



BlitzFunk

AW32R, CW32R

MANUAL

Release 2026/5



Revision History

Version	Change
<i>Release 2025/6</i>	• Initial release
<i>Release 2025/7</i>	• Added information on exposed network interfaces and services • Added description of <i>find</i> function • Added information on update notifications via mail
<i>Release 2025/8</i>	• Added description of VLAN segmentation • Added description of the <i>replace</i> function • Added description for time history display of received signal strength • Improved description of status view • Updated required legal information according to 2014/53/EU
<i>Release 2025/9</i>	• Description of VLAN segmentation revised • Extended manual for AW32R and CW32R device types
<i>Release 2025/10</i>	• Description of firmware update process improved
<i>Release 2026/2</i>	• Added FCC and ISED legal text
<i>Release 2026/3</i>	• Description of changing the IP address behavior added

Table of Contents

1	General Information	5
1.1	Product Names.....	5
1.2	Highlighting of Tips and Warnings	5
1.3	Legal Information.....	5
1.4	Open Source Software	6
1.5	Radio Frequencies and Transmit Power	6
1.6	CE	7
1.7	UKCA.....	7
1.8	WEEE Disposal and Recycling Information	8
2	About the Product	10
2.1	Intended Use	10
2.2	Physical Interfaces: Client.....	11
2.3	Physical Interfaces: Access Point	13
2.4	LED Indicators.....	16
3	Device Installation	18
3.1	Hardware Installation.....	18
3.2	Antenna Orientation and Device Positioning.....	18
3.3	Wall or Ceiling Mounting.....	20
3.4	Power and Data Connection.....	20
4	Device Configuration.....	23
4.1	Accessing the Configuration Interface.....	23
4.2	Password Protection.....	24
4.3	Assignment of Channel Groups	25
4.4	Extending Coverage with Additional Access Points	29
4.5	Increasing Capacity with Additional Access Points.....	31
4.6	Seperation into virtual Networks (VLANs)	32
4.7	Changing the Device Configuration During Operation	37
4.8	Replacing Devices.....	43
4.9	Locating Devices.....	44
		45

5 System Diagnostics 46

 5.1 *Link Status Monitoring 46*

6 Device Maintenance 51

 6.1 *Firmware Updates..... 51*

 6.2 *Factory Reset..... 54*

7 Technical Data..... 55

8 Troubleshooting and Support..... 57

 8.1 *Troubleshooting..... 57*

 8.2 *Support..... 58*

1 General Information

1.1 Product Names

This manual contains information on the products:

- BlitzFunk® Access Point AW32R
- BlitzFunk® Client CW32R

1.2 Highlighting of Tips and Warnings

Throughout the text the following symbols are used:



Tip: This symbol provides helpful guidance or additional details to assist with product use.



WARNING: This symbol indicates critical safety information. Ignoring these warnings may result in damage or injury.

1.3 Legal Information

This wireless system is classified as a Category 2 receiver in accordance with ETSI EN 300 440.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

The devices BlitzFunk AW32R und CW32R comply with ETSI electromagnetic compatibility (EMC) standards for industrial environments (Class A devices) and residential environments (Class B devices). Compliance with EMC regulations was verified using shielded Ethernet cables. To ensure continued compliance, always use shielded Ethernet cables when operating this equipment.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to

provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This equipment complies with EN IEC 62311, FCC and RSS-102 radiation exposure limits set forth for an uncontrolled environment. This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC RSS-102 établies pour un environnement non contrôlé.

Cet émetteur doit être installé pour fournir une distance de séparation d'au moins 20 cm de toutes les personnes et ne doit pas être colocalisé ou fonctionner en conjonction avec une autre antenne ou émetteur.

1.4 Open Source Software

Information about open-source licenses used can be viewed in the access point’s web interface under the *Support* section.

1.5 Radio Frequencies and Transmit Power

Frequency	Transmit Power (EIRP, single antenna port)	
	EU	USA / Canada
2.402 GHz – 2.472 GHz	max. 70 mW	max. 500 mW
5.17 GHz – 5.25 GHz	max. 80 mW	max. 100 mW
5.735 GHz – 5.875 GHz	max. 10 mW	max. 200 mW
5.945 GHz – 6.425 GHz	max. 70 mW	max. 60 mW (AW32R) max. 13 mW (CW32R)
6.425 GHz – 7.125 GHz	-	max. 60 mW (AW32R) max. 13 mW (CW32R)

In AT, BE, BG, CY, CZ, DE, DK, EE, EL, ES, FI, FR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, RO, SE, SI, SK the system may only be used indoors in the frequency ranges 5.15 GHz to 5.35 GHz and 5.945 GHz to 6.425 GHz.

In Canada, the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems. Devices shall not be used for control of or communications with unmanned aircraft systems. Operation shall be limited to indoor use only. Operation on oil platforms, automobiles, trains, maritime vessels and aircraft shall be prohibited except for on large aircraft flying above 3,048 m (10,000 ft).

Au Canada, les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement à une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes mobiles par satellite utilisant les mêmes canaux. Les dispositifs ne doivent pas être utilisés pour la commande ou la communication avec des systèmes d'aéronefs sans pilote. Le fonctionnement est limité à une utilisation à l'intérieur seulement. L'exploitation sur des plateformes pétrolières, dans les automobiles, les trains, les navires maritimes et les aéronefs est interdite, sauf à bord de gros aéronefs volant à une altitude supérieure à 3 048 m (10 000 pieds).

In the US, FCC regulations restrict the operation of this device to indoor use only. The operation of this device is prohibited on oil platforms, cars, trains, boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet in the 5.925-6.425 GHz band. Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.

1.6 CE



Hereby, fuenfeinhalb Funksysteme GmbH declares that the radio equipment type BlitzFunk AW32R and CW32R is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address:

https://fuenfeinhalb.de/pdf/CE_Declaration_of_Conformity.pdf

1.7 UKCA



Hereby, fuenfeinhalb Funksysteme GmbH declares that the radio equipment type BlitzFunk AW32R and CW32R is in compliance with the relevant UK statutory requirements.

The full text of the UK declaration of conformity is available at the following internet address:

https://fuenfeinhalb.de/pdf/UK_Declaration_of_Conformity.pdf

1.8 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.

1.9 ISED

The devices AW32R and CW32R comply with ISED requirements.

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

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

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

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

1.10 WEEE Disposal and Recycling Information



All products bearing this symbol are waste electrical and electronic equipment (WEEE as in directive 2012/19/EU) which should not be mixed with unsorted household waste. Instead, you should protect human health and the environment by handing over your waste equipment to a designated collection point for the recycling of waste electrical and electronic equipment, appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. Please contact the installer or local authorities for more information about the location as well as terms and conditions of such collection points.

2 About the Product

2.1 Intended Use

The BlitzFunk product line is a wireless networking solution designed to deliver highly reliable real-time wireless connectivity for industrial environments. It may serve as a replacement for wired Ethernet in industrial applications and enables wireless connections for mobile systems.

A BlitzFunk network requires at least one access point and one or more clients. The system is fully transparent to common industrial Ethernet protocols (e.g., PROFINET, PROFIsafe, EtherNet/IP, OPC UA) and functions as a Layer 2 switch. Unlike traditional wireless Ethernet bridges, it is not restricted to point-to-point links.

BlitzFunk is ideal for small to medium-sized networks with 1 to 20 clients, and can scale to support up to 100 clients.

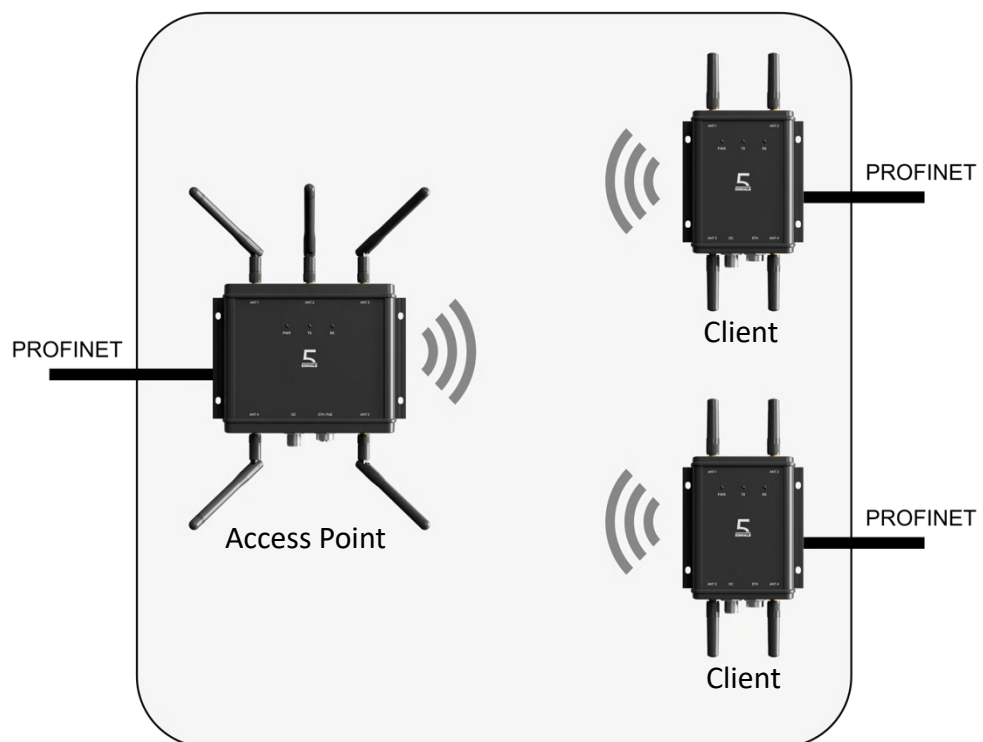


Figure 1 Example of a BlitzFunk access point and two BlitzFunk clients in an industrial Ethernet setup



WARNING: While measures have been taken to ensure high reliability at low latency of the wireless connection, wireless links remain subject to challenging propagation conditions and potential interference. This may result in data loss. Appropriate fail-safe mechanisms must be implemented to prevent injury and mitigate economic risks in the event of a communication failure.



