SP250/SP250-S5

11ax Access Point

TABLE OF CONTENTS

Chapter 1. Introduction 1
1.1. Product Description 1
Chapter 2. Hardware Components 2
2.1. Package Contents 2
2.2. Installation Requirements 2
2.3. Physical Ports 2
2.4. LED Indicator 3
Chapter 3. Hardware Installation 4
3.1. Mounting the Access Point on the Pole 4
3.2. Grounding Connection & Protect from Lightning 4
3.3. Safety Notice 4
3.4. Installing a Cable Gland (SP-WP-CM20) 5
3.5.Powering the AP 5
Chapter 4. The Https Interface 6
4.1. Login to the HTTPS Interface 6
4.1.1 Thin and Fat AP Swiching 6
4.2. Thin AP Mode 7
4.2.1 Access Point Configuration 7
4.2.2. Status 8
4.2.2.1. Overview 8
4.2.2.2. General 9
4.2.3. System 11
4.2.3.1. AP Mode 11
4.2.3.2. Reboot 11
4.3. Fat AP Mode 12
4.3.1. Status 12
4.3.1.1. Overview 12
4.3.1.2. Firewall 15
4.3.1.3. Routes 15
4.3.1.4. Processes 16
4.3.1.5. Realtime Graphs 17
4.3.2. System 18
4.3.2.1. System 18
4.3.2.2. Administration 18
4.3.2.3 5G-NR 19
4.3.2.5. Backup/Flash Firmware 20
4.3.2.6. AP Mode 21
4.3.2.7. Reboot 21
4.3.3. Network 22
4.3.3.1. Interfaces 22
4.3.3.2. Wifi 32
4.3.3.3. DHCP and DNS 44
4.3.3.4. Static Routes 49
4.3.3.5. Firewall 50

4.3.3.6. Diagnostics 52
Chapter 5. Technical Specifications 54
Chapter 6. Appendix 56
6.1. Warranty 56
6.1.1. General Warranty 56
6.1.2. Warranty Conditions 56
6.1.3. Disclaimer 56
6.2. Compliance 57
6.2.1. FCC 57
6.2.2. CE Marking 57
6.2.3. NCC 58
6.4. Optional Accessories 59
6.5. Contact Information 59

CHAPTER 1. INTRODUCTION

This manual is intended for installing and managing the SP250 using the HTTPS interface. The SP250 will simply be referred to as the Gateway within this guide. The installer should be familiar with network structures, terms, and concepts.

1.1. Product Description

The SP250 /SP250-S5 is high performance Wi-Fi 6 access point for high-density environment like warehouse, shopping center, airport and other locations.
The SP250 / SP250-S5 efficiently manage up to 1024 Wi-Fi client connections with improved capacity and faster speeds with dual-band concurrent up to 1.774Gbps data rates. With built-in coverage antennas, SP250 fully complies with IEEE 802.11ax, including OFDMA Modulation, MU-MIMO, and BSS Color Spatial Reuse.

Attestation ：Despite having a weatherized enclosure, and there being instructions for lightning safety, etc. in the manual, this device will only be used indoors.

Feature

- Dual-band Wi-Fi 6 (802.11ax), backward compatible with Wi-Fi 5 (802. 11ac)
- Maximum throughput up to 1,200 Mbps in 5GHz and 574 Mbps in 2.4GHz
- Max. ERIP up to 31dBm in 5GHz and 31dBm in 2.4GHz
- Target wake time to reduce the amount of time of a client/ IoT device at
- power save mode to be awaken
- Uplink and downlink of MU-MIMO improves transmission between AP and client
- devices
- with 2 x 2.5 GbE ports which are 2.5 times faster than standard Ethernet (1GbE)
- enhance network performance

CHAPTER 2. HARDWARE COMPONENTS

2.1. Package Contents

Carefully remove all the items from the packing of access point (AP). The following items should be included in the packaging:

SP250/SP250-S5

One mounting bracket
+ Four screws

cable gland (*Note)

One ground wire

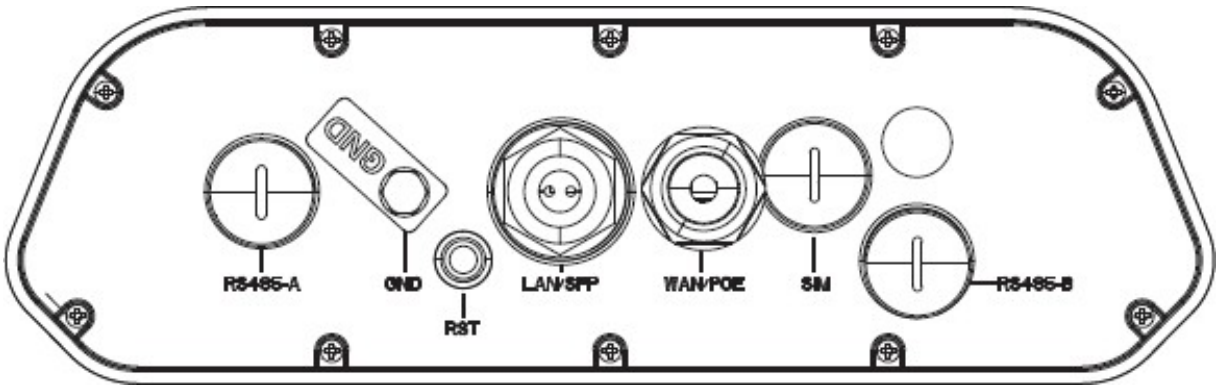
One clamp

2.2. Installation Requirements

TERMS OF USE: All Ethernet cabling runs suggest using CAT.6, 24 AWG (or above) Shielded Twisted Pair (STP) cabling. In addition, please cut the cable into a proper length, strip the cables on both ends, and crimp the wires into RJ45 connectors. It is the professional installer's responsibility to follow local country regulations, including operation within legal frequency channels, output power, indoor cabling requirements, and Dynamic Frequency Selection (DFS) requirements.

2.3. Physical Ports

The following physical ports are available on the SP250 /SP250-S5.



Port	Description
WAN / PoE Port	The WAN/PoE port operates at 10/100/1000/2500Mbps at supports an RJ45 connection. Supporting PoE In, the AP can receive power through the WAN port from PSE (Power Sourcing Equipment), rendering the need for a power supply into the power port unnecessary.
LAN Port	The LAN port operates at 10/100/1000/2500Mbps at supports an RJ45 connector.
GND Port	Ground through GND Port.
Reset Button	After use, the setting will be reset to default. Please press and hold about 15 seconds.
RS485-A/B (Not Available)	You can be transmitted through this port. (SP250-A04 Only)
SIM Card Port (Not Available)	SIM card can be inserted into this slot for use. (SP250-A04 Only)

2.4. LED Indicator

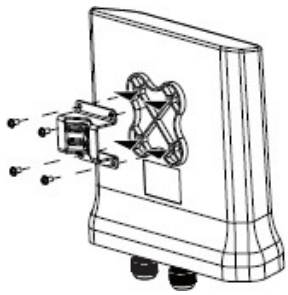
The following table describes the AP status referring to different LED behavior.

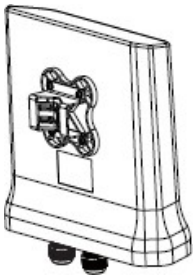
Color	Behavior	Description
Red	**on**	initialize
	blink	System is upgrading; do not touch or unplug power adaptor.
White	**on**	Connected to internet.
	blink	Unconnected to internet.

CHAPTER 3. HARDWARE INSTALLATION

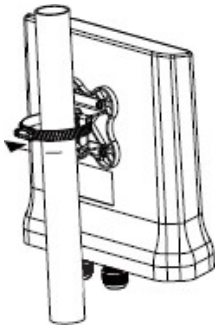
3.1. Mounting the Access Point on the Pole

①Place the mounting bracket to the device using four screws (included in the packaging). Securely tighten the screws.





② Attach the clamp to encircle pole and the mounting bracket. Securely tighten the clamp.

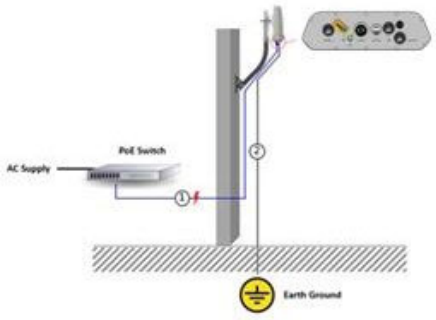


3.2. Grounding Connection & Protect from Lightning

1. Make your device GND port connect to ground wire.
2. The ground wire connects to the earth. In addition, the grounding wire meets to 6-AWG copper grounding wire.

Note: In order to prevent the radio inflection, it is recommended to power the device after rotate the antenna.

Note: Be sure that grounding is available and that it must comply with local and national electrical codes. For additional lightning protection, use lightning rods and lightning arrestors.

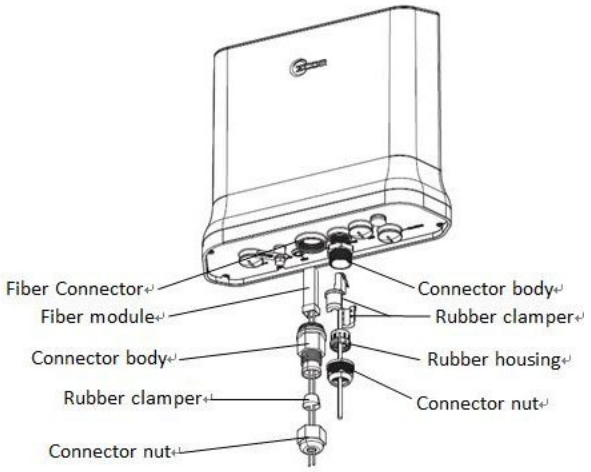


3.3. Safety Notice

1. Do not install the device close to any electrical grounding device or lightning protection system. Place the device's own grounding and lightning protection system apart from any electrical grounding device and lightning protection system as far as possible.
2. Protect components from electrostatic discharge: Please wear an ESD wrist strap or handle the power adapter by its edge and do not touch any component or printed circuit boards, especially for module device.
3. Make sure to keep the temperature and humidity of the installation location at an optimal level.
4. An excellent grounding system guarantees the stable operation of device, as well as to protect device from lightning, interference and electrostatic discharges.
5. Supply stable power to the device. Unstable power may cause the device to malfunction. The device supports PoE power supply and is recommended if the device is installed near grid lines within less than 100 meters radius.

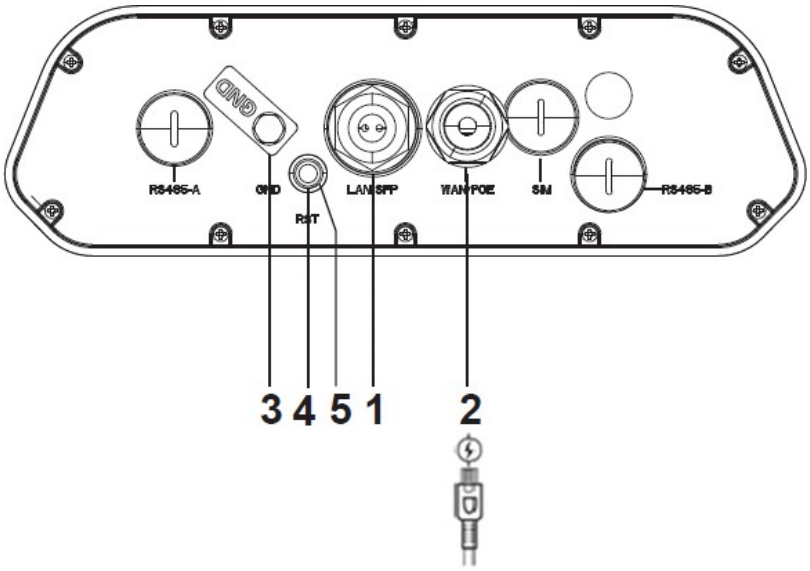
3.4. Installing a Cable Gland (SP-WP-CM20)

(1) Dismantle all the components of cable gland,
(2) Plug the cable in between of Rubber clamper.
(3) Insert rubber housing
(4) Insert the rubber housing back to connector body
(5) Tighten the connector nut.
(6) Recheck cable gland.



3.5. Powering the AP

Connect the PoE 48V, then it will power on.



Note: Please wait for 5-10 seconds while powering on.

CHAPTER 4. THE HTTPS INTERFACE

The AP can be configured through its supported software interface HTTP. The HTTP interface can be accessed using any standard web browsing software through any network. This chapter explains all the elements that are available on the HTTP interface of the AP.

Note: The default Username is **root** and Password is **password**.

Note: Click RESET Reset button to return the parameters on the page to their previously saved state.

Note: Click SAVE Save button to accept and save the modifications made on the page.

Note: Click SAVE & APPLY Save & Apply button to save and apply the modifications made on the page.

4.1. Login to the HTTPS Interface

① To access the HTTPS interface on the AP, enter the IP address of the AP into the web browser's address bar and press the Enter key.

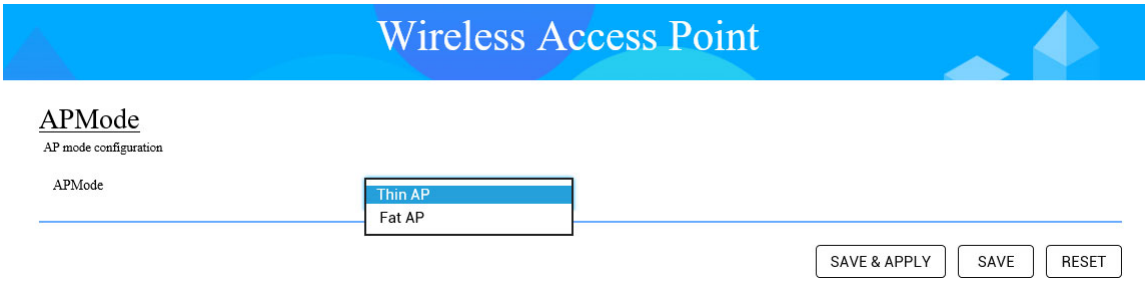
② Enter the Username and Password in the respective textboxes and click the Login button. To return the information, displayed in the textboxes to the defaults, click the Reset button.

③ In a default access point configuration is TAP mode.

④If you want to switch in FAP mode, please change it in **system→ AP Mode,** choose FAP and click **Save & Apply** to switch it from TAP to FAP.

4.1.1 Thin and Fat AP Switching

Click **System→AP Mode,** choose the AP mode you want and click SAVE&APPLY.



4.2. Thin AP Mode

The procedure for completing the access point's essential configuration depends on whether you want it to be managed by wireless LAN controllers (WLC).

To configure the access point to be managed by the WLC, you must ensure that the APs will be able to locate and connect to the WLC when powered on. When connected to the network, each AP is assigned a valid IP address.

4.2.1 Access Point Configuration

In a default access point configuration, the access point default AP mode is TAP mode, and obtains IP addresses from DHCP Option 43 protocol.

Note: In TAP mode, the AP must be able to go with Wireless LAN Controllers (WLCs) for bulk configuration and performing other commands of access points. Please refer to WLC QSG for settings first, then go back to finish the AP configuration. https://www.zcom.com.tw/index/downloads?keyword=&meterial_type=49

Step 1. Power on the access point. As the status of LED indicator from flashing change to steady red, the connection is successful.

Note: Please make sure DHCP server is enabled on the network once accomplished WLC settings. The access point must receive its IP address through DHCP server.

Note: Switching from DHCP to assign a static IP address or DNS and L2 discovery mode to the access point, please refer to the user manual for more information.
https://www.zcom.com.tw/index/downloads?keyword=&meterial_type=25

If the access point cannot connect to the WLC by DHCP broadcast, please refer to the following optional settings.

Optional: Set up a static IP address

Note: The following procedure assumes that Windows 10 is the operating system. Procedures for other operating systems are similar.

Step 1. On your computer, configure your network adapter from the "Local Area Connection "settings as follows:

- Start→Control Panel→Network & Internet→Change Adapter Options→Ethernet

Step 2. Edit the TCP/IPv4 address setting as follows:

- Properties→Internet Protocol Version 4 (TCP/IPv4)

Step 3. Select "Use the following IP address" and make the following entries:

- IP address: 192.168.1.168 (or any available address in the 192.168.1.x network, except 192.168.1.1)
- Subnet mask: 255.255.255.0

Leave the "Default gateway" and "DNS server" fields empty.

Step 4. Click "OK" to save your changes.

Login into the access point

Step 5. Launch a Web browser; type default URL https://192.168.1.1 to connect to the access point. When a security alert dialog box appears, click OK/Yes to proceed.

Step 6. When login page appears, enter the following: Username: **root**/Password: **password**

Step 7. Click login.

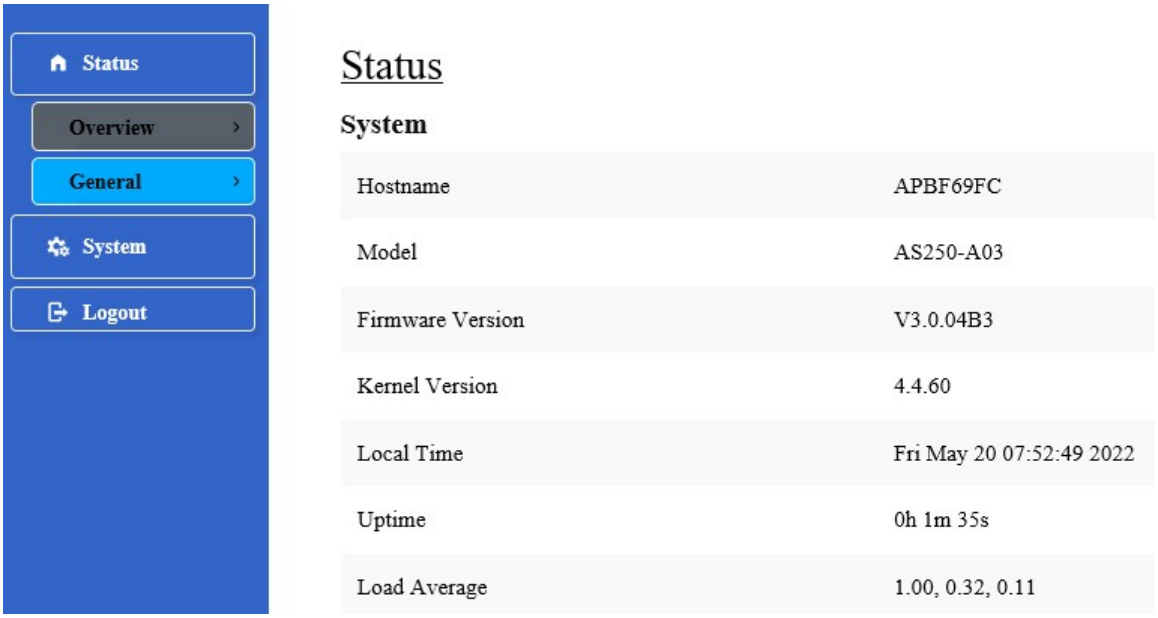
Customizing the Wireless Settings

On the Web interface menu, Select Status→General in the menu bar. Check your switchmod item to select "Connect with via IP", and setup your WLC IP address on "Wireless Switch Address 1".

Note: IP address of WLC needs to be assigned (ex. 192.168.1.228) while on operation.

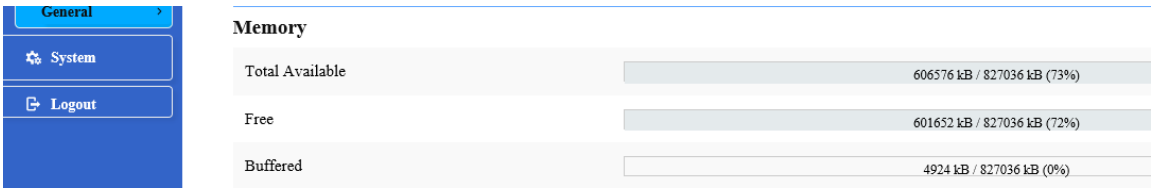
4.2.2. Status

4.2.2.1. Overview



This page is used to provide an overview of the software settings and status of the AP. The following parameters are available in this section:

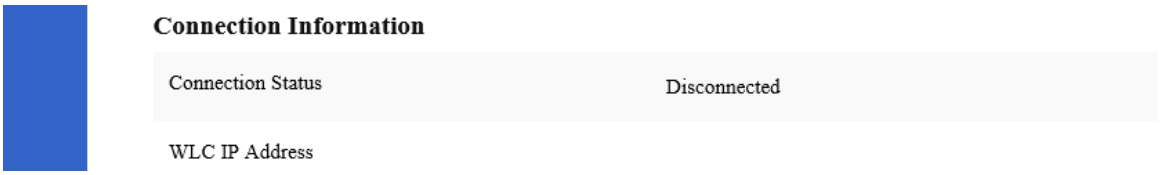
Parameter	Description
Hostname	Displays the hostnames of active DHCP clients connected to the AP. DHCP stands for Dynamic Host Configuration Protocol.
Model	Displays the AP Model.
Firmware Version	Displays the AP firmware version.
Kernel Version	Displays the Linux kernel version.
Local Time	Displays the local time in your area.
Uptime	Displays the how long the AP is active.
Load Average	Displays the average system load calculated over a given period of time of 1, 5 and 15 minutes.



The following parameters are available in this section:

Parameter	Description
Total Available	Displays the total memory supported by the AP in kilobytes and percentage.
Free	Displays the free memory on the AP in kilobytes and percentage.

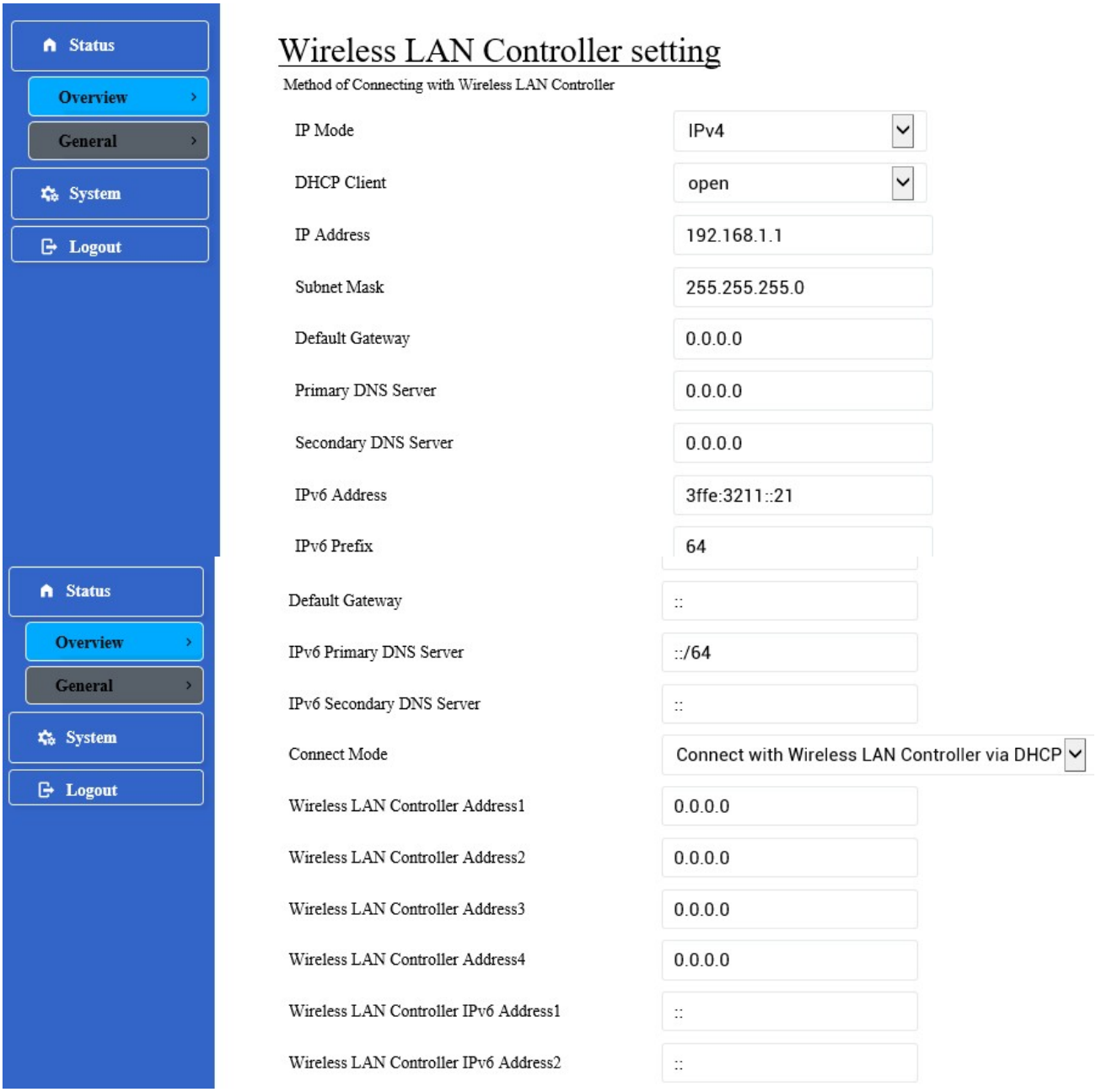
Parameter	Description
Buffered	Displays the buffered memory on the AP in kilobytes and percentage.

