



# SP250/SP250-S5

11ax Access Point

---



# TABLE OF CONTENTS

<b>Chapter 1. Introduction.....</b>	<b>1</b>
1.1. Product Description .....	1
<b>Chapter 2. Hardware Components.....</b>	<b>2</b>
2.1. Package Contents .....	2
2.2. Installation Requirements .....	2
2.3. Physical Ports .....	2
2.4. LED Indicator .....	3
<b>Chapter 3. Hardware Installation .....</b>	<b>4</b>
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
<b>Chapter 4. The Https Interface .....</b>	<b>6</b>
4.1. Login to the HTTPS Interface.....	6
4.1.1 Thin and Fat AP Switching .....	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
<b>Chapter 5. Technical Specifications .....</b>	<b>54</b>
<b>Chapter 6. Appendix .....</b>	<b>56</b>
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 outdoor 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. The SP250/SP250-S5 features the latest in rugged weatherproofing and Wi-Fi 6 technology with guaranteed performance and reliability in the harshest environments.

### 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



Waterproof cable gland (\*Note)



One ground wire



One clamp



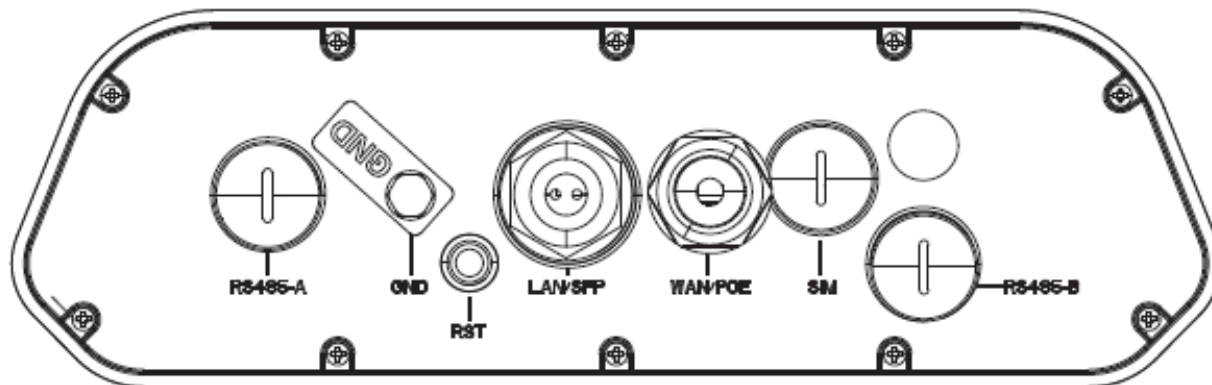
**Note:** provides two waterproof cable glands.

## 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
<b>WAN / PoE Port</b>	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.
<b>LAN Port</b>	The LAN port operates at 10/100/1000/2500Mbps at supports an RJ45 connector.
<b>GND Port</b>	Ground through GND Port.
<b>Reset Button</b>	After use, the setting will be reset to default. Please press and hold about 15 seconds.
<b>RS485-A/B (Not Available)</b>	You can be transmitted through this port. (SP250-A04 Only)
<b>SIM Card Port (Not Available)</b>	SIM card can be inserted into this slot for use. (SP250-A04 Only)

## 2.4. LED Indicator

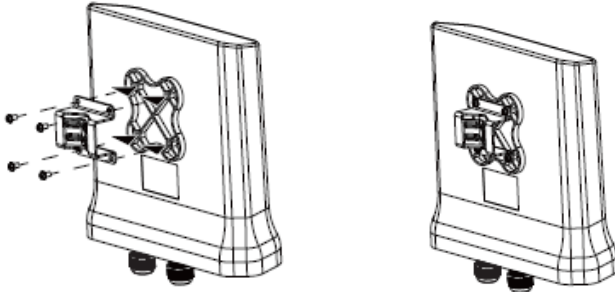
The following table describes the AP status referring to different LED behavior.

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

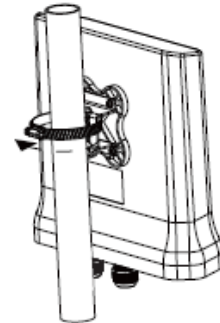
## CHAPTER 3. HARDWARE INSTALLATION

### 3.1. Mounting the Access Point on the Pole

① Place 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

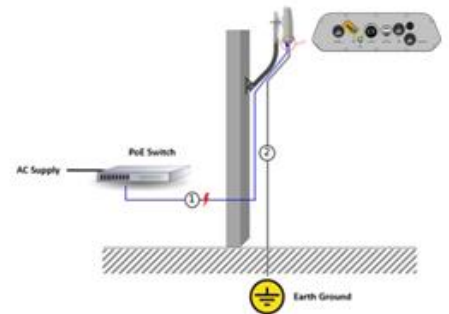
1. Make your device GND port connect to ground wire.
2. The ground wire connects to the earth. In addition, the grounding wire meets to 6-AWG copper grounding wire.



**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.

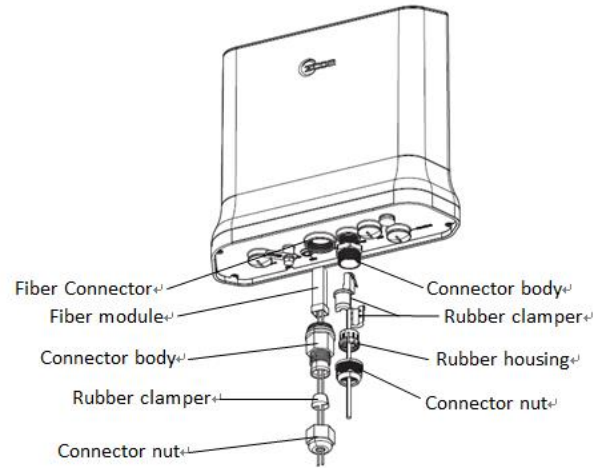


### 3.3. Safety Notice

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.

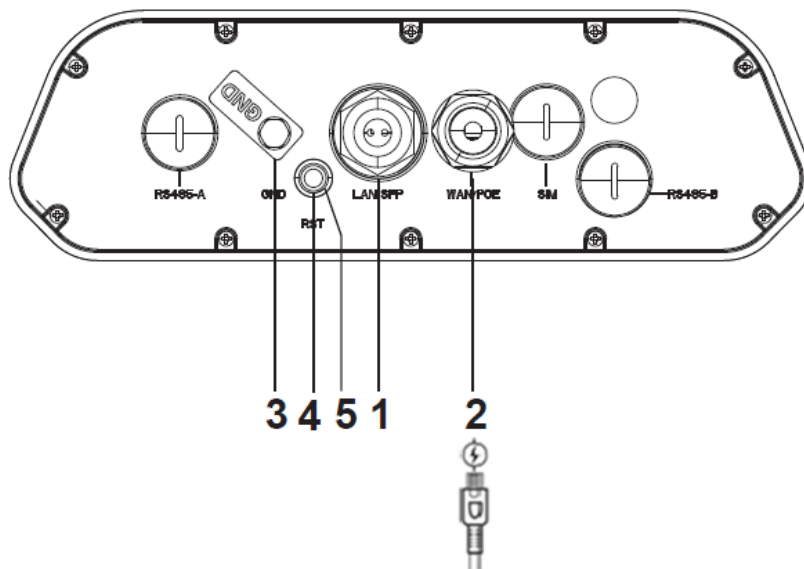
### 3.4. Installing a Cable Gland (SP-WP-CM20)

- (1) Dismantle all the components of waterproof cable gland,
- (2) Plug the cable in between of Rubber clamber.
- (3) Insert rubber housing
- (4) Insert the rubber housing back to connector body
- (5) Tighten the connector nut.
- (6) Recheck waterproof 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 button to return the parameters on the page to their previously saved state.



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



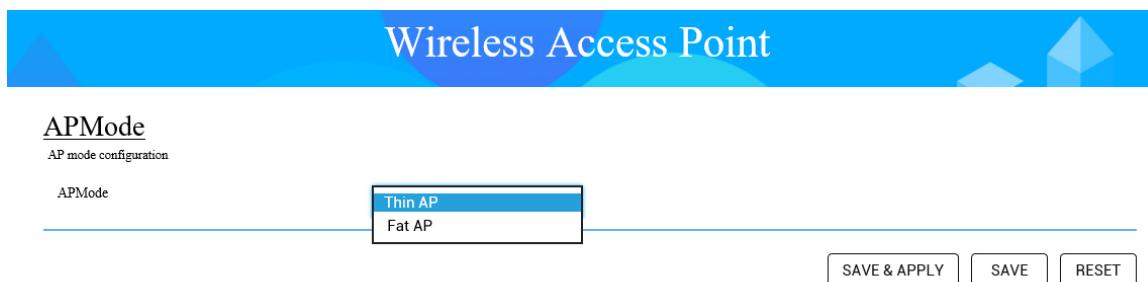
**Note:** Click  Save & Apply button to save and apply the modifications made on the page.

### 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.
- ④ If 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=&material\\_type=49](https://www.zcom.com.tw/index/downloads?keyword=&material_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=&material\\_type=25](https://www.zcom.com.tw/index/downloads?keyword=&material_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

- Home Status
- Overview >
- General >
- System
- Logout

### Status

#### System

Hostname	APBF69FC
Model	AS250-A03
Firmware Version	V3.0.04B3
Kernel Version	4.4.60
Local Time	Fri May 20 07:52:49 2022
Uptime	0h 1m 35s
Load Average	1.00, 0.32, 0.11

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

- General >
- System
- Logout

#### Memory

Total Available	606576 kB / 827036 kB (73%)
Free	601652 kB / 827036 kB (72%)
Buffered	4924 kB / 827036 kB (0%)

The following parameters are available in this section:

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

Parameter	Description
<b>Buffered</b>	Displays the buffered memory on the AP in kilobytes and percentage.

