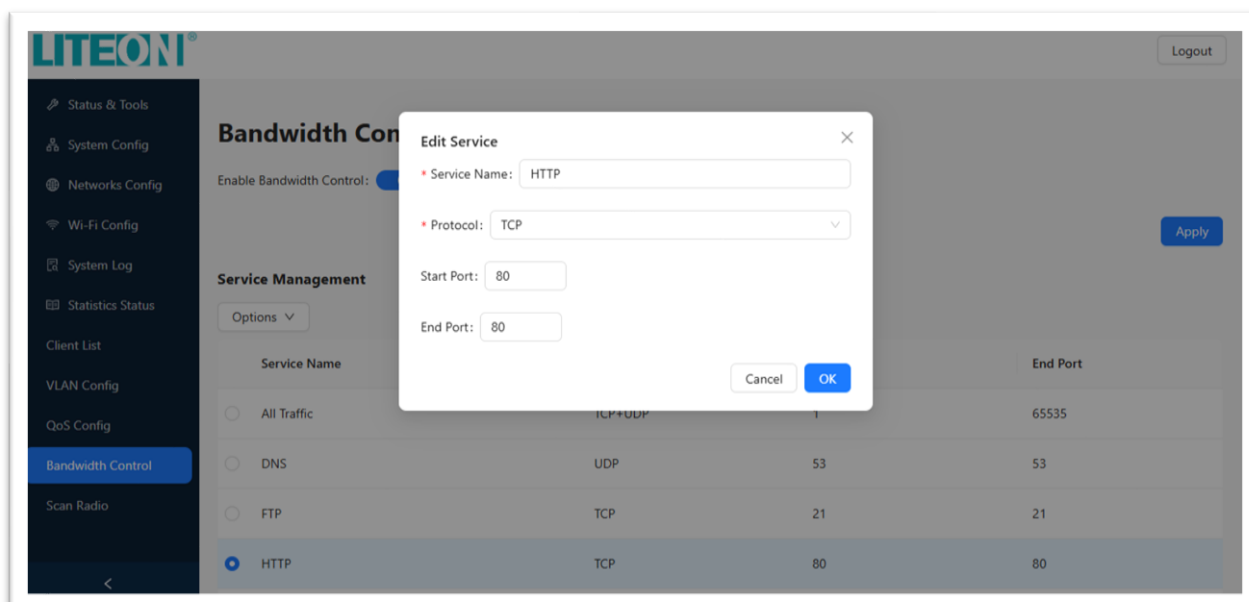


Figure 41. Bandwidth Control - Edit Service

➤ Delete Service

To delete a service, choose the service from the service table, and select “Delete” from the “Options”.

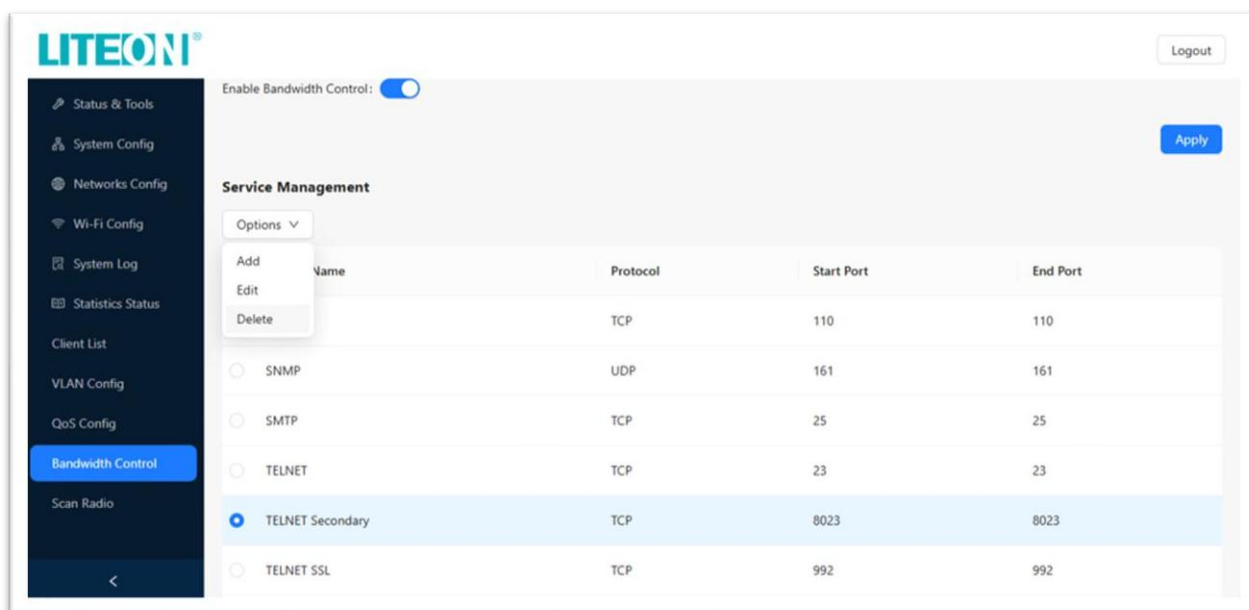


Figure 42. Bandwidth Control - Delete Service

(b) Bandwidth Control Settings

➤ Add Rule

- **Interface** - There is only one option “Wlan Clients”.
- **Service** - Select one of the services from service list.
- **Client MAC Address** - Select MAC address of the client.
- **Direction** - Select the traffic direction: Both (Downstream + Downstream), Downstream, Upstream.
- **Bandwidth (K bits/s)** - Set the bandwidth limit.
- **Enable** - Enable/disable this rule.