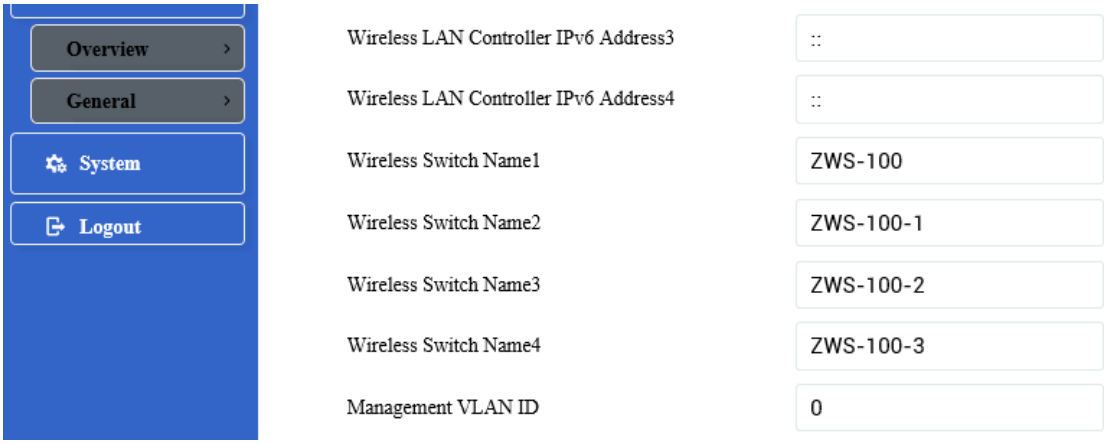


The following parameters are available in this section:

Parameter	Description
Connection Status	Displays the connection status of the client to AP.
WLC IP Address	Displays the IP address of the WLC connect to the AP.

4.2.2.2. General





Next click the General Button. Once login, first assign a fixed IP address or a DHCP IP to the AP under Current IP Setting. Under Wireless Switch Setting, select Connect with Wireless Switch via IP and input the IP address of the AP access controller, then click save & apply to take effect.

Parameter	Description
IP Mode	Displays basic mode information of the ipMod. IPv4 – Select IPv4 mode. IPv6 - Select IPv6 mode. Auto – Auto detected if it is IPv4 or IPv6.
DHCP Client	Choose the DHCP Client, which is Close, or Open by default it will be Open.
IP Address	Enter the IP address.
Subnet Mask	Enter the Subnet Mask.
Default Gateway	Enter the IPv4 address of the gateway for the interface.
Primary / Secondary DNS Server	Enter primary/secondary DNS server. (if require the second one)
IPv6 Address	Enter the IPv6 address.
IPv6 Prefix	Enter the IPv6 prefix IP address.
Default Gateway	Enter the IPv6 address of the gateway for the interface.
Connect mode	Displays basic information of the switch mod: Connect with via DHCP – connect the AP via DHCP of the network or provided by the Access controller DHCP IP address. IP – Connect the AP via Access controller IP address. DNS - Displays the MAC address of the interface.
Wireless LAN Controller Address 1/2/3/4	Enter wireless access controller IPv4 IP address.
Wireless LAN Controller IPv6 Address1/2/3/4	Enter wireless access controller IPv6 IP address.
Wireless Switch Name1/2/3/4	Enter access controller DNS value.
Management VLAN ID	Enter specific management VLAN ID which is providing from the Network.

4.2.3. System

4.2.3.1. AP Mode

This page is used to displayed and changed AP modes.

- Thin AP - Specifies to use and configure this AP with a wireless controller in the network. The wireless controller will be responsible for the configuration of this AP. Only a few functions are available to be configured on this AP in this mode.
- Fat AP - Specifies to use and configure this AP without a wireless controller in the network. More functions are available to be configured on this AP in this mode.

4.2.3.2. Reboot

Click the Perform reboot link to reboot the device any unsaved configuration.

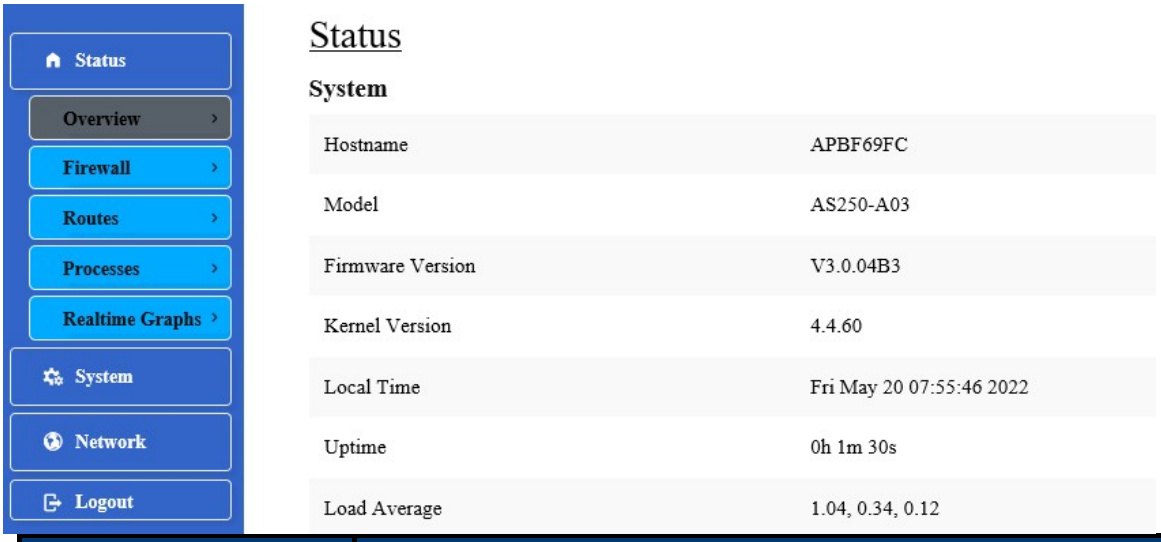
4.3. Fat AP Mode

A Fat AP is suitable for family and small-scaled networks and provides full features. This Fat AP is wireless equipment used to control and manage wireless clients. The Fat AP may support both 2.4GHz and 5GHz band in a single logic management domain. This Fat AP is used for wireless terminals to access a wired network; also it can communicate the bridge between the wireless clients and wired network. Before configuring the Fat AP make sure that AP is in Fat AP mode. If the AP is in Thin AP mode, please change into Fat AP mode and precede the following essential configuration.

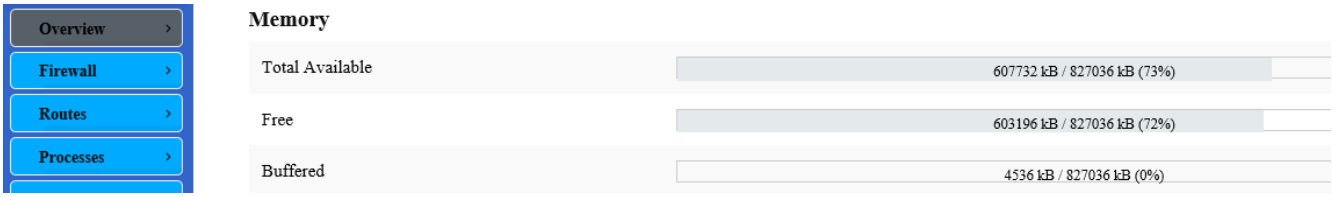
4.3.1. Status

4.3.1.1. Overview

This page is used to provide an overview of the software settings and status of the AP. The following parameters are available in the System section:



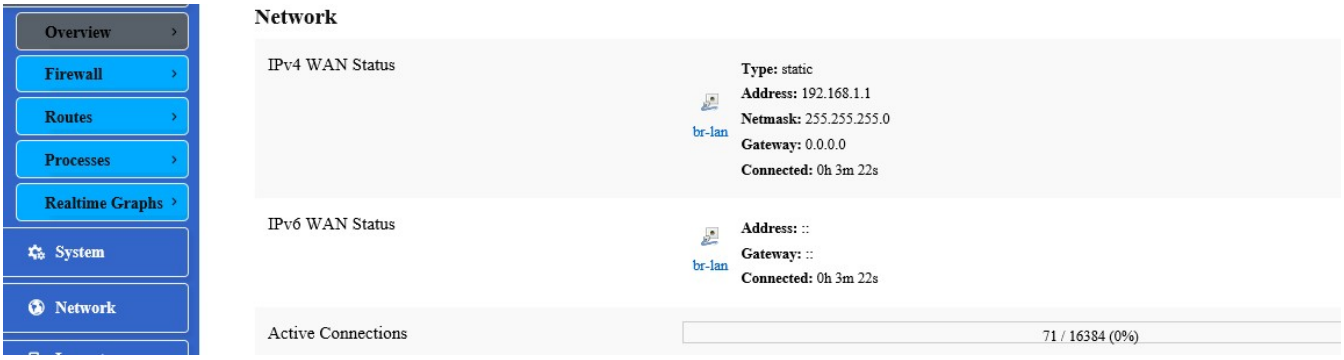
Parameter	Description
Hostname	Displays the hostnames of active DHCP clients connected to the AP. DHCP stands for Dynamic Host Configuration Protocol.
Model	Displays the AP Model.
Firmware Version	Displays the AP firmware version.
Kernel Version	Displays the Linux kernel version.
Local Time	Displays the local time in your area.
Uptime	Displays the how long the AP is active.
Load Average	Displays the average system load calculated over a given period of time of 1, 5 and 15 minutes.



The following parameters are available in the Memory section:

Parameter	Description
Total Available	Displays the total memory supported by the AP in kilobytes and percentage.
Free	Displays the free memory on the AP in kilobytes and percentage.

Parameter	Description
Buffered	Displays the buffered memory on the AP in kilobytes and percentage.

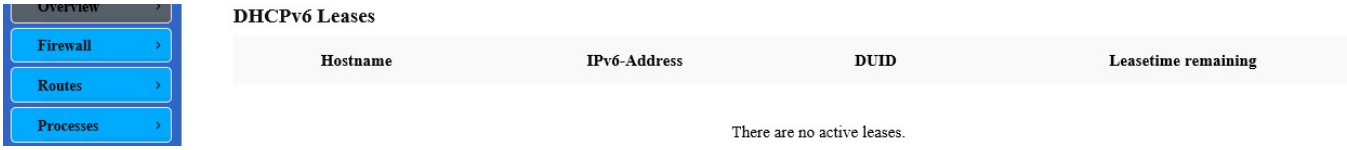


The following parameters are available in the Network section:

Parameter	Description
IPv4 WAN Status	Displays the IPv4 WAN (Wide Area Network) connection status.
IPv6 WAN Status	Displays the IPv6 WAN (Wide Area Network) connection status.
Active Connections	Displays the number of active network connections in integers and percentage.

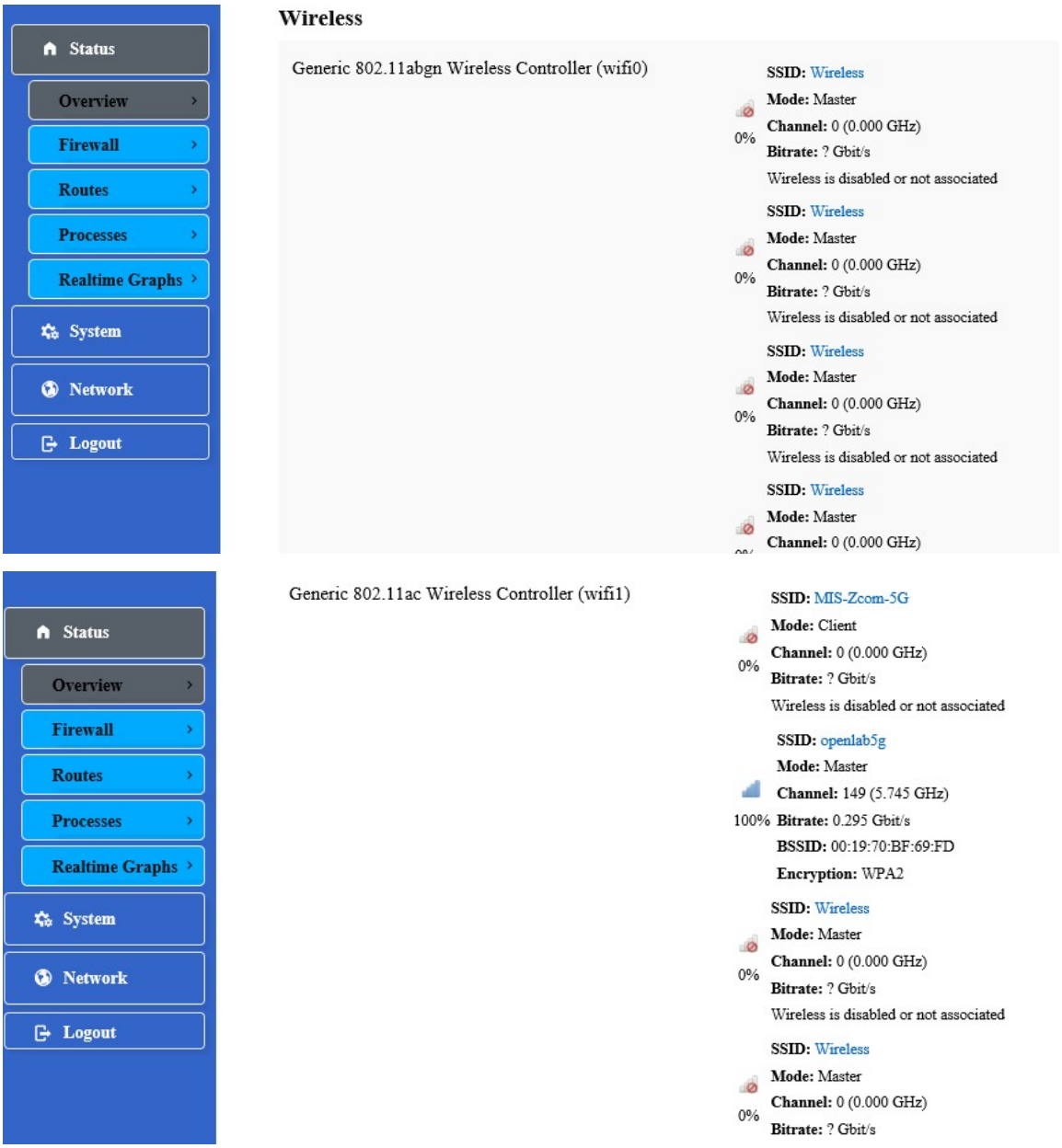
The following parameters are available in the DHCP Leases section:

Parameter	Description
Hostname	Displays the hostnames of active DHCP clients connected to the AP. DHCP stands for Dynamic Host Configuration Protocol.
IPv4 Address	Displays the IP addresses of active DHCP clients connected to the AP. IP stands for Internet Protocol.
MAC Address	Displays the MAC addresses of active DHCP clients connected to the AP. MAC stands for Medium Access Control.
Lease Time Remaining	Displays the DHCP lease time remaining for the DHCP clients connected to the AP.



The following parameters are available in the DHCPv6 Leases section:

Parameter	Description
Hostname	Displays the hostnames of active DHCPv6 clients connected to the AP.
IPv6 Address	Displays the IPv6 addresses of active DHCPv6 clients connected to the AP.
DUID	Displays the DUID (DHCP Unique Identifier) of active DHCPv6 clients connected to the AP.
Lease Time Remaining	Displays the DHCPv6 lease time remaining for the DHCPv6 clients connected to the AP.



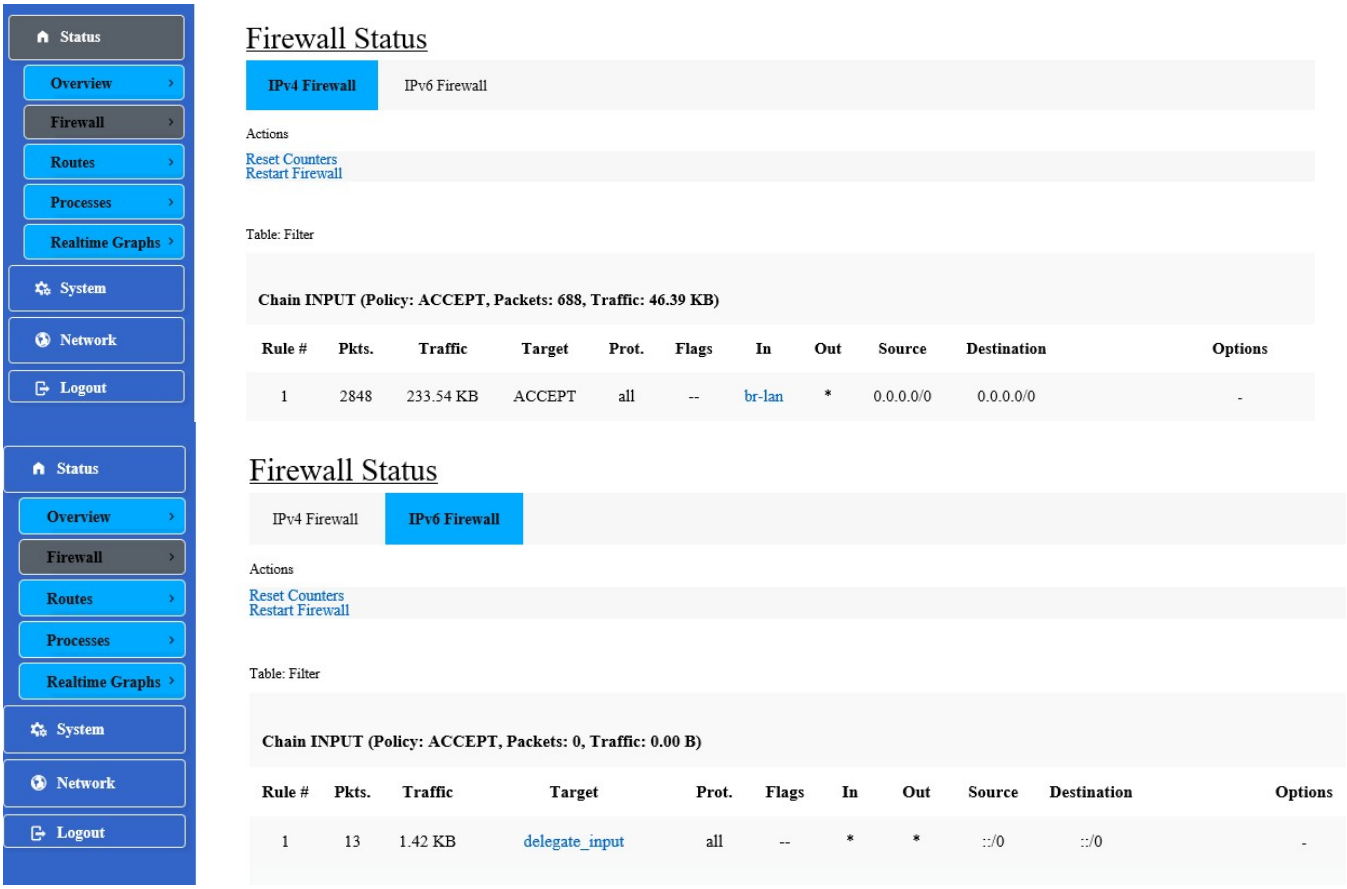
The following parameters are available in the Wireless section:

Parameter	Description
Generic 802.11abgn Wireless Controller (wifi0)/ Generic 802.11ac Wireless Controller (wifi1)/ Generic 802.11ac Wireless Controller (wifi2)	Displays information about the generic 802.11abgn wireless controller (wifi0) , Generic 802.11ac Wireless Controller (wifi1) and Generic 802.11ac Wireless Controller (wifi2). SSID - Displays the SSID (Service Set Identifiers) for this wireless interface. Click on the hyperlink to configure this wireless interface. Mode - Displays the mode of the wireless interface. Channel - Displays the wireless channel (frequency) hosted by this wireless interface. Bitrate - Display the bitrate provided through this wireless interface. BSSID –Displays the BSSID (Basic Service Set Identifier) hosted by the wireless interface. ENCRYPTION - Displays the wireless encryption used on the wireless interface.

4.3.1.2. Firewall

4.3.1.2.1. IPv4 / IPv6 Firewall

This page is used to display the detailed status of the IPv4 and IPv6 firewall features provided on the AP.



4.3.1.3. Routes

This page is used to display the IPv4/IPv6 routing information. The following parameters are available in this section:

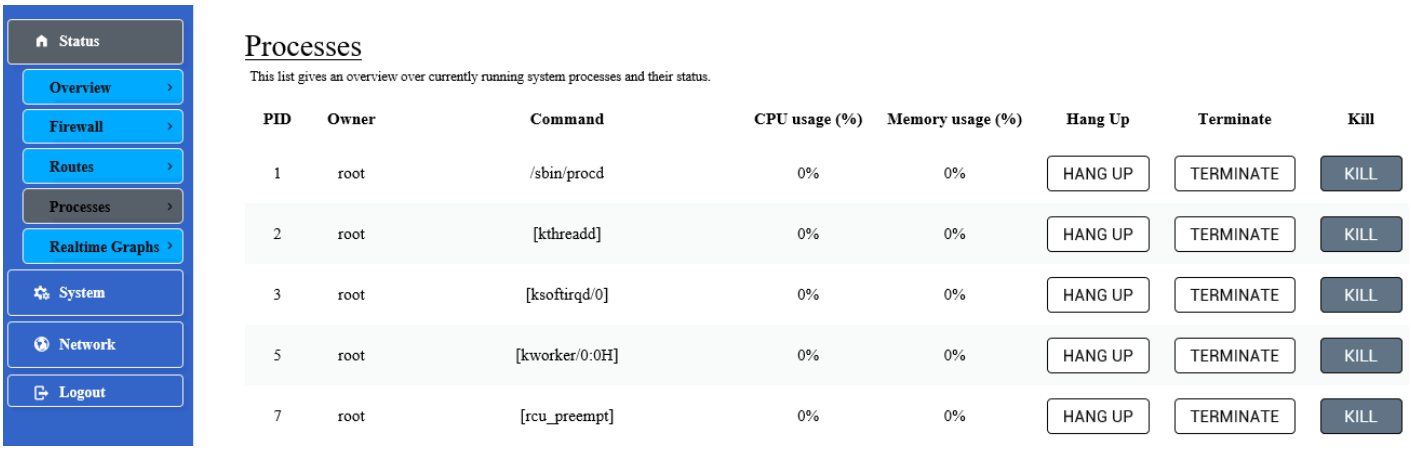
Parameter	Description
IPv4 Address	Displays the IPv4 address of the ARP (Address Resolution Protocol) entry.
IPv6 Address	Displays the IPv6 address of the neighbour entry.

Parameter	Description
MAC Address	Displays the MAC address of the ARP/neighbour entry.
Interface	Displays the physical interface that the ARP/neighbour entry resides on.

The following parameters are available in the Active IPv4/IPv6 Routes section:

Parameter	Description
Network	Displays the physical or logical interface the active IPv4/IPv6 route resides on.
Target	Displays the target IPv4 network range of the active IPv4/IPv6 route.
IPv4 Gateway	Displays the IPv4 gateway address used by the active IPv4 route.
Metric	Displays the metric used by the active IPv4/IPv6 route.

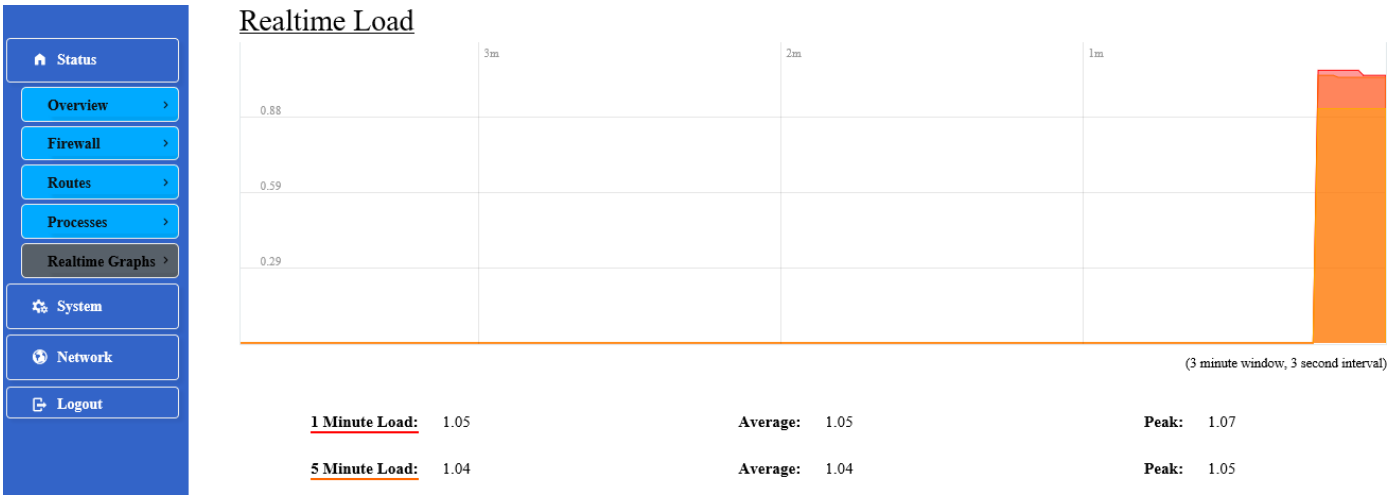
4.3.1.4. Processes



This page is used to display currently running system processes and their status. The following parameters are available in this section:

Parameter	Description
Owner	Display the Owner's name with the process.
Command	Display the Command with the process.
CPU usage	Display the CPU usage (%) with the process.
Memory usage	Display the Memory usage (%) with the process.
Hang Up	Hang up the process.
Terminate	Terminate the process.
Kill	Kill the process.

4.3.1.5. Realtime Graphs

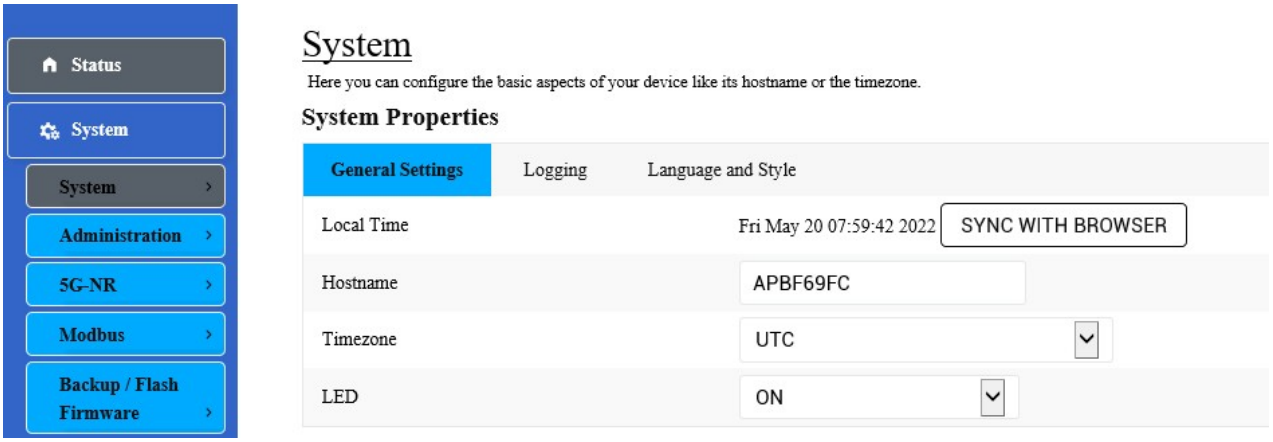


This page is used to display the load graph in real time. The following parameters are available in the Realtime Load section:

Parameter	Description
1/5/15 Minute Load	Displays the 1/5/15-minute load in real time. • Average - Displays the average measurement for the 1/5/15-minute load. • Peak - Displays the peak measurement for the 1-minute load.