WARNING: This equipment is not suitable for use in locations where children are likely to be present.

2.2 Physical Interfaces: Client

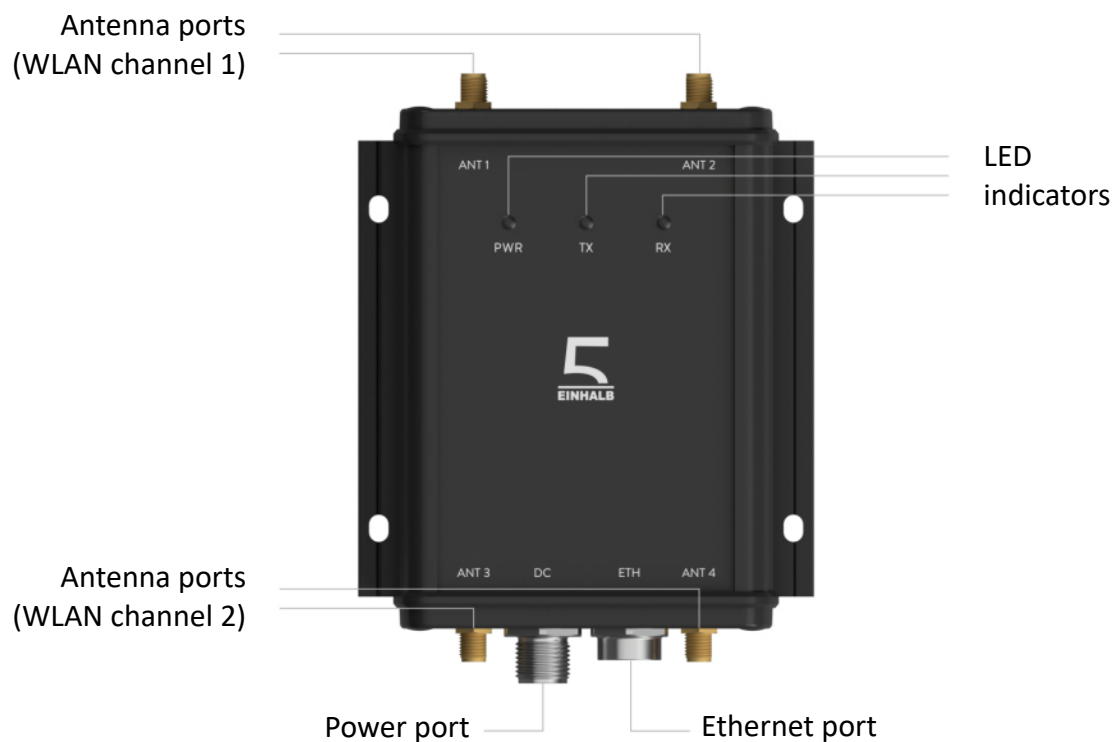


Figure 2 Front panel of a BlitzFunk client

Clients are powered via the device’s DC port using an external power supply. The data connection is established via the device's ETH port, which supports a 100 Mbit/s Ethernet connection.

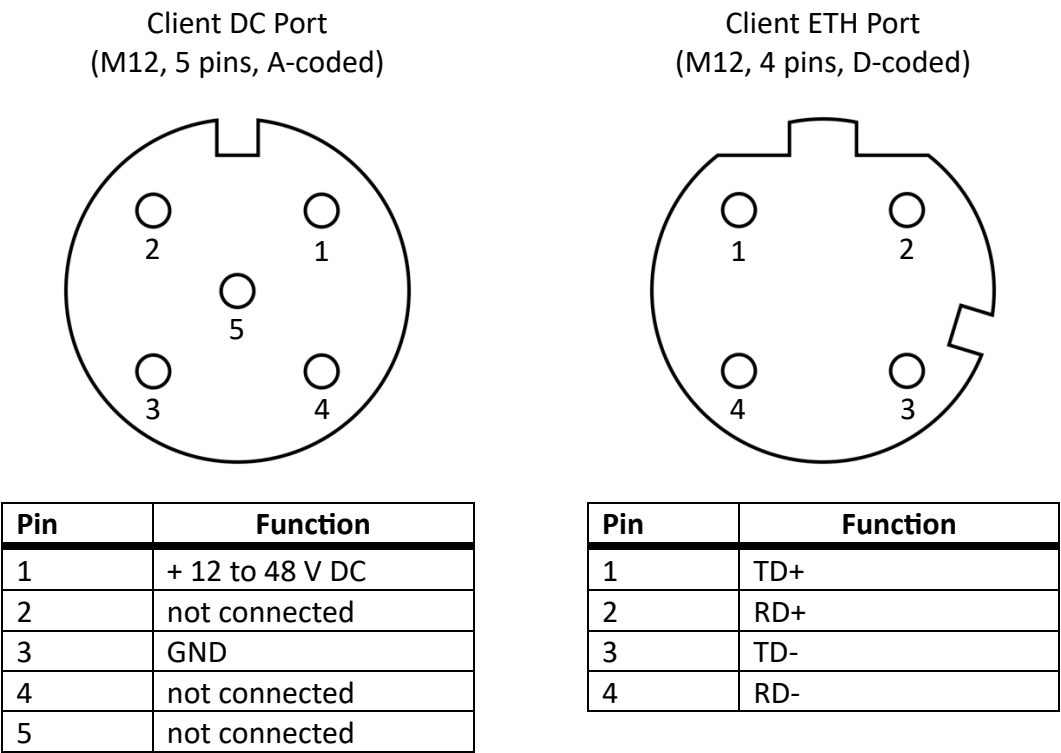


Figure 3 Pin mapping of client connectors (view towards device)

Tip: A reverse polarity protection is in place in case the external power supply is connected to the wrong pins at the DC port.

Clients have four RP-SMA female connectors (Reverse Polarity SubMiniature Version A) for attaching antennas. Each port serves different functions, such as exchange of setup messages, data transmission or reception, depending on the operating state of the device:

Interface	Direction	Function	Exposed Service
ANT1	RX / TX	WLAN channel 1: user data & device setup	Proprietary protocol
ANT2	RX	WLAN channel 1: user data & device setup	Proprietary protocol
ANT3	RX / TX	WLAN channel 2: user data	Proprietary protocol
ANT4	RX	WLAN channel 2: user data	Proprietary protocol
<i>ETH</i>	RX / TX	User data	DHCP client, ARP, ICMP

2.3 Physical Interfaces: Access Point

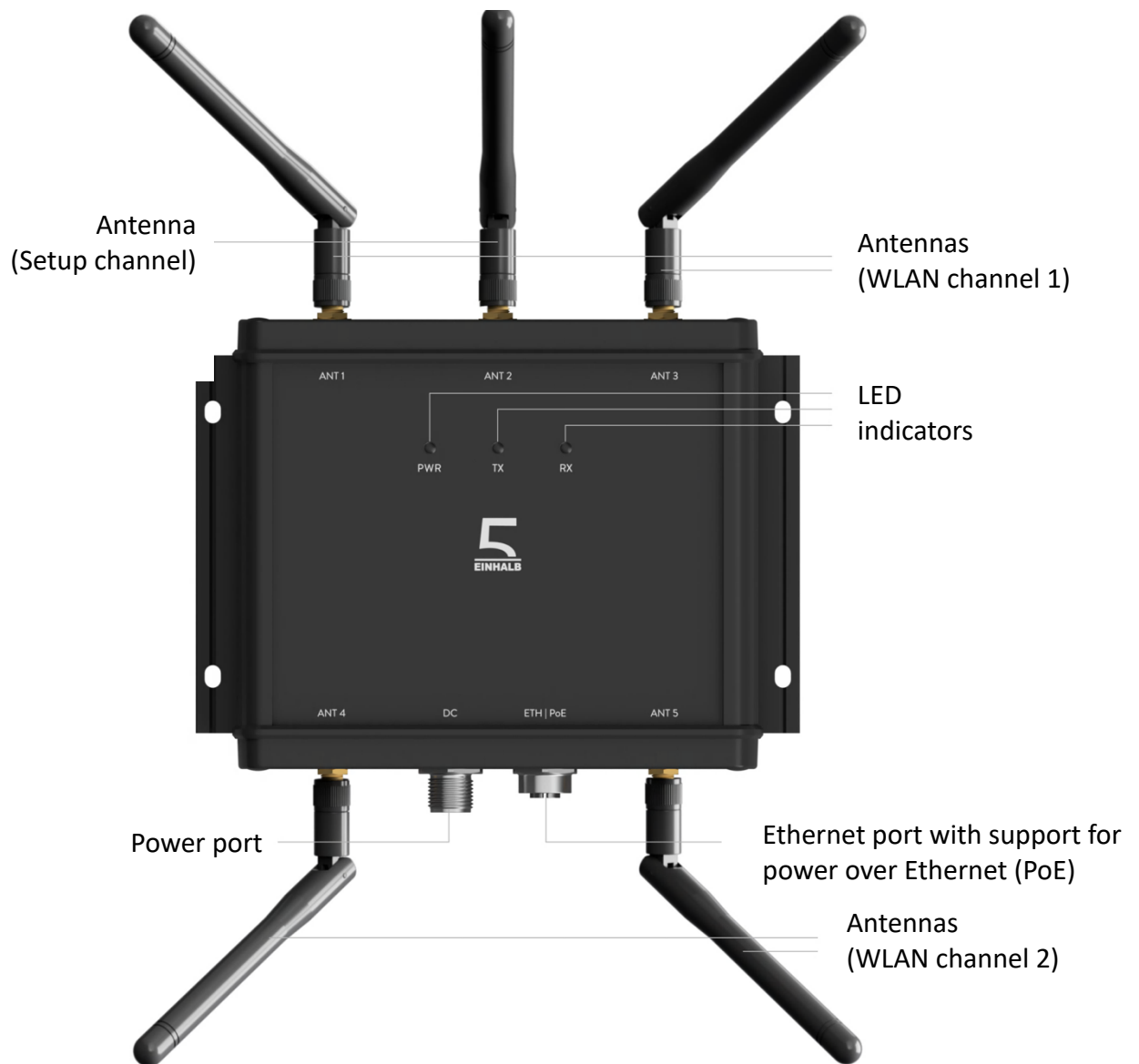


Figure 4 Front panel of a BlitzFunk access point

Access points can be powered either via the DC port using an external power supply or via Power over Ethernet (PoE) according to the IEEE 802.3af standard. Both PoE mode A and mode B are supported.