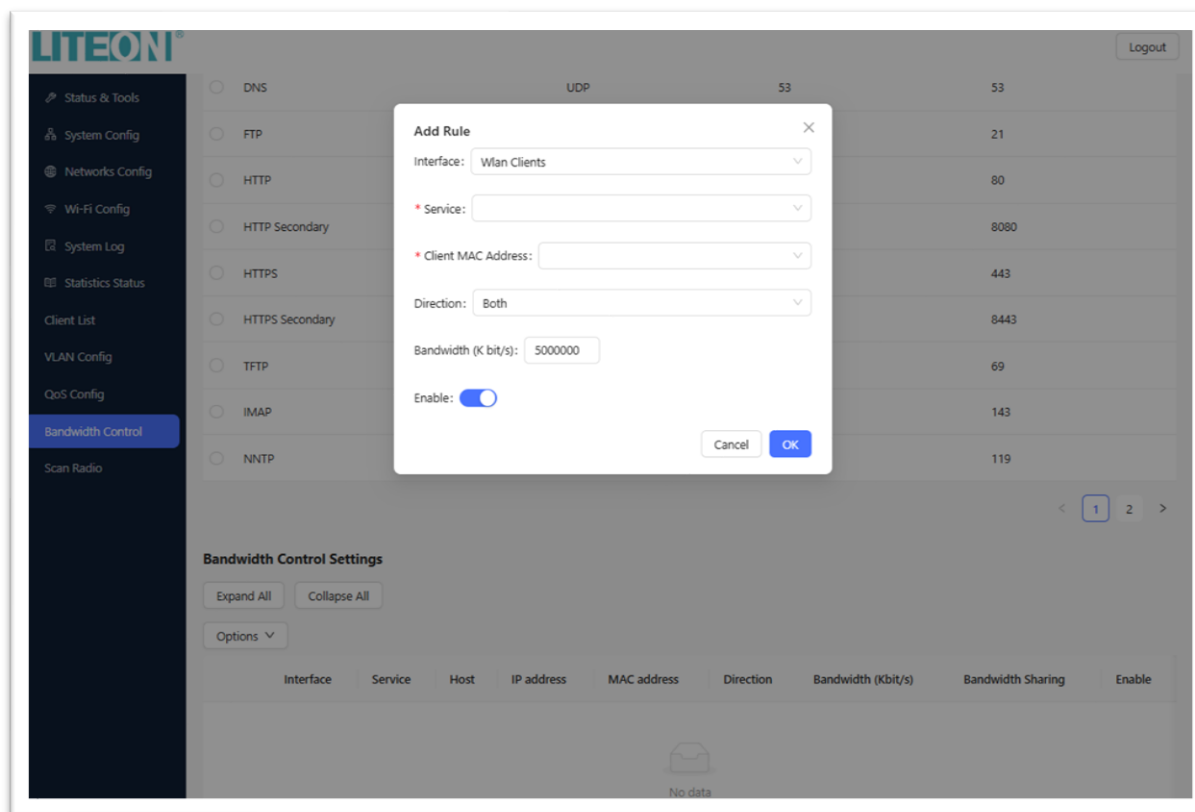


Figure 43. Bandwidth Control - Add Rule

➤ Edit Rule

To edit a rule, select the rule from the rule table, and select “Edit” from the “Options”. A page will be displayed for editing.