4.3.2. System

4.3.2.1. System



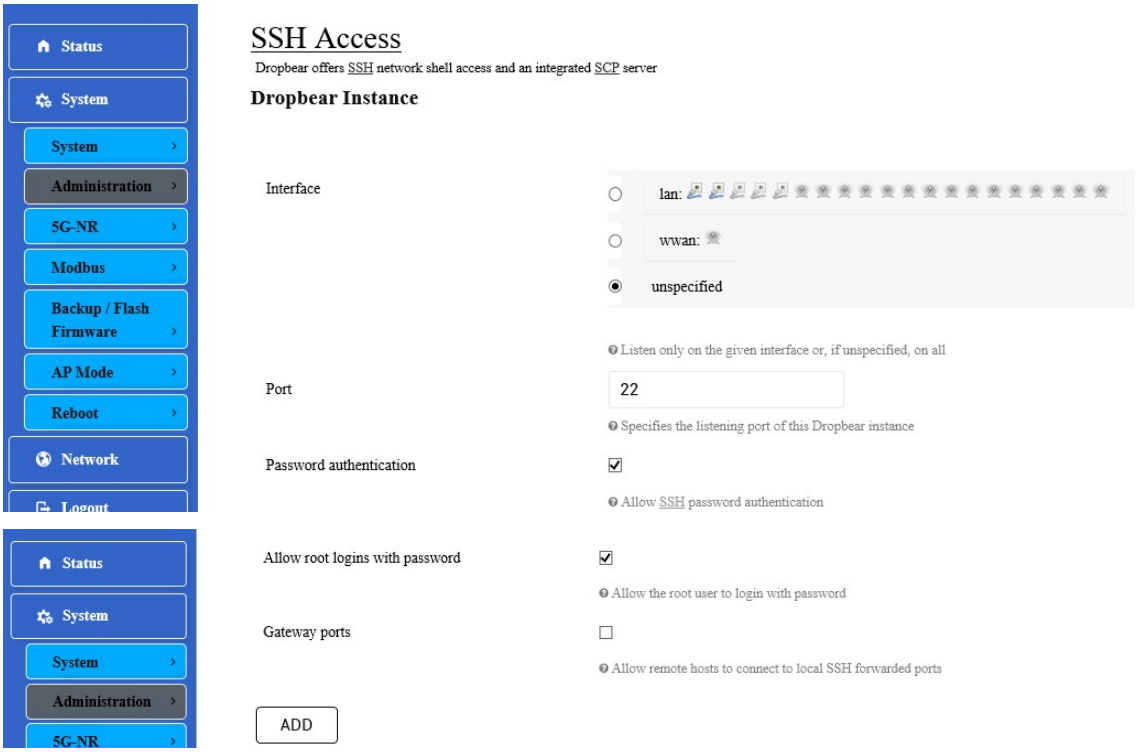
This page is used to display and configure basic system settings like the logging and the language and style settings.

4.3.2.2. Administration

4.3.2.2.1. Router Password

This page is used to change the password for accessing on the AP.

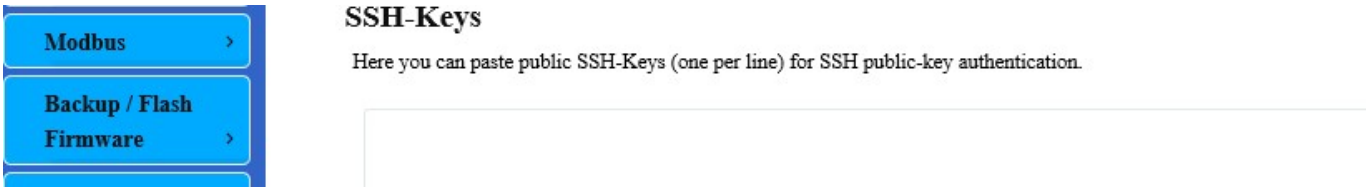
4.3.2.2.2. SSH Access



The following parameters are available in this section:

Parameter	Description
Interface	Select the physical interface that will be associated with this interface configuration here.
Port	Enter the TCP/UDP port number for the SSH connection. The default port number is 22.
Password authentication	Tick the checkbox to allow SSH password authentication.
Allow root logins with password	Tick the checkbox to allow the root user to login with password.
Gateway ports	Tick the checkbox to allow remote hosts to connect to local SSH forwarded ports.

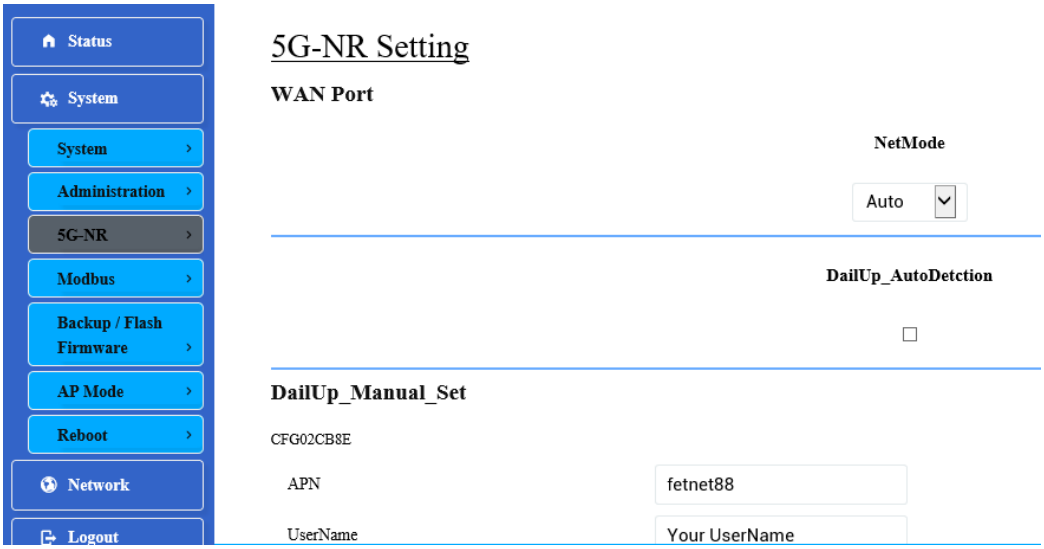
4.3.2.2.3. SSH-Keys

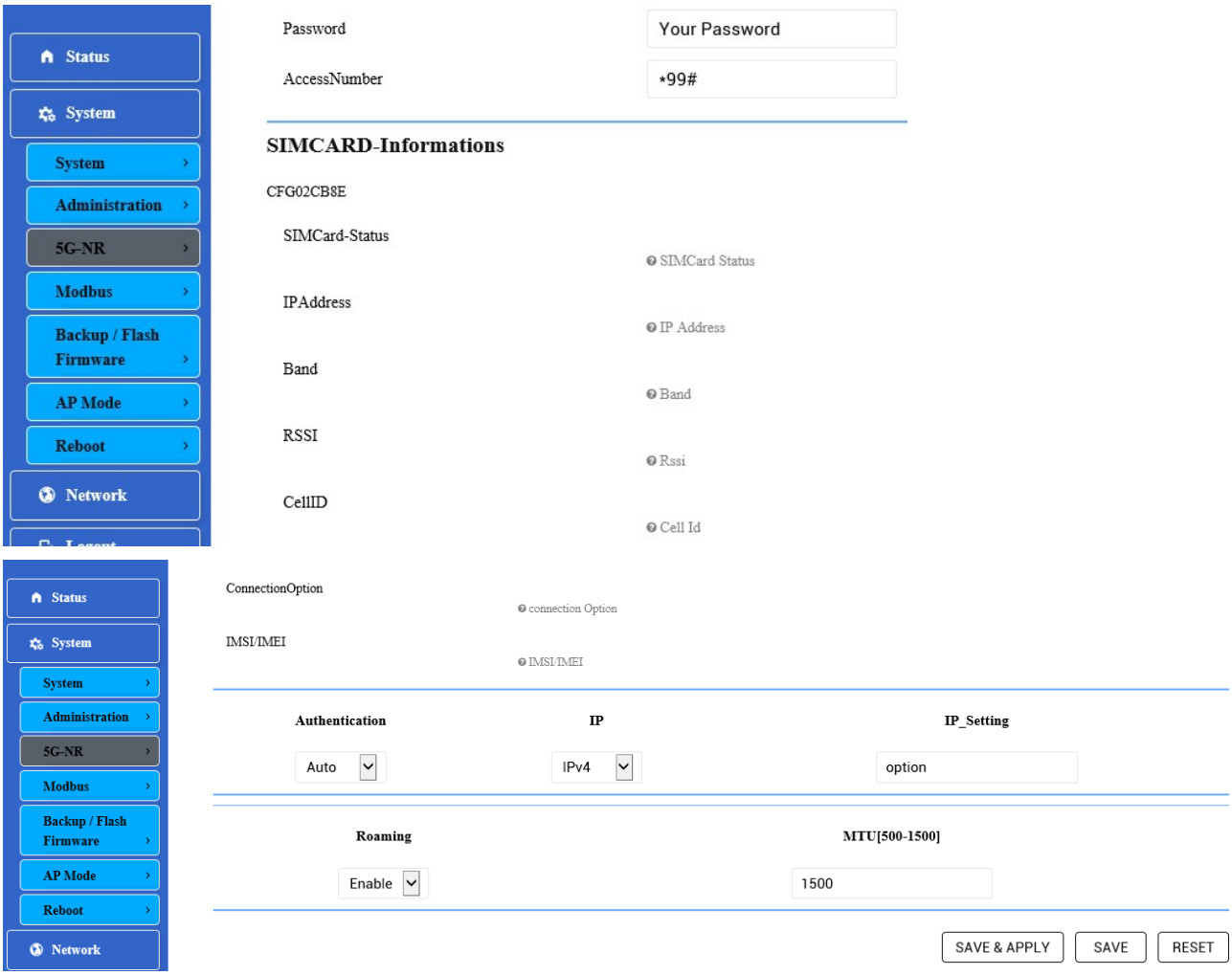


This page is used to SSH-KEYS authentication. Enter the public SSH-Keys for SSH public-key authentication.

4.3.2.3 5G-NR

In this page, you can set the NetMode for WAN Port and enter the APN here.

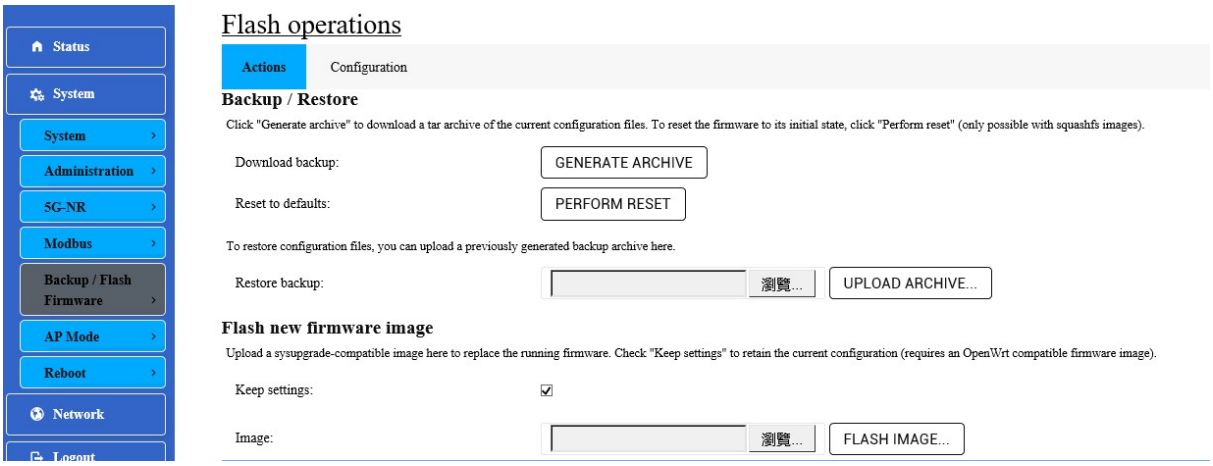




Parameter	Description
NetMode	Select the Net, you can see 4 options: Auto, WCDM, LTE or NR5G.
DailUp_AutoDetction	If you check the button, you can enter the APN here.

4.3.2.5. Backup/Flash Firmware

This page is used to backup/restore the configuration or to update the firmware on the AP. A factory reset of the software configuration can also be performed on this page.



4.3.2.6. AP Mode

This page is used to displayed and changed AP modes.

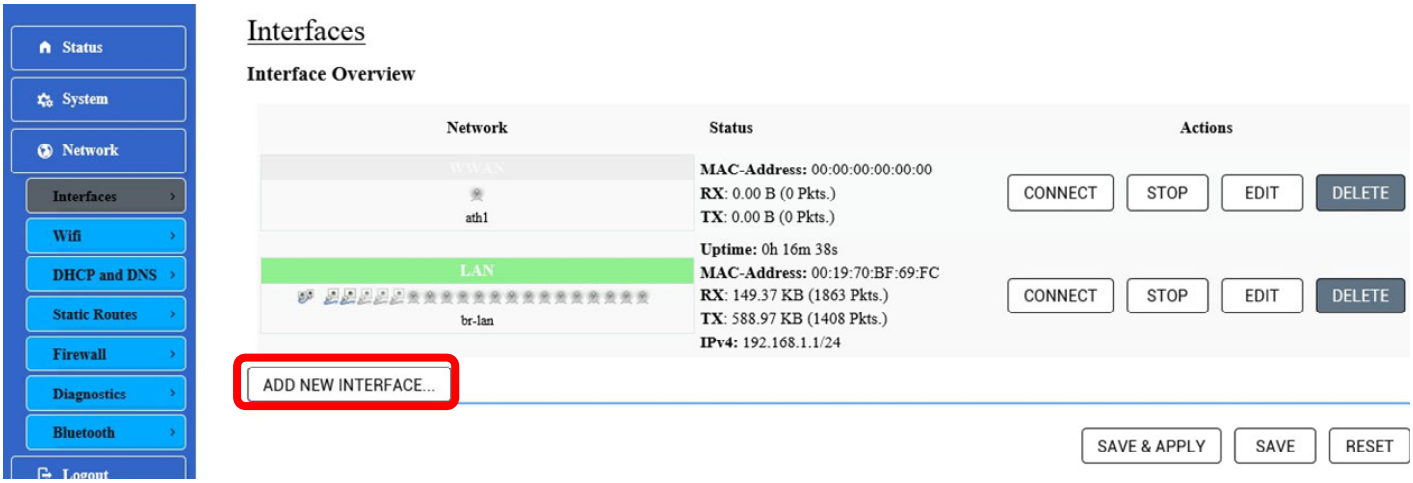
- Thin AP - Specifies to use and configure this AP with a wireless controller in the network. The wireless controller will be responsible for the configuration of this AP. Only a few functions are available to be configured on this AP in this mode.
- Fat AP - Specifies to use and configure this AP without a wireless controller in the network. More functions are available to be configured on this AP in this mode.

4.3.2.7. Reboot

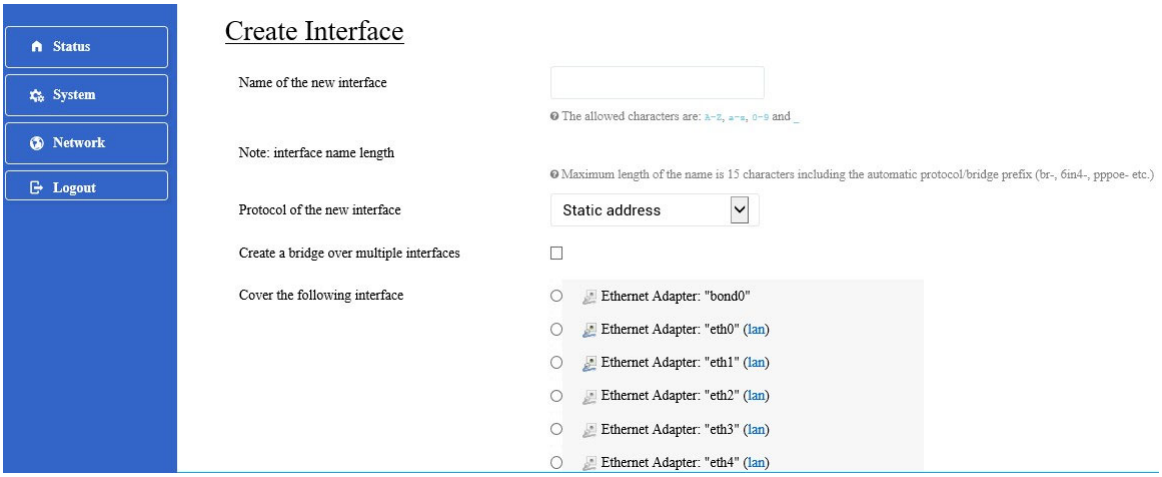
Click the Perform reboot link to reboot the device any unsaved configuration.

4.3.3. Network

4.3.3.1. Interfaces

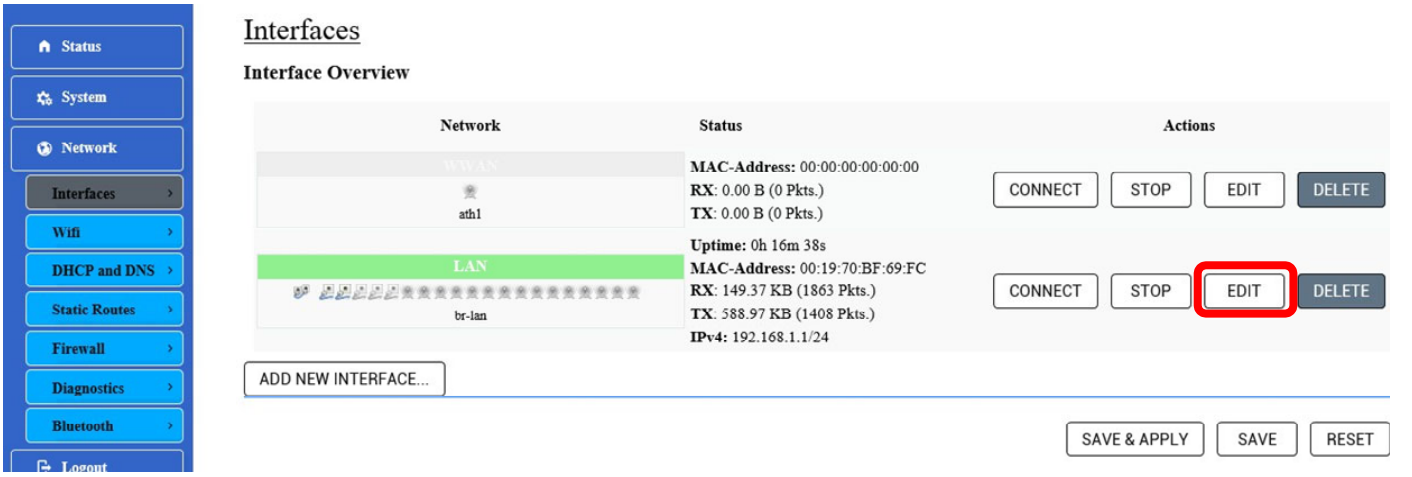


After clicking the Add New Interface button, the following page will appear:



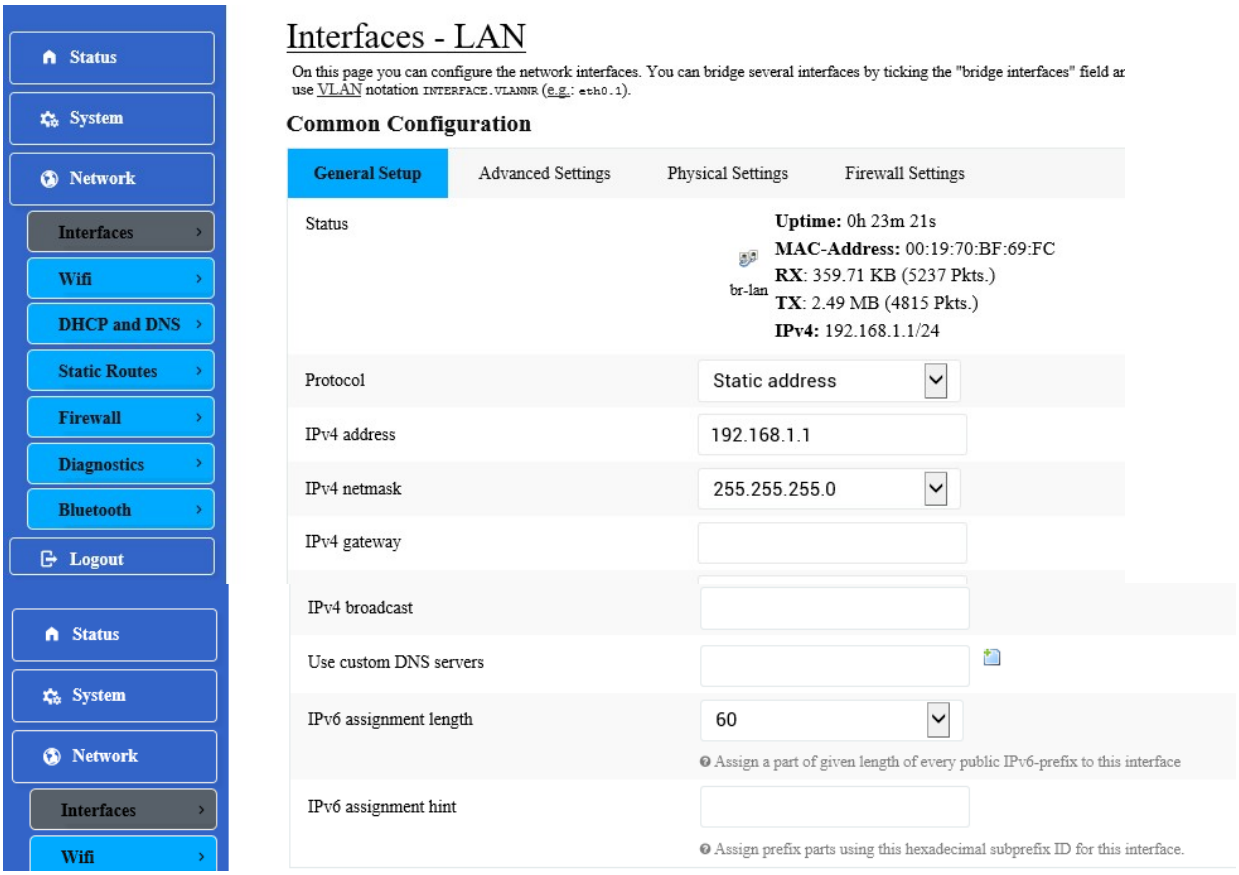
To configure the WAN / LAN interfaces, click the Edit button.

Note: The following web page take LAN interfaces for example, WAN interfaces are similar.



4.3.3.1.1. Static Address

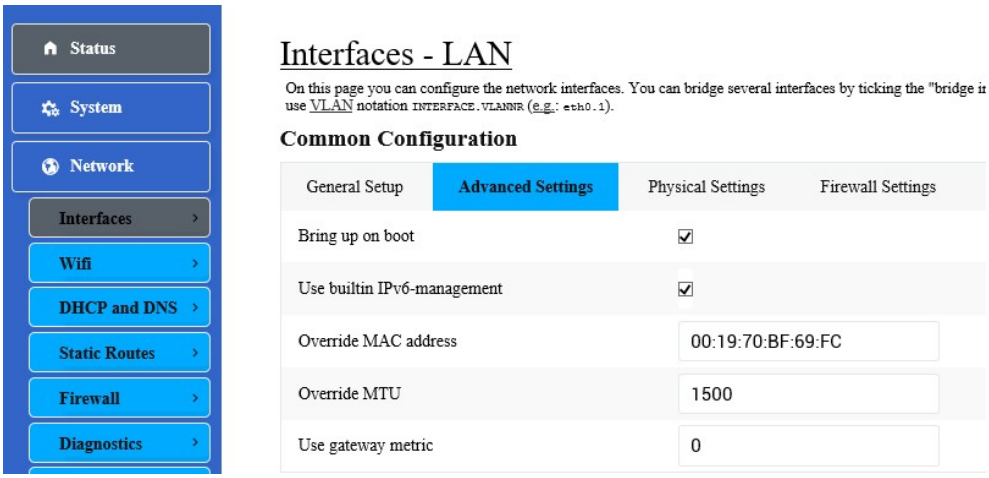
4.3.3.1.1.1. General Setup



The following parameters are available in this section:

Parameter	Description
Status	Displays basic status information of the interface. • Port - Displays the interface name. For example, "eth0.2". • Uptime - Displays the how long the interface is active. • MAC Address - Displays the MAC address of the interface. • RX - Displays the RX (receiving) data rate through the interface. • IPv4-Displays the internet IP. TX - Displays the TX (transmitting) data rate through the interface.
Use Custom DNS Servers	Enter the IPv4 address or domain name of the DNS (Domain Name System) server for the WAN connection here. More than one entry can be created.
IPv6 Assignment Length / Hint	**Note:** This option is only available if Accept router advertisements are enabled.