The data connection is established via the ETH port, which supports a 1000 Mbit/s Ethernet connection.

Access Point DC Port
(M12, 5 pins, A-coded)

Access Point ETH | PoE Port
(M12, 8 pins, X-coded)

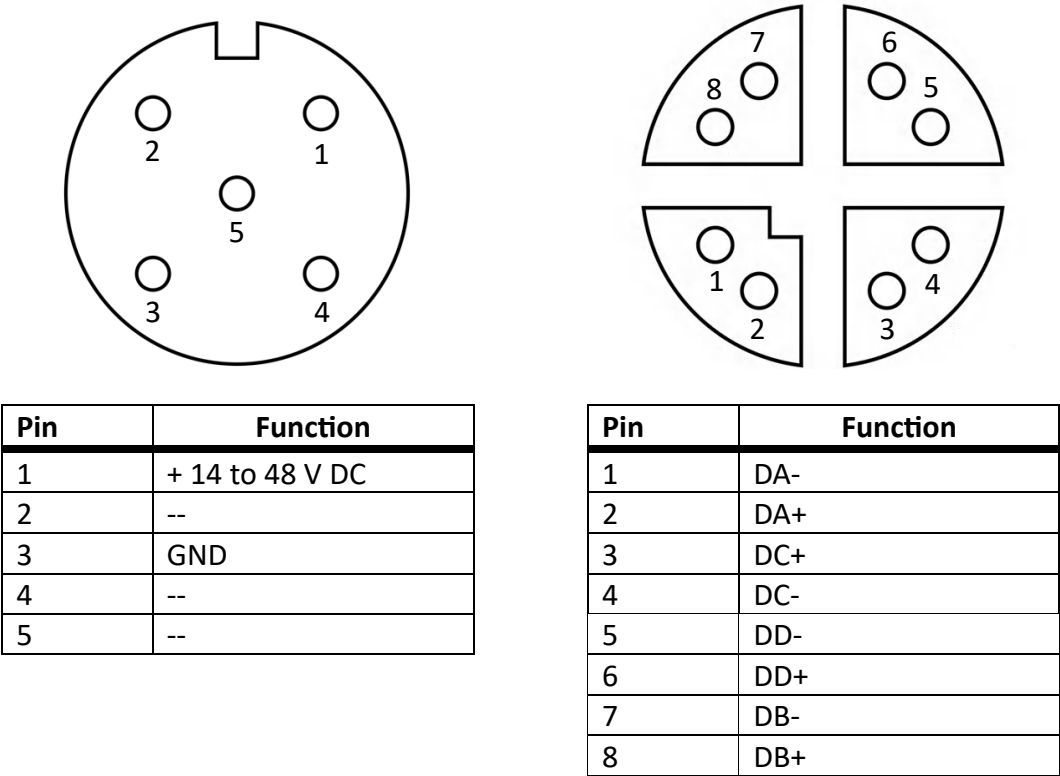


Figure 5 Pin mapping access point connectors (view towards device)

Access points have five non-detachable antennas. In addition to the clients, access points include a dedicated interface for device management, separate from the interfaces used for data transmission.

Interface	Direction	Function	Exposed Service
ANT1	RX/TX	WLAN channel 1: user data	Proprietary protocol
ANT2	RX / TX	Device setup	Proprietary protocol
ANT3	RX	WLAN channel 1: user data	Proprietary protocol
ANT4	RX / TX	WLAN channel 2: user data	Proprietary protocol
ANT5	RX	WLAN channel 2: user data	Proprietary protocol
ETH	RX / TX	HTTP-configuration interface, user data, access point coordination	Proprietary protocol, DHCP server, DHCP client, HTTP, ARP

2.4 LED Indicators

LED	Color	Status
PWR	Off	No power to device
	Yellow	Device is waiting for configuration
	White	<i>Pulsing:</i> device is starting <i>Permanently on:</i> device is ready for data
	Red	Error
TX	Off	No data is being transmitted wirelessly
	White	Data is being transmitted wirelessly
RX	Off	No data is being received wirelessly

	White	Data is being received wirelessly
<i>PWR/TX/RX</i>	Blue	Animation for finding a device
	Turquoise	Indication for a factory reset

3 Device Installation

3.1 Hardware Installation

Before using client devices, connect all included antennas to their designated antenna ports. Only use antennas that come with the device. Antennas should be fastened by hand tight or tightened with a maximum torque of 0.9 Nm. Access point devices come with antennas already attached.



WARNING: Powering the device without connecting all antennas to the RP-SMA ports may cause damage. Using only some antennas can result in the device not functioning as intended.



WARNING: Only antennas provided with this device shall be used. The use of any unauthorized or non-approved antennas may result in non-compliance with regulatory requirements and could cause harmful interference. Unauthorized modifications or substitutions may void the user's authority to operate this equipment.



Tip: For installations in tight spaces, such as interior-mounted equipment, clients can operate with reduced reliability by routing only the RX/TX ports to the exterior (e.g. ANT1 and ANT3). The other antennas are receive-only, they do not need to be RF-terminated if unused.

3.2 Antenna Orientation and Device Positioning

The angle of the antennas can impact both coverage and connection stability. For maximum range with line-of-sight, the antennas of access point and client must be aligned parallel to each other.



Figure 6 Recommended antenna positioning

Avoid placing antennas inside or behind metallic enclosures, such as control cabinets or within automated guided vehicles, as this will degrade signal quality significantly. If the device must be installed inside a metal enclosure, use RP-SMA extension cables to route the antennas to the outside.

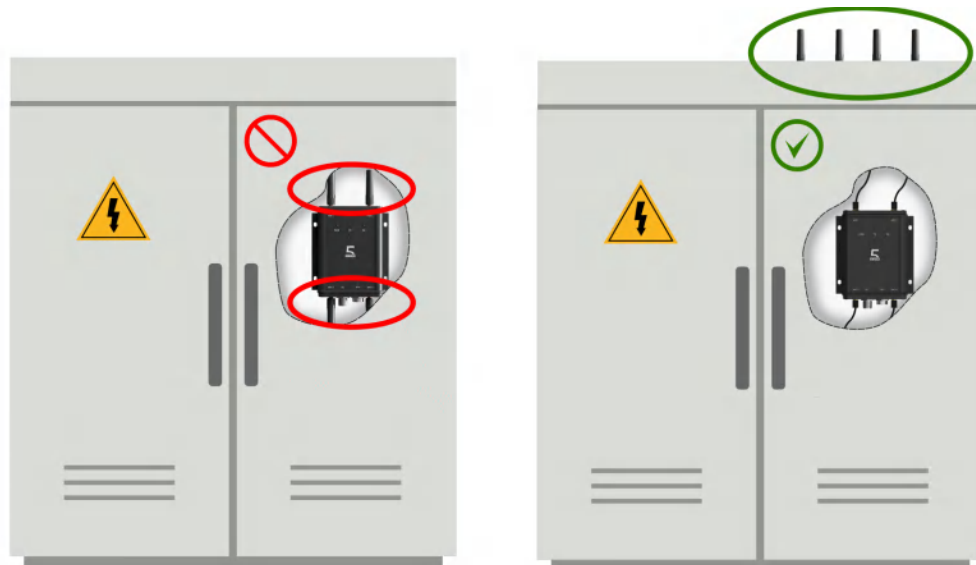


Figure 7 Antenna mounting outside of metallic enclosures

The achievable range of the system depends on environmental conditions. Optimal range is typically achieved when there is a clear line of sight between the access point and the client.



WARNING: This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

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

3.3 Wall or Ceiling Mounting

At the desired location, the device should be securely mounted to a wall or ceiling using its integrated mounting holes.



WARNING: To prevent injury from falling equipment, the device should be secured by an expert. Depending on the material of the wall or ceiling, suitable wall anchors have to be selected. It always needs to be verified that the mounting surface is stable and capable of bearing the weight of the device.

3.4 Power and Data Connection

Connect both the client and access points to power. They must be supplied with an external DC power source via the DC port. An access point device can alternatively be powered through its ETH/PoE port using Power over Ethernet (PoE).



WARNING: To ensure the safety of the product, the devices shall always be supplied with ES1 and LPS | PS2 | Class 2 power sources.