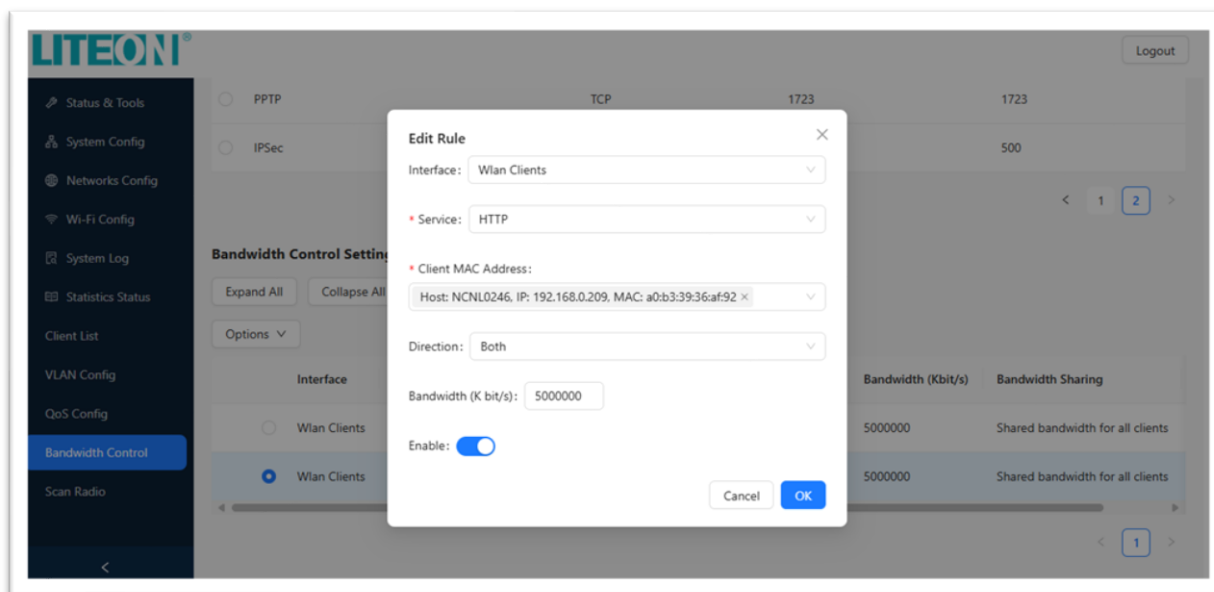


Figure 44. Bandwidth Control - Edit Rule

➤ Delete Rule

To delete a rule, select the rule from the rule table, and select “Delete” from the “Options”.

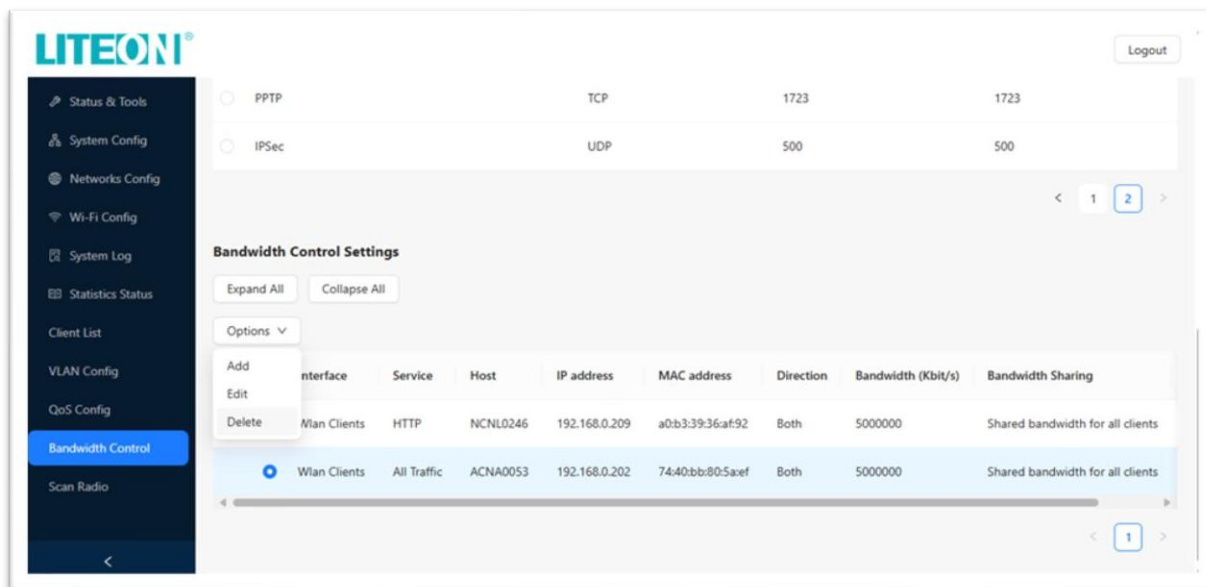


Figure 45. Bandwidth Control - Delete Rule

4.12. Scan Radio

Disabled by default. Can enable specific scanning feature from the “Mode” list.