**Connection Information**

Connection Status	Disconnected
WLC IP Address	

The following parameters are available in this section:

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

**4.2.2.2. General**

[Status](#)

[Overview](#)

[General](#)

[System](#)

[Logout](#)

[Status](#)

[Overview](#)

[General](#)

[System](#)

[Logout](#)

Wireless LAN Controller setting

Method of Connecting with Wireless LAN Controller

IP Mode	IPv4
DHCP Client	open
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
IPv6 Address	3ffe:3211::21
IPv6 Prefix	64
Default Gateway	::
IPv6 Primary DNS Server	::/64
IPv6 Secondary DNS Server	::
Connect Mode	Connect with Wireless LAN Controller via DHCP
Wireless LAN Controller Address1	0.0.0.0
Wireless LAN Controller Address2	0.0.0.0
Wireless LAN Controller Address3	0.0.0.0
Wireless LAN Controller Address4	0.0.0.0
Wireless LAN Controller IPv6 Address1	::
Wireless LAN Controller IPv6 Address2	::

Overview >	Wireless LAN Controller IPv6 Address3	<input type="text" value="::"/>
General >	Wireless LAN Controller IPv6 Address4	<input type="text" value="::"/>
* System	Wireless Switch Name1	<input type="text" value="ZWS-100"/>
Logout	Wireless Switch Name2	<input type="text" value="ZWS-100-1"/>
	Wireless Switch Name3	<input type="text" value="ZWS-100-2"/>
	Wireless Switch Name4	<input type="text" value="ZWS-100-3"/>
	Management VLAN ID	<input type="text" value="0"/>

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
<b>IP Mode</b>	Displays basic mode information of the ipMod. IPv4 – Select IPv4 mode. IPv6 - Select IPv6 mode. Auto – Auto detected if it is IPv4 or IPv6.
<b>DHCP Client</b>	Choose the DHCP Client, which is Close, or Open by default it will be Open.
<b>IP Address</b>	Enter the IP address.
<b>Subnet Mask</b>	Enter the Subnet Mask.
<b>Default Gateway</b>	Enter the IPv4 address of the gateway for the interface.
<b>Primary / Secondary DNS Server</b>	Enter primary/secondary DNS server. (if require the second one)
<b>IPv6 Address</b>	Enter the IPv6 address.
<b>IPv6 Prefix</b>	Enter the IPv6 prefix IP address.
<b>Default Gateway</b>	Enter the IPv6 address of the gateway for the interface.
<b>Connect mode</b>	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.
<b>Wireless LAN Controller Address 1/2/3/4</b>	Enter wireless access controller IPv4 IP address.
<b>Wireless LAN Controller IPv6 Address1/2/3/4</b>	Enter wireless access controller IPv6 IP address.
<b>Wireless Switch Name1/2/3/4</b>	Enter access controller DNS value.
<b>Management VLAN ID</b>	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:

System	
Hostname	APBF69FC
Model	AS250-A03
Firmware Version	V3.0.04B3
Kernel Version	4.4.60
Local Time	Fri May 20 07:55:46 2022
Uptime	0h 1m 30s
Load Average	1.04, 0.34, 0.12

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

Memory Type	Usage
Total Available	607732 kB / 827036 kB (73%)
Free	603196 kB / 827036 kB (72%)
Buffered	4536 kB / 827036 kB (0%)

The following parameters are available in the Memory section:

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

Parameter	Description
<b>Buffered</b>	Displays the buffered memory on the AP in kilobytes and percentage.

- Overview >
- Firewall >
- Routes >
- Processes >
- Realtime Graphs >
- System
- Network

### Network

IPv4 WAN Status

Type: static

Address: 192.168.1.1

Netmask: 255.255.255.0

Gateway: 0.0.0.0

Connected: 0h 3m 22s

br-lan

IPv6 WAN Status

Address: ::

Gateway: ::

Connected: 0h 3m 22s

br-lan

Active Connections 71 / 16384 (0%)

The following parameters are available in the Network section:

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

- Firewall >
- Routes >
- Processes >
- Realtime Graphs >

### DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
There are no active leases.			

The following parameters are available in the DHCP Leases section:

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

- Overview >
- Firewall >
- Routes >
- Processes >

### DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining
There are no active leases.			

The following parameters are available in the DHCPv6 Leases section:

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



- [Status](#)
- [Overview](#)
- [Firewall](#)
- [Routes](#)
- [Processes](#)
- [Realtime Graphs](#)
- [System](#)
- [Network](#)
- [Logout](#)

### Wireless

Generic 802.11abgn Wireless Controller (wifi0)

- SSID: [Wireless](#)
- Mode: Master
- Channel: 0 (0.000 GHz)
- Bitrate: ? Gbit/s
- Wireless is disabled or not associated
- SSID: [Wireless](#)
- Mode: Master
- Channel: 0 (0.000 GHz)
- Bitrate: ? Gbit/s
- Wireless is disabled or not associated
- SSID: [Wireless](#)
- Mode: Master
- Channel: 0 (0.000 GHz)
- Bitrate: ? Gbit/s
- Wireless is disabled or not associated
- SSID: [Wireless](#)
- Mode: Master
- Channel: 0 (0.000 GHz)
- Bitrate: ? Gbit/s
- Wireless is disabled or not associated

- [Status](#)
- [Overview](#)
- [Firewall](#)
- [Routes](#)
- [Processes](#)
- [Realtime Graphs](#)
- [System](#)
- [Network](#)
- [Logout](#)

Generic 802.11ac Wireless Controller (wifi1)

- SSID: [MIS-Zoom-5G](#)
- Mode: Client
- Channel: 0 (0.000 GHz)
- Bitrate: ? Gbit/s
- Wireless is disabled or not associated
- SSID: [openlab5g](#)
- Mode: Master
- Channel: 149 (5.745 GHz)
- Bitrate: 0.295 Gbit/s
- BSSID: 00:19:70:BF:69:FD
- Encryption: WPA2
- SSID: [Wireless](#)
- Mode: Master
- Channel: 0 (0.000 GHz)
- Bitrate: ? Gbit/s
- Wireless is disabled or not associated
- SSID: [Wireless](#)
- Mode: Master
- Channel: 0 (0.000 GHz)
- Bitrate: ? Gbit/s

The following parameters are available in the Wireless section:

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

### 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.

- Status
- Overview >
- Firewall >
- Routes >
- Processes >
- Realtime Graphs >
- System
- Network
- Logout

#### Firewall Status

IPv4 Firewall IPv6 Firewall

Actions  
[Reset Counters](#)  
[Restart Firewall](#)

Table: Filter

Chain INPUT (Policy: ACCEPT, Packets: 688, Traffic: 46.39 KB)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	2848	233.54 KB	ACCEPT	all	--	br-lan	*	0.0.0.0/0	0.0.0.0/0	-

- Status
- Overview >
- Firewall >
- Routes >
- Processes >
- Realtime Graphs >
- System
- Network
- Logout

#### Firewall Status

IPv4 Firewall IPv6 Firewall

Actions  
[Reset Counters](#)  
[Restart Firewall](#)

Table: Filter

Chain INPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	13	1.42 KB	delegate_input	all	--	*	*	::/0	::/0	-

### 4.3.1.3. Routes

- Status
- Overview >
- Firewall >
- Routes >
- Processes >
- Realtime Graphs >
- System
- Network
- Logout

#### Routes

The following rules are currently active on this system.

##### ARP

IPv4-Address	MAC-Address	Interface
192.168.1.35	00:e0:4c:68:00:7a	br-lan

##### Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
lan	192.168.1.0/24		0	main

##### Active IPv6-Routes

Network	Target	Source	Metric	Table
lan	ff00::/8		256	local

##### IPv6 Neighbours

IPv6-Address	MAC-Address	Interface
--------------	-------------	-----------

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
<b>MAC Address</b>	Displays the MAC address of the ARP/neighbour entry.
<b>Interface</b>	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
<b>Network</b>	Displays the physical or logical interface the active IPv4/IPv6 route resides on.
<b>Target</b>	Displays the target IPv4 network range of the active IPv4/IPv6 route.
<b>IPv4 Gateway</b>	Displays the IPv4 gateway address used by the active IPv4 route.
<b>Metric</b>	Displays the metric used by the active IPv4/IPv6 route.

### 4.3.1.4. Processes

- Status
- Overview >
- Firewall >
- Routes >
- Processes >
- Realtime Graphs >
- System
- Network
- Logout

#### Processes

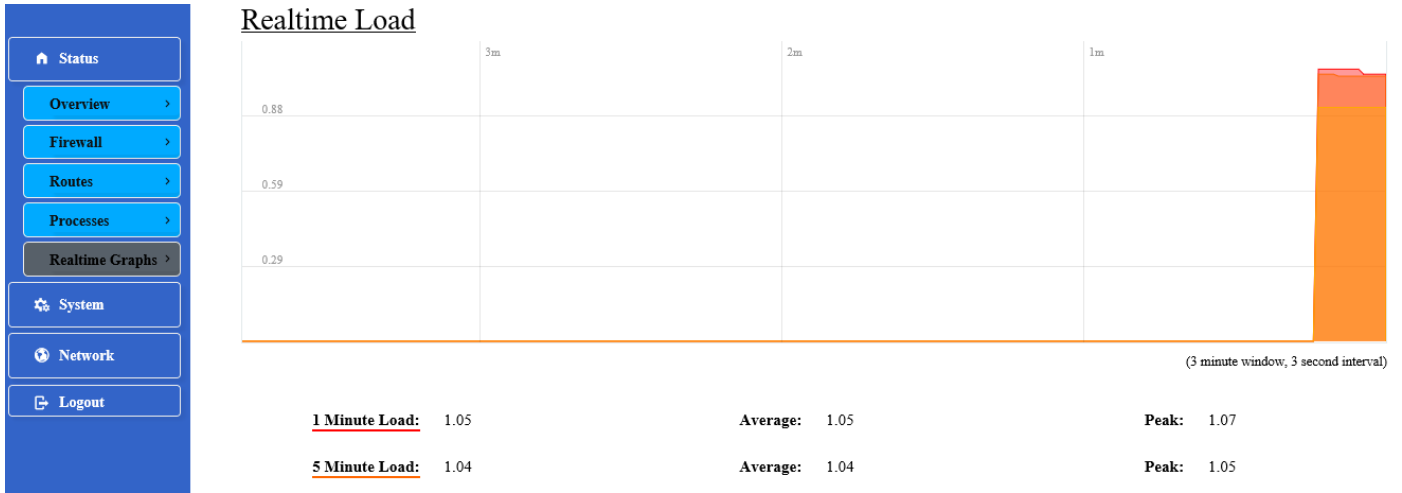
This list gives an overview over currently running system processes and their status.