Pour garantir la sécurité du produit, les appareils doivent toujours être alimentés par des sources d'alimentation ES1 et LPS | PS2 | Classe 2.

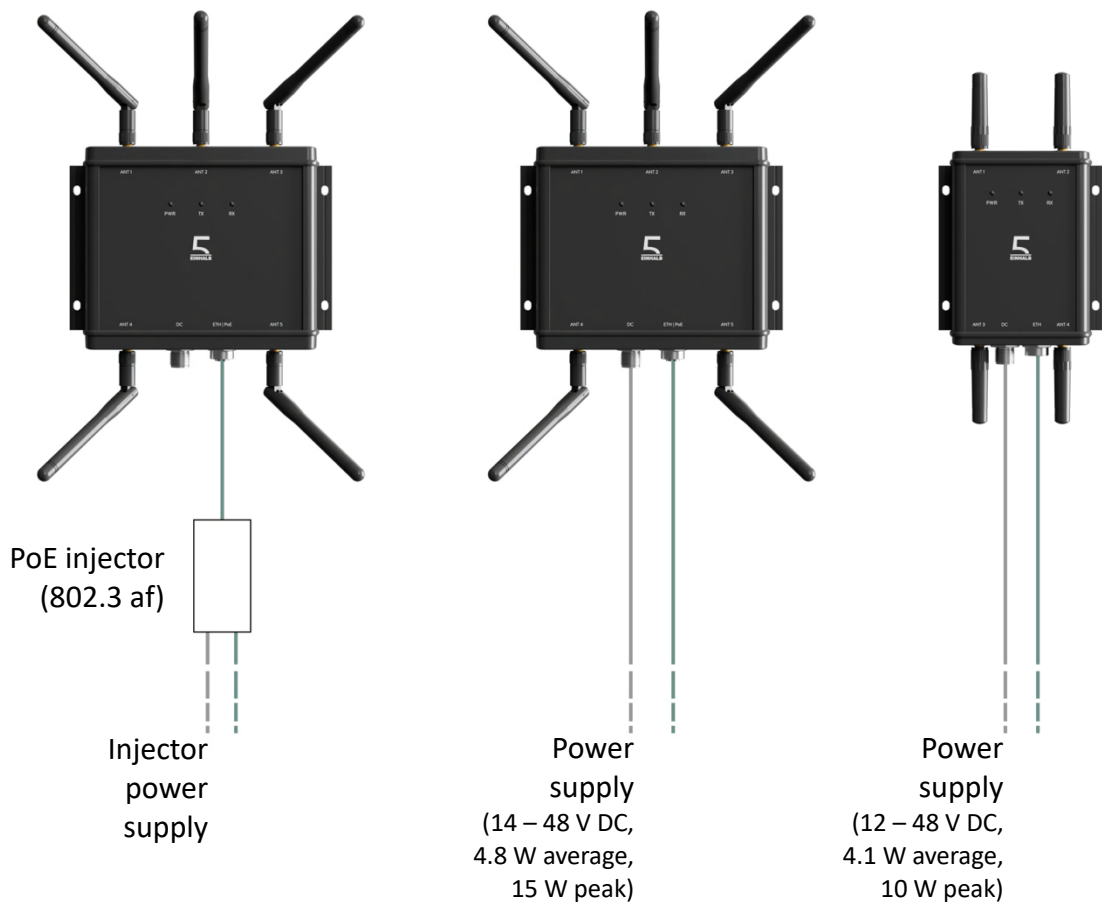


Figure 8 Options for powering clients and access point



Tip: If both DC and PoE are connected, the device will draw power from the DC supply. In this configuration, PoE will act as a backup in case the DC supply fails.

Connect the data ports of the devices to the end devices which shall establish connection. In systems with multiple access points, the ETH ports of all access points must be interconnected, for example via a network switch. To ensure proper synchronization between access points, the network infrastructure must support 1 Gbit/s Ethernet speeds and maintain a maximum latency of 50 microseconds. Typical Gigabit Ethernet switches forward packets in less than 15 microseconds,

allowing up to three switches in series. The VLAN ID 512 is used for communication between the access points. When a managed Ethernet switch is used to connect the access points, it must be ensured that traffic with this VLAN ID is forwarded to all connected access points.

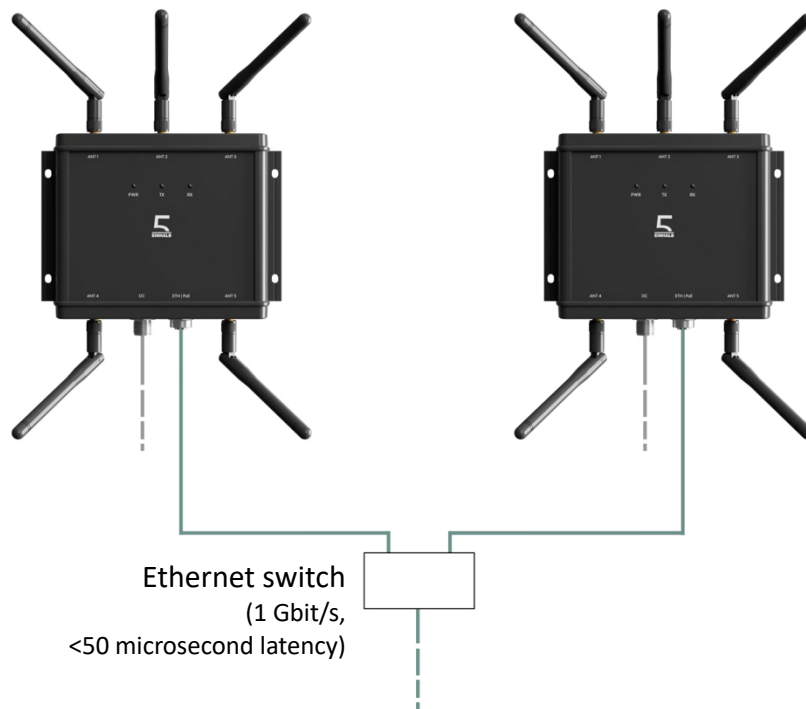


Figure 8 Access point connection in a setup consisting of multiple access points



WARNING: To maintain protection against dust and water ingress, both M12 ports must be connected. It is recommended to tighten the connectors to a torque of 0.6 Nm. To tighten the ports using a torque wrench, the antennas must be removed to allow access. If a port is not in use, it must be sealed with a suitable protective cap to preserve the device's protection rating.

4 Device Configuration

Before data transmission can take place, when powering the devices for the first time or when replacing existing ones, the system must be configured. Configuration is performed using the web-based interface of the access point, which can be accessed from any standard, up-to-date web browser. The following sections explain the available functions of the configuration interface using example setups.



Tip: Issues that may occur when using the system for the first time are summarized in chapter 8 (ref. *Troubleshooting*).

4.1 Accessing the Configuration Interface

To access the configuration interface, a computer is required with:

- a web-browser
- one free Ethernet port

Connect the computer via Ethernet to the access points that are awaiting configuration. Power must be supplied to the access points.

Clients that require configuration must be powered on and within wireless range of at least one access point. Clients must not be connected to the access points by cable, as this will create a network loop once the system is configured.



Tip: The system can be configured while already installed in its final location. Although a temporary connection to a computer is needed for configuration, the cabling used during configuration is the same as in the system's operational state.

By default, the configuration interface is accessible at:

`http://10.5.0.1`

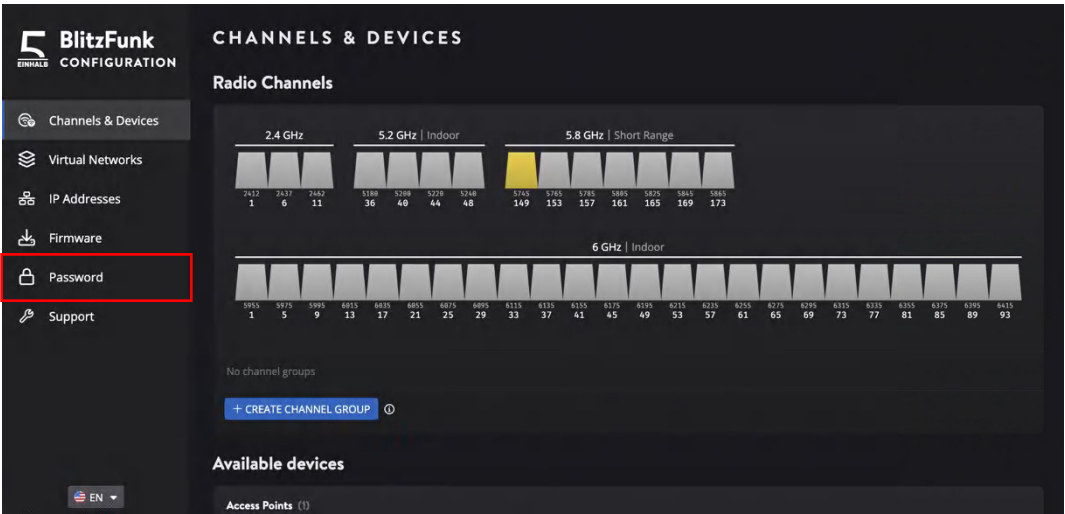
In networks with more than one BlitzFunk access point, the access point with the lowest serial number is automatically designated as the coordinating access point (coordinator). The web interface is provided by the coordinating access point.

In the factory default configuration, the coordinating Access Point operates with an integrated DHCP server enabled, assigning IP addresses in the range 10.5.0.12 to 10.5.0.254. The IP address and DHCP server settings of the coordinating Access Point can be configured through the configuration interface (ref. *Changing the IP Address Behaviour*).