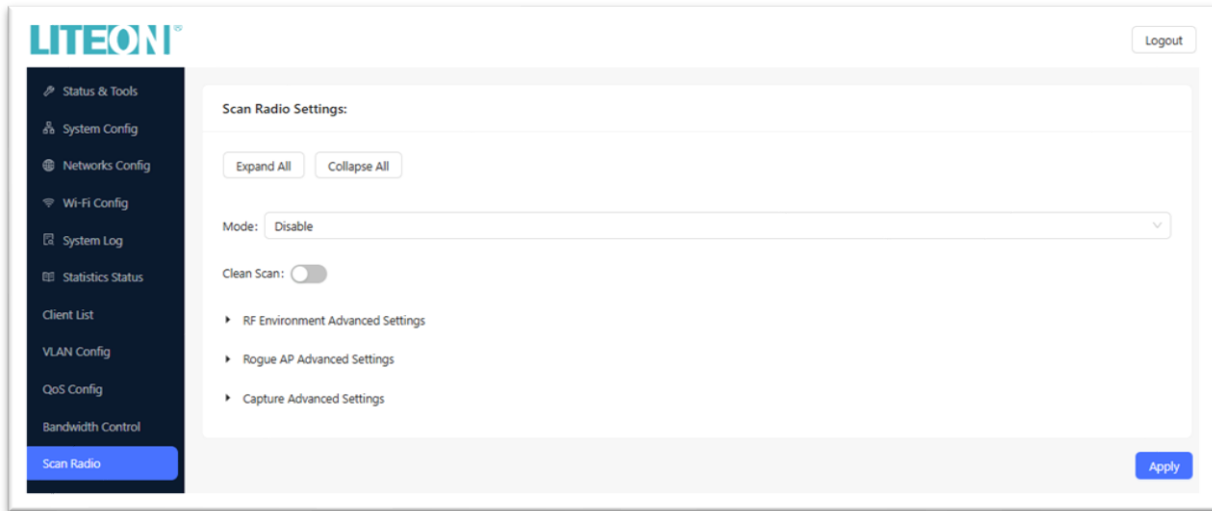


Figure 46. Scan Radio Settings

(a) Scan Mode

➤ RF Environment Scan

To analyze 2.4G, 5G and 6G radio frequency spectrum including information of each channel and each BSS. Select “RF Environment Scan” as mode and click “Apply”

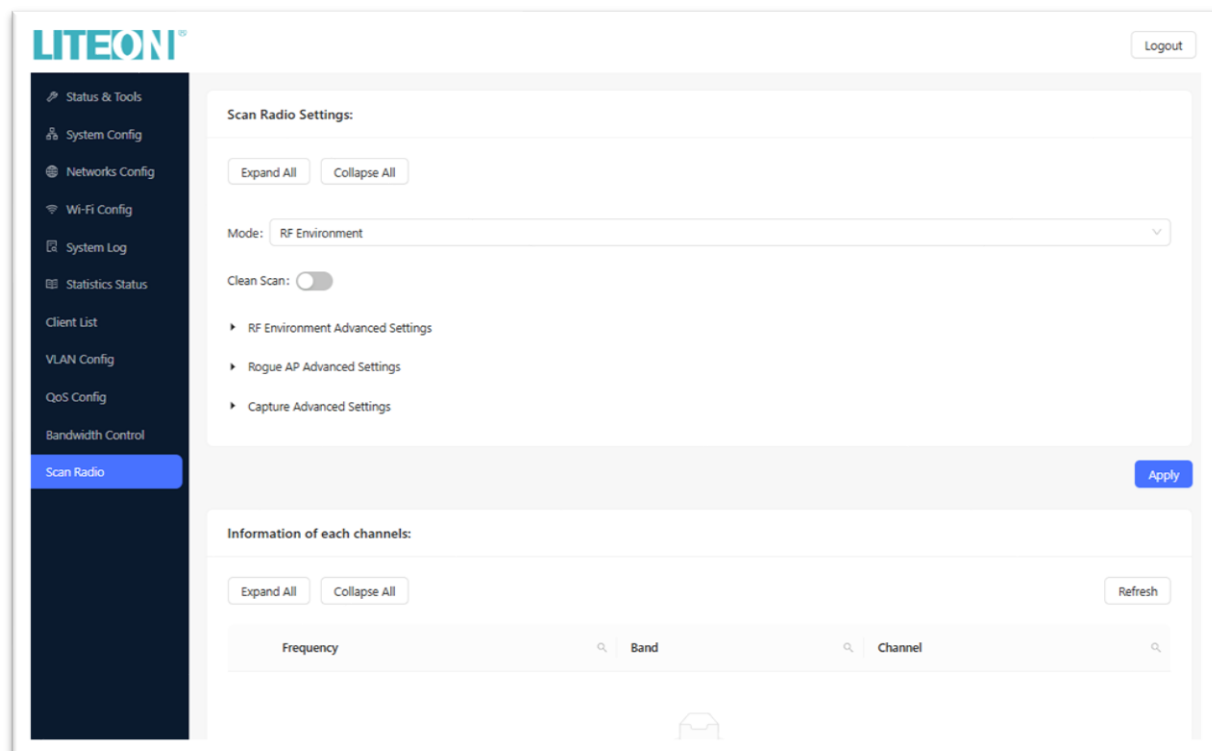


Figure 47. Scan Radio Settings - RF Environment Scan

- **Information of each channel: Frequency, Band, Channel**

Frequency	Band	Channel
+ 2412	2G	1
+ 2417	2G	2
+ 2422	2G	3
+ 2427	2G	4
+ 2432	2G	5
+ 2437	2G	6
+ 2442	2G	7
+ 2447	2G	8
+ 2452	2G	9

Figure 48. RF Environment Scan - Information of each channel

- **Information of each BSS: MAC, ESSID, Band, Channel, Bandwidth, Phymode, First Detect Time.**