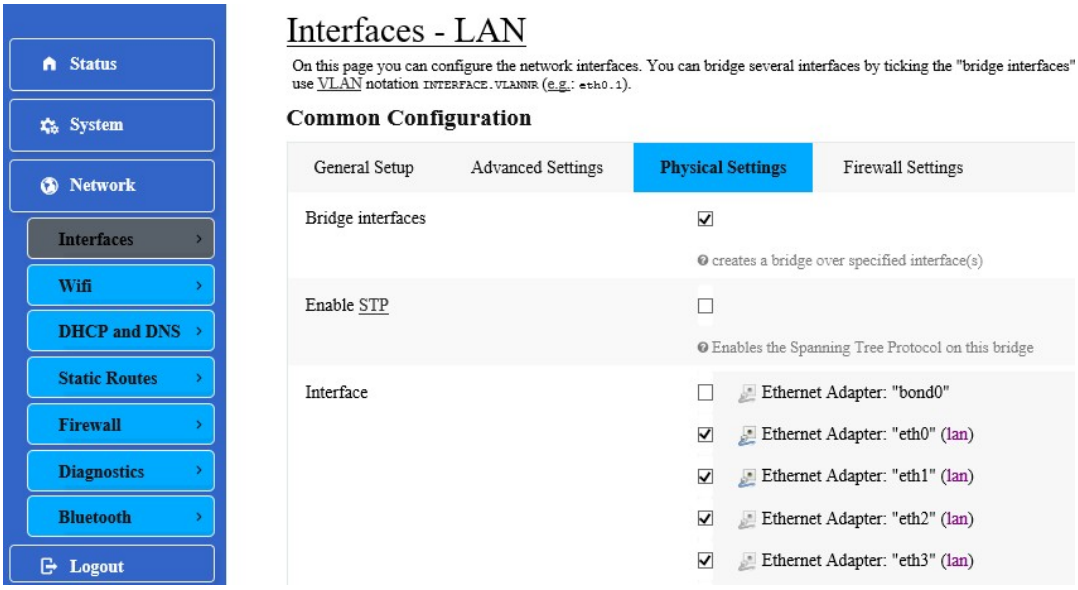
4.3.3.1.1.2. Advanced Settings



The following parameters are available in this section:

Parameter	Description
Bring Up On Boot	Select this option to bring up this interface when the device rebooted.
Use Builtin IPv6-Management	Using the Builtin IPv6-Management.
Override MAC Address	Enter a MAC address here to override the default MAC address for this interface.
Override MTU	Enter the MTU (Maximum Transmission Unit) value here to override the default MTU value used on this interface.
Use Gateway Metric	Enter the metric for the gateway here.

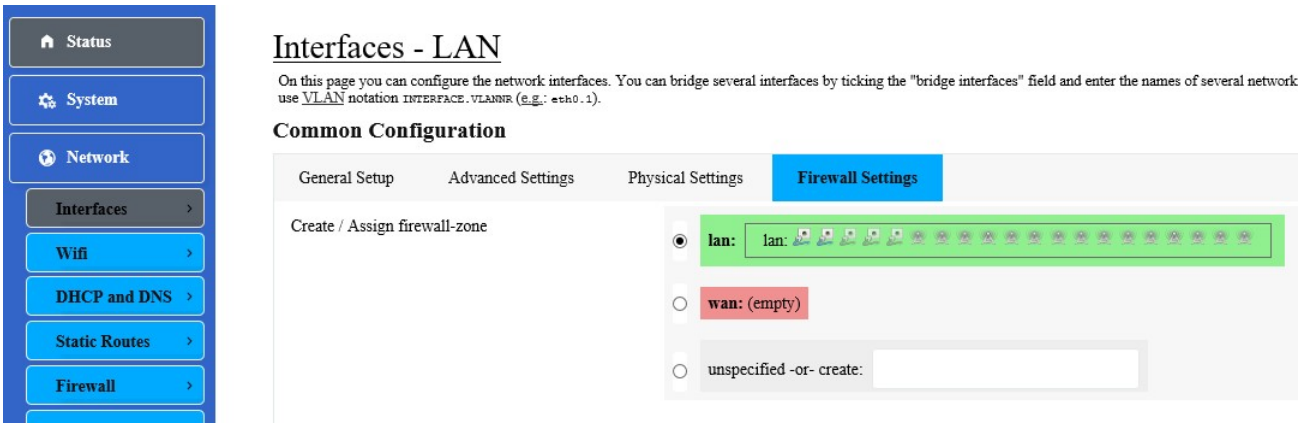
4.3.3.1.1.3. Physical Settings



The following parameters are available in this section:

Parameter	Description
Bridge Interfaces	Select this option to bridge this interface with another interface.
Enable STP	**Note:** This option is only available if Bridge interfaces are enabled.
Interface	If desired, select and enter a Custom Interface name in the textbox provided. **Note:** Multiple selections are only available when the Bridge interfaces option is selected. Normally, only one interface can be selected here.

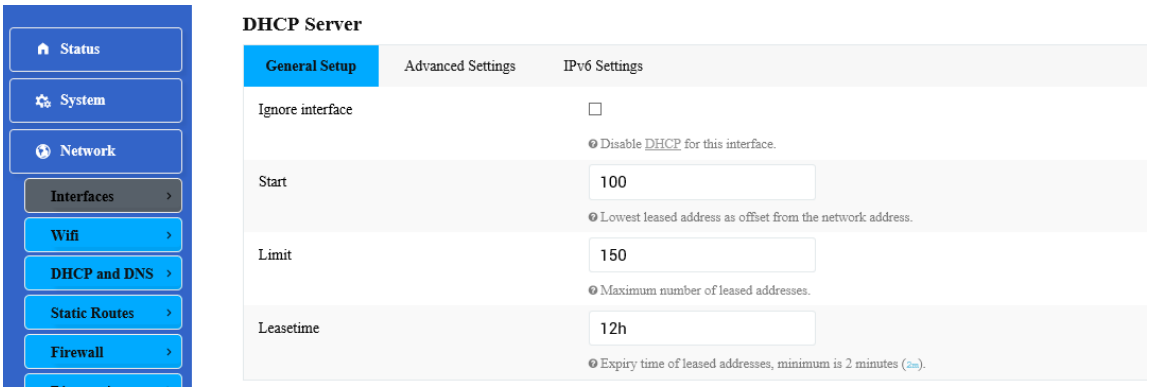
4.3.3.1.1.4. Firewall Settings



The following parameters are available in this section:

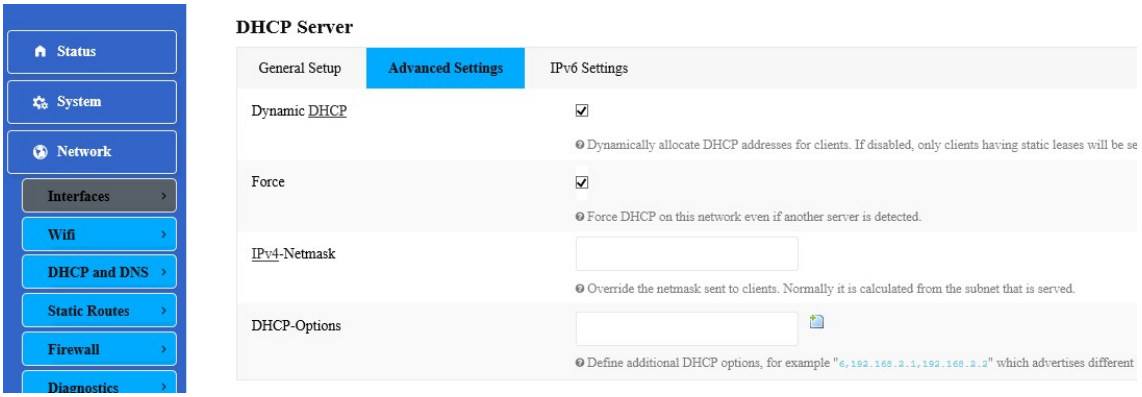
Parameter	Description
Create / Assign Firewall-Zone	Select the firewall zone that is assigned to this interface. Select unspecified to remove the interface from a firewall zone. To create a new firewall zone, enter the name of the new firewall zone in the space provided.

4.3.3.1.1.5. DHCP Server



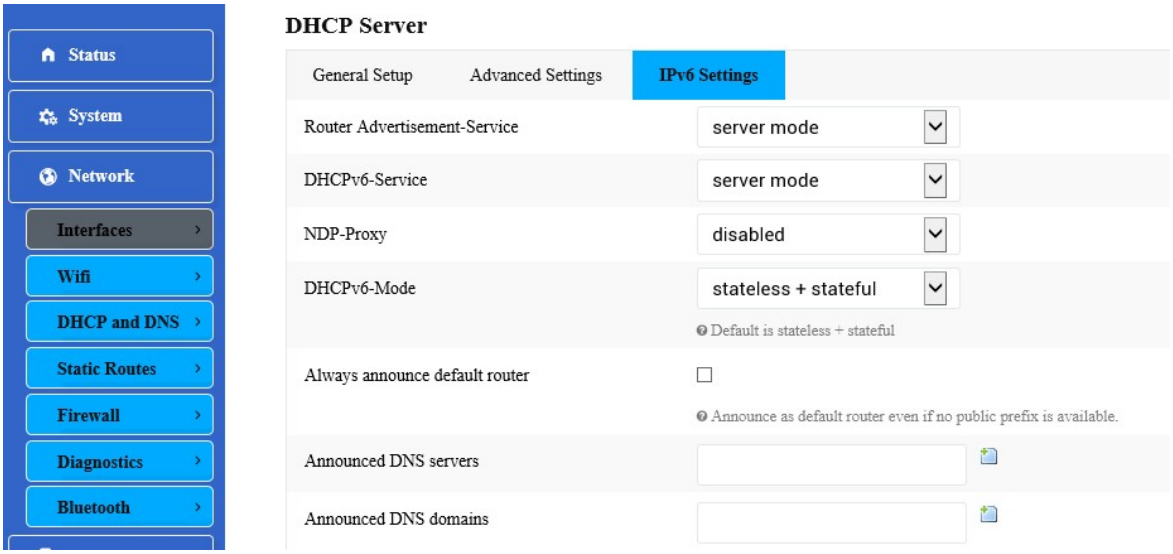
The following parameters are available in this section:

Parameter	Description
Ignore Interface	Enable / Disable the DHCP Server for this Interface.
Start	Enter the lowest leased address as offset from the network address.
Limit	Enter the maximum number of leased addresses.
Leasetime	Enter the expiry time of leased addresses.



The following parameters are available in this section:

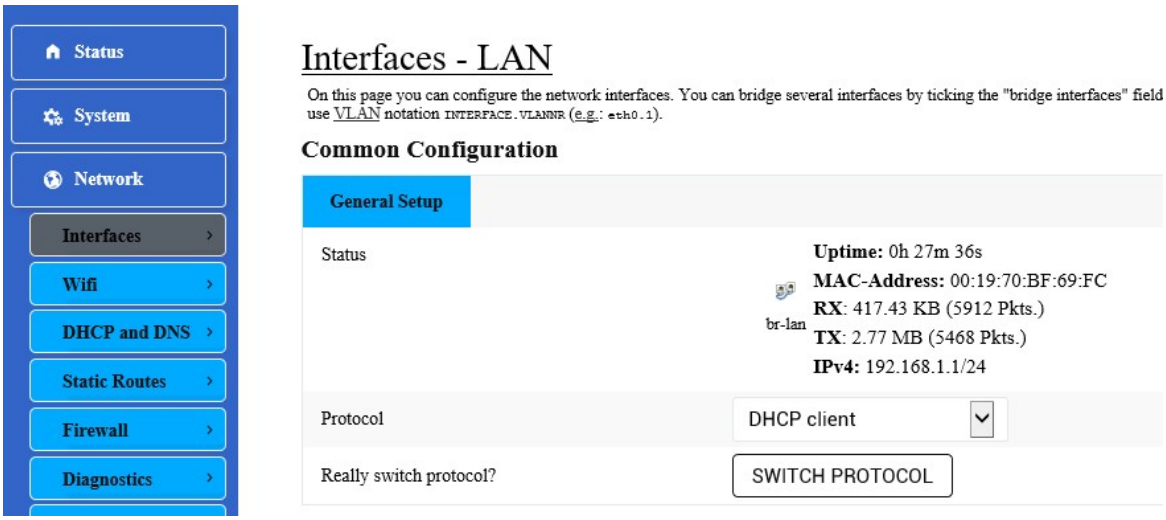
Parameter	Description
Dynamic DHCP	Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served
Force	Force DHCP on this network even if another server is detected.
IPv4-Network	Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
DHCP-Options	Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.



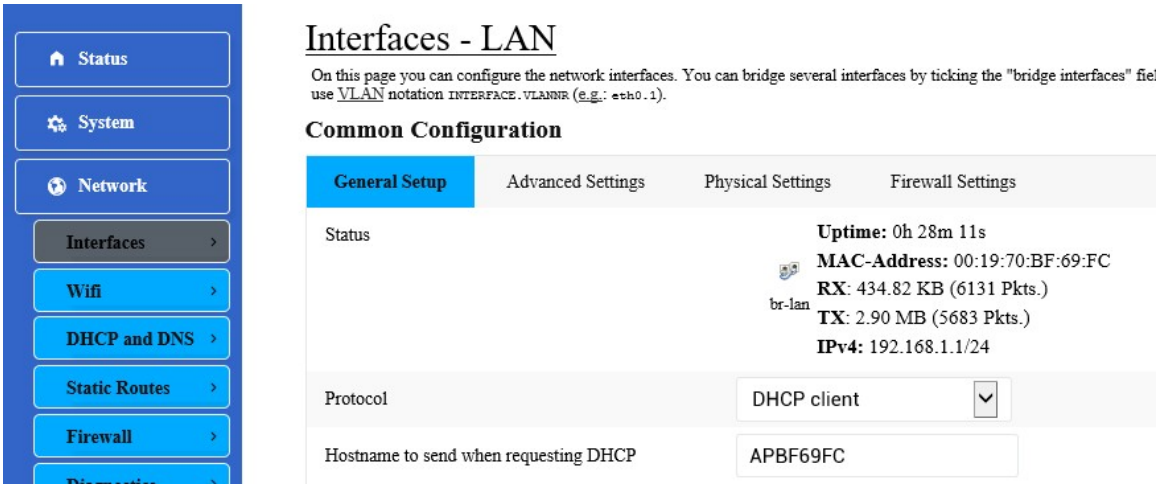
The following parameters are available in this section:

Parameter	Description
Router Advertisement-Service	Select the Router Advertisement-Service (Disable / Server / Relay / Hybrid Mode).
DHCPv6-Service	Select the DHCPv6 -Service (Disable / Server / Relay / Hybrid Mode).
NDP-Proxy	Select the NDP-Proxy (Disable Relay / Hybrid Mode).
DHCPv6-Mode	Select the DHCPv6 -Service (Stateless / Stateless + Stateful / Stateful Only).
Always announce default router	Announce as default router even if no public prefix is available.
Announced DNS servers	Enter the announced DNS servers IP.
Announced DNS domains	Enter the announced DNS domain.

4.3.3.1.2. DHCP Client

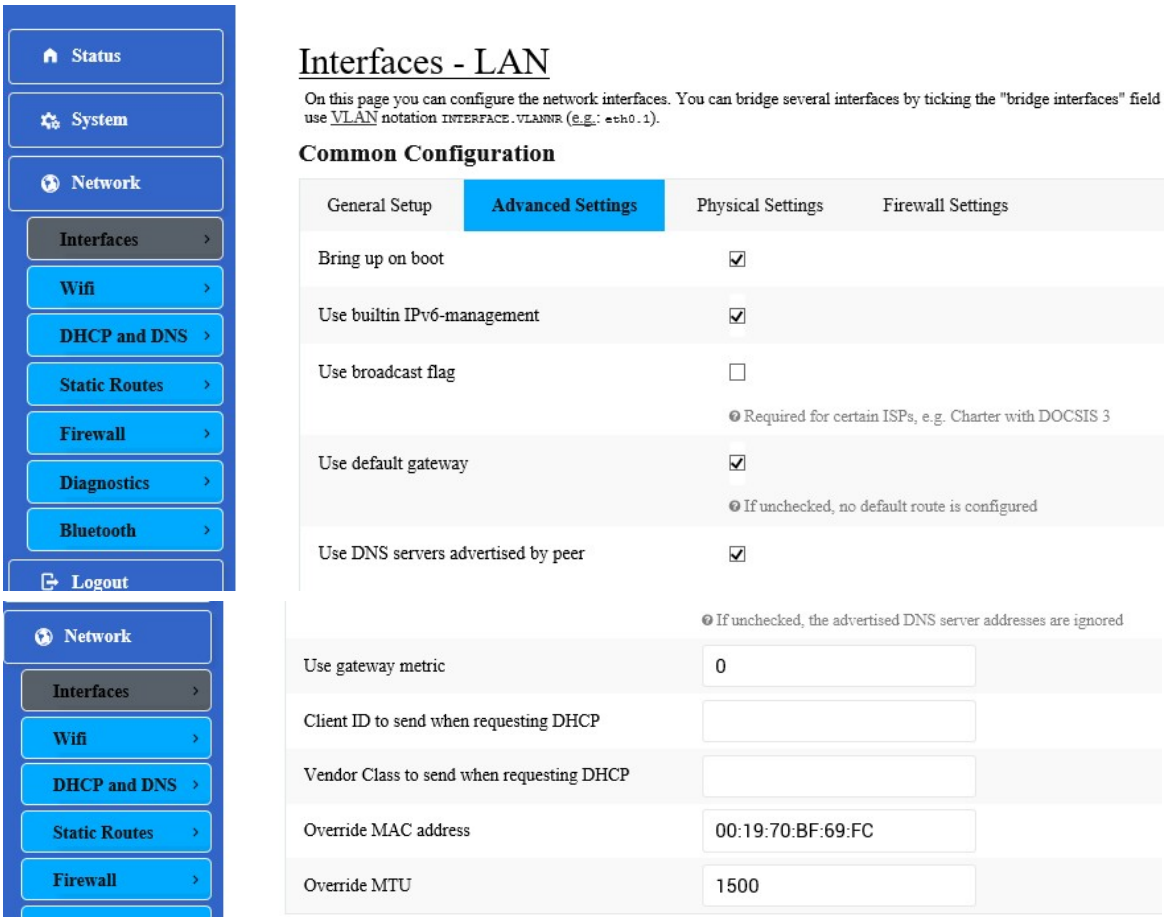


After clicking the Switch protocol button, the following will appear:



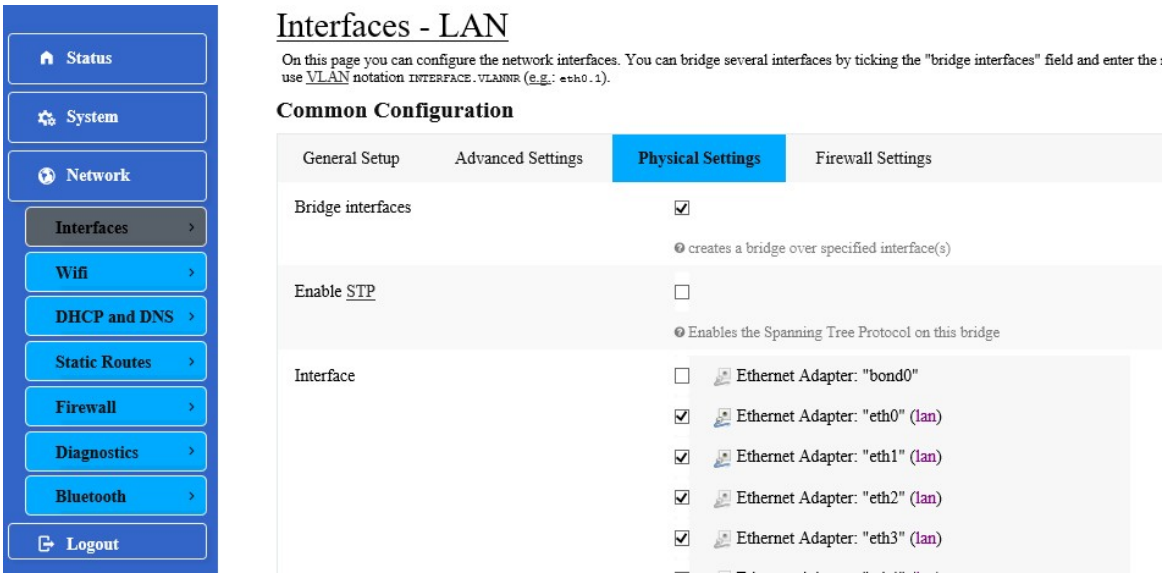
The following parameters are available in this section:

Parameter	Description
Status	Displays basic status information of the interface. • Port - Displays the interface name. For example, "eth0.2". • Uptime - Displays the how long the interface is active. • MAC Address - Displays the MAC address of the interface. • RX - Displays the RX (receiving) data rate through the interface. • IPv4-Displays the internet IP. TX - Displays the TX (transmitting) data rate through the interface.
Hostname to Send When Requesting DHCP	Enter the hostname that is sent when requesting DHCP here.



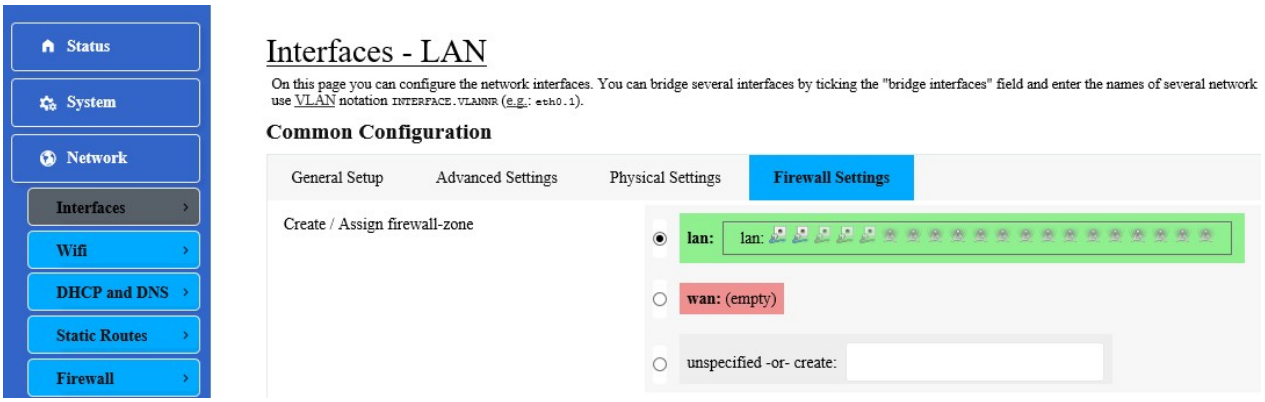
The following parameters are available in this section:

Parameter	Description
Bring up on Boot	Select this option to bring up this interface when the device rebooted.
Use Builtin IPv6-Management	Using the Builtin IPv6-Management.
Use Broadcast Flag	Select this option to use the broadcast flag on this interface.
Use Default Gateway	Select this option to use the DHCP assigned default gateway on this interface.
Use DNS Servers Advertised by Peer	Select this option to use the DHCP assigned DNS server addresses on this interface.
Use Gateway Metric	Enter the metric for the gateway here.
Client ID / Vendor Class to Send When Requesting DHCP	Enter the ID/vendor class of the DHCP client that is sent when the DHCP service is requested here.
Override MAC Address / MTU	Enter a MAC address/ MTU value here to override the default MAC address/MTU value for this interface.



The following parameters are available in this section:

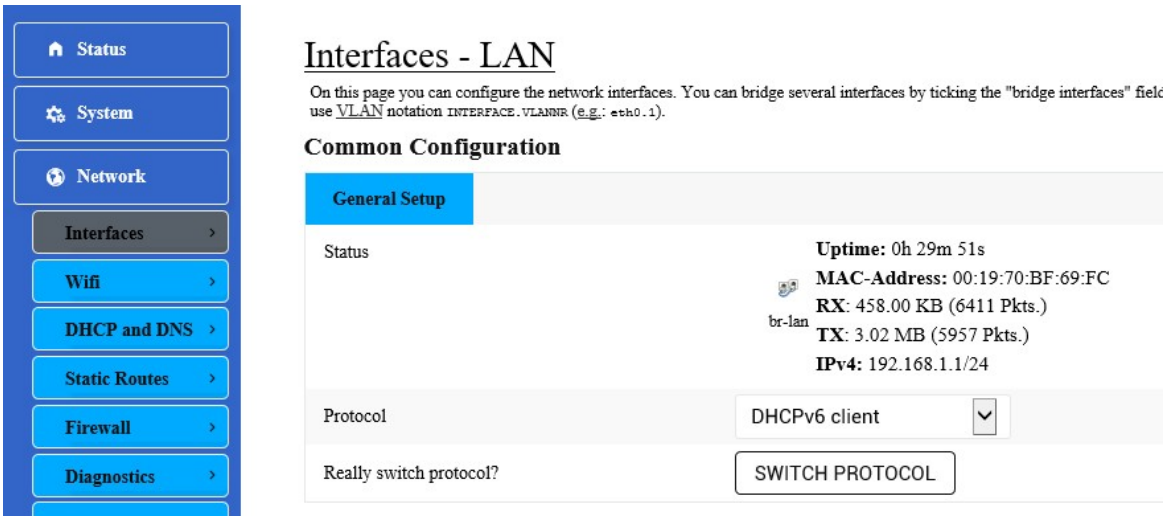
Parameter	Description
Bridge interfaces	Select this option to bridge this interface with another interface.
Enable STP	Select this option to enable the STP function on this interface. **Note:** This option is only available if Bridge mode is enabled.
Interface	Select the physical interface that will be associated with this interface configuration here. If desired, select and enter a Custom Interface name in the textbox provided. **Note:** Multiple selections are only available when the Bridge interfaces option is selected. Normally, only one interface can be selected here.