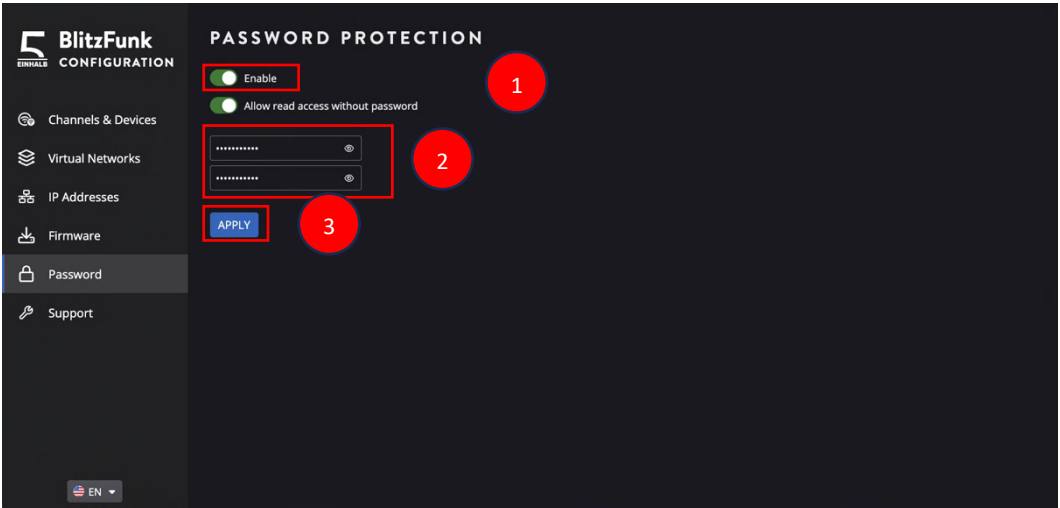
Ensure that the computer used for configuration has an IP address in the same subnet as the coordinating access point.

4.2 Password Protection

By default, the configuration interface is accessible from any device within the same network. To restrict access, you can set a password in the *Password* tab of the configuration interface. This ensures that only authorized users can modify system settings.



To set a password, click the *Enable* toggle, enter the desired password, and click *Apply*. You can choose whether read access (viewing without making changes) is allowed without a password or not.

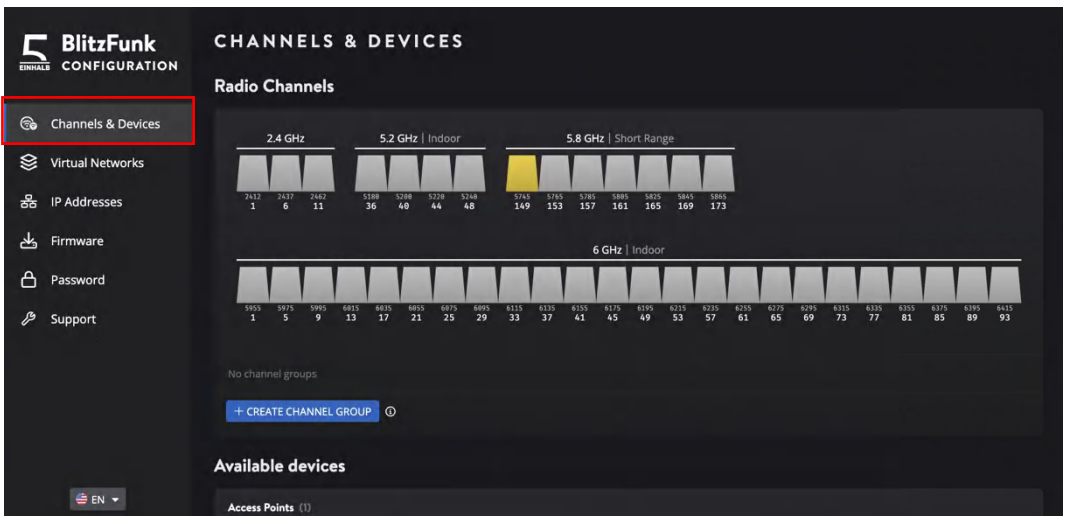


Tip: Please note that the HTTP connection to the web interface is not secured. For security reasons, ensure that the chosen password is not used anywhere else.

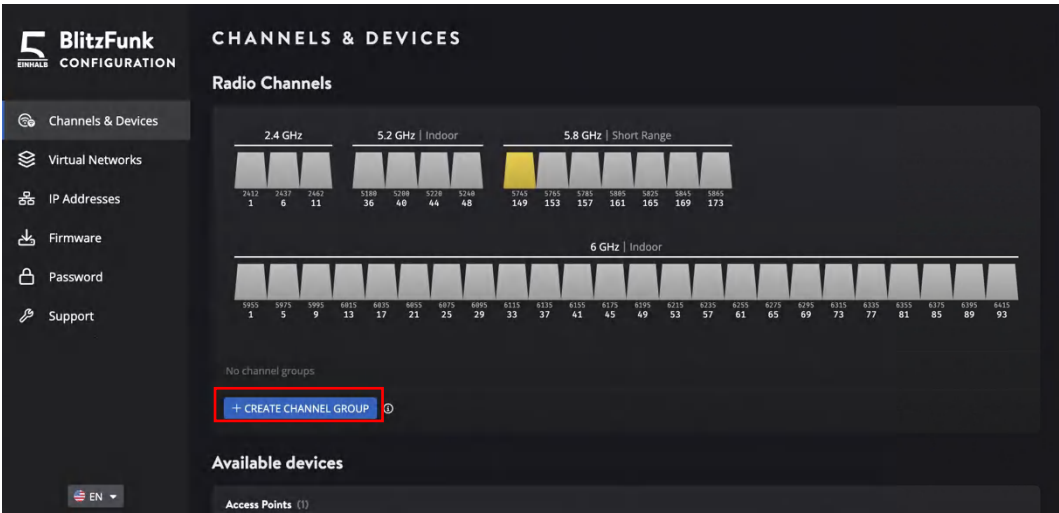
After applying, you are automatically logged in. You may log out via the *Log Out* Button.

4.3 Assignment of Channel Groups

Before data can be transmitted between devices, they need to be assigned to a channel group. To do this use the *Channels & Devices* tab.



BlitzFunk devices communicate within channel groups. A channel group uses two redundant 20 MHz channels for data transmission. To create a channel group, first select two operating channels by clicking *Create Channel Group*.



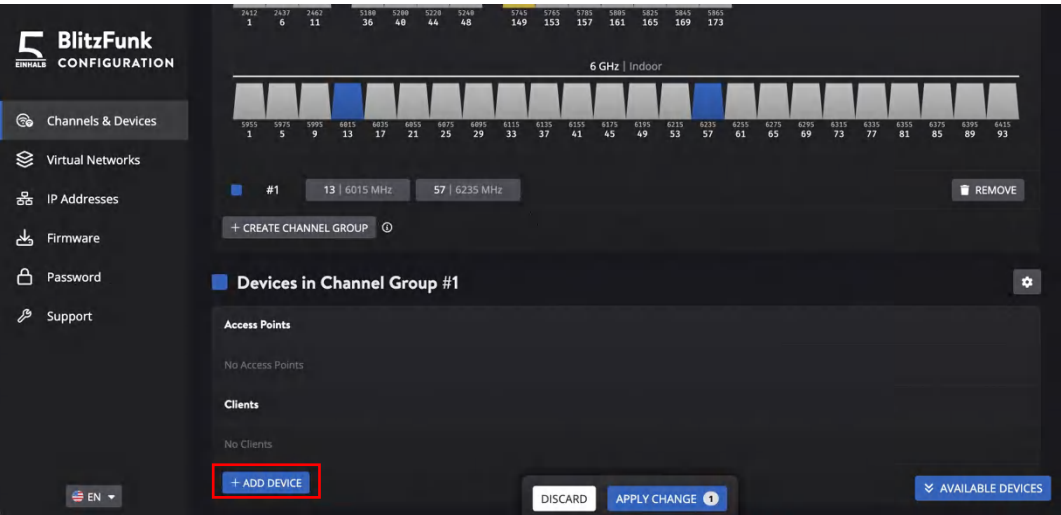
To increase the reliability of the system, it is recommended to separate the two channels with more than 100 MHz separation. Adjacent channels cannot be selected.

For device management, BlitzFunk uses channel 149 at 5745 MHz. This channel is currently fixed but will be made configurable in a future.

Tip: The achievable range depends on the legally permitted transmission power. At 2.4 and 5.2 GHz, greater ranges can be expected than at 5.8 and 6 GHz. Channels in the latter frequency ranges are therefore referred to as *Short Range*.

Tip: The frequency bands with shorter range at 5.8 GHz (5765 – 5865 MHz) and 6 GHz (5955 – 6415 MHz), are generally less crowded than other frequency bands and therefore more reliable than the lower frequencies.