MAC	ESSID	Band	Channel	Bandwidth	Phymode	First Detect Time
+ EA:C7:4F:25:C6:F2	WRB8326_IoT_c6d0	6G	213	320	11BEA_EHT320	Thu Mar 13 17:38:57 2025
+ EA:C7:4F:25:C6:F1		6G	213	320	11BEA_EHT320	Thu Mar 13 17:38:57 2025
+ EA:C7:4F:25:C6:F0	WRB8326_c6d0	6G	213	320	11BEA_EHT320	Thu Mar 13 17:38:57 2025
+ EA:C7:4F:D6:06:E2	WRB8326_IoT_c6d0	6G	213	320	11BEA_EHT320	Thu Mar 13 17:38:57 2025
+ EA:C7:4F:D6:06:E1		6G	213	320	11BEA_EHT320	Thu Mar 13 17:38:57 2025
+ EA:C7:4F:D6:06:E0	WRB8326_c6d0	6G	213	320	11BEA_EHT320	Thu Mar 13 17:38:57 2025
+ D2:39:57:FF:D5:90	WPB8326-6G-xHB	6G	213	320	11BEA_EHT320	Thu Mar 13 17:38:57 2025
+ EA:C7:4F:25:C0:02	WRB8326_IoT_c6d0	6G	213	320	11BEA_EHT320	Thu Mar 13 17:38:57 2025
+ EA:C7:4F:25:C0:01		6G	213	320	11BEA_EHT320	Thu Mar 13 17:38:57 2025
+ EA:C7:4F:25:C0:00	WRB8326_c6d0	6G	213	320	11BEA_EHT320	Thu Mar 13 17:38:57 2025

Figure 49. RF Environment Scan - Information of each BSS

➤ Rouge AP Scan

To scan Rouge AP information, select “Rogue AP” as mode and click “Apply”

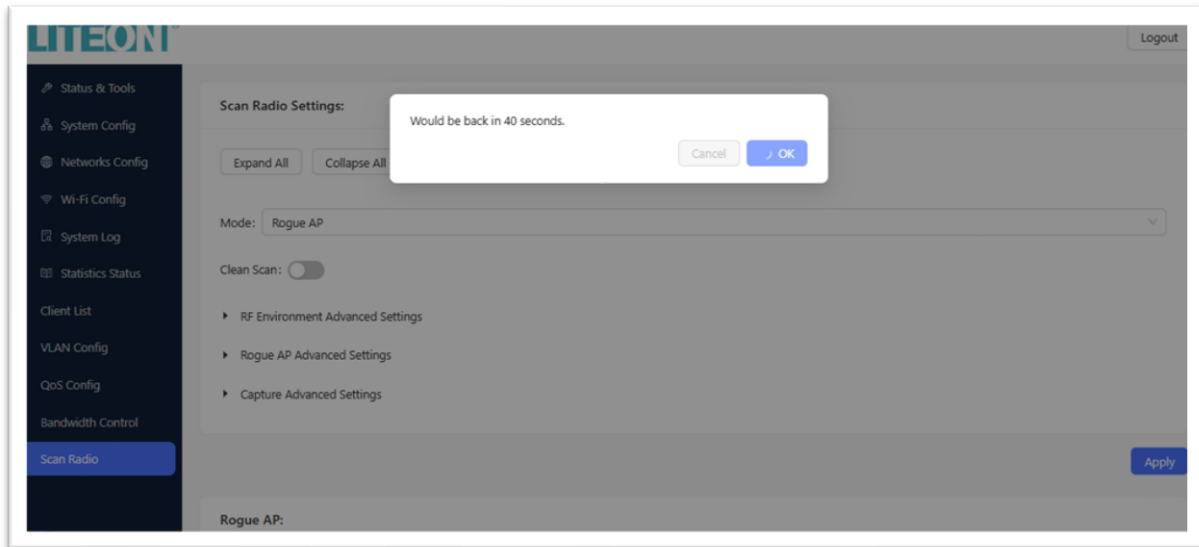


Figure 50. Rouge AP Scan

- **Rouge AP Scan Result:** MAC, ESSID, Band, Channel, Bandwidth, Security, 802.11w, Phymode, First Detect Time.

	MAC	ESSID	Band	Channel	Bandwidth	Security	802.11w	Phymode	First Detect Time
+	7C:78:B2:D6:40:99	liteon-kurt	2G	1	20	wpa2-psk	optional	11AXG_HE20	Th
+	E8:C7:4F:25:8A:48	WRB8326_ba40	2G	2	20	wpa2-psk/wpa3-sae	optional	11BEG_EHT20	Th
+	E8:C7:4F:25:8A:49		2G	2	20	wpa3-sae	required	11BEG_EHT20	Th
+	E8:C7:4F:25:8A:4A	WRB8326_iot_ba40	2G	2	20	wpa-psk/wpa2-psk	optional	11BEG_EHT20	Th
+	E8:C7:4F:D6:06:C8	WRB8326_c6d0	2G	5	20	wpa2-psk/wpa3-sae	optional	11BEG_EHT20	Th
+	E8:C7:4F:D6:06:C9		2G	5	20	wpa3-sae	required	11BEG_EHT20	Th
+	E8:C7:4F:8A:01:0A	/EF-Oo^!ePWY>fZ/WinZvD.r]	2G	5	20	wpa-psk/wpa2-psk	optional	11BEG_EHT20	Th
+	E8:C7:4F:D6:06:CA	WRB8326_iot_c6d0	2G	5	20	wpa-psk/wpa2-psk	optional	11BEG_EHT20	Th
+	E8:C7:4F:25:8B:98	Jose_H1	2G	5	20	wpa2-psk/wpa3-sae	optional	11BEG_EHT20	Th
+	E8:C7:4F:25:C6:D9	WRB8326_iot_c6d0	2G	5	20	wpa-psk/wpa2-psk	optional	11BEG_EHT20	Th