PID	Owner	Command	CPU usage (%)	Memory usage (%)	Hang Up	Terminate	Kill
1	root	/sbin/procd	0%	0%	HANG UP	TERMINATE	KILL
2	root	[kthreadd]	0%	0%	HANG UP	TERMINATE	KILL
3	root	[ksoftirqd/0]	0%	0%	HANG UP	TERMINATE	KILL
5	root	[kworker/0:0H]	0%	0%	HANG UP	TERMINATE	KILL
7	root	[rcu_preempt]	0%	0%	HANG UP	TERMINATE	KILL

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

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

### 4.3.1.5. Realtime Graphs

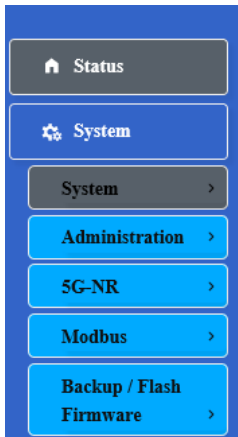


This page is used to display the load graph in real time. The following parameters are available in the Realtime Load section:

Parameter	Description
<b>1/5/15 Minute Load</b>	Displays the 1/5/15-minute load in real time. <ul style="list-style-type: none"> <li>Average - Displays the average measurement for the 1/5/15-minute load.</li> <li>Peak - Displays the peak measurement for the 1-minute load.</li> </ul>

## 4.3.2. System

### 4.3.2.1. System



### System

Here you can configure the basic aspects of your device like its hostname or the timezone.

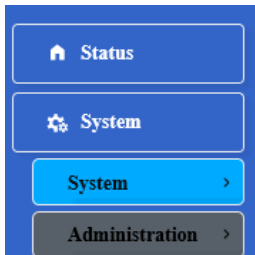
#### System Properties

General Settings	Logging	Language and Style
Local Time	Fri May 20 07:59:42 2022	<input type="button" value="SYNC WITH BROWSER"/>
Hostname	<input type="text" value="APBF69FC"/>	
Timezone	UTC <input type="button" value="v"/>	
LED	ON <input type="button" value="v"/>	

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



### Router Password

Changes the administrator password for accessing the device

Password(Password length:8-32)

Confirmation

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

### 4.3.2.2.2. SSH Access



### SSH Access

Dropbear offers [SSH](#) network shell access and an integrated [SCP](#) server

#### Dropbear Instance

Interface	<input type="radio"/> lan: <input type="radio"/> wwan: <input checked="" type="radio"/> unspecified
Port	<input type="text" value="22"/> <p><small>ⓘ Specifies the listening port of this Dropbear instance</small></p>
Password authentication	<input checked="" type="checkbox"/> <p><small>ⓘ Allow <a href="#">SSH</a> password authentication</small></p>
Allow root logins with password	<input checked="" type="checkbox"/> <p><small>ⓘ Allow the root user to login with password</small></p>
Gateway ports	<input type="checkbox"/> <p><small>ⓘ Allow remote hosts to connect to local SSH forwarded ports</small></p>

The following parameters are available in this section:

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

#### 4.3.2.2.3. SSH-Keys

Modbus >

Backup / Flash Firmware >

### SSH-Keys

Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

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.

Status

System

System >

Administration >

5G-NR >

Modbus >

Backup / Flash Firmware >

AP Mode >

Reboot >

Network

Logout

### 5G-NR Setting

**WAN Port**

**NetMode**

Auto ▼

---

**DailUp\_AutoDetction**

---

**DailUp\_Manual\_Set**

CFG02CB8E

APN

fetnet88

UserName

Your UserName

- Home Status
- System
  - System >
  - Administration >
  - 5G-NR >
  - Modbus >
  - Backup / Flash Firmware >
  - AP Mode >
  - Reboot >
- Network

Password

AccessNumber

---

**SIMCARD-Information**

CFG02CB8E

SIMCard-Status  SIMCard Status

IPAddress  IP Address

Band  Band

RSSI  Rssi

CellID  Cell Id

ConnectionOption  connection Option

IMSI/IMEI  IMSI/IMEI

---

<b>Authentication</b>	<b>IP</b>	<b>IP_Setting</b>
Auto <input type="button" value="v"/>	IPv4 <input type="button" value="v"/>	<input type="text" value="option"/>

---

<b>Roaming</b>	<b>MTU[500-1500]</b>
Enable <input type="button" value="v"/>	<input type="text" value="1500"/>

Parameter	Description
<b>NetMode</b>	Select the Net, you can see 4 options: Auto, WCDM, LTE or NR5G.
<b>DailUp_AutoDetction</b>	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.

- Home Status
- System
  - System >
  - Administration >
  - 5G-NR >
  - Modbus >
  - Backup / Flash Firmware >
  - AP Mode >
  - Reboot >
- Network

Flash operations

**Actions** Configuration

**Backup / Restore**

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup:

Reset to defaults:

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup:

**Flash new firmware image**

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

Keep settings:

Image:

### 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

**Interfaces**  
Interface Overview

Network	Status	Actions
<b>WAN</b> ath1	<b>MAC-Address:</b> 00:00:00:00:00:00 <b>RX:</b> 0.00 B (0 Pkts.) <b>TX:</b> 0.00 B (0 Pkts.)	CONNECT STOP EDIT <b>DELETE</b>
<b>LAN</b> br-lan	<b>Uptime:</b> 0h 16m 38s <b>MAC-Address:</b> 00:19:70:BF:69:FC <b>RX:</b> 149.37 KB (1863 Pkts.) <b>TX:</b> 588.97 KB (1408 Pkts.) <b>IPv4:</b> 192.168.1.1/24	CONNECT STOP EDIT <b>DELETE</b>

ADD NEW INTERFACE...

SAVE & APPLY SAVE RESET

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

**Create Interface**

Name of the new interface:

Note: interface name length

Protocol of the new interface: Static address

Create a bridge over multiple interfaces:

Cover the following interface:

- Ethernet Adapter: "bond0"
- Ethernet Adapter: "eth0" (lan)
- Ethernet Adapter: "eth1" (lan)
- Ethernet Adapter: "eth2" (lan)
- Ethernet Adapter: "eth3" (lan)
- Ethernet Adapter: "eth4" (lan)

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



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

**Interfaces**  
Interface Overview

Network	Status	Actions
<b>WAN</b> ath1	<b>MAC-Address:</b> 00:00:00:00:00:00 <b>RX:</b> 0.00 B (0 Pkts.) <b>TX:</b> 0.00 B (0 Pkts.)	CONNECT STOP EDIT <b>DELETE</b>
<b>LAN</b> br-lan	<b>Uptime:</b> 0h 16m 38s <b>MAC-Address:</b> 00:19:70:BF:69:FC <b>RX:</b> 149.37 KB (1863 Pkts.) <b>TX:</b> 588.97 KB (1408 Pkts.) <b>IPv4:</b> 192.168.1.1/24	CONNECT STOP <b>EDIT</b> <b>DELETE</b>

ADD NEW INTERFACE...

SAVE & APPLY SAVE RESET

### 4.3.3.1.1. Static Address

#### 4.3.3.1.1.1. General Setup

🏠 Status

⚙️ System

🌐 Network

🔌 Interfaces >

📶 Wifi >

🌐 DHCP and DNS >

📍 Static Routes >

🔥 Firewall >

🔍 Diagnostics >

📶 Bluetooth >

🚪 Logout

---

🏠 Status

⚙️ System

🌐 Network

🔌 Interfaces >

📶 Wifi >

### Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field or use VLAN notation `INTERFACE.VLANID` (e.g.: `eth0.1`).

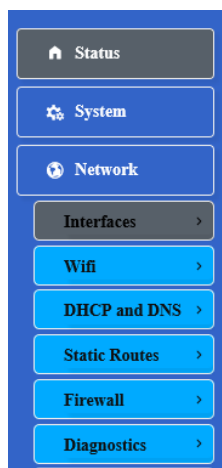
#### Common Configuration

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Status		Uptime: 0h 23m 21s MAC-Address: 00:19:70:BF:69:FC RX: 359.71 KB (5237 Pkts.) TX: 2.49 MB (4815 Pkts.) IPv4: 192.168.1.1/24	
Protocol	Static address <input type="button" value="v"/>		
IPv4 address	<input type="text" value="192.168.1.1"/>		
IPv4 netmask	255.255.255.0 <input type="button" value="v"/>		
IPv4 gateway	<input type="text"/>		
IPv4 broadcast	<input type="text"/>		
Use custom DNS servers	<input type="text"/> <input type="button" value="add"/>		
IPv6 assignment length	60 <input type="button" value="v"/> <small>ⓘ Assign a part of given length of every public IPv6-prefix to this interface</small>		
IPv6 assignment hint	<input type="text"/> <small>ⓘ Assign prefix parts using this hexadecimal subprefix ID for this interface.</small>		

The following parameters are available in this section:

Parameter	Description
<b>Status</b>	Displays basic status information of the interface. <ul style="list-style-type: none"> <li>Port - Displays the interface name. For example, "eth0.2".</li> <li>Uptime - Displays the how long the interface is active.</li> <li>MAC Address - Displays the MAC address of the interface.</li> <li>RX - Displays the RX (receiving) data rate through the interface.</li> <li>IPv4-Displays the internet IP.</li> <li>TX - Displays the TX (transmitting) data rate through the interface.</li> </ul>
<b>Use Custom DNS Servers</b>	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.
<b>IPv6 Assignment Length / Hint</b>	<b>Note:</b> This option is only available if Accept router advertisements are enabled.