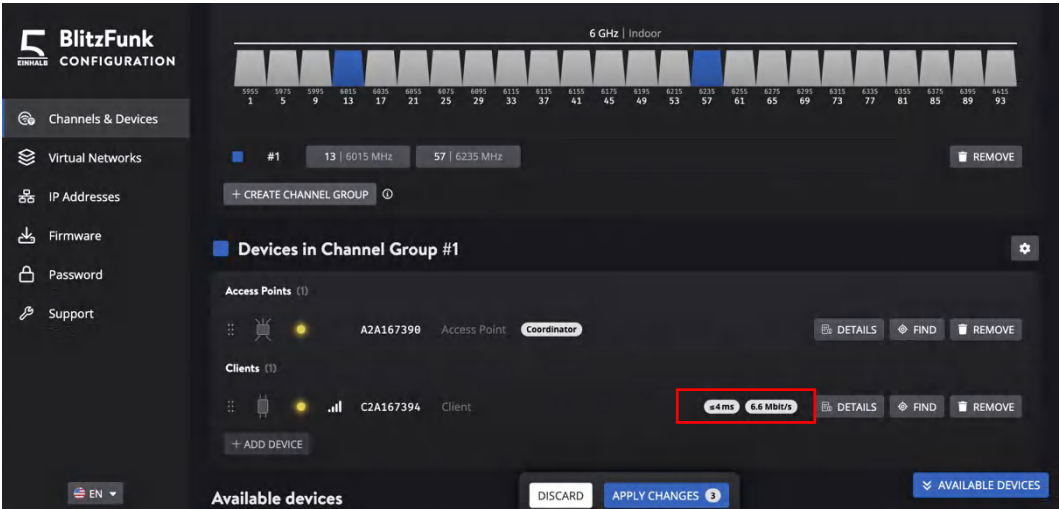
Add devices to a channel group by dragging and dropping them into it, or by selecting the desired devices using the *Add Device* button. Available devices are shown at the bottom in the *Available Devices* section. Access points are always available when connected via Ethernet. Clients are available when they are not assigned to any channel group (indicated by the yellow PWR LED), or when they cannot find an access point belonging to their channel group.



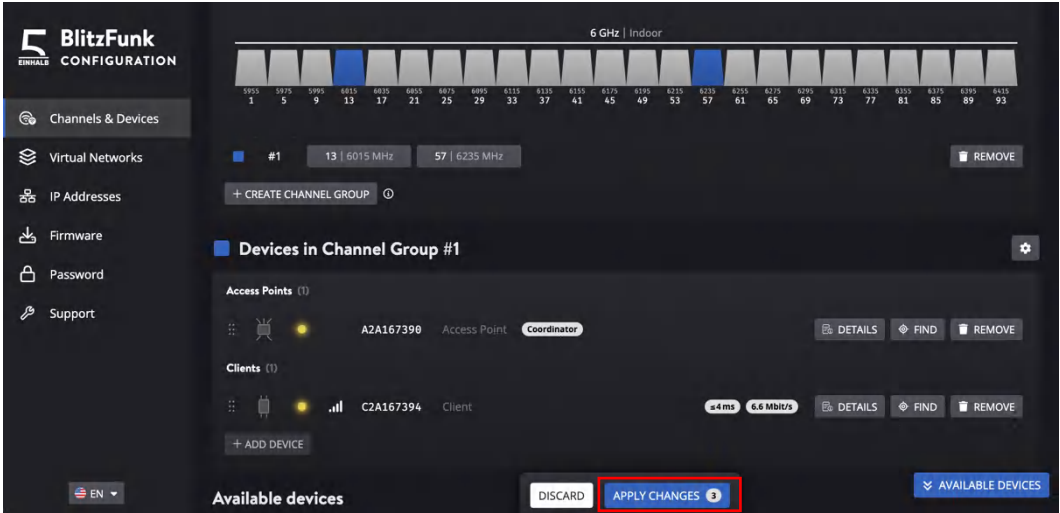
The number of clients in a channel group affects both latency and data throughput. The first client is connected with a data rate of 6 Mbit/s and a maximum one-way latency of 4 ms. Each additional client increases latency by 2 ms. The data rate is evenly distributed among all clients in a channel group. Some example values are provided in the table below.

Clients per Channel Group	Max. One-Way Latency [ms]	Data Rate [Mbit/s]
1	4	6
2	6	3
4	10	1.5
10	22	0.6
24	50	0.25
48	100	0.125

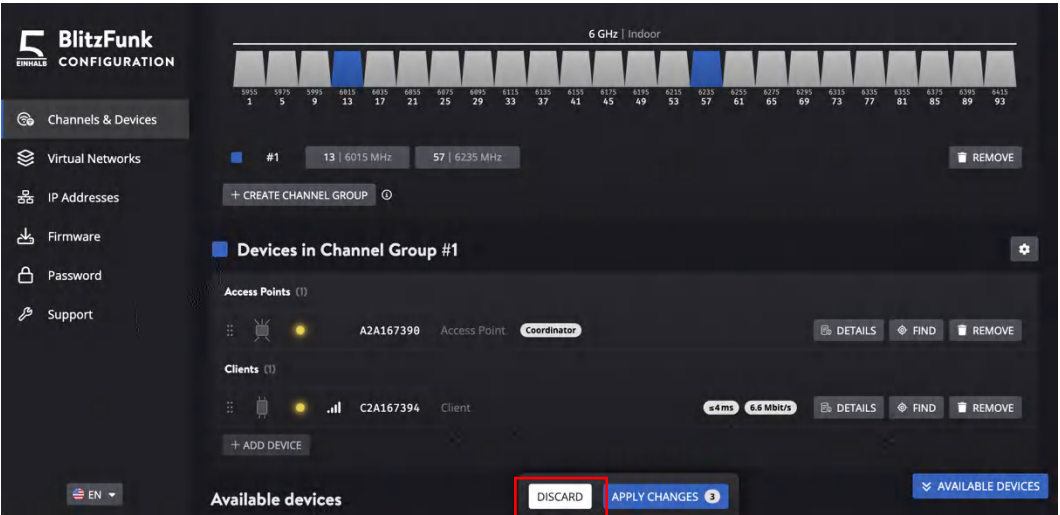
The expected maximum one-way latency and data rate are displayed for each client during configuration.



When changes to the configuration are pending, two buttons appear at the bottom center of the screen. To apply the configuration, click *Apply Changes*. As soon as at least one access point and one client have been assigned to a channel group, data transmission between the devices can begin, and the PWR LEDs of the devices will turn white.



Alternatively, pending changes can be reverted using the *Discard* option. The configuration interface will then be reloaded.



WARNING: Changing the configuration of devices that are already configured may cause an interruption in data transmission. To avoid unplanned downtime of your machines, please observe the instructions in the section *Changing the Device Configuration during Operation*.

4.4 Extending Coverage with Additional Access Points

To extend the coverage of a BlitzFunk network, additional access points can be assigned to a channel group. No additional channels are required for this since the access points coordinate with each other and use the same two channels.

Clients can move freely between access points within the same channel group without interruptions and without affecting latency or data rate (latency-free roaming).

For a stable connection, it must simply be ensured that the signal strength is sufficient at every possible client position (ref. *Link Status Monitoring*). To achieve this, an unobstructed line of sight to at least one of the access points should always be maintained. When using channels in the 6 GHz band, the distance to the nearest access point should be less than 40 meters.

To use this functionality, access points need to be connected via Gigabit-Ethernet (ref. *Power and Data Connection*) and placed with overlapping coverage. The connecting switch should ideally not have to process any other data traffic and should not exceed a latency of 50 microseconds for frame sizes up to 1522 bytes.

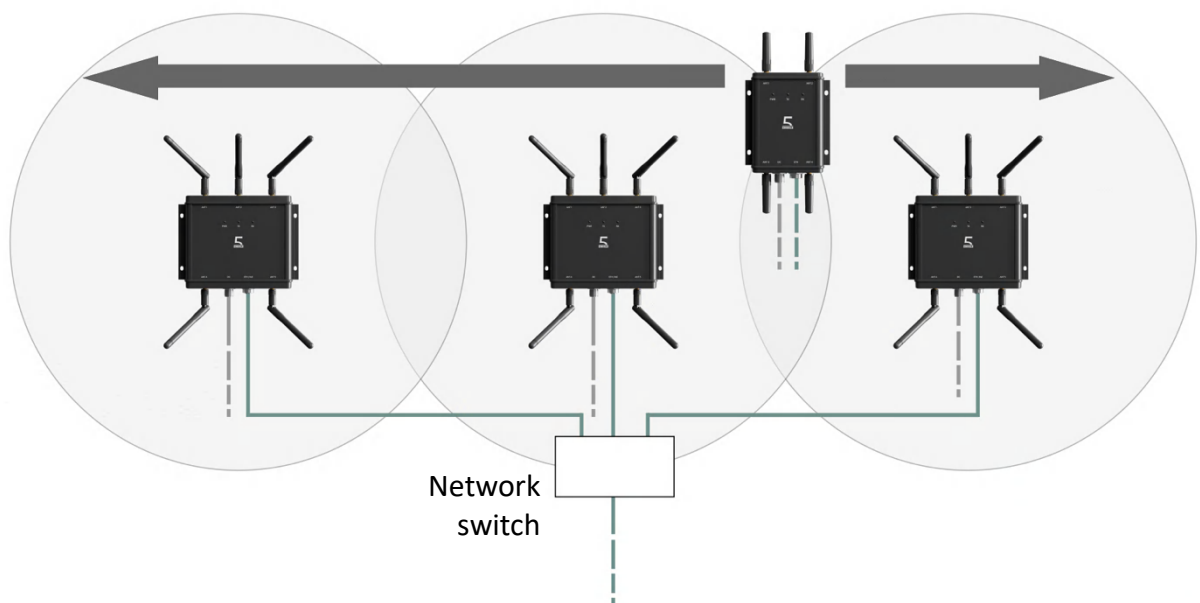
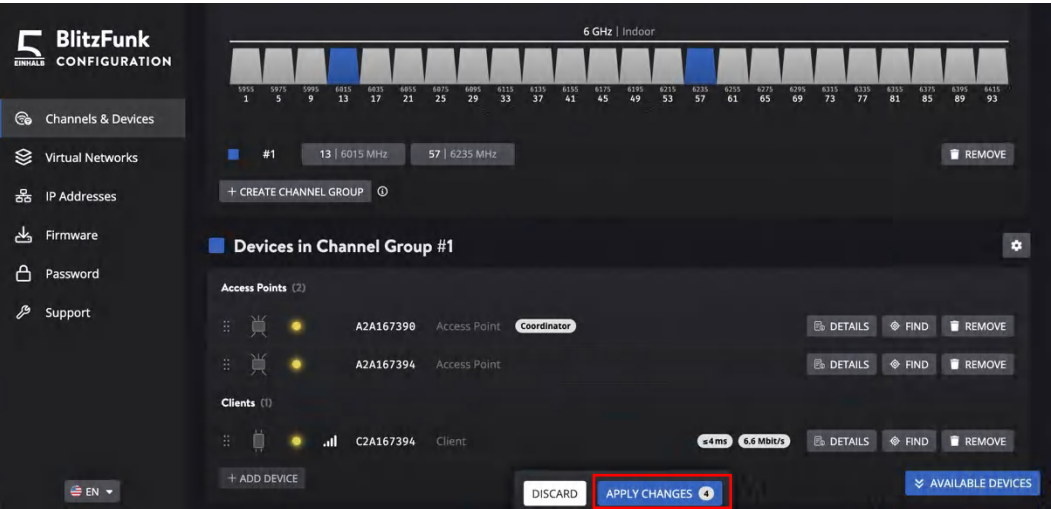