Figure 51. Rouge AP Scan Result

➤ Capture mode

To capture packets on the specified radio and channel. Select “Capture” as mode and click “Apply”

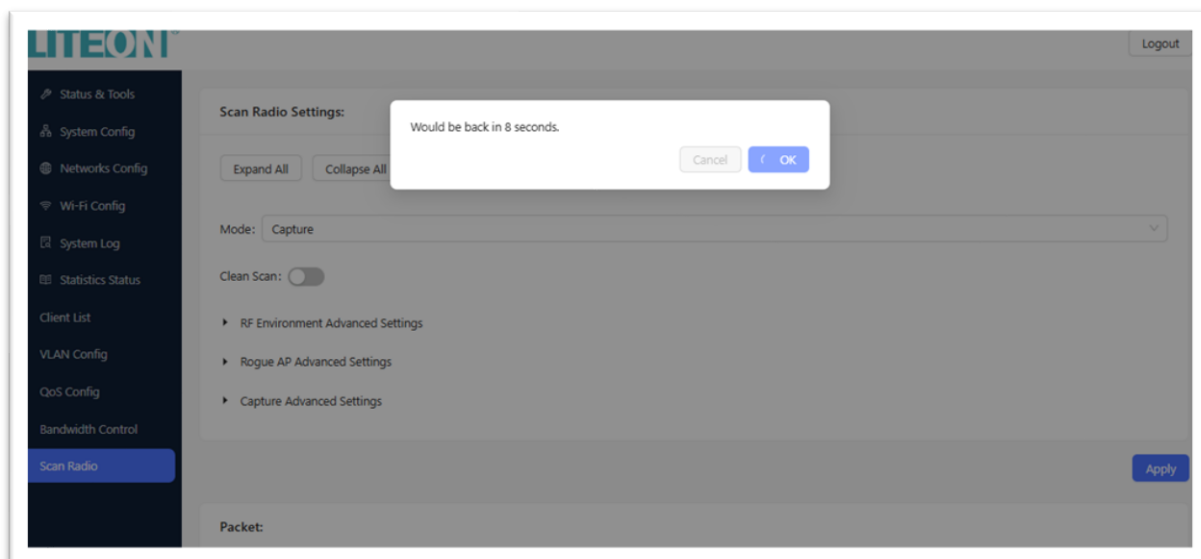


Figure 52. Capture Mode

- **Capture result** - Click the link on the packet list and download captured packets (.pcap).