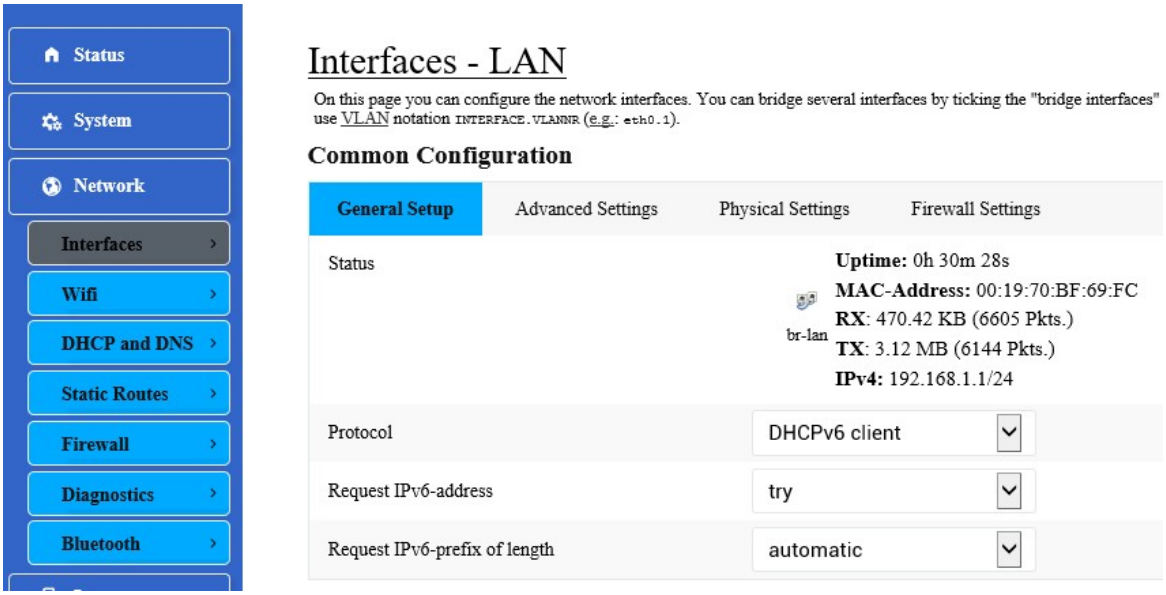
The following parameters are available in this section:

Parameter	Description
Create / Assign Firewall-Zone	Select the firewall zone that is assigned to this interface. Select unspecified to remove the interface from a firewall zone. To create a new firewall zone, enter the name of the new firewall zone in the space provided.

4.3.3.1.3. DHCPv6 Client

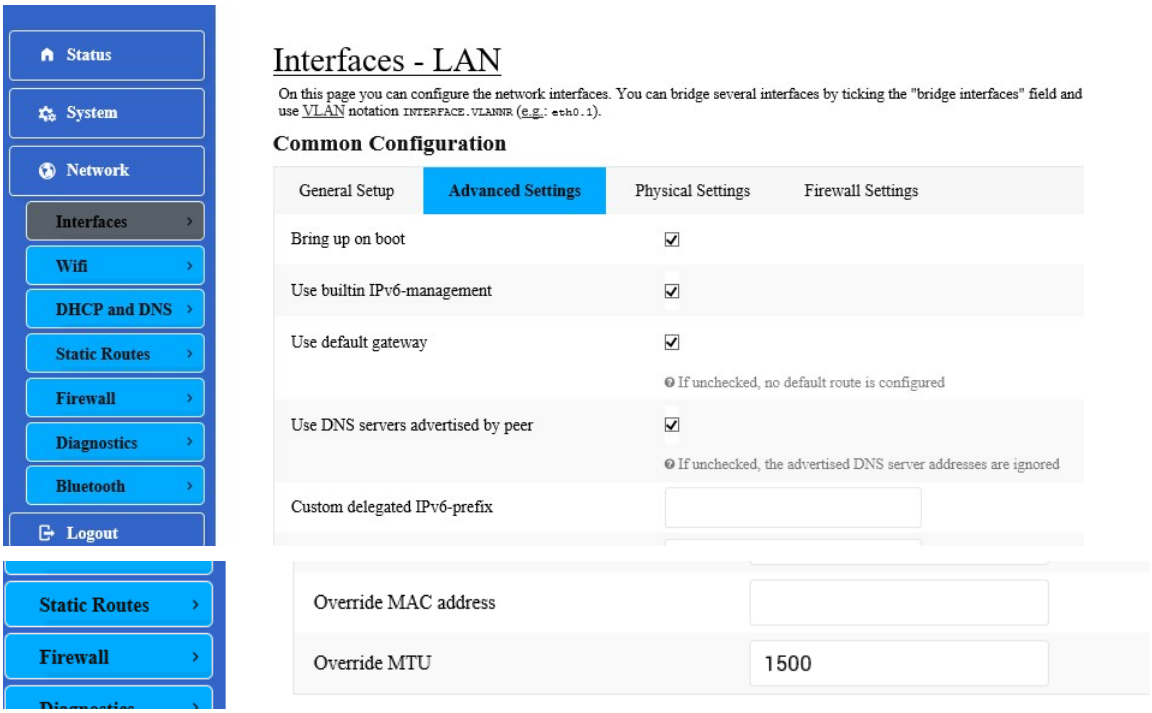


After clicking the Switch protocol button, the following will appear:



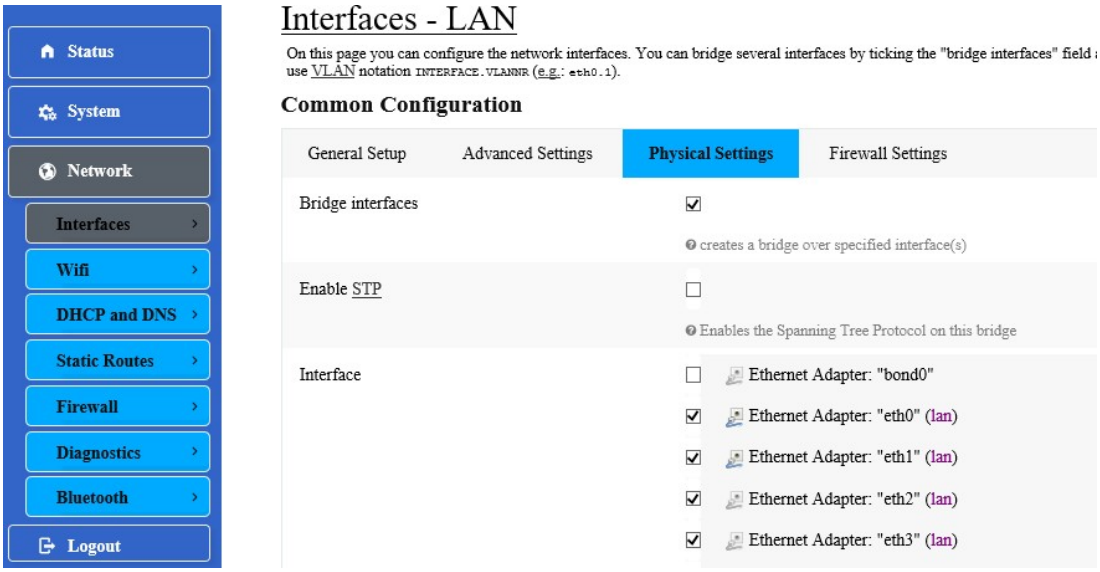
The following parameters are available in this section:

Parameter	Description
Request IPv6-Address	Select the request IPv6-address (Try / Force / Disable).
Request IPv6-Prefix of Length	Select the IPv6-Prefix of Length.



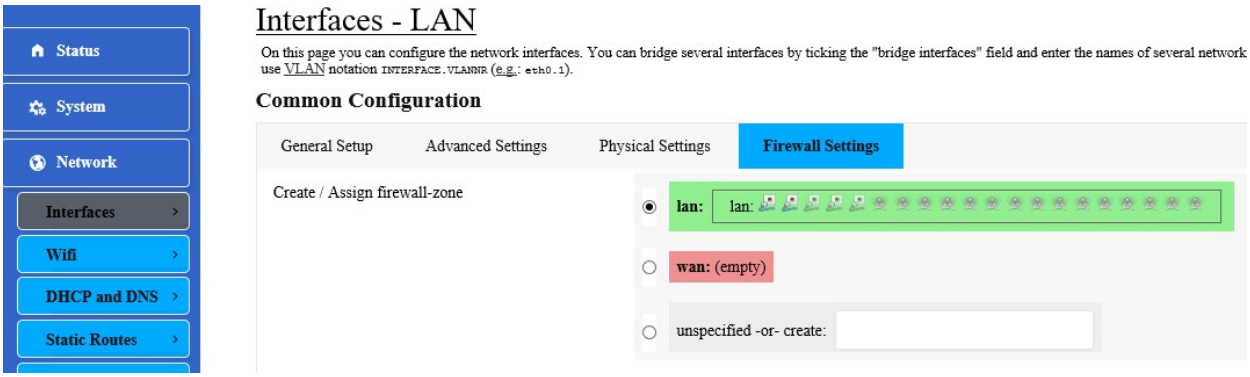
The following parameters are available in this section:

Parameter	Description
Bring up on Boot	Select this option to bring up this interface when the device rebooted.
Use Builtin IPv6-Management	Using the Builtin IPv6-Management.
Use Broadcast Flag	Select this option to use the broadcast flag on this interface.
Use Default Gateway	Select this option to use the DHCP assigned default gateway on this interface.
Use DNS Servers Advertised by Peer	Select this option to use the DHCP assigned DNS server addresses on this interface.
Custom Delegated IPv6-Prefix	Using the Custom Delegated IPv6-Prefix.
Client ID / Vendor Class to Send When Requesting DHCP	Enter the ID/vendor class of the DHCP client that is sent when the DHCP service is requested here.
Override MAC Address / MTU	Enter a MAC address/ MTU value here to override the default MAC address/MTU value for this interface.



The following parameters are available in this section:

Parameter	Description
Bridge interfaces	Select this option to bridge this interface with another interface.
Enable STP	Select this option to enable the STP function on this interface. **Note:** This option is only available if Bridge mode is enabled.
Interface	Select the physical interface that will be associated with this interface configuration here. If desired, select and enter a Custom Interface name in the textbox provided. **Note:** Multiple selections are only available when the Bridge interfaces option is selected. Normally, only one interface can be selected here.



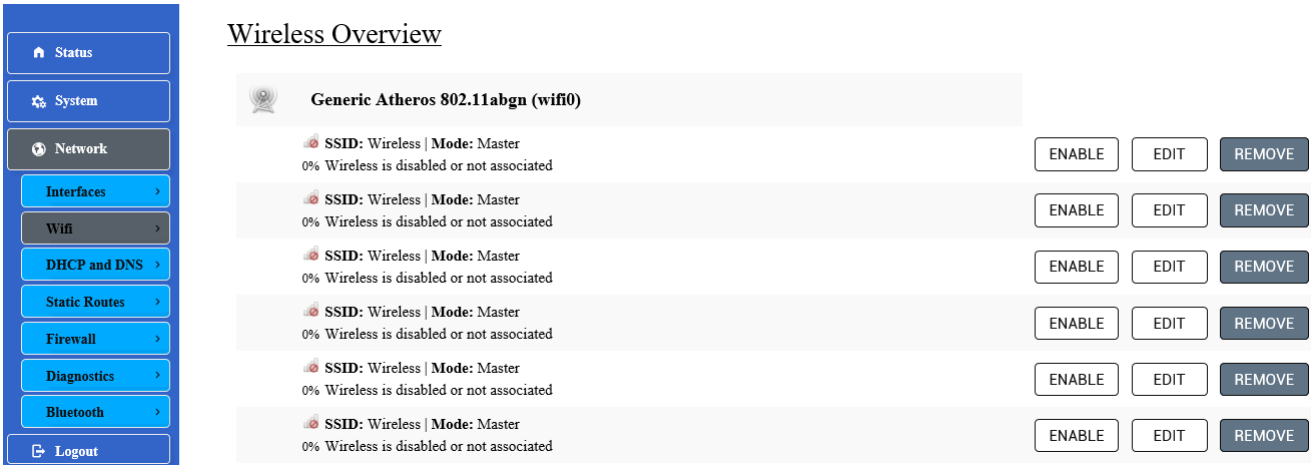
The following parameters are available in this section:

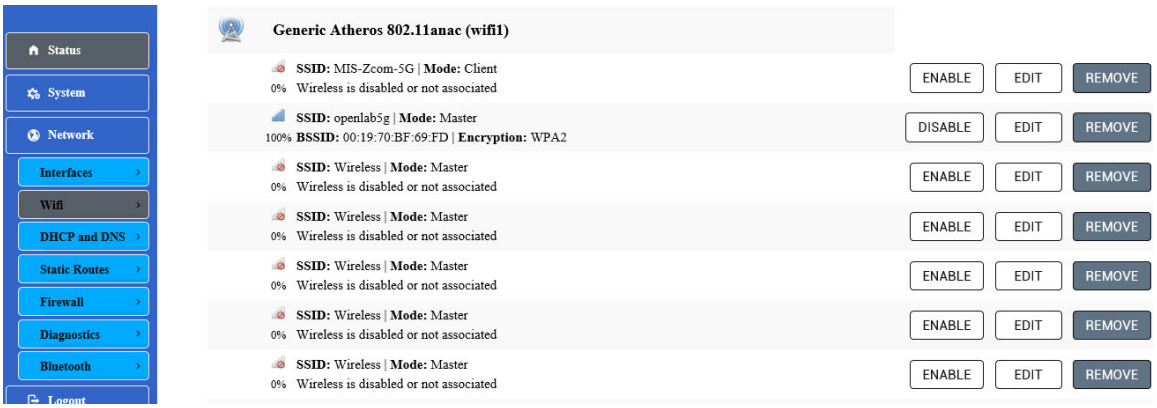
Parameter	Description
Create / Assign Firewall-Zone	Select the firewall zone that is assigned to this interface. Select unspecified to remove the interface from a firewall zone. To create a new firewall zone, enter the name of the new firewall zone in the space provided.

4.3.3.2. Wifi

4.3.3.2.1. Wireless Overview

This page is used to display and configure the 802.11 wireless settings.



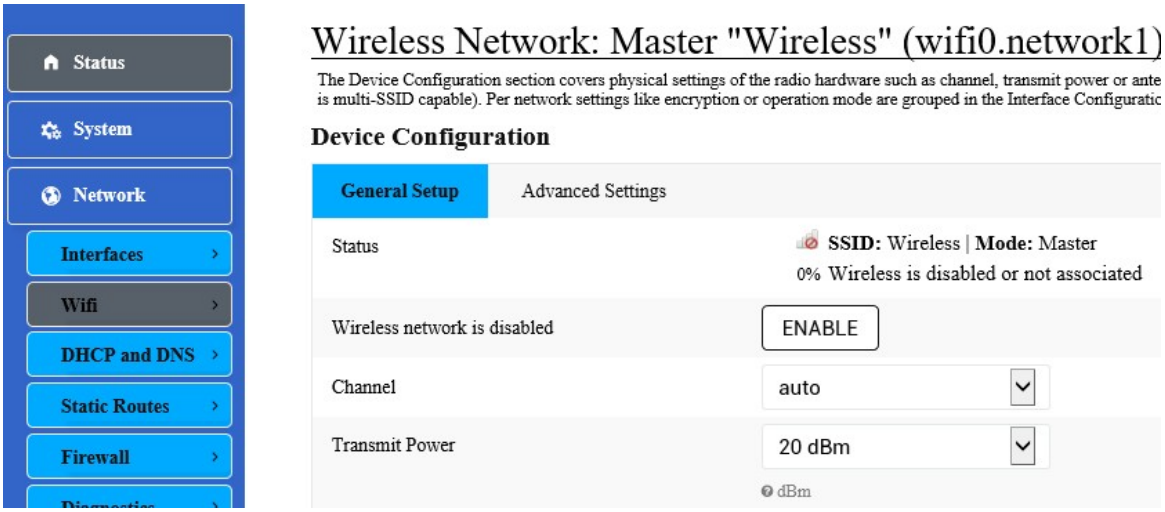


The following parameters are available in this section:

Parameter	Description
Generic Atheros 802.11abgn (wifi0)	Displays information about the generic Atheros IEEE 802.11abgn (wifi0) interface. • Channel - Displays the wireless channel number and frequency. • Bitrate - Displays the current data rate (in megabits per second) through the wireless interface. • SSID - Displays the SSID hosted by the wireless interface. • Mode - Displays the configuration mode of the wireless interface. • BSSID - Displays the BSSID (Basic Service Set Identifier) hosted by the wireless interface. • Encryption - Displays the wireless encryption used on the wireless interface.
Generic Atheros 802.11anac(wifi1)	Displays information about the generic Atheros IEEE 802.11anac (wifi1) interface. • Channel - Displays the wireless channel number and frequency. • Bitrate - Displays the current data rate (in megabits per second) through the wireless interface. • SSID - Displays the SSID hosted by the wireless interface. • Mode - Displays the configuration mode of the wireless interface. • BSSID - Displays the BSSID hosted by the wireless interface. • Encryption - Displays the wireless encryption used on the wireless interface.

4.3.3.2.1.1. Generic Atheros 802.11abgn (wifi0)

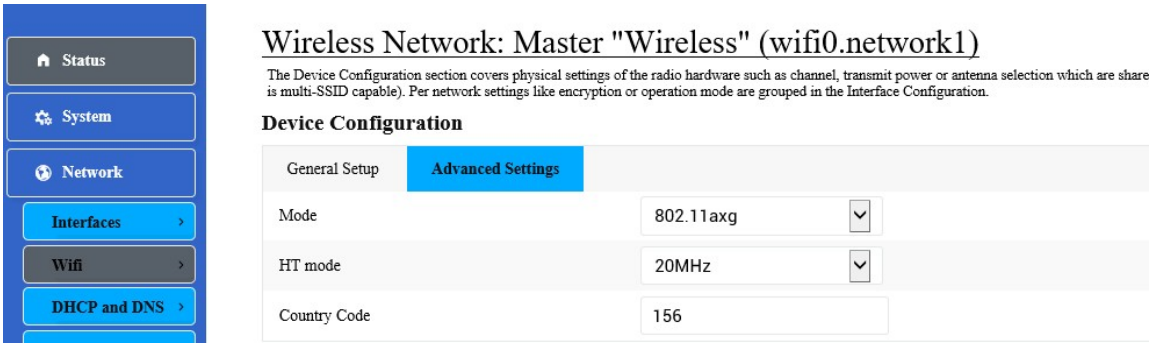
After clicking the Edit button in the Generic Atheros 802.11bgn (wifi0) entry, the following will appear:



The following parameters are available in this section:

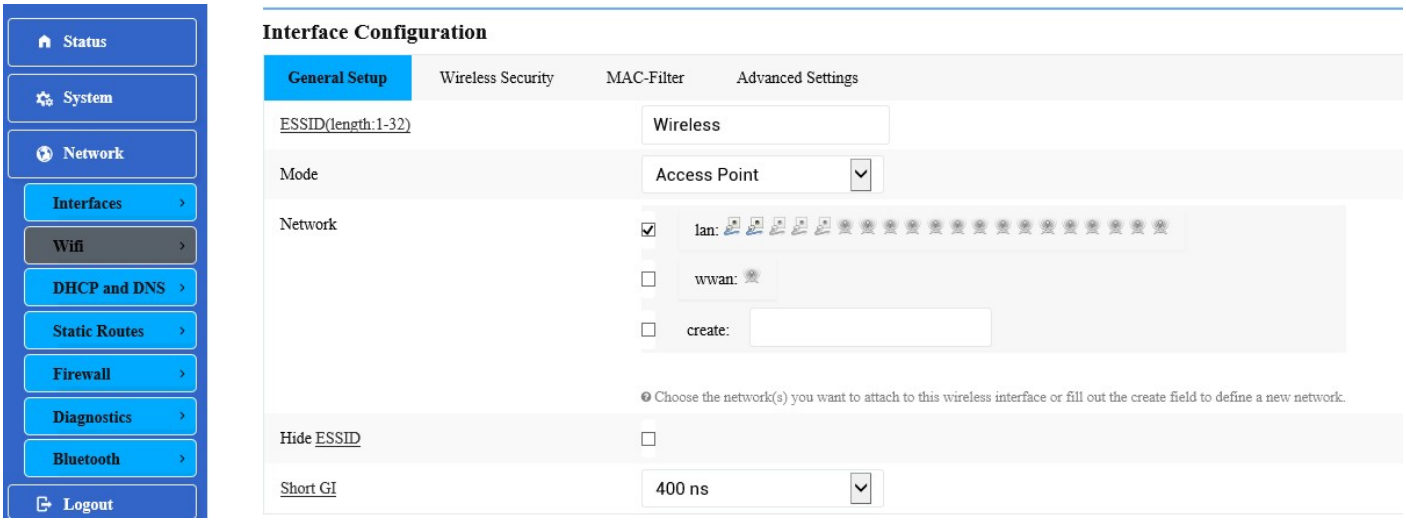
Parameter	Description
Status	Displays a summary of the wireless configuration on this wireless interface. • Signal Strength - Displays the wireless signal strength. • Mode - Displays the wireless operating mode of the wireless interface.

Parameter	Description
	• SSID - Displays the SSID hosted by the wireless interface. • BSSID - Displays the BSSID hosted by the wireless interface. • Encryption - Displays the wireless encryption used on the wireless interface. • Channel - Displays the wireless channel number and frequency. • TX-Power - Displays the TX (transmit) power of the wireless interface. • Signal - Displays the wireless signal strength (in dBm) on the wireless interface. • Noise - Displays the wireless noise level (in dBm) on the wireless interface. • Bitrate - Displays the active data bitrate (in megabits per second) through the wireless interface. • Country - Display the country setting on the wireless interface.
Wireless Network is Enabled	Displays the current status of the wireless interface.
Channel	Select the wireless channel for the wireless interface here. The range is from 1 (2.412 GHz) to 11 (2.462 GHz). Select the auto option to allow the AP to automatically determine the best wireless channel for this interface. Select the custom option to manually entry the channel number.
Transmit Power	Select the wireless transmit power for the interface here.



The following parameters are available in this section:

Parameter	Description
Mode	Select the wireless mode on this interface here. Options to choose from are 802.11g, 802.11gn, and 802.11axg.
HT Mode	Select the HT mode here. Options to choose from are 20MHz and 40MHz.
Country Code	Enter the country code here.

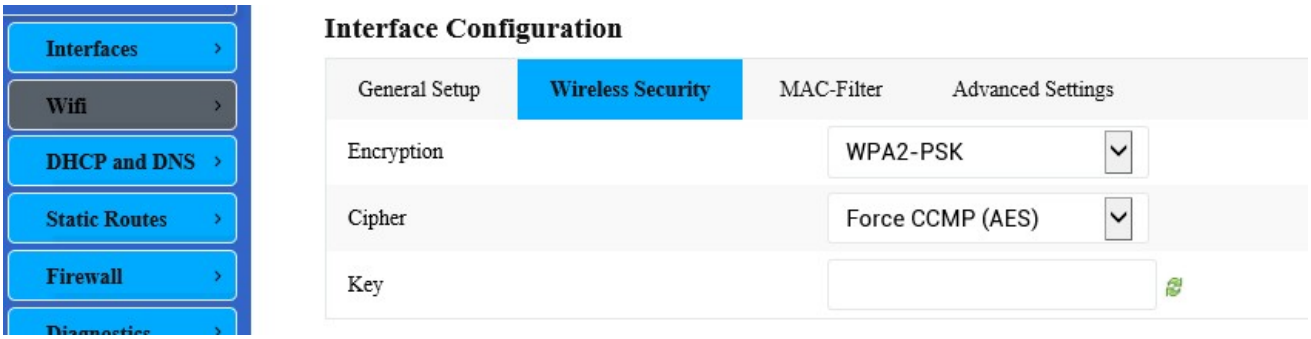


The following parameters are available in this section:

Parameter	Description
ESSID	Enter the ESSID (Extended SSID) here.
Mode	Select the wireless mode for the interface here. Options to choose from are Access Point.
Network	Select the network interface to attach to this wireless interface here. Select the *create* option to enter and create and new network interface.
Hide ESSID	Select this option to hide the ESSID from wireless clients. Wireless clients will not be able to detect this interface by simply scanning for available wireless networks.
Short GI	Select the short GI to decrease the time between data characters being sent.

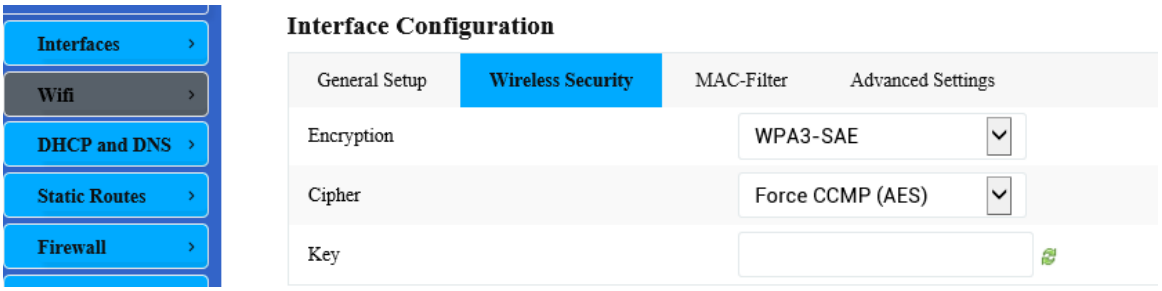
The following parameters are available in this section:

Parameter	Description
Encryption	Select the wireless encryption for this interface here. Options to choose from are No Encryption, WPA2-PSK, WPA3-SAE and WPA2-EAP. WPA2 stands for Wi-Fi Protected Access II. WPA2 stands for Wi-Fi Protected Access III. PSK stands for Pre-Shared Key. SAE stands for Simultaneous Authentication of Equals. EAP stands for Extensible Authentication Protocol.