Figure 9 Example for a setup containing multiple access points to increase coverage

In the configuration interface, add multiple access points to a channel group. Add clients to the channel group and press *Apply Changes* to confirm.



4.5 Increasing Capacity with Additional Access Points

To increase the data rate per client and reduce latency, multiple channel groups can be operated in parallel. Latency and data rate scale independently for each channel group. Unless separated from each other by virtual networks (ref. *Segmentation into Virtual Networks (VLANs)*), a client can exchange data with all other clients, regardless of which channel group they belong to.

For a setup with multiple channel groups, a separate access point is required for each group. The access points must be connected to each other via Gigabit-Ethernet (ref. *Power and Data Connection*).

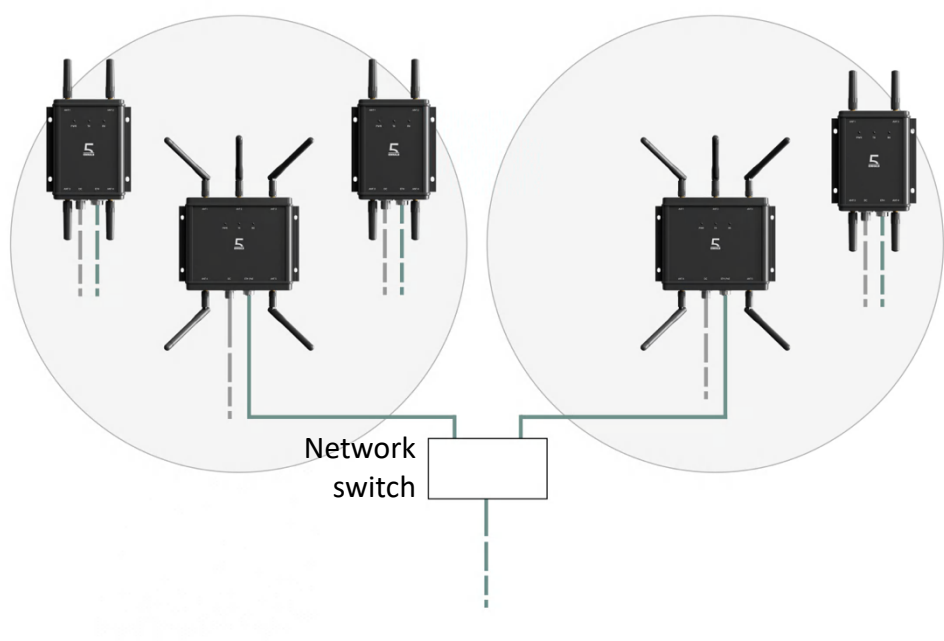
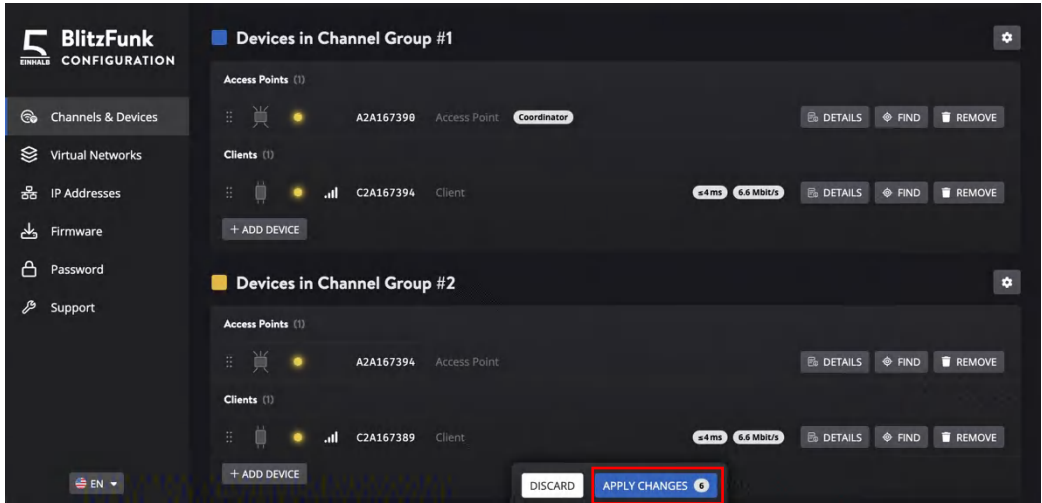


Figure 10 Example for a network with multiple access points to increase capacity and reduce latency

In the configuration interface, create multiple channel groups and assign one access point to each group. Add clients to the corresponding channel group and press *Apply Changes* to confirm the configuration.



4.6 Seperation into virtual Networks (VLANs)

Clients in a BlitzFunk network can be isolated from one another using virtual networks (VLANs). This allows independent applications to operate on the same infrastructure without mutual interference. It also helps limit the impact of cybersecurity incidents and reduces the scope of broadcast frames, thereby providing more capacity for each application.

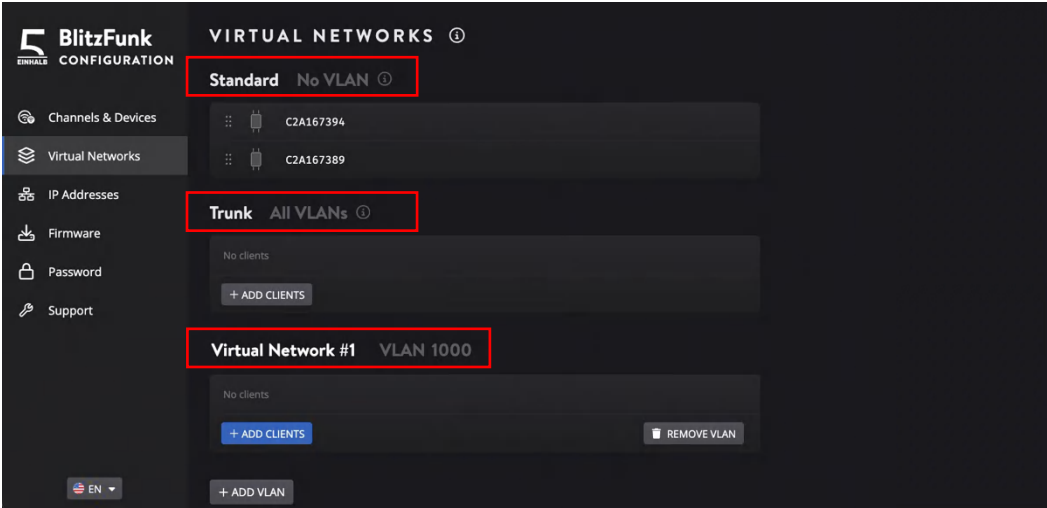
VLAN-specific settings are configured in the *Virtual Networks* tab.



BlitzFunk implements VLANs according to the IEEE 802.1Q standard. Data is assigned to a VLAN by means of an additional field (the so-called VLAN ID) in the

header of the Ethernet frame. A VLAN is identified by a number between 1 and 4095.

For each client, the following VLAN options can be assigned:



Mode	Function
Standard	Devices connected to the client receive only data without a VLAN ID or data with a VLAN ID 0 (e.g. PROFINET). Data entering the client via Ethernet is accepted only if it has no VLAN ID or a VLAN ID 0 and is then forwarded to the access point. For traffic with VLAN ID 0, the complete 802.1Q header is transmitted unchanged.
Virtual Network	Devices connected to the client receive only data with the matching VLAN ID. The complete 802.1Q-Header including its VLAN ID is removed by the client when outputting data via Ethernet, so the connected devices do not need to process VLAN IDs. Data entering the client via Ethernet without a VLAN ID is assigned the appropriate ID and forwarded to the access point. Data entering the client via Ethernet with an 802.1Q-Header, the VLAN ID is replaced with the configured value.
Trunk	All data is forwarded regardless of its VLAN ID. The complete 802.1Q header is transmitted unchanged. This allows VLAN-capable switches to be operated on this client.

Access points are always in trunk mode. If clients have been assigned to a virtual network and this virtual network needs to be accessed on the access-point side, a VLAN-capable switch must be used.



Tip: The DHCP server and HTTP server of the access point are not part of any VLAN. This means that only clients in standard mode or trunk mode, as well as devices connected to these clients, can obtain an IP address from the built-in DHCP server. Likewise, the configuration interface is only accessible through clients in standard or trunk mode.