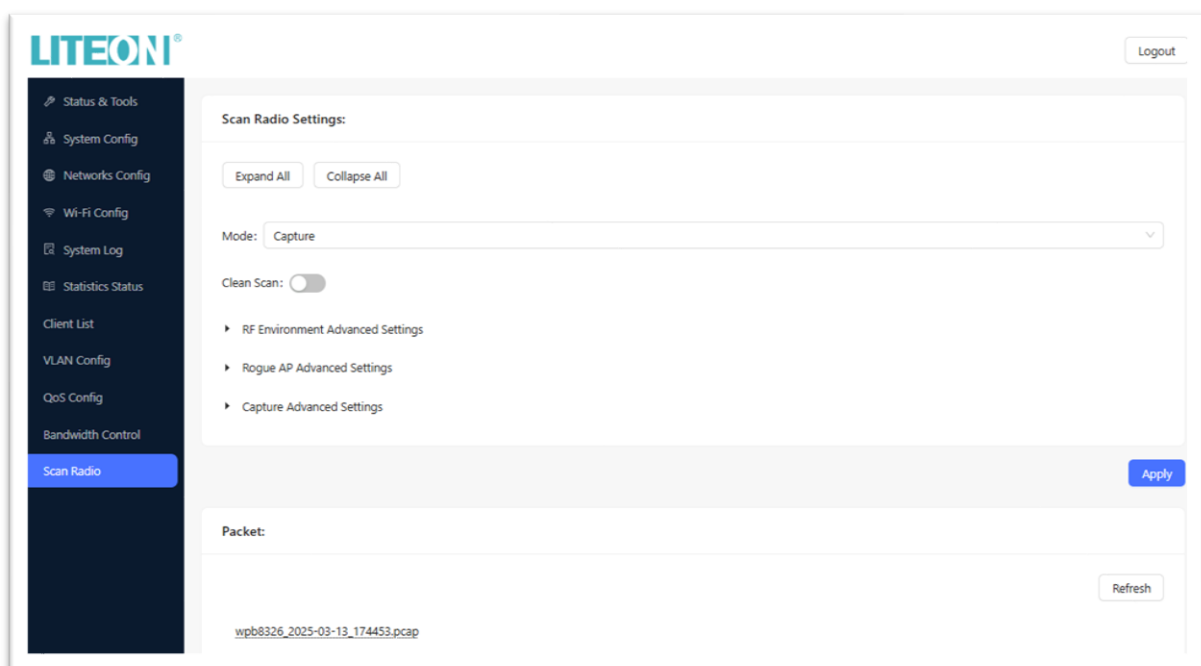
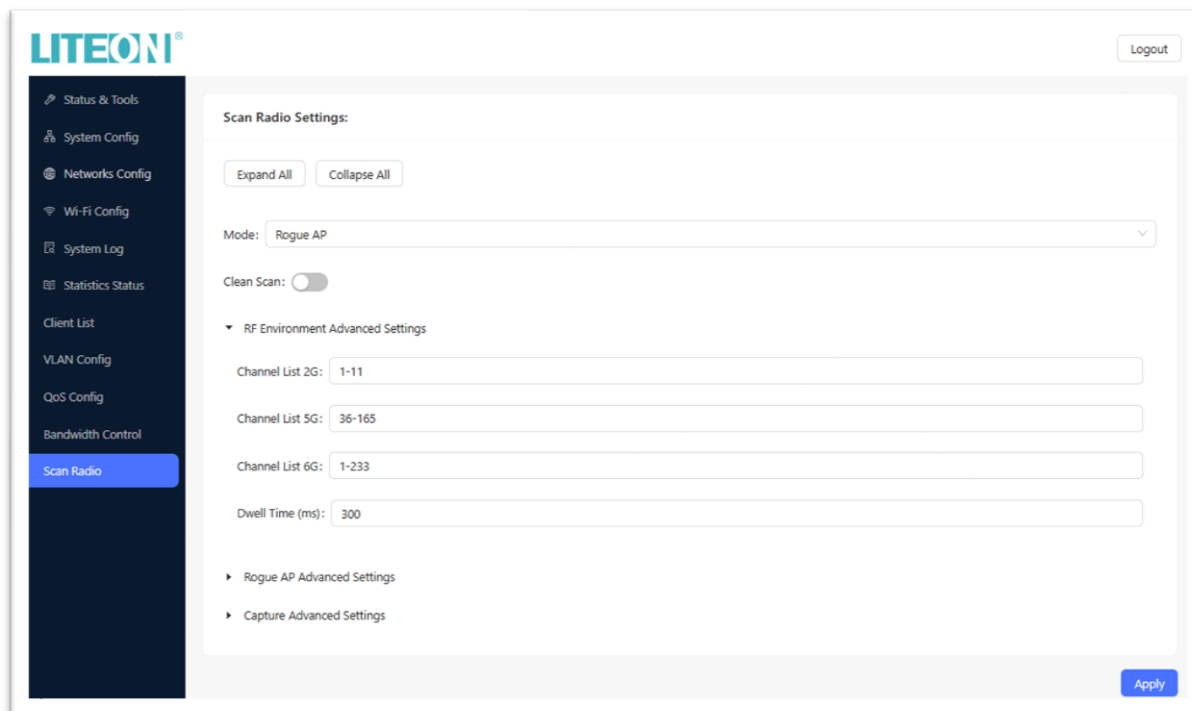


Figure 53. Capture Result

(b) Scan Radio Advanced Settings

➤ RF Environment Advanced Settings

- **Channel List 2G** - Specify the range of 2G channels for scanning.
- **Channel List 5G** - Specify the range of 5G channels for scanning.
- **Channel List 6G** - Specify the range of 6G channels for scanning.
- **Dwell Time** - Set the dwell time on each scanning channel (ms).



The screenshot displays the LITEON web management interface. On the left is a dark sidebar with a navigation menu. The main content area is titled 'Scan Radio Settings:'. It features a 'Logout' button in the top right corner. Below the title, there are 'Expand All' and 'Collapse All' buttons. A 'Mode:' dropdown menu is set to 'Rogue AP'. A 'Clean Scan:' toggle switch is currently turned off. Under the 'RF Environment Advanced Settings' section, there are four input fields: 'Channel List 2G:' with the value '1-11', 'Channel List 5G:' with '36-165', 'Channel List 6G:' with '1-233', and 'Dwell Time (ms):' with '300'. Below these fields are two expandable sections: 'Rogue AP Advanced Settings' and 'Capture Advanced Settings'. An 'Apply' button is located at the bottom right of the settings area.

Figure 54. RF Environment Scan - Advanced Settings

➤ Rouge AP Advanced Settings

- **Channel List 2G** - Specify the range of 2G channels for scanning.
- **Channel List 5G** - Specify the range of 5G channels for scanning.
- **Channel List 6G** - Specify the range of 6G channels for scanning.
- **Dwell Time** - Set the dwell time on each scanning channel (ms).
- **SSID Blacklist** - SSID added to this blacklist will be considered as rouge AP.
- **OUI Whitelist** - OUI added to this whitelist to exclude from rouge AP.