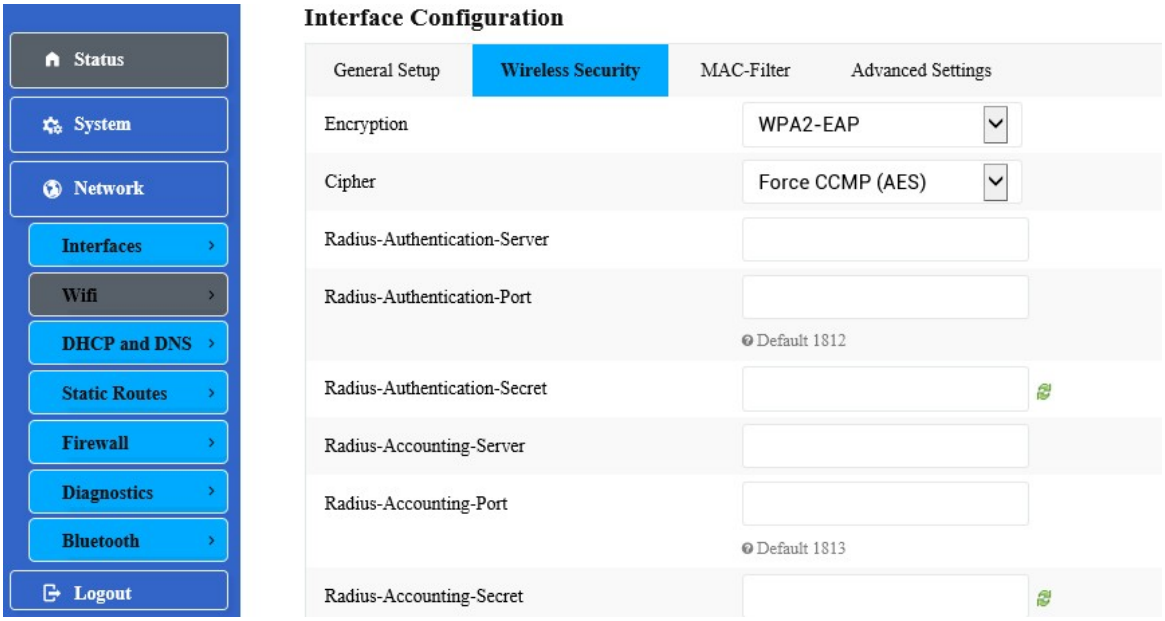
The following parameters are available in this section:

Parameter	Description
Encryption	After selecting the WPA2-PSK option, the following settings are available.
Cipher	Select the cipher method here. Options to choose from are Force CCMP (AES). CCMP stands for CCM Mode Protocol. CCM stands for Counter with CBC-MAC. CBC-MAC stands for Cipher Block Chaining Message Authentication Code. AES stands for Advanced Encryption Standard.
Key	Enter the WPA2 passphrase here.



The following parameters are available in this section:

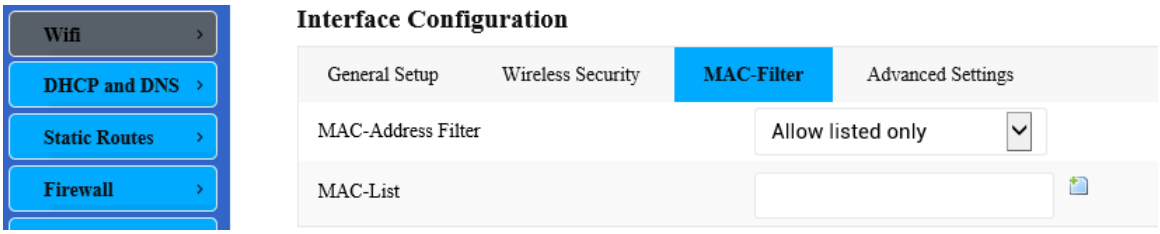
Parameter	Description
Encryption	After selecting the WPA3-SAE option, the following settings are available.
Cipher	Select the cipher method here. Options to choose from are Force CCMP (AES).
Key	Enter the WPA3 passphrase here.



Parameter	Description
Encryption	After selecting the WPA2-EAP option, the following settings are available.
Cipher	Select the cipher method here. Options to choose from are Force CCMP (AES).
RADIUS-Authentication-Server	Enter the RADIUS authentication server IP.
RADIUS-Authentication-Port	Enter the RADIUS authentication port number (Default 1812).
RADIUS-Authentication-Secret	Enter the RADIUS authentication password.
RADIUS-Accounting-Server	Enter the RADIUS accounting server IP.
RADIUS-Accounting-Port	Enter the RADIUS accounting server port number (Default 1813).
RADIUS-Accounting-Secret	Enter the RADIUS accounting server password.

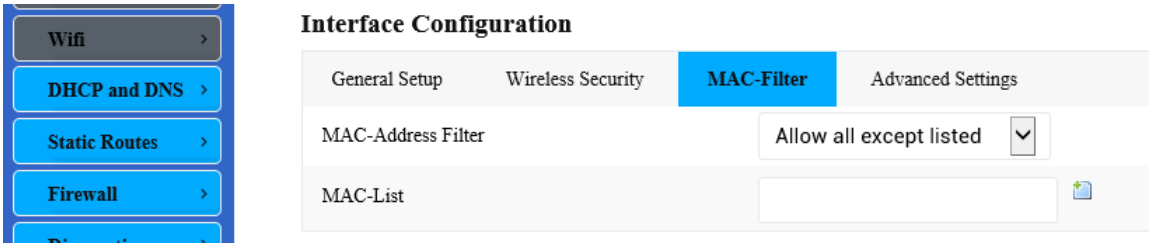
The following parameters are available in this section:

Parameter	Description
MAC Address Filter	Select to enable or disable MAC address filtering here. Options to choose from are disable, allow listed only, and allow all except listed.



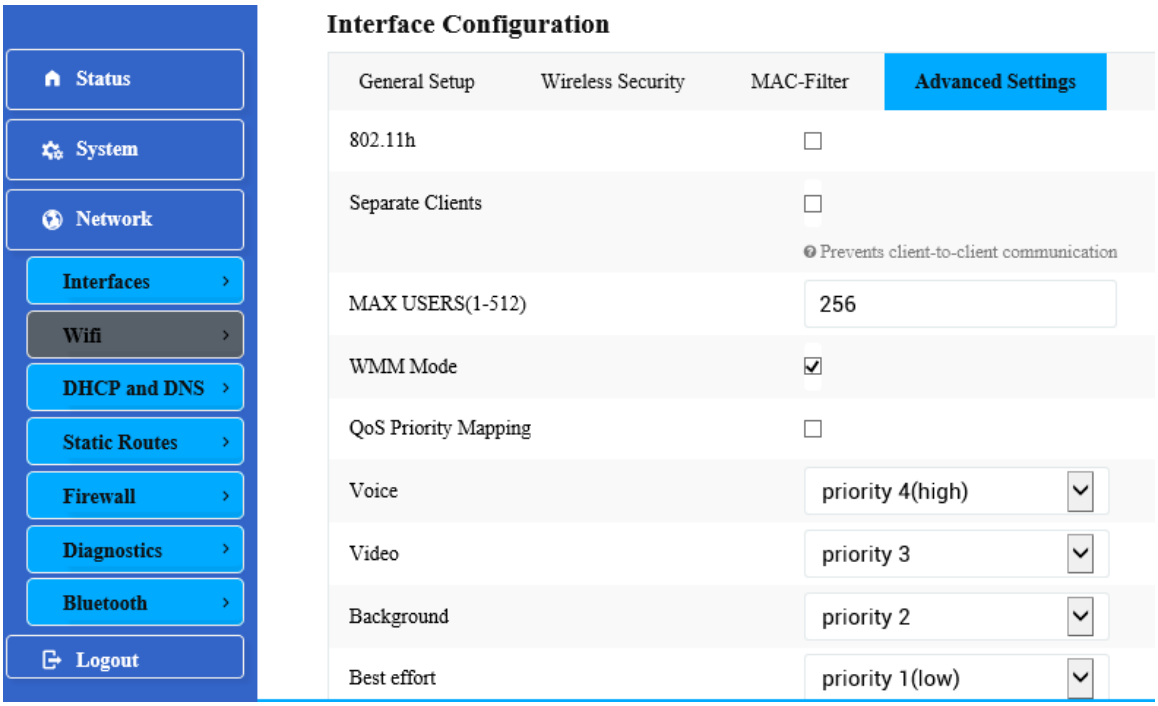
The following parameters are available in this section:

Parameter	Description
MAC Address Filter	After selecting the Allow listed only option, the following setting is available.
MAC List	Select the MAC address that is allowed access to the wireless interface here. Select custom option to manually enter the MAC address here.



The following parameters are available in this section:

Parameter	Description
MAC Address Filter	After selecting the Allow all except listed option, the following setting is available.
MAC List	Select the MAC address that is denied access to the wireless interface here. Select custom option to manually enter the MAC address here.

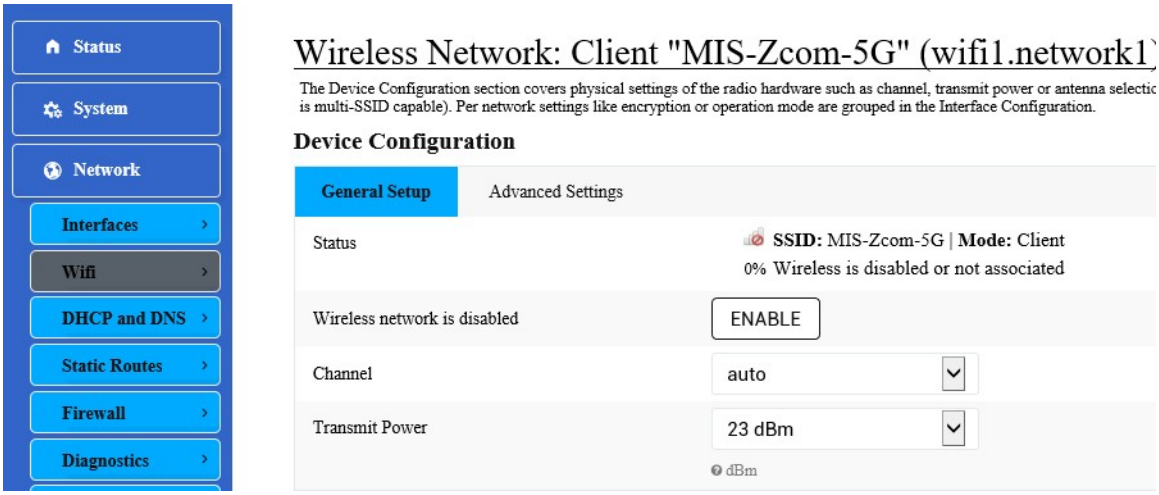


The following parameters are available in this section:

Parameter	Description
802.11h	Select this option to enable 802.11h amendment here.
Separate Clients	Select to enable the function that separates client-to-client communication here.
MAX Users	Enter the max users from 1 to 512.
WMM Mode	Select this option to enable the WMM (Wi-Fi Multimedia) mode here.
QoS Priority Mapping	Select this option to enable the QoS Priority Mapping mode here.
Voice / Vedeo / Background / Best effort	Select the priority for voice, video, background and best effort here.

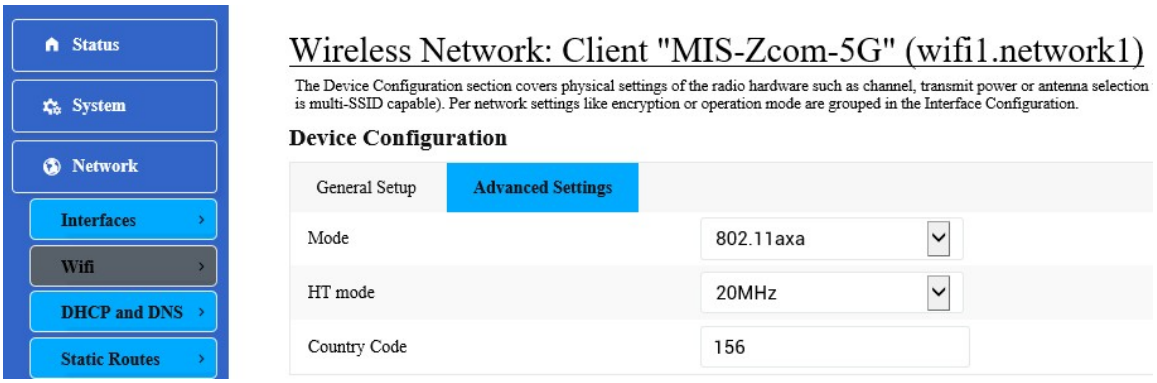
4.3.3.2.1.2. Generic Atheros 802.11an 802.11anac (wifi1)

After clicking the Edit button in the Generic Atheros 802.11anac (wifi1) entry, the following will appear:



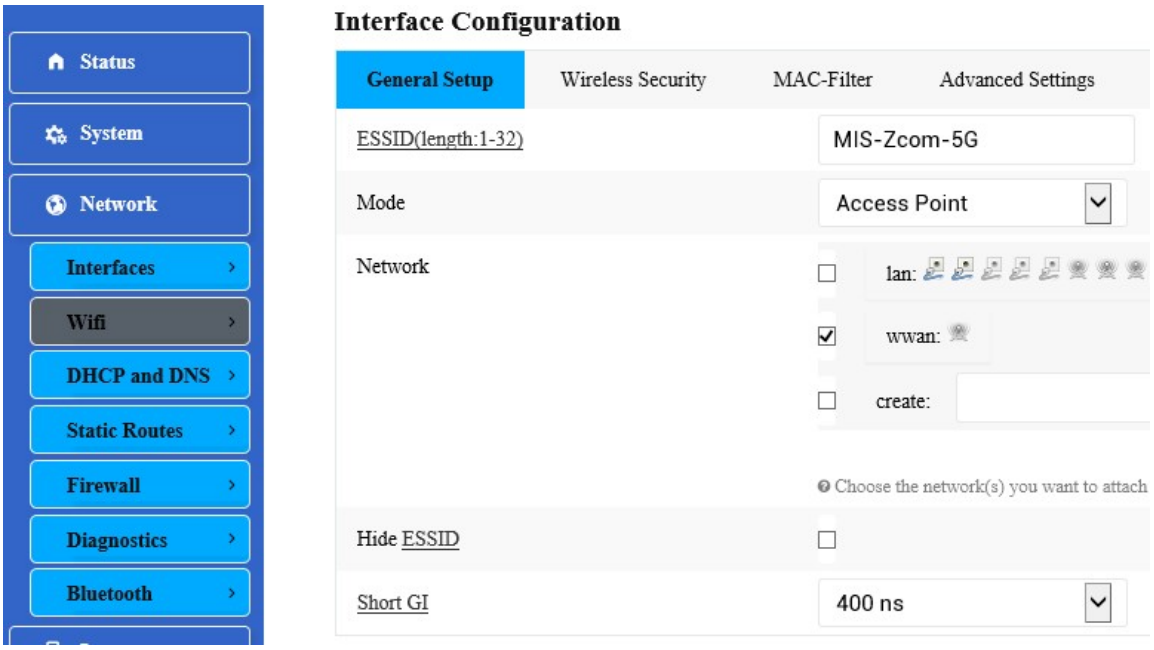
The following parameters are available in this section:

Parameter	Description
Status	Displays a summary of the wireless configuration on this wireless interface. • Signal Strength - Displays the wireless signal strength. • Mode - Displays the wireless operating mode of the wireless interface. • SSID - Displays the SSID hosted by the wireless interface. • BSSID - Displays the BSSID hosted by the wireless interface. • Encryption - Displays the wireless encryption used on the wireless interface. • Channel - Displays the wireless channel number and frequency. • TX-Power - Displays the TX (transmit) power of the wireless interface. • Signal - Displays the wireless signal strength (in dBm) on the wireless interface. • Noise - Displays the wireless noise level (in dBm) on the wireless interface. • Bitrate - Displays the active data bitrate (in megabits per second) through the wireless interface. • Country - Display the country setting on the wireless interface.
Wireless Network is Enabled	Displays the current status of the wireless interface.
Channel	Select the wireless channel for the wireless interface here. The range is from 36 (5.180 GHz) to 165 (5.825 GHz). Select the auto option to allow the AP to automatically determine the best wireless channel for this interface. Select the custom option to manually entry the channel number.
Transmit Power	Select the wireless transmit power for the interface here.



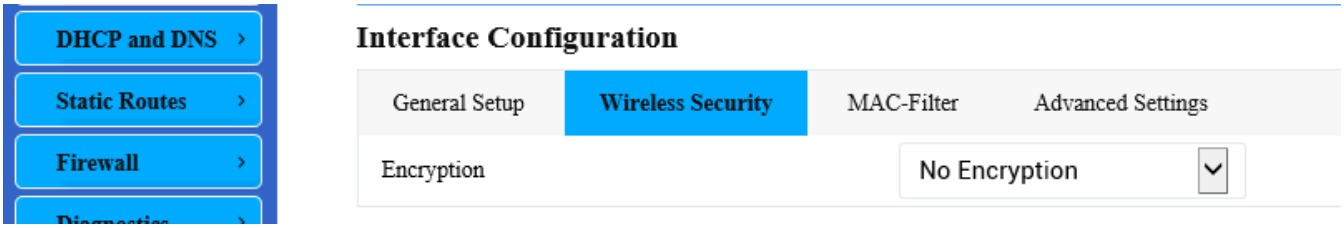
The following parameters are available in this section:

Parameter	Description
Mode	Select the wireless mode on this interface here. Options to choose from are 802.11an, 802.11ac, and 802.11axa.
HT mode	Select the HT mode here. Options to choose from are 20MHz, 40MHz and 80MHz.
Country Code	Enter the country code here.



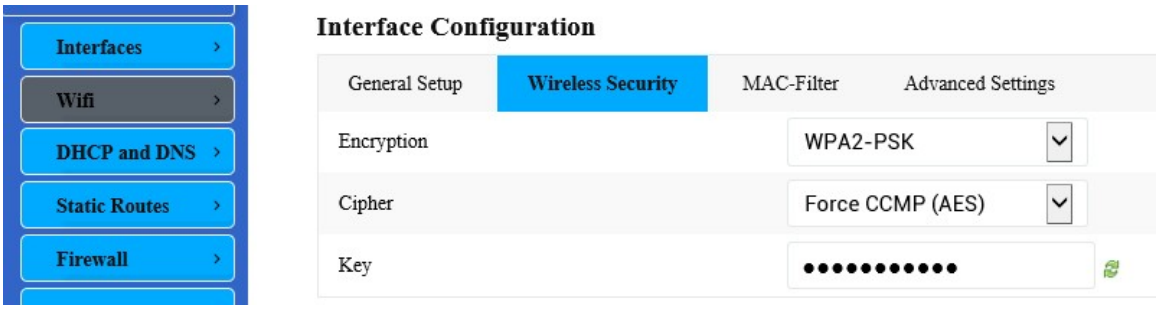
The following parameters are available in this section:

Parameter	Description
ESSID	Enter the ESSID (Extended SSID) here.
Mode	Select the wireless mode for the interface here. Options to choose from are Access Point.
Network	Select the network interface to attach to this wireless interface here. Select the *create* option to enter and create and new network interface.
Hide ESSID	Select this option to hide the ESSID from wireless clients. Wireless clients will not be able to detect this interface by simply scanning for available wireless networks.
Short GI	Select the short GI to decrease the time between data characters being sent.



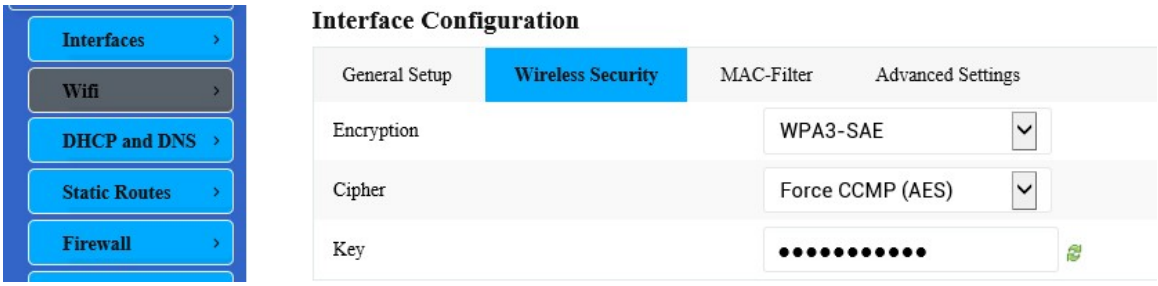
The following parameters are available in this section:

Parameter	Description
Encryption	Select the wireless encryption for this interface here. Options to choose from are No Encryption, WPA2-PSK, WPA3-SAE and WPA2-EAP. WPA2 stands for Wi-Fi Protected Access II. WPA2 stands for Wi-Fi Protected Access III. PSK stands for Pre-Shared Key. SAE stands for Simultaneous Authentication of Equals. EAP stands for Extensible Authentication Protocol.



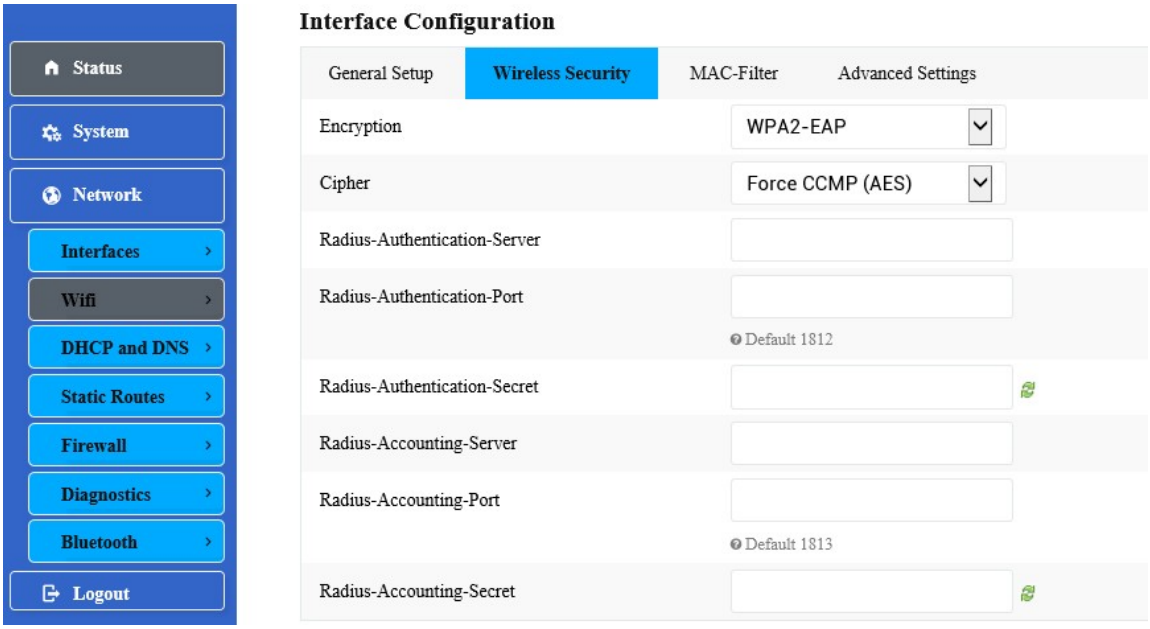
The following parameters are available in this section:

Parameter	Description
Encryption	After selecting the WPA2-PSK option, the following settings are available.
Cipher	Select the cipher method here. Options to choose from are Force CCMP (AES). CCMP stands for CCM Mode Protocol. CCM stands for Counter with CBC-MAC. CBC-MAC stands for Cipher Block Chaining Message Authentication Code. AES stands for Advanced Encryption Standard.
Key	Enter the WPA2 passphrase here.



The following parameters are available in this section:

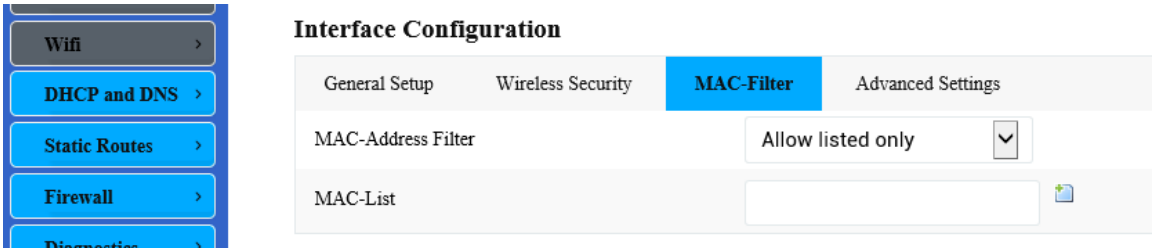
Parameter	Description
Encryption	After selecting the WPA3-SAE option, the following settings are available.
Cipher	Select the cipher method here. Options to choose from are Force CCMP (AES).
Key	Enter the WPA3 passphrase here.



Parameter	Description
Encryption	After selecting the WPA2-EAP option, the following settings are available.
Cipher	Select the cipher method here. Options to choose from are Force CCMP (AES).
RADIUS-Authentication-Server	Enter the RADIUS authentication server IP.
RADIUS-Authentication-Port	Enter the RADIUS authentication port number (Default 1812).
RADIUS-Authentication-Secret	Enter the RADIUS authentication password.
RADIUS-Accounting-Server	Enter the RADIUS accounting server IP.
RADIUS-Accounting-Port	Enter the RADIUS accounting server port number (Default 1813).
RADIUS-Accounting-Secret	Enter the RADIUS accounting server password.

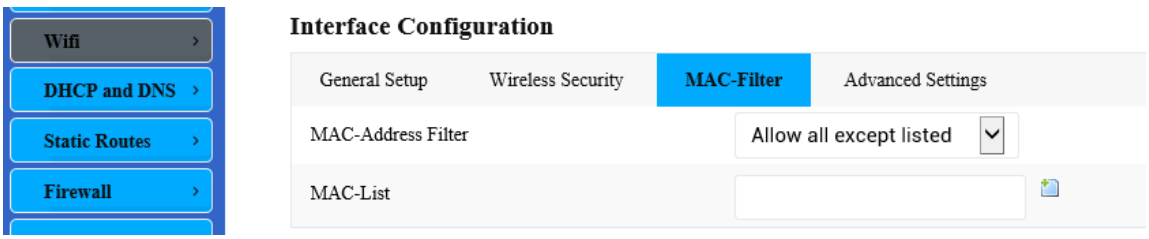
The following parameters are available in this section:

Parameter	Description
MAC Address Filter	Select to enable or disable MAC address filtering here. Options to choose from are disable, allow listed only, and allow all except listed.