### 4.3.3.1.1.2. Advanced Settings



#### Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" option. Use VLAN notation INTERFACE.VLANID (e.g.: eth0.1).

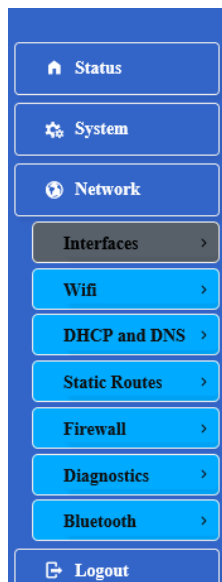
##### Common Configuration

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Bring up on boot	<input checked="" type="checkbox"/>		
Use builtin IPv6-management	<input checked="" type="checkbox"/>		
Override MAC address	<input type="text" value="00:19:70:BF:69:FC"/>		
Override MTU	<input type="text" value="1500"/>		
Use gateway metric	<input type="text" value="0"/>		

The following parameters are available in this section:

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

### 4.3.3.1.1.3. Physical Settings



#### Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" option. Use VLAN notation INTERFACE.VLANID (e.g.: eth0.1).

##### Common Configuration

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Bridge interfaces	<input checked="" type="checkbox"/>		
	<input type="radio"/> creates a bridge over specified interface(s)		
Enable STP	<input type="checkbox"/>		
	<input type="radio"/> Enables the Spanning Tree Protocol on this bridge		
Interface	<input type="checkbox"/>	Ethernet Adapter: "bond0"	
	<input checked="" type="checkbox"/>	Ethernet Adapter: "eth0" (lan)	
	<input checked="" type="checkbox"/>	Ethernet Adapter: "eth1" (lan)	
	<input checked="" type="checkbox"/>	Ethernet Adapter: "eth2" (lan)	
	<input checked="" type="checkbox"/>	Ethernet Adapter: "eth3" (lan)	

The following parameters are available in this section:

Parameter	Description
<b>Bridge Interfaces</b>	Select this option to bridge this interface with another interface.
<b>Enable STP</b>	<b>Note:</b> This option is only available if Bridge interfaces are enabled.
<b>Interface</b>	If desired, select and enter a Custom Interface name in the textbox provided. <b>Note:</b> 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



#### Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network use VLAN notation INTERFACE.VLANID (e.g.: eth0.1).

#### Common Configuration

General Setup    Advanced Settings    Physical Settings    **Firewall Settings**

Create / Assign firewall-zone

lan:

wan: (empty)

unspecified -or- create:

The following parameters are available in this section:

Parameter	Description
<b>Create / Assign Firewall-Zone</b>	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



#### DHCP Server

General Setup    Advanced Settings    IPv6 Settings

Ignore interface

Disable DHCP for this interface.

Start

Lowest leased address as offset from the network address.

Limit

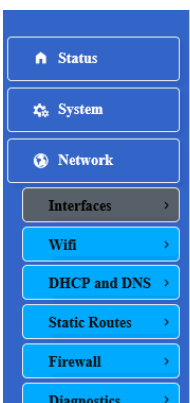
Maximum number of leased addresses.

Leasetime

Expiry time of leased addresses, minimum is 2 minutes (>=).

The following parameters are available in this section:

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



#### DHCP Server

General Setup    **Advanced Settings**    IPv6 Settings

Dynamic DHCP

Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be se

Force

Force DHCP on this network even if another server is detected.

IPv4-Netmask

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

The following parameters are available in this section:

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

- Status
- System
- Network
- Interfaces >
- Wifi >
- DHCP and DNS >
- Static Routes >
- Firewall >
- Diagnostics >
- Bluetooth >

### DHCP Server

General Setup
Advanced Settings
IPv6 Settings

Router Advertisement-Service	server mode <input type="button" value="v"/>
DHCPv6-Service	server mode <input type="button" value="v"/>
NDP-Proxy	disabled <input type="button" value="v"/>
DHCPv6-Mode	stateless + stateful <input type="button" value="v"/>
<small>⊙ Default is stateless + stateful</small>	
Always announce default router	<input type="checkbox"/>
<small>⊙ Announce as default router even if no public prefix is available.</small>	
Announced DNS servers	<input type="text" value=""/> <input type="button" value="add"/>
Announced DNS domains	<input type="text" value=""/> <input type="button" value="add"/>

The following parameters are available in this section:

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

### 4.3.3.1.2. DHCP Client



## Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

### Common Configuration

**General Setup**

Status Uptime: 0h 27m 36s

**MAC-Address:** 00:19:70:BF:69:FC  
**RX:** 417.43 KB (5912 Pkts.)  
**TX:** 2.77 MB (5468 Pkts.)  
**IPv4:** 192.168.1.1/24

br-lan

Protocol DHCP client

Really switch protocol? SWITCH PROTOCOL

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



## Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

### Common Configuration

**General Setup**    Advanced Settings    Physical Settings    Firewall Settings

Status Uptime: 0h 28m 11s

**MAC-Address:** 00:19:70:BF:69:FC  
**RX:** 434.82 KB (6131 Pkts.)  
**TX:** 2.90 MB (5683 Pkts.)  
**IPv4:** 192.168.1.1/24

br-lan

Protocol DHCP client

Hostname to send when requesting DHCP APBF69FC

The following parameters are available in this section:

Parameter	Description
<b>Status</b>	Displays basic status information of the interface. <ul style="list-style-type: none"> <li>Port - Displays the interface name. For example, "eth0.2".</li> <li>Uptime - Displays the how long the interface is active.</li> <li>MAC Address - Displays the MAC address of the interface.</li> <li>RX - Displays the RX (receiving) data rate through the interface.</li> <li>IPv4-Displays the internet IP.</li> <li>TX - Displays the TX (transmitting) data rate through the interface.</li> </ul>
<b>Hostname to Send When Requesting DHCP</b>	Enter the hostname that is sent when requesting DHCP here.

[Status](#)  
[System](#)  
[Network](#)  
[Interfaces](#) >  
[Wifi](#) >  
[DHCP and DNS](#) >  
[Static Routes](#) >  
[Firewall](#) >  
[Diagnostics](#) >  
[Bluetooth](#) >  
[Logout](#)

[Network](#)  
[Interfaces](#) >  
[Wifi](#) >  
[DHCP and DNS](#) >  
[Static Routes](#) >  
[Firewall](#) >

## Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field use VLAN notation INTERFACE.VLANID (e.g.: eth0.1).

### Common Configuration

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Bring up on boot	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Use builtin IPv6-management	<input checked="" type="checkbox"/>		
Use broadcast flag	<input type="checkbox"/>		
		ⓘ Required for certain ISPs, e.g. Charter with DOCSIS 3	
Use default gateway	<input checked="" type="checkbox"/>		
		ⓘ If unchecked, no default route is configured	
Use DNS servers advertised by peer	<input checked="" type="checkbox"/>		
		ⓘ If unchecked, the advertised DNS server addresses are ignored	
Use gateway metric	<input type="text" value="0"/>		
Client ID to send when requesting DHCP	<input type="text"/>		
Vendor Class to send when requesting DHCP	<input type="text"/>		
Override MAC address	<input type="text" value="00:19:70:BF:69:FC"/>		
Override MTU	<input type="text" value="1500"/>		

The following parameters are available in this section:

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



## Interfaces - LAN

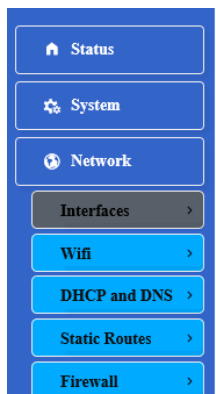
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the : use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

### Common Configuration

General Setup	Advanced Settings	<b>Physical Settings</b>	Firewall Settings
Bridge interfaces		<input checked="" type="checkbox"/>	
		<small>creates a bridge over specified interface(s)</small>	
Enable STP		<input type="checkbox"/>	
		<small>Enables the Spanning Tree Protocol on this bridge</small>	
Interface		<input type="checkbox"/> Ethernet Adapter: "bond0" <input checked="" type="checkbox"/> Ethernet Adapter: "eth0" (lan) <input checked="" type="checkbox"/> Ethernet Adapter: "eth1" (lan) <input checked="" type="checkbox"/> Ethernet Adapter: "eth2" (lan) <input checked="" type="checkbox"/> Ethernet Adapter: "eth3" (lan)	

The following parameters are available in this section:

Parameter	Description
<b>Bridge interfaces</b>	Select this option to bridge this interface with another interface.
<b>Enable STP</b>	Select this option to enable the STP function on this interface. <b>Note:</b> This option is only available if Bridge mode is enabled.
<b>Interface</b>	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. <b>Note:</b> Multiple selections are only available when the Bridge interfaces option is selected. Normally, only one interface can be selected here.



## Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

### Common Configuration

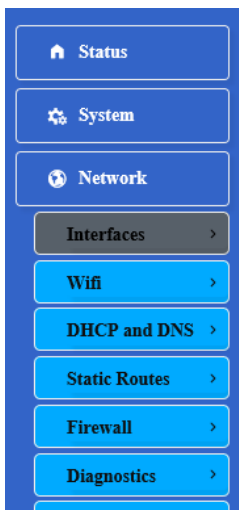
General Setup	Advanced Settings	Physical Settings	<b>Firewall Settings</b>
Create / Assign firewall-zone		<input checked="" type="radio"/> lan: lan: [interface icons]	
		<input type="radio"/> wan: (empty)	
		<input type="radio"/> unspecified -or- create: [input box]	

The following parameters are available in this section:

Parameter	Description
<b>Create / Assign Firewall-Zone</b>	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



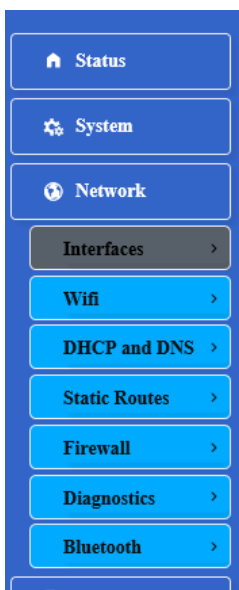
#### Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

##### Common Configuration

General Setup	
Status	<b>Uptime:</b> 0h 29m 51s <b>MAC-Address:</b> 00:19:70:BF:69:FC <b>RX:</b> 458.00 KB (6411 Pkts.) <b>TX:</b> 3.02 MB (5957 Pkts.) <b>IPv4:</b> 192.168.1.1/24
Protocol	DHCPv6 client
Really switch protocol?	SWITCH PROTOCOL

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



#### Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

##### Common Configuration

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Status	<b>Uptime:</b> 0h 30m 28s <b>MAC-Address:</b> 00:19:70:BF:69:FC <b>RX:</b> 470.42 KB (6605 Pkts.) <b>TX:</b> 3.12 MB (6144 Pkts.) <b>IPv4:</b> 192.168.1.1/24		
Protocol	DHCPv6 client		
Request IPv6-address	try		
Request IPv6-prefix of length	automatic		

The following parameters are available in this section:

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

- Status
- System
- Network
  - Interfaces
  - Wifi
  - DHCP and DNS
  - Static Routes
  - Firewall
  - Diagnostics
  - Bluetooth
- Logout

## Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

### Common Configuration

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Bring up on boot	<input checked="" type="checkbox"/>		
Use builtin IPv6-management	<input checked="" type="checkbox"/>		
Use default gateway	<input checked="" type="checkbox"/>		
	● If unchecked, no default route is configured		
Use DNS servers advertised by peer	<input checked="" type="checkbox"/>		
	● If unchecked, the advertised DNS server addresses are ignored		
Custom delegated IPv6-prefix	<input type="text"/>		
Override MAC address	<input type="text"/>		
Override MTU	<input type="text" value="1500"/>		

The following parameters are available in this section:

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

- Status
- System
- Network
  - Interfaces
  - Wifi
  - DHCP and DNS
  - Static Routes
  - Firewall
  - Diagnostics
  - Bluetooth
- Logout

## Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field : use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

### Common Configuration

General Setup	Advanced Settings	Physical Settings	Firewall Settings
Bridge interfaces	<input checked="" type="checkbox"/>		
	● creates a bridge over specified interface(s)		
Enable STP	<input type="checkbox"/>		
	● Enables the Spanning Tree Protocol on this bridge		
Interface	<input type="checkbox"/>	<input type="checkbox"/>	Ethernet Adapter: "bond0"
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Ethernet Adapter: "eth0" (lan)
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Ethernet Adapter: "eth1" (lan)
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Ethernet Adapter: "eth2" (lan)
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Ethernet Adapter: "eth3" (lan)

The following parameters are available in this section:

Parameter	Description
<b>Bridge interfaces</b>	Select this option to bridge this interface with another interface.
<b>Enable STP</b>	Select this option to enable the STP function on this interface. <b>Note:</b> This option is only available if Bridge mode is enabled.
<b>Interface</b>	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. <b>Note:</b> Multiple selections are only available when the Bridge interfaces option is selected. Normally, only one interface can be selected here.

- [Status](#)
- [System](#)
- [Network](#)
- Interfaces
- [Wifi](#)
- [DHCP and DNS](#)
- [Static Routes](#)

## Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network use **VLAN** notation **INTERFACE.VLANID** (e.g.: eth0.1).

### Common Configuration

General Setup
Advanced Settings
Physical Settings
Firewall Settings

Create / Assign firewall-zone

**lan:**

**wan:** (empty)

unspecified -or- create:

The following parameters are available in this section:

Parameter	Description
<b>Create / Assign Firewall-Zone</b>	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

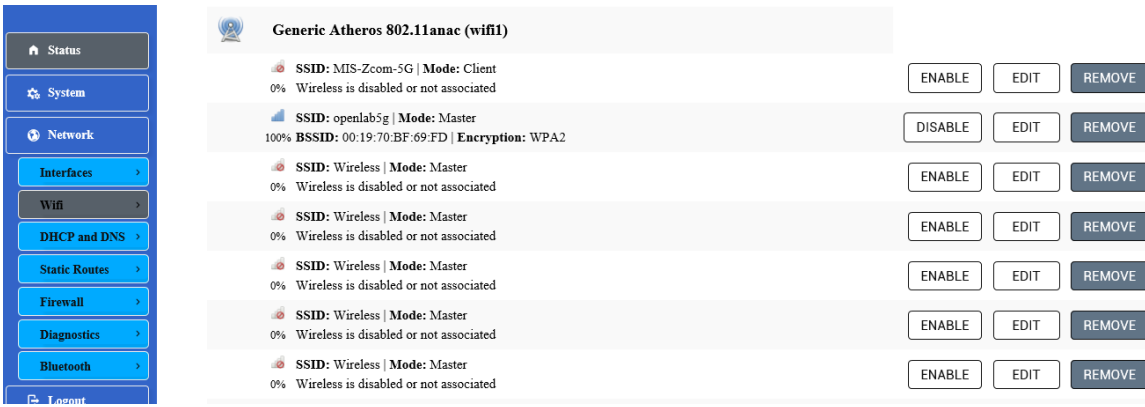
This page is used to display and configure the 802.11 wireless settings.

- [Status](#)
- [System](#)
- Network
- [Interfaces](#)
- Wifi
- [DHCP and DNS](#)
- [Static Routes](#)
- [Firewall](#)
- [Diagnostics](#)
- [Bluetooth](#)
- [Logout](#)

## Wireless Overview

**Generic Atheros 802.11abgn (wifi0)**

<b>SSID:</b> Wireless   <b>Mode:</b> Master 0% Wireless is disabled or not associated	<input type="button" value="ENABLE"/> <input type="button" value="EDIT"/> <input type="button" value="REMOVE"/>
<b>SSID:</b> Wireless   <b>Mode:</b> Master 0% Wireless is disabled or not associated	<input type="button" value="ENABLE"/> <input type="button" value="EDIT"/> <input type="button" value="REMOVE"/>
<b>SSID:</b> Wireless   <b>Mode:</b> Master 0% Wireless is disabled or not associated	<input type="button" value="ENABLE"/> <input type="button" value="EDIT"/> <input type="button" value="REMOVE"/>
<b>SSID:</b> Wireless   <b>Mode:</b> Master 0% Wireless is disabled or not associated	<input type="button" value="ENABLE"/> <input type="button" value="EDIT"/> <input type="button" value="REMOVE"/>
<b>SSID:</b> Wireless   <b>Mode:</b> Master 0% Wireless is disabled or not associated	<input type="button" value="ENABLE"/> <input type="button" value="EDIT"/> <input type="button" value="REMOVE"/>
<b>SSID:</b> Wireless   <b>Mode:</b> Master 0% Wireless is disabled or not associated	<input type="button" value="ENABLE"/> <input type="button" value="EDIT"/> <input type="button" value="REMOVE"/>

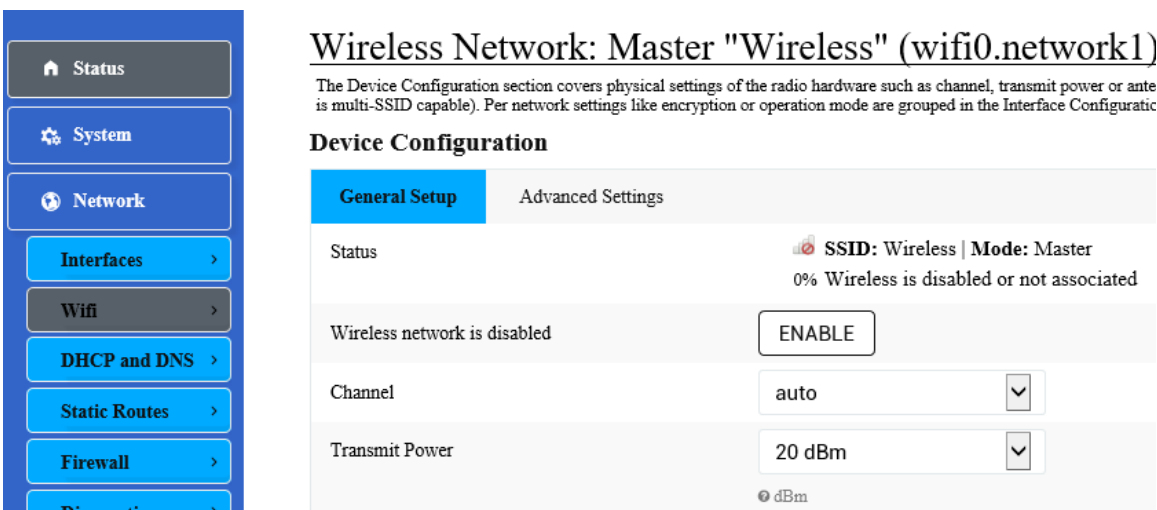


The following parameters are available in this section:

Parameter	Description
<b>Generic Atheros 802.11abgn (wifi0)</b>	Displays information about the generic Atheros IEEE 802.11abgn (wifi0) interface. <ul style="list-style-type: none"> <li>Channel - Displays the wireless channel number and frequency.</li> <li>Bitrate - Displays the current data rate (in megabits per second) through the wireless interface.</li> <li>SSID - Displays the SSID hosted by the wireless interface.</li> <li>Mode - Displays the configuration mode of the wireless interface.</li> <li>BSSID - Displays the BSSID (Basic Service Set Identifier) hosted by the wireless interface.</li> <li>Encryption - Displays the wireless encryption used on the wireless interface.</li> </ul>
<b>Generic Atheros 802.11anac(wifi1)</b>	Displays information about the generic Atheros IEEE 802.11anac (wifi1) interface. <ul style="list-style-type: none"> <li>Channel - Displays the wireless channel number and frequency.</li> <li>Bitrate - Displays the current data rate (in megabits per second) through the wireless interface.</li> <li>SSID - Displays the SSID hosted by the wireless interface.</li> <li>Mode - Displays the configuration mode of the wireless interface.</li> <li>BSSID - Displays the BSSID hosted by the wireless interface.</li> <li>Encryption - Displays the wireless encryption used on the wireless interface.</li> </ul>