The screenshot displays the LITEON web interface. On the left is a dark sidebar with navigation links: Status & Tools, System Config, Networks Config, Wi-Fi Config, System Log, Statistics Status, Client List, VLAN Config, QoS Config, Bandwidth Control, and Scan Radio (highlighted in blue). The main content area is titled 'RF Environment Advanced Settings' and contains a sub-section 'Rogue AP Advanced Settings'. This section includes four input fields: 'Channel List 2G' with the value '1-11', 'Channel List 5G' with '36-165', 'Channel List 6G' with '1-233', and 'Dwell Time (ms)' with '300'. Below these are two sections: 'SSID Blacklist' and 'OUI Whitelist'. Each section has an 'Options' dropdown menu and a large light gray area with a folder icon and the text 'No data'. A 'Logout' button is located in the top right corner.

Figure 55. Rouge AP - Advanced Settings

➤ Capture Advanced Settings

- **Capture Band** - Capture packets on selected radio band.
- **Capture Channel** - Capture packets on selected channel.
- **Capture Duration (s)** - Stop capturing for specified time duration.
- **Capture Buffer (MB)** - Stop capturing when captured data reaches the buffer size.
- **Capture MAC Filter** - Only capture packets for selected MAC address.
- **Capture Protocol Filter** - Only capture packets for selected protocols.
- **Store FTP** - Captured packets are uploaded to FTP server.
 - **FTP IP** - FTP Server IP address
 - **FTP Port** - FTP Server Port
 - **FTP Username** - Account for accessing FTP Server
 - **FTP Password** - Account password for accessing FTP Server

▼ Capture Advanced Settings

Capture Band: 5G

Capture Channel: 100

Capture Duration (s): 10

Capture Buffer (MB): 10

Capture MAC Filter:

Capture Protocol Filter: all packets

Store FTP: ☒

* FTP IP:

* FTP Port:

* FTP Username:

* FTP Password:

Apply

Figure 56. Capture Mode - Advanced Settings

Chapter 5 FAQ

Q1. Why can't some legacy clients connect to WPB8326?

Please check if the SSID security is set to "WPA3 SAE" or "WPA3 ENTERPRISE". Some legacy clients do not support WPA3. Please connect these legacy devices to an SSID configured with WPA2 PSK or WPA2 ENTERPRISE security.

Besides, check if the "11r Enable" configuration option for the SSID is toggled on. If it is, please uncheck the "11r Enable" option.

Q2. Why can't the Radius MAC function be enabled under a SSID?

The Radius MAC feature can only be activated when the security is set to "OPEN" for 2G and 5G SSIDs. This function is currently disabled for the 6G SSID.

FCC

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

- FCC regulations restrict the operation of this device to indoor use only.
- This device is prohibited from being operated on oil platforms, cars, trains, boats, and aircraft, except it can be operated in large aircraft while flying above 10,000 feet in the 5.925-6.425 GHz band.
- Transmitters in the 5.925-7.125 GHz band are prohibited from operating to control or communicate with unmanned aircraft systems.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 22cm between the radiator C your body.

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

ISED

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

【French】 L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. L'appareil ne doit pas produire de brouillage;
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

- Devices shall not be used for control of or communications with unmanned aircraft systems.
- Devices shall not be used on oil platforms.
- Devices shall not be used on aircraft, except for the low-power indoor access points, indoor subordinate devices, low-power client devices, and very low-power devices operating in the 5925-6425 MHz band, that may be used on large aircraft as defined in the [Canadian Aviation Regulations](#), while flying above 3,048 metres (10,000 feet).

【French】

- Les dispositifs ne doivent pas être utilisés pour commander des systèmes d'aéronef sans pilote ni pour communiquer avec de tels systèmes.
- Les dispositifs ne doivent pas être utilisés sur les plateformes de forage pétrolier.
- Les dispositifs ne doivent pas être utilisés dans les aéronefs, à l'exception des points d'accès intérieurs de faible puissance, des dispositifs subordonnés intérieurs, des dispositifs clients de faible puissance et des dispositifs de très faible puissance fonctionnant dans la bande de 5 925 à 6 425 MHz, qui peuvent être utilisés dans les gros aéronefs tel qu'il est défini dans le [Règlement de l'aviation canadien](#), et ce, lorsqu'ils volent à une altitude supérieure à 3 048 mètres (10 000 pieds).

Operation shall be limited to indoor use only.

【French】 Le fonctionnement doit être limitée à une utilisation à l'intérieur seulement.

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24cm between the radiator C your body.

【French】 Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 24cm de distance entre la source de rayonnement et votre corps

EU

the following table provides information on the frequency bands used and the maximum RF transmit power of the product for sale in the EU:

Frequency range (MHz)	Maximum output power (dBm)
2400-2483.5	19.98
5150-5350	22.96
5470-5725	29.98
5945-6425	22.99
Bluetooth; 2.4GHz	9.99
Zigbee; 2.4GHz	9.89

This equipment should be installed and operated with minimum distance 20cm between the radiator C your body.

Hereby, LITE-ON TECHNOLOGY CORP. declares that the radio equipment type Indoor Wi-Fi 7 2x2 Tri-Band Enterprise Access Point is in compliance with Directive 2014/53/EU

The device is restricted to indoor use only when operating in the 5150-5350 MHz and 5945-6425 MHz frequency ranges.

LITE-ON TECHNOLOGY CORP

22 F., No. 392, Ruiguang Rd., Neihu Dist., Taipei City 114753, Taiwan (R.O.C.)