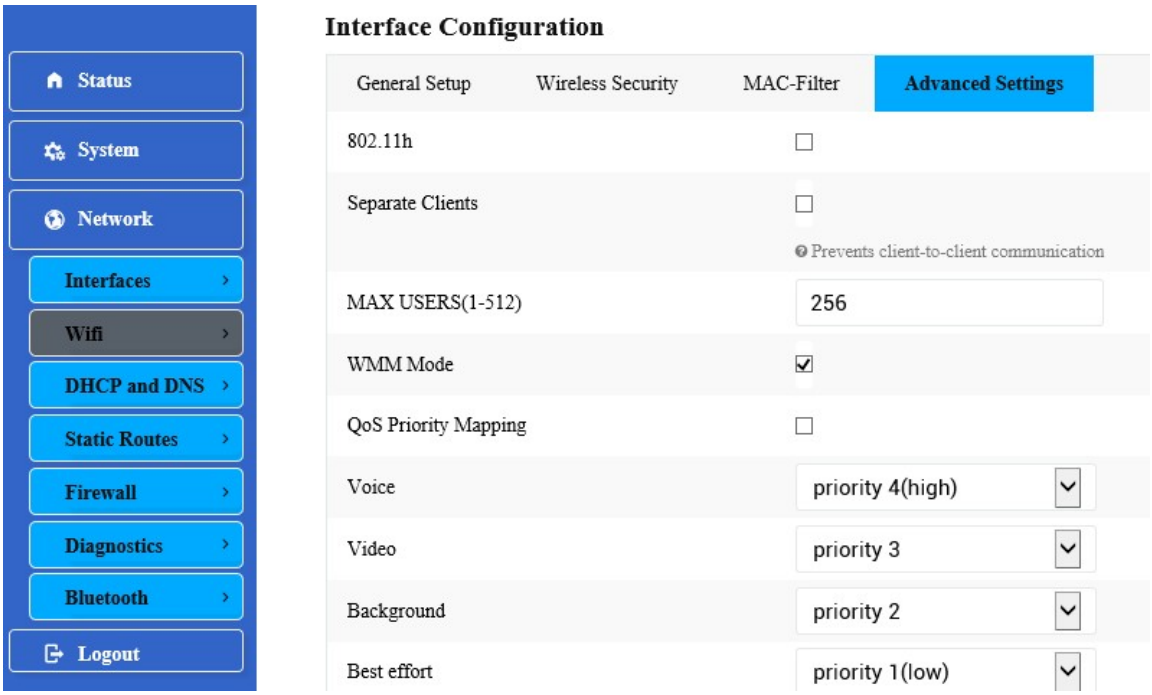
The following parameters are available in this section:

Parameter	Description
MAC Address Filter	After selecting the Allow listed only option, the following setting is available.
MAC List	Select the MAC address that is allowed access to the wireless interface here. Select custom option to manually enter the MAC address here.



The following parameters are available in this section:

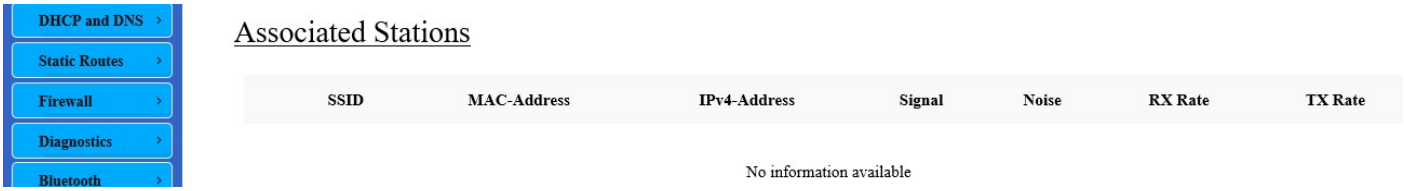
Parameter	Description
MAC Address Filter	After selecting the Allow all except listed option, the following setting is available.
MAC List	Select the MAC address that is denied access to the wireless interface here. Select custom option to manually enter the MAC address here.



The following parameters are available in this section:

Parameter	Description
802.11h	Select this option to enable 802.11h amendment here.
Separate Clients	Select to enable the function that separates client-to-client communication here.
MAX Users	Enter the max users from 1 to 512.
WMM Mode	Select this option to enable the WMM (Wi-Fi Multimedia) mode here.
QoS Priority Mapping	Select this option to enable the QoS Priority Mapping mode here.
Voice / Vedeo / Background / Best effort	Select the priority for voice, video, background and best effort here.

4.3.3.2.1.3. Associated Stations



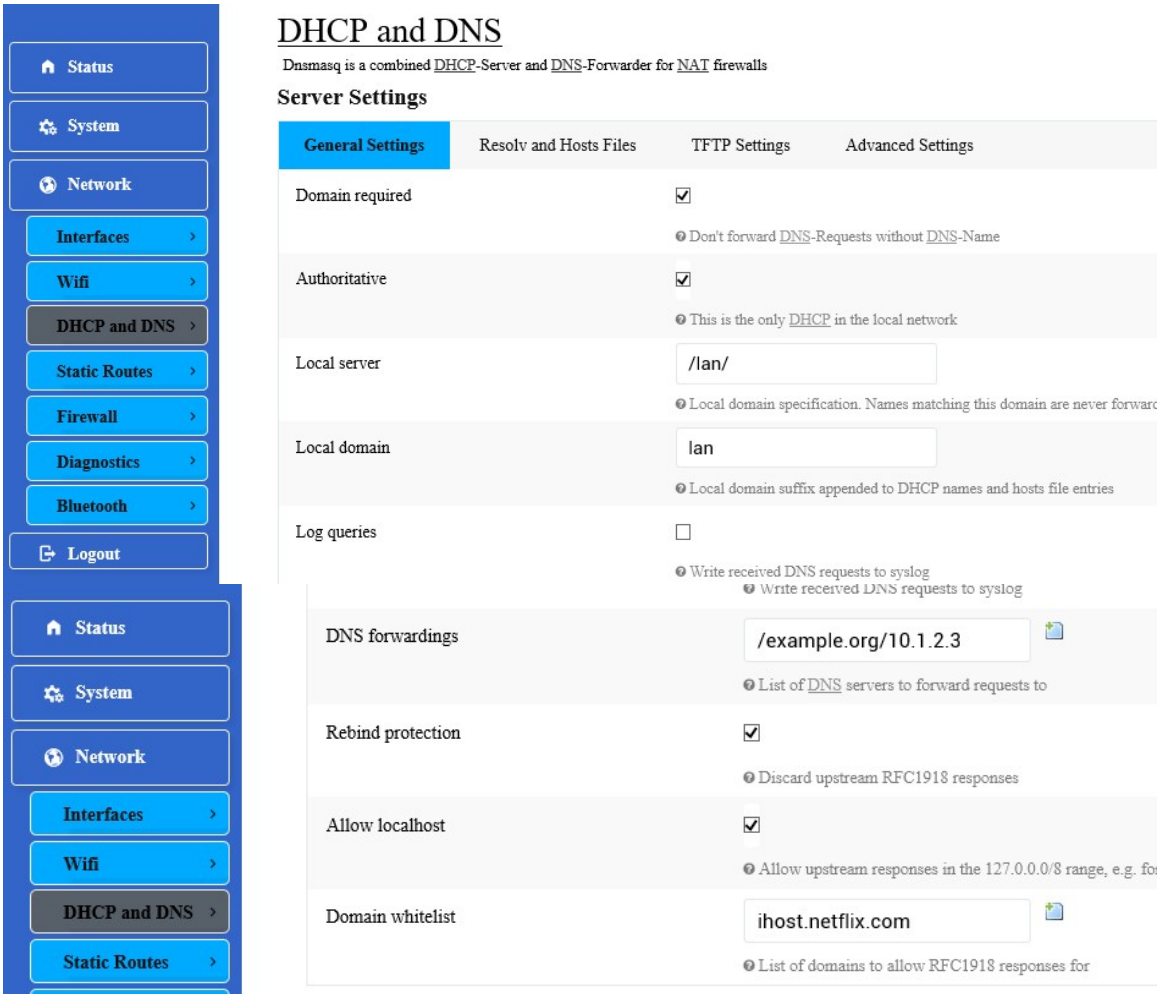
The following parameters are available in this section:

Parameter	Description
Signal Strength	Displays the signal strength of the associated wireless station.
SSID	Displays the SSID of the associated wireless station.
MAC Address	Displays the MAC address of the associated wireless station.

Parameter	Description
IPv4 Address	Displays the IPv4 address of the associated wireless station.
Signal	Displays the signal strength of the associated wireless station.
Noise	Displays the wireless signal noise of the associated wireless station.
RX Rate	Displays the RX (receiving) wireless data rate of the associated wireless station.
TX Rate	Displays the TX (transmitting) wireless data rate of the associated wireless station.

4.3.3.3. DHCP and DNS

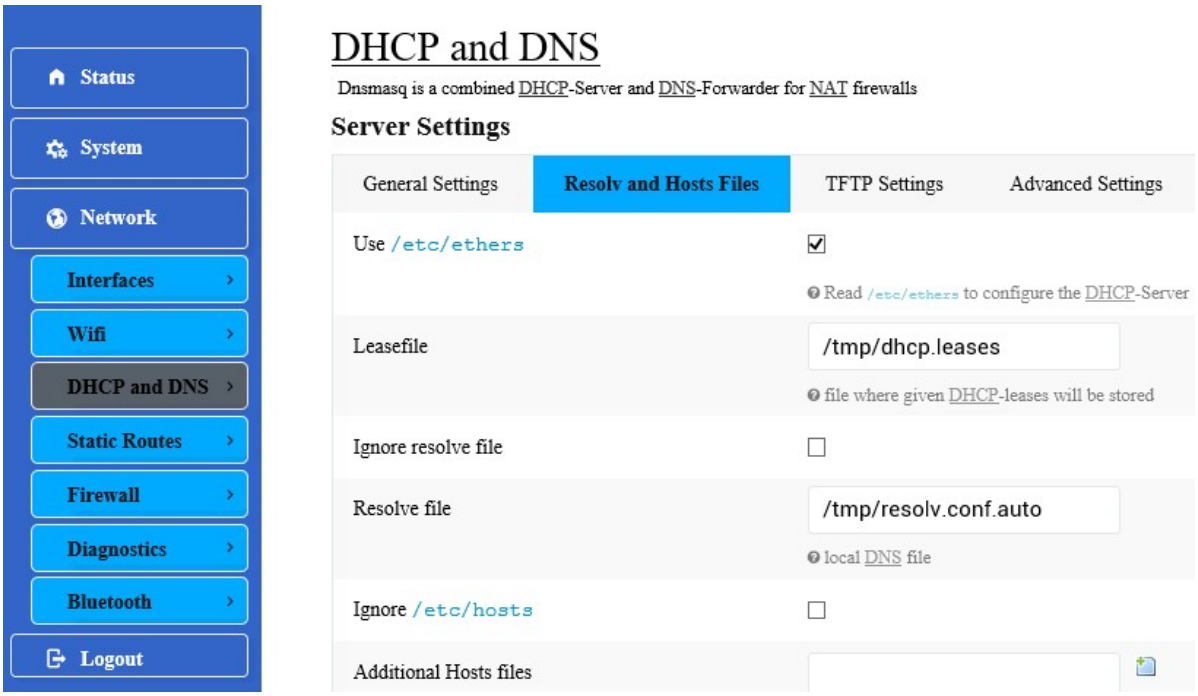
This page is used to display and configure the DHCP server and DNS settings on the AP.



The following parameters are available in this section:

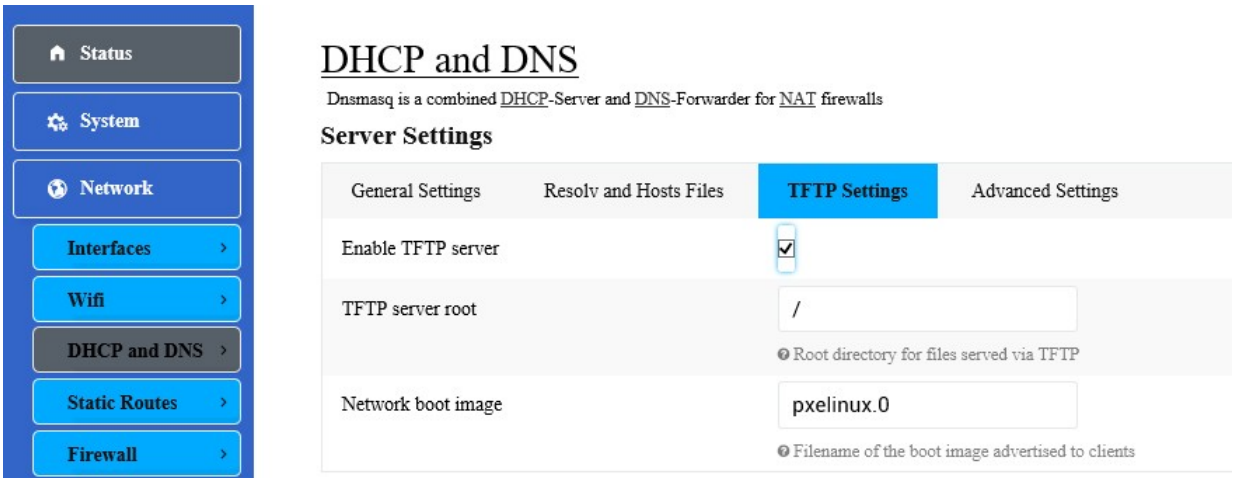
Parameter	Description
Domain Required	Select this option to stop forwarding DNS request without the DNS name.
Authoritative	Select this option to specify that this DHCP server is the only DHCP server on the local network.
Local Server	Enter the domain specification of the local DHCP server here. Names matching this domain are never forwarded and resolved from DHCP or host files only.
Local Domain	Enter the local domain here. The local domain suffix is appended to DHCP names and hosts file entries.
Log Queries	Select this option to write received DNS requests to the syslog.

Parameter	Description
DNS Forwardings	Enter the IP address or domain name of the DNS server to which DNS requests are forwarded to. More than one entry can be created.
Rebind Protection	Select this option to discard upstream RFC 1918 (Address Allocation for Private Internets) responses.
Allow Localhost	Select this option to allow upstream responses in the 127.0.0.0/8 (loopback purposes) range.
Domain Whitelist	Enter the domain name that is whitelisted for RFC 1918 responses here. More than one entry can be created.



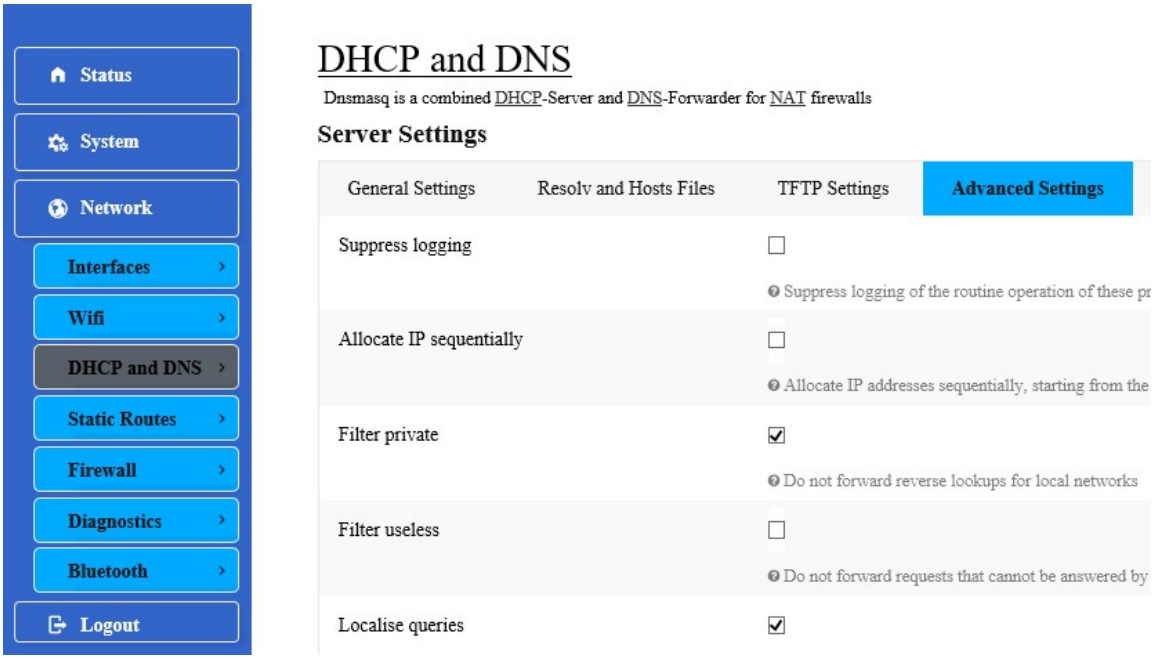
The following parameters are available in this section:

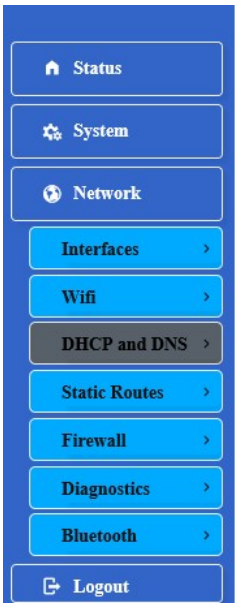
Parameter	Description
Use /etc/ethers	Select this option to use /etc/ethers to configure the DHCP server here.
Leasefile	Enter the name and path where the DHCP lease file will be saved here.
Ignore Resolve File	Select this option to ignore the resolve file.
Resolve File	Enter the name and path for the DNS file here.
Ignore /etc/hosts	Select this option to ignore hosts files.
Additional Hosts Files	Enter the name and path of the additional hosts files here. More than one entry can be created.

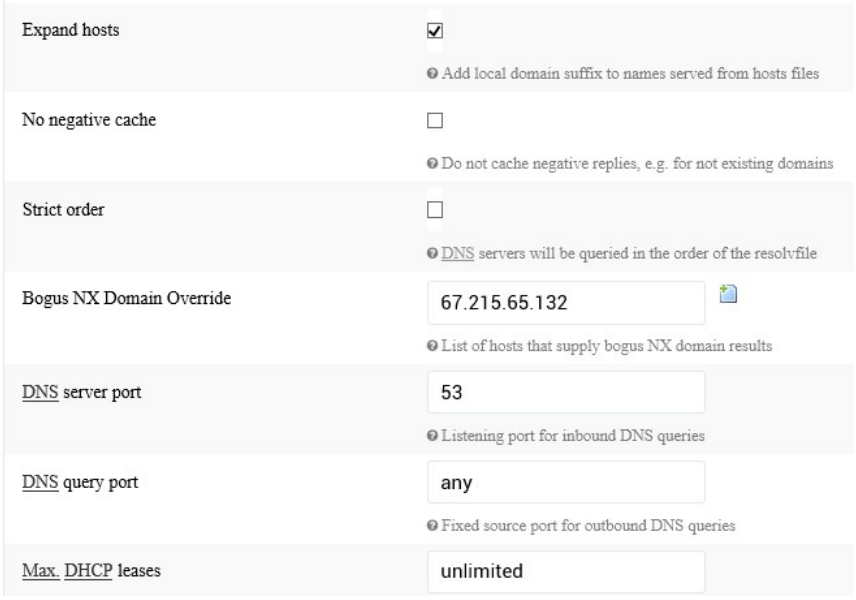


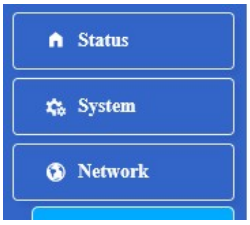
The following parameters are available in this section:

Parameter	Description
Enable TFTP Server	Select this option to enable the TFTP (Trivial File Transfer Protocol) server function here.
TFTP Server Root	Enter the TFTP server root directory here.
Network Boot Image	Enter the name of the boot image file that is advertised to client here.









The following parameters are available in this section:

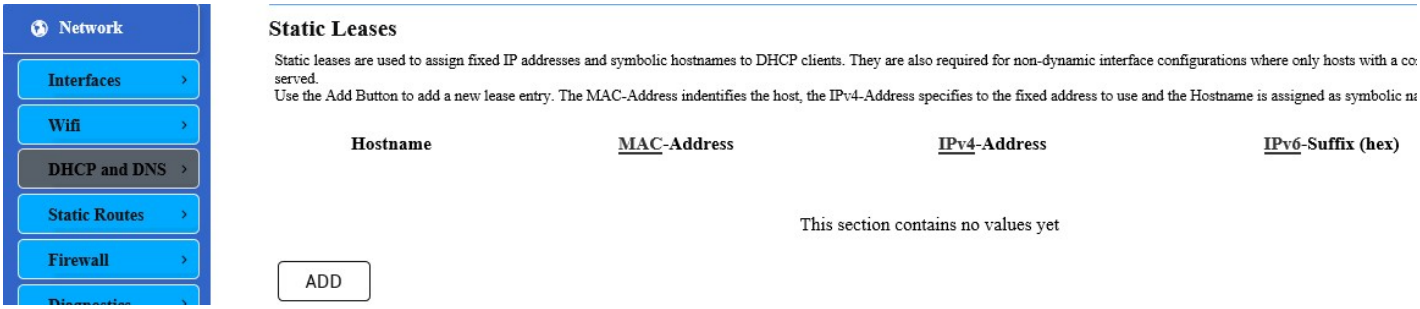
Parameter	Description
Suppress Logging	Select this option to suppress logging of the routine operation of these protocols.
Allocate IP Sequentially	Select this option Allocate IP addresses sequentially, starting from the lowest available address
Filter Private	Select this option not to forward reverse lookups for local networks.
Filter Useless	Select this option not to forward requests that cannot be answered by public name servers.
Localize Queries	Select this option to localize the hostname depending on the requesting subnet if multiple IP addresses are available.
Expand Hosts	Select this option to add a local domain suffix to the names served from the hosts files.
No Negative Cache	Select this option not to cache negative replies.
Strict Order	Select this option to only query DNS server in the order specified in the "resolvfile".
Bogus NX Domain Override	Enter the IP addresses of the host that supply bogus NX domain results here. More than one entry can be created.
DNS Server Port	Enter the TCP/UDP port number for the DNS server connection here. This port is used for inbound DNS queries.
DNS Query Port	Enter the TCP/UDP source port number for outbound DNS queries here.
Max. DHCP Leases	Enter the maximum number of active DHCP leases allowed here.
Max. EDNS0 Packet Size	Enter the maximum size allowed for EDNS.0 (Extension mechanisms for DNS) UDP packets here.
Max. Concurrent Queries	Enter the maximum number of concurrent DNS queries allowed here.

The following parameters are available in this section:

Parameter	Description
Hostname	Displays the hostname of the active DHCP lease.
IPv4 / MAC Address	Displays the IPv4/MAC address of the active DHCP lease.
Leasetime Remaining	Displays the lease time remaining for the active DHCP lease.

The following parameters are available in this section:

Parameter	Description
Hostname / IPv6 Address / DUID / Leasetime Remaining	Displays the hostname/IPv6 Address/DUID/ Leasetime remaining of the active DHCPv6 lease.

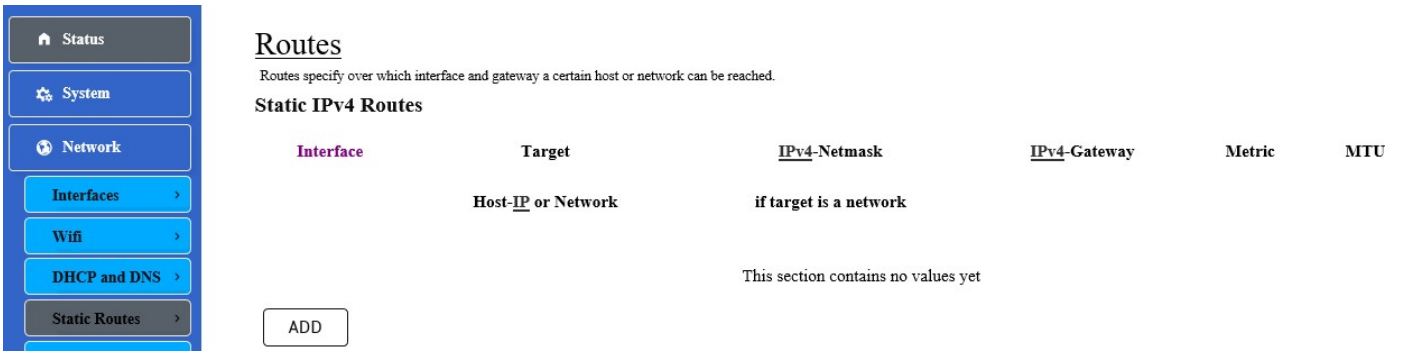


The following parameters are available in this section:

Parameter	Description
Hostname / MAC Address / IPv4 Address / IPv6-Suffix (hex)	Enter the Hostname / MAC Address / IPv4 Address / IPv6-Suffix (hex) for the static DHCP client lease here.

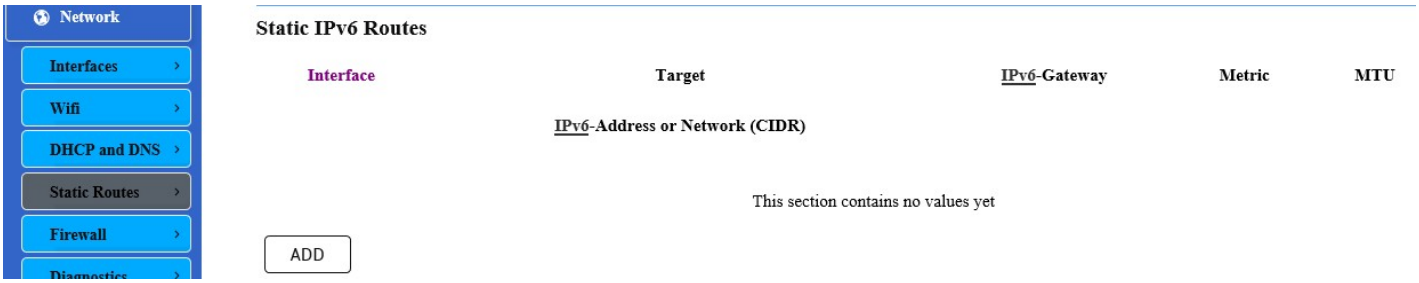
4.3.3.4. Static Routes

This page is used to display and configure static IPv4 / IPv6 routes on the AP.