#### 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
<b>Status</b>	Displays a summary of the wireless configuration on this wireless interface. <ul style="list-style-type: none"> <li>Signal Strength - Displays the wireless signal strength.</li> <li>Mode - Displays the wireless operating mode of the wireless interface.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• SSID - Displays the SSID hosted by the wireless interface.</li> <li>• BSSID - Displays the BSSID hosted by the wireless interface.</li> <li>• Encryption - Displays the wireless encryption used on the wireless interface.</li> <li>• Channel - Displays the wireless channel number and frequency.</li> <li>• TX-Power - Displays the TX (transmit) power of the wireless interface.</li> <li>• Signal - Displays the wireless signal strength (in dBm) on the wireless interface.</li> <li>• Noise - Displays the wireless noise level (in dBm) on the wireless interface.</li> <li>• Bitrate - Displays the active data bitrate (in megabits per second) through the wireless interface.</li> <li>• Country - Display the country setting on the wireless interface.</li> </ul>
<b>Wireless Network is Enabled</b>	Displays the current status of the wireless interface.
<b>Channel</b>	<p>Select the wireless channel for the wireless interface here. The range is from 1 (2.412 GHz) to 11 (2.462 GHz).</p> <p>Select the auto option to allow the AP to automatically determine the best wireless channel for this interface.</p> <p>Select the custom option to manually entry the channel number.</p>
<b>Transmit Power</b>	Select the wireless transmit power for the interface here.

- Status
- System
- Network
  - Interfaces >
  - Wifi >
  - DHCP and DNS >

### Wireless Network: Master "Wireless" (wifi0.network1)

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are share is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.

#### Device Configuration

General Setup	Advanced Settings
Mode	802.11axg
HT mode	20MHz
Country Code	156

The following parameters are available in this section:

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

- Status
- System
- Network
  - Interfaces >
  - Wifi >
  - DHCP and DNS >
  - Static Routes >
  - Firewall >
  - Diagnostics >
  - Bluetooth >
- Logout

#### Interface Configuration

General Setup	Wireless Security	MAC-Filter	Advanced Settings
ESSID(length:1-32)	Wireless		
Mode	Access Point		
Network	<input checked="" type="checkbox"/> lan: <input type="checkbox"/> wwan: <input type="checkbox"/> create: <input type="text"/>		
Ⓞ Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.			
Hide ESSID	<input type="checkbox"/>		
Short GI	400 ns		

The following parameters are available in this section:

Parameter	Description
<b>ESSID</b>	Enter the ESSID (Extended SSID) here.
<b>Mode</b>	Select the wireless mode for the interface here. Options to choose from are Access Point.
<b>Network</b>	Select the network interface to attach to this wireless interface here. Select the <i>create</i> option to enter and create a new network interface.
<b>Hide ESSID</b>	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.
<b>Short GI</b>	Select the short GI to decrease the time between data characters being sent.

- DHCP and DNS
>
- Static Routes
>
- Firewall
>

**Interface Configuration**

General Setup
Wireless Security
MAC-Filter
Advanced Settings

Encryption No Encryption ▼

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. WPA3 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.

- Interfaces
>
- Wifi
>
- DHCP and DNS
>
- Static Routes
>
- Firewall
>
- Diagnostics
>

**Interface Configuration**

General Setup
Wireless Security
MAC-Filter
Advanced Settings

Encryption WPA2-PSK ▼

Cipher Force CCMP (AES) ▼

Key  🗑️

The following parameters are available in this section:

Parameter	Description
<b>Encryption</b>	After selecting the WPA2-PSK option, the following settings are available.
<b>Cipher</b>	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.
<b>Key</b>	Enter the WPA2 passphrase here.

- Interfaces >
- Wifi >
- DHCP and DNS >
- Static Routes >
- Firewall >

### Interface Configuration

General Setup	Wireless Security	MAC-Filter	Advanced Settings
Encryption	WPA3-SAE <input type="button" value="v"/>		
Cipher	Force CCMP (AES) <input type="button" value="v"/>		
Key	<input style="width: 100%;" type="text"/> <input type="button" value="🔄"/>		

The following parameters are available in this section:

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

- 🏠 Status
- ⚙️ System
- 🌐 Network
- Interfaces >
- Wifi >
- DHCP and DNS >
- Static Routes >
- Firewall >
- Diagnostics >
- Bluetooth >
- 🚪 Logout

### Interface Configuration

General Setup	Wireless Security	MAC-Filter	Advanced Settings
Encryption	WPA2-EAP <input type="button" value="v"/>		
Cipher	Force CCMP (AES) <input type="button" value="v"/>		
Radius-Authentication-Server	<input style="width: 100%;" type="text"/>		
Radius-Authentication-Port	<input style="width: 100%;" type="text"/> <small>🔊 Default 1812</small>		
Radius-Authentication-Secret	<input style="width: 100%;" type="text"/> <input type="button" value="🔄"/>		
Radius-Accounting-Server	<input style="width: 100%;" type="text"/>		
Radius-Accounting-Port	<input style="width: 100%;" type="text"/> <small>🔊 Default 1813</small>		
Radius-Accounting-Secret	<input style="width: 100%;" type="text"/> <input type="button" value="🔄"/>		

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

- DHCP and DNS >
- Static Routes >
- Firewall >

**Interface Configuration**

General Setup	Wireless Security	MAC-Filter	Advanced Settings
MAC-Address Filter		disable	▼

The following parameters are available in this section:

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

- Wifi >
- DHCP and DNS >
- Static Routes >
- Firewall >

**Interface Configuration**

General Setup	Wireless Security	MAC-Filter	Advanced Settings
MAC-Address Filter		Allow listed only	▼
MAC-List			📄

The following parameters are available in this section:

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

- Wifi >
- DHCP and DNS >
- Static Routes >
- Firewall >

**Interface Configuration**

General Setup	Wireless Security	MAC-Filter	Advanced Settings
MAC-Address Filter		Allow all except listed	▼
MAC-List			📄

The following parameters are available in this section:

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



**Interface Configuration**

General Setup | Wireless Security | MAC-Filter | **Advanced Settings**

802.11h

Separate Clients   
⊙ Prevents client-to-client communication

MAX USERS(1-512)

WMM Mode

QoS Priority Mapping

Voice

Video

Background

Best effort

The following parameters are available in this section:

Parameter	Description
<b>802.11h</b>	Select this option to enable 802.11h amendment here.
<b>Separate Clients</b>	Select to enable the function that separates client-to-client communication here.
<b>MAX Users</b>	Enter the max users from 1 to 512.
<b>WMM Mode</b>	Select this option to enable the WMM (Wi-Fi Multimedia) mode here.
<b>QoS Priority Mapping</b>	Select this option to enable the QoS Priority Mapping mode here.
<b>Voice / Vedeo / Background / Best effort</b>	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:

**Wireless Network: Client "MIS-Zcom-5G" (wifi1.network1)**

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selectic is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.

**Device Configuration**

General Setup | Advanced Settings

Status 📶 **SSID: MIS-Zcom-5G | Mode: Client**  
0% Wireless is disabled or not associated

Wireless network is disabled

Channel

Transmit Power    
⊙ dBm

The following parameters are available in this section:

Parameter	Description
<b>Status</b>	Displays a summary of the wireless configuration on this wireless interface. <ul style="list-style-type: none"> <li>• Signal Strength - Displays the wireless signal strength.</li> <li>• Mode - Displays the wireless operating mode of the wireless interface.</li> <li>• SSID - Displays the SSID hosted by the wireless interface.</li> <li>• BSSID - Displays the BSSID hosted by the wireless interface.</li> <li>• Encryption - Displays the wireless encryption used on the wireless interface.</li> <li>• Channel - Displays the wireless channel number and frequency.</li> <li>• TX-Power - Displays the TX (transmit) power of the wireless interface.</li> <li>• Signal - Displays the wireless signal strength (in dBm) on the wireless interface.</li> <li>• Noise - Displays the wireless noise level (in dBm) on the wireless interface.</li> <li>• Bitrate - Displays the active data bitrate (in megabits per second) through the wireless interface.</li> <li>• Country - Display the country setting on the wireless interface.</li> </ul>
<b>Wireless Network is Enabled</b>	Displays the current status of the wireless interface.
<b>Channel</b>	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.
<b>Transmit Power</b>	Select the wireless transmit power for the interface here.

- 🏠 Status
- ⚙️ System
- 🌐 Network
  - 🔌 Interfaces >
  - 📶 Wifi >
  - 🌐 DHCP and DNS >
  - 📍 Static Routes >

### Wireless Network: Client "MIS-Zcom-5G" (wifi1.network1)

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection (is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.

#### Device Configuration

General Setup	Advanced Settings
Mode	802.11axa <input type="button" value="v"/>
HT mode	20MHz <input type="button" value="v"/>
Country Code	156

The following parameters are available in this section:

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



**Interface Configuration**

General Setup | Wireless Security | MAC-Filter | Advanced Settings

ESSID(length:1-32)

Mode

Network  lan:  wwan:  create:

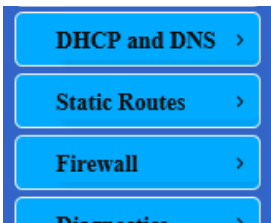
Choose the network(s) you want to attach

Hide ESSID

Short GI

The following parameters are available in this section:

Parameter	Description
<b>ESSID</b>	Enter the ESSID (Extended SSID) here.
<b>Mode</b>	Select the wireless mode for the interface here. Options to choose from are Access Point.
<b>Network</b>	Select the network interface to attach to this wireless interface here. Select the <i>create</i> option to enter and create and new network interface.
<b>Hide ESSID</b>	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.
<b>Short GI</b>	Select the short GI to decrease the time between data characters being sent.



**Interface Configuration**

General Setup | **Wireless Security** | MAC-Filter | Advanced Settings

Encryption

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. WPA3 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.

- Interfaces >
- Wifi >
- DHCP and DNS >
- Static Routes >
- Firewall >

**Interface Configuration**

General Setup	Wireless Security	MAC-Filter	Advanced Settings
Encryption	WPA2-PSK <input type="button" value="v"/>		
Cipher	Force CCMP (AES) <input type="button" value="v"/>		
Key	<input style="width: 100%;" type="password" value="••••••••"/> <input style="float: right; width: 20px; height: 20px; border: none; background-color: #ccc; cursor: pointer;" type="button"/>		

The following parameters are available in this section:

Parameter	Description
<b>Encryption</b>	After selecting the WPA2-PSK option, the following settings are available.
<b>Cipher</b>	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.
<b>Key</b>	Enter the WPA2 passphrase here.

- Interfaces >
- Wifi >
- DHCP and DNS >
- Static Routes >
- Firewall >

**Interface Configuration**

General Setup	Wireless Security	MAC-Filter	Advanced Settings
Encryption	WPA3-SAE <input type="button" value="v"/>		
Cipher	Force CCMP (AES) <input type="button" value="v"/>		
Key	<input style="width: 100%;" type="password" value="••••••••"/> <input style="float: right; width: 20px; height: 20px; border: none; background-color: #ccc; cursor: pointer;" type="button"/>		

The following parameters are available in this section:

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

- Status
- System
- Network
- Interfaces >
- Wifi >
- DHCP and DNS >
- Static Routes >
- Firewall >
- Diagnostics >
- Bluetooth >
- Logout

**Interface Configuration**

General Setup	Wireless Security	MAC-Filter	Advanced Settings
Encryption	WPA2-EAP <input type="button" value="v"/>		
Cipher	Force CCMP (AES) <input type="button" value="v"/>		
Radius-Authentication-Server	<input style="width: 100%;" type="text"/>		
Radius-Authentication-Port	<input style="width: 100%;" type="text"/> <small>Default 1812</small>		
Radius-Authentication-Secret	<input style="width: 100%;" type="password" value="••••••"/> <input style="float: right; width: 20px; height: 20px; border: none; background-color: #ccc; cursor: pointer;" type="button"/>		
Radius-Accounting-Server	<input style="width: 100%;" type="text"/>		
Radius-Accounting-Port	<input style="width: 100%;" type="text"/> <small>Default 1813</small>		
Radius-Accounting-Secret	<input style="width: 100%;" type="password" value="••••••"/> <input style="float: right; width: 20px; height: 20px; border: none; background-color: #ccc; cursor: pointer;" type="button"/>		

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

- DHCP and DNS >
- Static Routes >
- Firewall >
- Disruption >

**Interface Configuration**

General Setup
Wireless Security
MAC-Filter
Advanced Settings

MAC-Address Filter

disable
▼

The following parameters are available in this section:

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

- Wifi >
- DHCP and DNS >
- Static Routes >
- Firewall >
- Disruption >

**Interface Configuration**

General Setup
Wireless Security
MAC-Filter
Advanced Settings

MAC-Address Filter

Allow listed only
▼

MAC-List

+

The following parameters are available in this section:

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

- Wifi >
- DHCP and DNS >
- Static Routes >
- Firewall >
- Disruption >

**Interface Configuration**

General Setup
Wireless Security
MAC-Filter
Advanced Settings

MAC-Address Filter

Allow all except listed
▼

MAC-List

+

The following parameters are available in this section:

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

- Status
- System
- Network
- Interfaces**
- Wifi
- DHCP and DNS
- Static Routes
- Firewall
- Diagnostics
- Bluetooth
- Logout

**Interface Configuration**

General Setup	Wireless Security	MAC-Filter	Advanced Settings
802.11h		<input type="checkbox"/>	
Separate Clients		<input type="checkbox"/>	<small>Prevents client-to-client communication</small>
MAX USERS(1-512)		<input type="text" value="256"/>	
WMM Mode		<input checked="" type="checkbox"/>	
QoS Priority Mapping		<input type="checkbox"/>	
Voice		<input type="text" value="priority 4(high)"/>	<input type="button" value="v"/>
Video		<input type="text" value="priority 3"/>	<input type="button" value="v"/>
Background		<input type="text" value="priority 2"/>	<input type="button" value="v"/>
Best effort		<input type="text" value="priority 1(low)"/>	<input type="button" value="v"/>

The following parameters are available in this section:

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

**4.3.3.2.1.3. Associated Stations**

- DHCP and DNS
- Static Routes
- Firewall
- Diagnostics
- Bluetooth

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
No information available						

The following parameters are available in this section:

Parameter	Description
<b>Signal Strength</b>	Displays the signal strength of the associated wireless station.
<b>SSID</b>	Displays the SSID of the associated wireless station.
<b>MAC Address</b>	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.

- Status
- System
- Network
  - Interfaces >
  - Wifi >
  - DHCP and DNS >
  - Static Routes >
  - Firewall >
  - Diagnostics >
  - Bluetooth >
  - Logout

## DHCP and DNS

Dnsmasq is a combined [DHCP-Server](#) and [DNS-Forwarder](#) for [NAT](#) firewalls

### Server Settings

General Settings

Resolv and Hosts Files

TFTP Settings

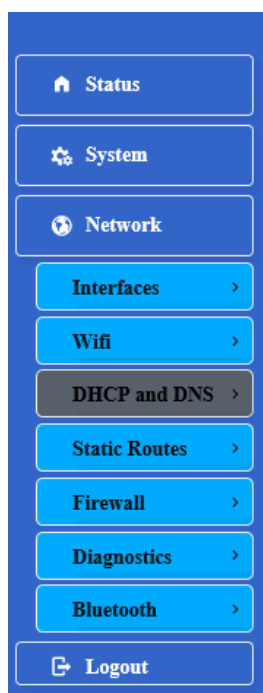
Advanced Settings

Domain required	<input checked="" type="checkbox"/>
	ⓘ Don't forward DNS-Requests without DNS-Name
Authoritative	<input checked="" type="checkbox"/>
	ⓘ This is the only DHCP in the local network
Local server	<input type="text" value="/lan/"/>
	ⓘ Local domain specification. Names matching this domain are never forward
Local domain	<input type="text" value="lan"/>
	ⓘ Local domain suffix appended to DHCP names and hosts file entries
Log queries	<input type="checkbox"/>
	ⓘ Write received DNS requests to syslog
	ⓘ Write received DNS requests to syslog
DNS forwardings	<input type="text" value="/example.org/10.1.2.3"/>
	ⓘ List of DNS servers to forward requests to
Rebind protection	<input checked="" type="checkbox"/>
	ⓘ Discard upstream RFC1918 responses
Allow localhost	<input checked="" type="checkbox"/>
	ⓘ Allow upstream responses in the 127.0.0.0/8 range, e.g. fo
Domain whitelist	<input type="text" value="ihost.netflix.com"/>
	ⓘ List of domains to allow RFC1918 responses for

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
<b>DNS Forwardings</b>	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.
<b>Rebind Protection</b>	Select this option to discard upstream RFC 1918 (Address Allocation for Private Internets) responses.
<b>Allow Localhost</b>	Select this option to allow upstream responses in the 127.0.0.0/8 (loopback purposes) range.
<b>Domain Whitelist</b>	Enter the domain name that is whitelisted for RFC 1918 responses here. More than one entry can be created.



## DHCP and DNS

Dnsmasq is a combined [DHCP-Server](#) and [DNS-Forwarder](#) for [NAT](#) firewalls

### Server Settings

General Settings	Resolv and Hosts Files	TFTP Settings	Advanced Settings
Use <a href="#">/etc/ethers</a>	<input checked="" type="checkbox"/>		
	<small>Read <a href="#">/etc/ethers</a> to configure the <a href="#">DHCP-Server</a></small>		
Leasefile	<input type="text" value="/tmp/dhcp.leases"/>		
	<small>file where given <a href="#">DHCP</a>-leases will be stored</small>		
Ignore resolve file	<input type="checkbox"/>		
Resolve file	<input type="text" value="/tmp/resolv.conf.auto"/>		
	<small>local <a href="#">DNS</a> file</small>		
Ignore <a href="#">/etc/hosts</a>	<input type="checkbox"/>		
Additional Hosts files	<input type="text"/>		

The following parameters are available in this section:

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



- Status
- System
- Network
  - Interfaces >
  - Wifi >
  - DHCP and DNS >**
  - Static Routes >
  - Firewall >

## DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

### Server Settings

General Settings	Resolv and Hosts Files	<b>TFTP Settings</b>	Advanced Settings
Enable TFTP server		<input checked="" type="checkbox"/>	
TFTP server root		<input type="text" value="/"/>	<small>ⓘ Root directory for files served via TFTP</small>
Network boot image		<input type="text" value="pxelinux.0"/>	<small>ⓘ Filename of the boot image advertised to clients</small>

The following parameters are available in this section:

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

- Status
- System
- Network
  - Interfaces >
  - Wifi >
  - DHCP and DNS >**
  - Static Routes >
  - Firewall >
  - Diagnostics >
  - Bluetooth >
  - Logout

## DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

### Server Settings

General Settings	Resolv and Hosts Files	TFTP Settings	<b>Advanced Settings</b>
Suppress logging		<input type="checkbox"/>	<small>ⓘ Suppress logging of the routine operation of these pr</small>
Allocate IP sequentially		<input type="checkbox"/>	<small>ⓘ Allocate IP addresses sequentially, starting from the</small>
Filter private		<input checked="" type="checkbox"/>	<small>ⓘ Do not forward reverse lookups for local networks</small>
Filter useless		<input type="checkbox"/>	<small>ⓘ Do not forward requests that cannot be answered by</small>
Localise queries		<input checked="" type="checkbox"/>	

🏠 Status

⚙️ System

🌐 Network

🔌 Interfaces >

📶 Wifi >

📡 DHCP and DNS >

📍 Static Routes >

🔥 Firewall >

🔍 Diagnostics >

📶 Bluetooth >

🚪 Logout

**Expand hosts**  ➤ Add local domain suffix to names served from hosts files

**No negative cache**  ➤ Do not cache negative replies, e.g. for not existing domains

**Strict order**  ➤ DNS servers will be queried in the order of the resolvfile

**Bogus NX Domain Override**  ➤ List of hosts that supply bogus NX domain results

**DNS server port**  ➤ Listening port for inbound DNS queries

**DNS query port**  ➤ Fixed source port for outbound DNS queries

**Max. DHCP leases**  ➤ Maximum allowed number of active DHCP leases

**Max. EDNS0 packet size**  ➤ Maximum allowed size of EDNS.0 UDP packets

**Max. concurrent queries**  ➤ Maximum allowed number of concurrent DNS queries

The following parameters are available in this section:

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

- Status
- System
- Network

**Active DHCP Leases**

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
----------	--------------	-------------	---------------------

There are no active leases.