The following parameters are available in this section:

Parameter	Description
Interface	Select the interface for the static IPv4 route here. Options to choose from are lan and wan.
Target	Enter the target IPv4 address or IPv4 network address for the static IPv4 route here.
IPv4 Netmask	Enter the IPv4 subnet mask for the static IPv4 route here.
IPv4 Gateway	Enter the IPv4 address of the gateway for the static IPv4 route here.
Metric / MTU	Enter the Metric / MTU for the static IPv4 route here.

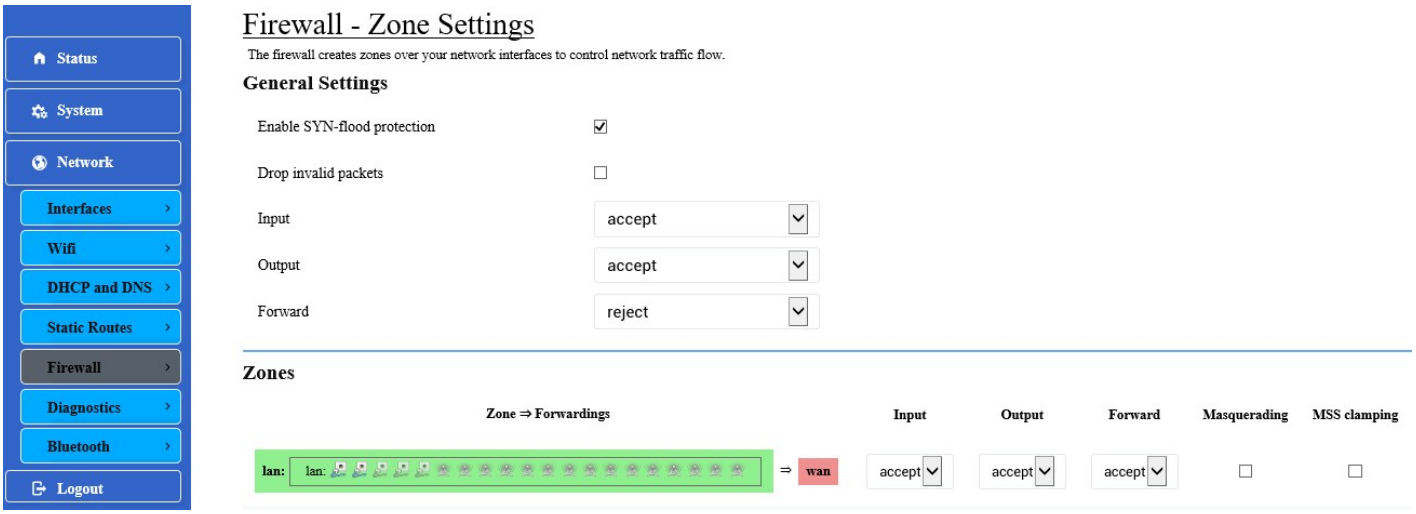


The following parameters are available in this section:

Parameter	Description
Interface	Select the interface for the static IPv6 route here. Options to choose from are lan and wan.
Target	Enter the target IPv6 address or network CIDR (Classless Inter-Domain Routing) for the static IPv6 route here.
IPv6 Gateway	Enter the IPv6 address of the gateway for the static IPv6 route here.
Metric / MTU	Enter the metric/MTU for the static IPv6 route here.

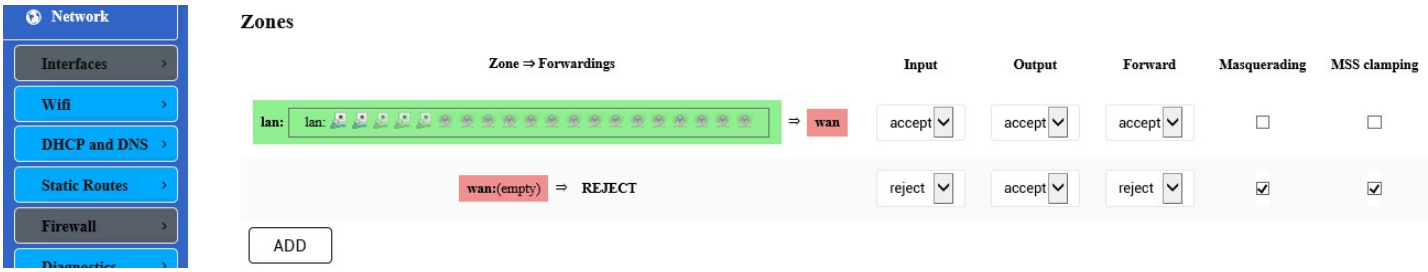
4.3.3.5. Firewall

This page is used to display and configure the firewall settings on the AP.



The following parameters are available in this section:

Parameter	Description
Enable SYN-flood protection	Select this option to enable the SYN-flood protection function. SYN stands for the synchronize step in the TCP three-way handshake.
Drop Invalid Packets	Select this option to enable the firewall function that will drop invalid received packets in the firewall zone.
Input	Select the input (incoming) action here. Options to choose from are reject, drop, and accept.
Output	Select the output (outgoing) action here. Options to choose from are reject, drop, and accept.
Forward	Select the forwarding action here. Options to choose from are reject, drop, and accept.

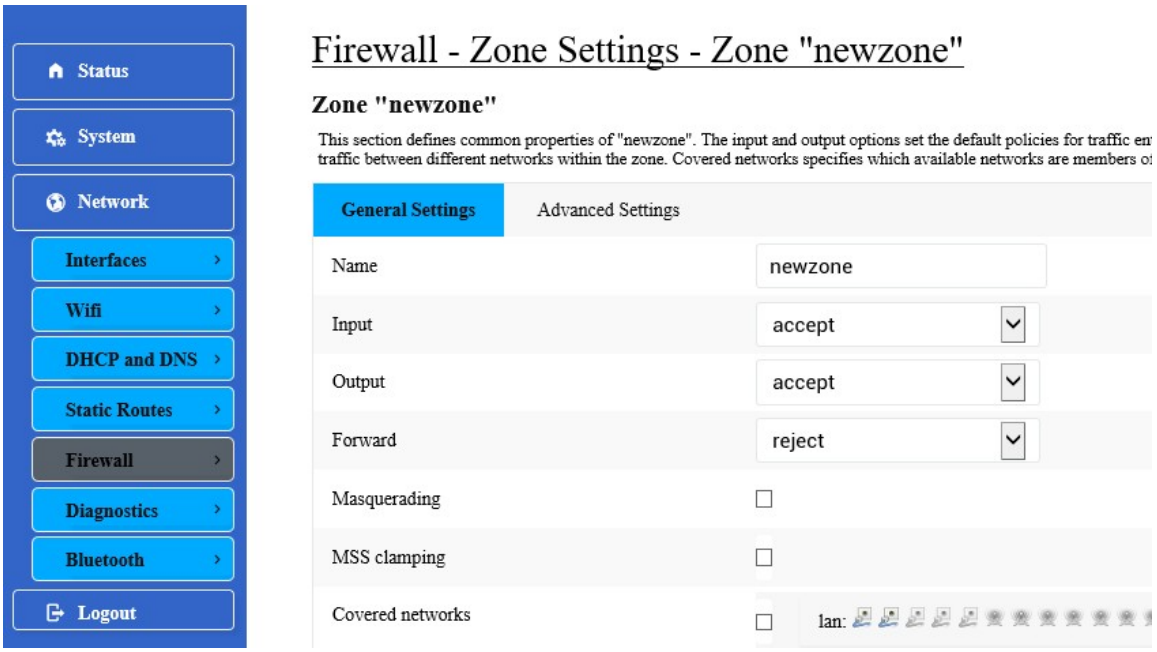


The following parameters are available in this section:

Parameter	Description
Zone >> Forwarding	Displays the visual flow for the firewall zone here.

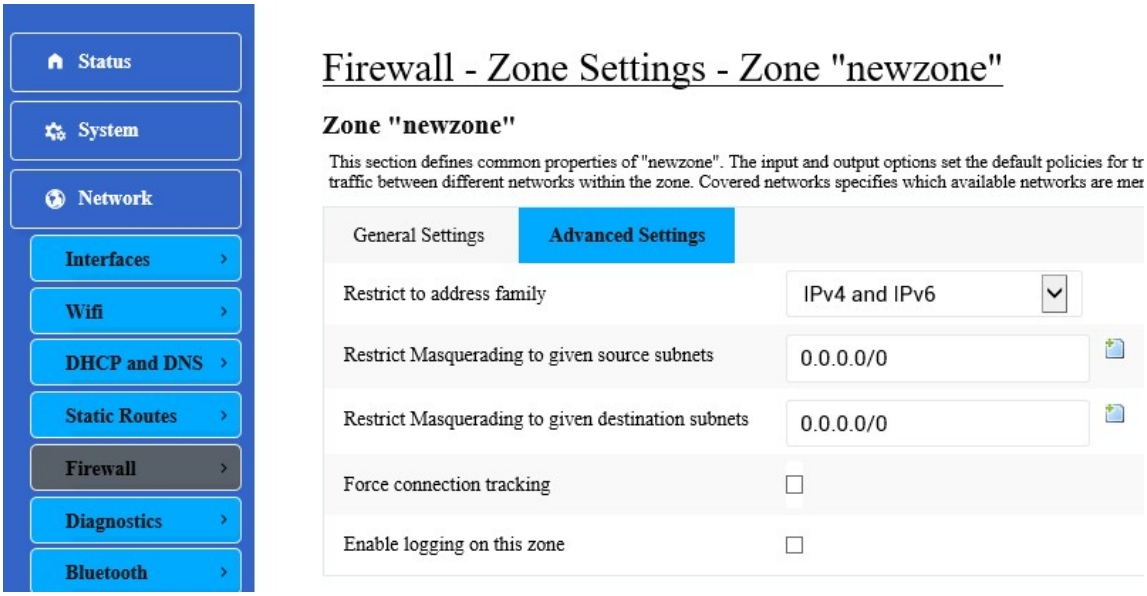
Click the Add / Edit / Delete button to add / delete a new or modify the existing firewall zone.

After clicking the Add button, the following page will appear:



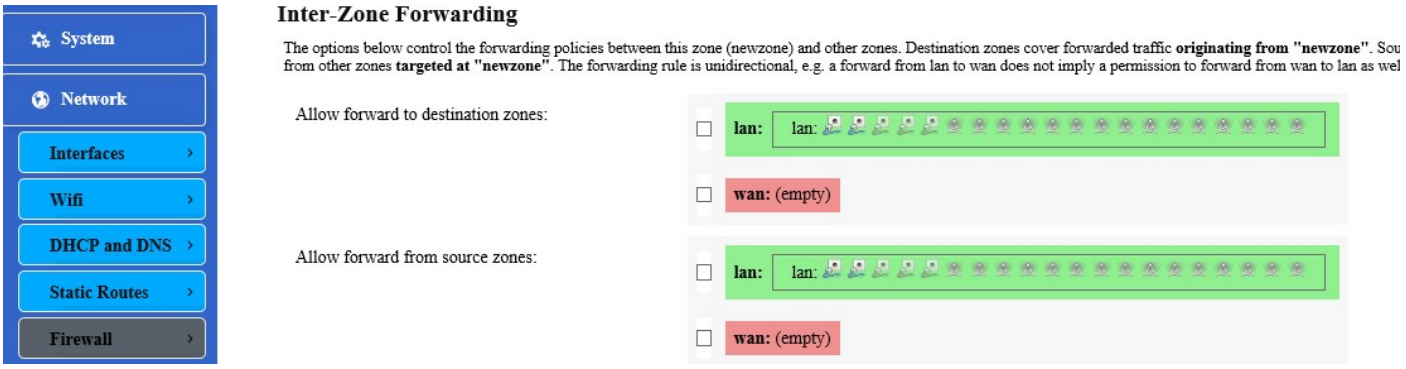
The following parameters are available in this section:

Parameter	Description
Name	Enter the name for the firewall zone here.
Input	Select the input (incoming) action here. Options to choose from are reject, drop, and accept.
Output	Select the output (outgoing) action here. Options to choose from are reject, drop, and accept.
Forward	Select the forwarding action here. Options to choose from are reject, drop, and accept.
Masquerading	Select this option to enable the masquerading function on the firewall zone.
MSS clamping	Select this option to enable the MSS clamping function on the firewall zone.
Covered networks	Select the interface that is included in this firewall zone here. Multiple interfaces can be selected. Select the create option to create a new interface for the firewall zone. Enter the name for the new interface in the space provided.



The following parameters are available in this section:

Parameter	Description
Restrict to address family	Select the IP address family that will be restricted here. Options to choose from are IPv4 and IPv6, IPv4 only, and IPv6 only.
Restrict Masquerading to given source subnets	To restrict the masquerading function to a given source subnet, enter the IPv4 subnet of the source here. This option is not available for the IPv6 address family. More than one entry can be created.
Restrict Masquerading to given destination subnets	To restrict the masquerading function to a given destination subnet, enter the IPv4 subnet of the destination here. This option is not available for the IPv6 address family. ore than one entry can be created.
Force connection tracking	Select this option to force connection tracking.
Enable logging on this zone	Select this option enable logging on this firewall zone.

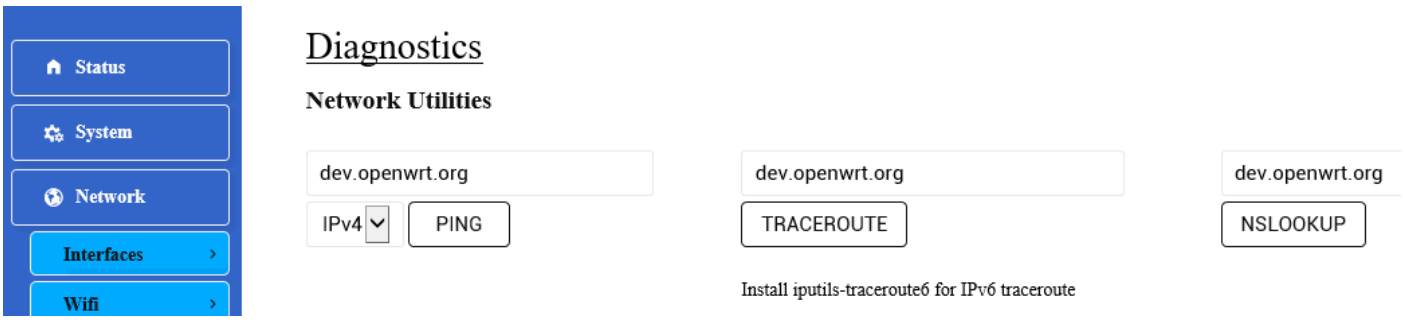


The following parameters are available in this section:

Parameter	Description
Allow forward to destination zones	Select the destination zone here. Traffic is forwarded to this zone from the "newzone".
Allow forward from source zones	Select the source zone here. Traffic is forwarded from this zone to the "newzone".

4.3.3.6. Diagnostics

This page provides useful network utilities that can be used to troubleshoot network connectivity between the AP and other networking nodes.



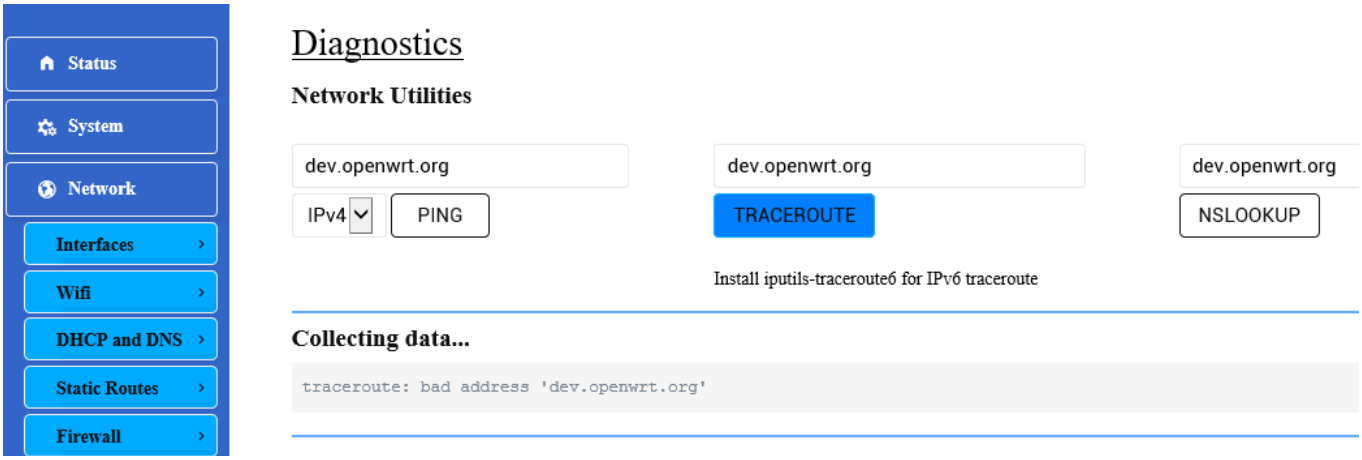
The following parameters are available in this section:

Parameter	Description
Ping	To use the ping utility, enter an IPv4/IPv6 address or domain name in the textbox and click the Ping button. The ping utility is used to send an ICMP request to nodes to probe if the node is active or not.

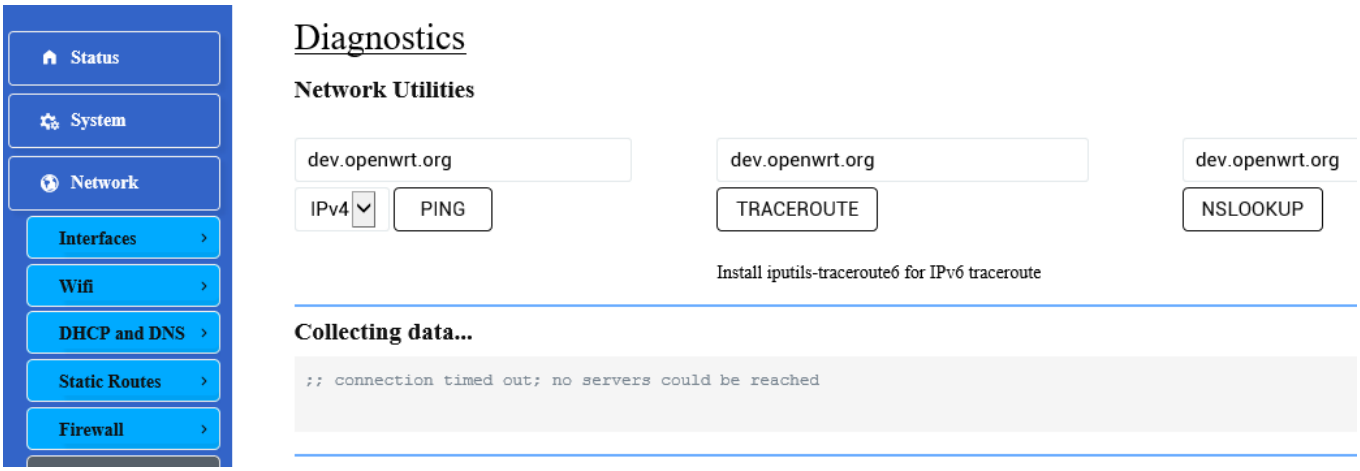
Parameter	Description
Traceroute	To use the traceroute utility, enter an IPv4 address or domain name in the textbox and click the Traceroute button. This is used to display the route across the IP network and measure the transit delays of packets from hop to hop.
Nslookup	To use the nslookup (name server lookup) utility, enter an IPv4 address or domain name in the textbox and click the Nslookup button. This is used to querying the DNS to obtain domain name mapping, IP address mapping, and/or DNS records.

After clicking the PING button, the following page will appear:

After clicking the TRACEROUTE button, the following page will appear:



After clicking the NSLOOKUP button, the following page will appear:



CHAPTER 5. TECHNICAL SPECIFICATIONS

Physical			
Dimensions (L x W x H)		296(L) x 92(W) x 283(H) mm	
Weight		2.5KG	
Device		**SP250/ SP250-S5**	
WAN/PoE In Port		One 10/100/1000/2500Mbps	
LAN Port		One 10/100/1000/2500Mbps	
Antenna	**2.4GHz**	Internal PIFA	
	5GHz	Internal PIFA	
Power Supply		DC 53V, 600mA (PoE)	
Power Consumption		Max. 25 Watts	
Wireless			
Frequency Bands	**Country**	**2.4GHz Radio**	**5GHz Radio**
	US	2.412 – 2.462GHz	5.18GHz – 5.32GHz 5.745GHz – 5.825GHz
	EU	2.412 – 2.472GHz	5.18GHz – 5.32GHz 5.5GHz – 5.7GHz
	China	2.412 – 2.472GHz	5.18GHz – 5.32GHz 5.745GHz – 5.825GHz
	Taiwan	2.412 – 2.462GHz	5.18GHz – 5.32GHz 5.745GHz – 5.825GHz
Operating Channels (@20MHz)	**Country**	**2.4GHz Radio**	**5GHz Radio**
	US	1 – 11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
	EU	1 – 13	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140
	China	1 – 13	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
	Taiwan	1-11	36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165
Bandwidth		2.4GHz: 20 / 40 MHz 5GHz: 20 / 40 / 80 MHz	
Wireless Security		**Security:** Open System, WPA2-PSK, WPA2-EAP, WPA3-SAE **Extensible Authentication Protocol (EAP) types:** WPA2/WPA3-Personal (TKIP and AES)	
Operating Mode		Thin AP (TAP) / Fat AP (FAP)	
Wireless SSIDs		2.4 GHz (Up to 8 SSIDs), 5.8 GHz (Up to 8 SSIDs)	

Environmental		
	Temperature	**Humidity**
Operating	-40°C to 65°C (-40°F to 149°F)	5% to 95 (Non-condensing)
Storage	-40°C to 70°C (-40°F to 158°F)	5% to 95

Compliance Standards
IEC/EN 62368-1 EN55032 & EN55024 WEEE & RoHS **IEEE standards :** IEEE 802.11a/b/g/n/ac/ax IEEE 802.11d, e, h, i, j, k, r, u, v time stamp, w, and z standards **Multimedia :** Wi-Fi multimedia (WMM) *Above partial functions should be configured by Z-COM Wireless LAN Controllers (WLC)

CHAPTER 6. APPENDIX

6.1. Warranty

6.1.1. General Warranty

The warranty period stated below replaces the warranty period as stated in the user manuals for the relevant Products. If there is no proof indicating the purchase date, the manufacture date shall be considered as the beginning of the warranty period. The Warranty extends only to the original end-user purchaser and is not transferable to anyone who obtains ownership of the Product from the original end-user purchaser.

1. Z-COM provides one year of conditional warranty depends on different models.
2. Lifetime warranty covers product itself, excluding consumable products, accessories, second-hand products, and software. Lifetime warranty is only effective when products are still in the Z-COM Product list. After the EOL (End of Life) announcement for any Products, the warranty will be one year from the date of such Product EOL announcement. To grant the lifetime warranty, Products should have a proof of purchase (such as the invoice or sales receipt) must be provided upon receiving warranty service. The standard warranty period for any Product had a proof of purchase shall be one year from the date of purchase or manufacture.
3. Products are considered as DOA (Dead on Arrival) after conclusive test within the first 30 days of its shipping date from Z-COM. After 30 days from the shipping date, defective products covered within the warranty are considered as RMA (Return Material Authorization).
4. Z-COM reserves the right to inspect all defective products which must be returned and paid shipping fee by purchasers.

6.1.2. Warranty Conditions

Warranty service will be excluded if following conditions occurred:

1. The product has been tampered, repaired and/or modified by non-authorized personnel
2. The SN (Serial Number) or MAC (Media Access Control) address has been changed, cancelled, or removed
3. The damage is caused by third party software or virus
4. The software loss or data loss that may occur during repair or replacement

6.1.3. Disclaimer

PRODUCTS ARE NOT WARRANTED TO OPERATE UNINTERRUPTED OR ERROR FREE. Z-COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS. Z-COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, FOREC MAJEURE EVENT OR ANY OTHER HAZARD. THE INFORMATION CONTAINED HEREIN IS SUBJECT TO CHANGE WITHOUT NOTICE.

6.2. Compliance

6.2.1. FCC

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

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

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

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

This radio transmitter (FCC ID: M4Y-SP250) has been approved by FCC.

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

You are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user’s authority to operate the equipment.

Radiation Exposure Warning

This equipment complies with radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 51 cm between the radiator and your body.

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

6.2.2. CE Marking

CE marking on this product represents the product is in compliance with all directives that are applicable to it.

CE

Note: This device meets Max. TX power limit per ETSI regulations.

WEEE Compliance Statement

European Directive 2012/19/EU requires that the equipment bearing this symbol on the product and/ or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

Declaration of Conformity

Hereby, Z-COM, Inc. declares that the radio devices are in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address:
https://www.zcom.com.tw/index/downloads?keyword=&meterial_type=56

6.2.3. NCC

根據 NCC 規定：
取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

- 「本產品電磁波曝露量(MPE)標準值 1 mW/cm^2，送測產品實測值為 0.12152 mW/cm^2，建議使用時至少距離人體 51 cm」。

6.4. Optional Accessories

PN	Item	Picture	SP250	SP250-S5
64-000004-L7N	mounting bracket		yes	yes
64-000003-ZNN	cable gland		yes	yes
64-000517-00N	cable gland		yes	yes
60-200001-00N	ground wire		yes	yes
64-800003-00N	clamp		yes	yes
61-100092-00N	Screws		yes	yes

Note: When ordering power adaptors, you must specify the destination region by indicating -US, -EU instead of -XX.

6.5. Contact Information

All information may be changed by Z-COM at any time without prior notice or explanation to the user. For further information please refer to our website: www.zcom.com.tw