The following parameters are available in this section:

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

- Status
- System
- Network

**Active DHCPv6 Leases**

Hostname	IPv6-Address	DUID	Leasetime remaining
----------	--------------	------	---------------------

There are no active leases.

The following parameters are available in this section:

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

- Network
- Interfaces >
- Wifi >
- DHCP and DNS >**
- Static Routes >
- Firewall >
- Diagnostics >

**Static Leases**

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a co-served.

Use the Add Button to add a new lease entry. The MAC-Address identifies the host, the IPv4-Address specifies to the fixed address to use and the Hostname is assigned as symbolic n

Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)
----------	-------------	--------------	-------------------

This section contains no values yet

ADD

The following parameters are available in this section:

Parameter	Description
<b>Hostname / MAC Address / IPv4 Address / IPv6-Suffix (hex)</b>	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
<b>Interface</b>	Select the interface for the static IPv4 route here. Options to choose from are lan and wan.
<b>Target</b>	Enter the target IPv4 address or IPv4 network address for the static IPv4 route here.
<b>IPv4 Netmask</b>	Enter the IPv4 subnet mask for the static IPv4 route here.
<b>IPv4 Gateway</b>	Enter the IPv4 address of the gateway for the static IPv4 route here.
<b>Metric / MTU</b>	Enter the Metric / MTU for the static IPv4 route here.

The following parameters are available in this section:

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

**Firewall - Zone Settings**  
The firewall creates zones over your network interfaces to control network traffic flow.

**General Settings**

- Enable SYN-flood protection
- Drop invalid packets
- Input: accept
- Output: accept
- Forward: reject

**Zones**

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping
lan: lan ⇒ wan	accept	accept	accept	<input type="checkbox"/>	<input type="checkbox"/>

The following parameters are available in this section:

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

**Zones**

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping
lan: lan ⇒ wan	accept	accept	accept	<input type="checkbox"/>	<input type="checkbox"/>
wan:(empty) ⇒ REJECT	reject	accept	reject	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

ADD

The following parameters are available in this section:

Parameter	Description
<b>Zone &gt;&gt; Forwarding</b>	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:

- 🏠 Status
- ⚙️ System
- 🌐 Network
  - 🔌 Interfaces >
  - 📶 Wifi >
  - DHCP and DNS >
  - Static Routes >
  - Firewall >**
  - Diagnostics >
  - Bluetooth >
- 🚪 Logout

## Firewall - Zone Settings - Zone "newzone"

### Zone "newzone"

This section defines common properties of "newzone". The input and output options set the default policies for traffic entering and leaving the zone. Covered networks specifies which available networks are members of the zone.

General Settings	Advanced Settings
Name	newzone
Input	accept
Output	accept
Forward	reject
Masquerading	<input type="checkbox"/>
MSS clamping	<input type="checkbox"/>
Covered networks	<input type="checkbox"/> lan:

The following parameters are available in this section:

Parameter	Description
<b>Name</b>	Enter the name for the firewall zone here.
<b>Input</b>	Select the input (incoming) action here. Options to choose from are reject, drop, and accept.
<b>Output</b>	Select the output (outgoing) action here. Options to choose from are reject, drop, and accept.
<b>Forward</b>	Select the forwarding action here. Options to choose from are reject, drop, and accept.
<b>Masquerading</b>	Select this option to enable the masquerading function on the firewall zone.
<b>MSS clamping</b>	Select this option to enable the MSS clamping function on the firewall zone.
<b>Covered networks</b>	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.

- 🏠 Status
- ⚙️ System
- 🌐 Network
  - 🔌 Interfaces >
  - 📶 Wifi >
  - DHCP and DNS >
  - Static Routes >
  - Firewall >**
  - Diagnostics >
  - Bluetooth >

## Firewall - Zone Settings - Zone "newzone"

### Zone "newzone"

This section defines common properties of "newzone". The input and output options set the default policies for traffic entering and leaving the zone. Covered networks specifies which available networks are members of the zone.

General Settings	Advanced Settings
Restrict to address family	IPv4 and IPv6
Restrict Masquerading to given source subnets	0.0.0.0/0
Restrict Masquerading to given destination subnets	0.0.0.0/0
Force connection tracking	<input type="checkbox"/>
Enable logging on this zone	<input type="checkbox"/>

The following parameters are available in this section:

Parameter	Description
<b>Restrict to address family</b>	Select the IP address family that will be restricted here. Options to choose from are IPv4 and IPv6, IPv4 only, and IPv6 only.
<b>Restrict Masquerading to given source subnets</b>	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.
<b>Restrict Masquerading to given destination subnets</b>	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.
<b>Force connection tracking</b>	Select this option to force connection tracking.
<b>Enable logging on this zone</b>	Select this option enable logging on this firewall zone.

- System
- Network
- Interfaces >
- Wifi >
- DHCP and DNS >
- Static Routes >
- Firewall >

### Inter-Zone Forwarding

The options below control the forwarding policies between this zone (newzone) and other zones. Destination zones cover forwarded traffic **originating from "newzone"**. Sou from other zones **targeted at "newzone"**. The forwarding rule is **unidirectional**, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as wel

Allow forward to destination zones:

lan: lan: [IP icons]

wan: (empty)

Allow forward from source zones:

lan: lan: [IP icons]

wan: (empty)

The following parameters are available in this section:

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

- Status
- System
- Network
- Interfaces >
- Wifi >

### Diagnostics

#### Network Utilities

dev.openwrt.org      dev.openwrt.org      dev.openwrt.org

IPv4 [v]    PING      TRACEROUTE      NSLOOKUP

Install iputils-traceroute6 for IPv6 traceroute

The following parameters are available in this section:

Parameter	Description
<b>Ping</b>	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
<b>Traceroute</b>	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.
<b>Nslookup</b>	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:

**Diagnostics**  
**Network Utilities**

dev.openwrt.org      dev.openwrt.org      dev.openwrt.org

IPv4 ▾    PING    TRACEROUTE    NSLOOKUP

Install iputils-traceroute6 for IPv6 traceroute

**Collecting data...**

```
ping: bad address 'dev.openwrt.org'
```

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

**Diagnostics**  
**Network Utilities**

dev.openwrt.org      dev.openwrt.org      dev.openwrt.org

IPv4 ▾    PING    **TRACEROUTE**    NSLOOKUP

Install iputils-traceroute6 for IPv6 traceroute

**Collecting data...**

```
traceroute: bad address 'dev.openwrt.org'
```

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

**Diagnostics**  
**Network Utilities**

dev.openwrt.org      dev.openwrt.org      dev.openwrt.org

IPv4 ▾    PING    TRACEROUTE    **NSLOOKUP**

Install iputils-traceroute6 for IPv6 traceroute

**Collecting data...**

```
;; connection timed out; no servers could be reached
```



## CHAPTER 5. TECHNICAL SPECIFICATIONS

Physical			
<b>Dimensions (L x W x H)</b>		296(L) x 92(W) x 283(H) mm	
<b>Weight</b>		2.5KG	
<b>Device</b>		SP250/ SP250-S5	
<b>WAN/PoE In Port</b>		One 10/100/1000/2500Mbps	
<b>LAN Port</b>		One 10/100/1000/2500Mbps	
<b>Antenna</b>	<b>2.4GHz</b>	Internal PIFA	
	<b>5GHz</b>	Internal PIFA	
<b>Power Supply</b>		DC 53V, 600mA (PoE)	
<b>Power Consumption</b>		Max. 25 Watts	
Wireless			
<b>Frequency Bands</b>	<b>Country</b>	<b>2.4GHz Radio</b>	<b>5GHz Radio</b>
	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
<b>Operating Channels (@20MHz)</b>	<b>Country</b>	<b>2.4GHz Radio</b>	<b>5GHz Radio</b>
	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
<b>Bandwidth</b>	2.4GHz: 20 / 40 MHz 5GHz: 20 / 40 / 80 MHz		
<b>Wireless Security</b>	<b>Security:</b> Open System, WPA2-PSK, WPA2-EAP, WPA3-SAE <b>Extensible Authentication Protocol (EAP) types:</b> WPA2/WPA3-Personal (TKIP and AES)		
<b>Operating Mode</b>	Thin AP (TAP) / Fat AP (FAP)		
<b>Wireless SSIDs</b>	2.4 GHz (Up to 8 SSIDs), 5.8 GHz (Up to 8 SSIDs)		
Environmental			
	<b>Temperature</b>		<b>Humidity</b>
<b>Operating</b>	-40°C to 65°C (-40°F to 149°F)		5% to 95 (Non-condensing)
<b>Storage</b>	-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, NEGLIGENCE, 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.



**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=&material\\_type=56](https://www.zcom.com.tw/index/downloads?keyword=&material_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  $1 \text{ mW/cm}^2$ ，送測產品實測值為  $0.12152 \text{ mW/cm}^2$ ，建議使用時至少距離人體  $51 \text{ cm}$ 」。

## 6.4. Optional Accessories

PN	Item	Picture	SP250	SP250-S5
64-000004-L7N	mounting bracket		yes	yes
64-000003-ZNN	Waterproof		yes	yes
64-000517-00N	Waterproof		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](http://www.zcom.com.tw)



Z-COM, Inc.  
www.zcom.com.tw

Copyright © 2020 Z-COM Inc. All rights reserved.