In the following example, a virtual network is set up for each client in order to create logically separated point-to-point connections at the Ethernet level between controllers at the access point and a remote I/O module at each client.

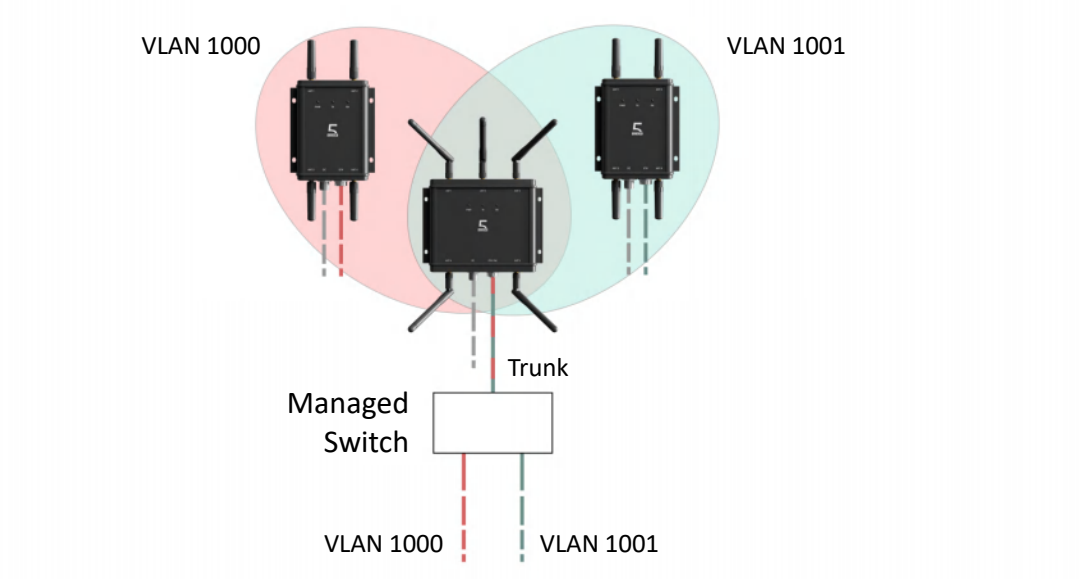
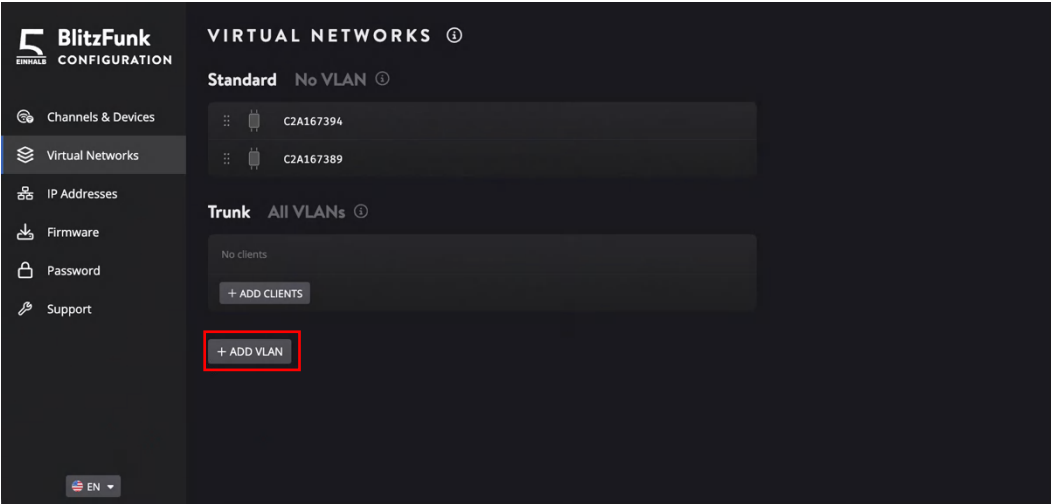
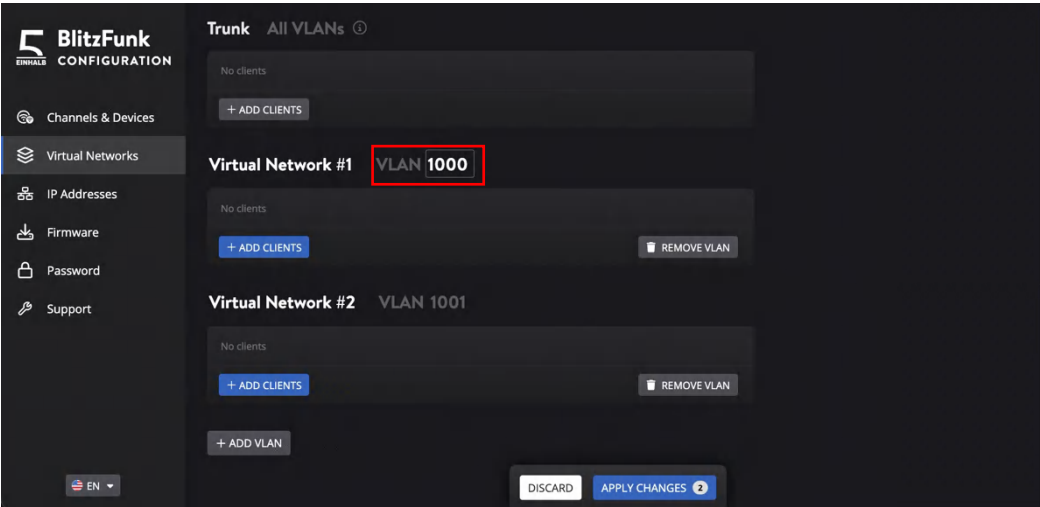


Figure 11 Example of two logically separated point-to-point connections over a shared physical BlitzFunk network

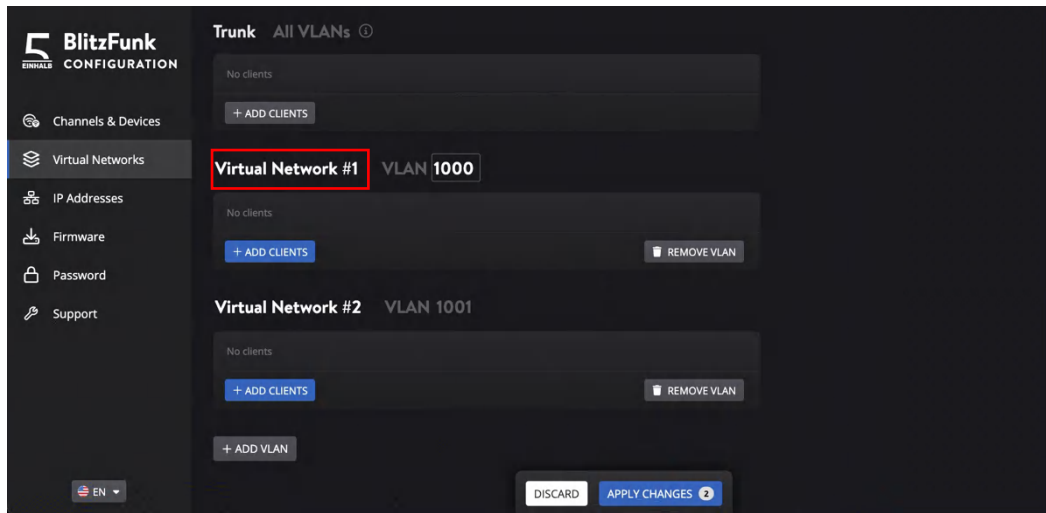
In the configuration interface of the access point, create two VLANs by clicking the *Add VLAN* button twice.



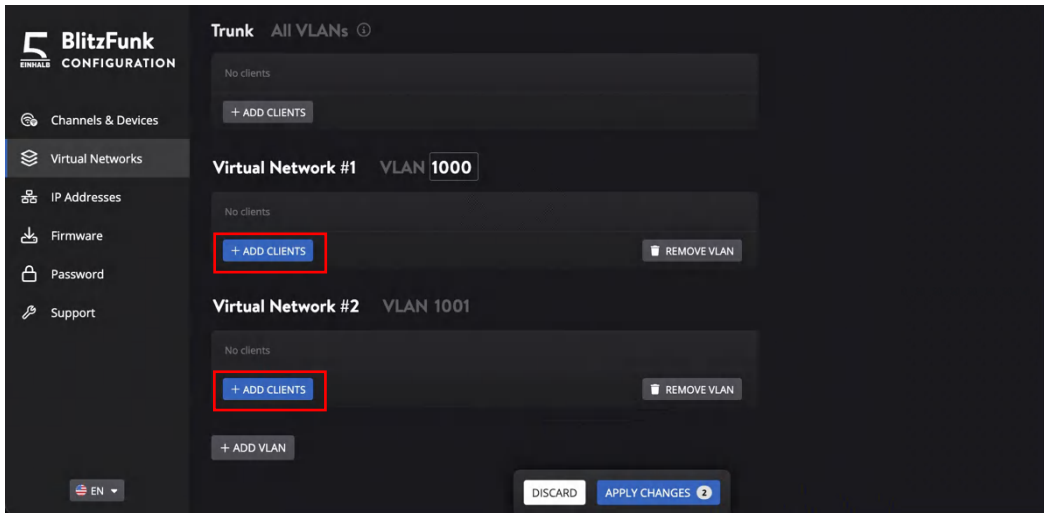
The used VLAN ID can be modified via the entry in the table header.



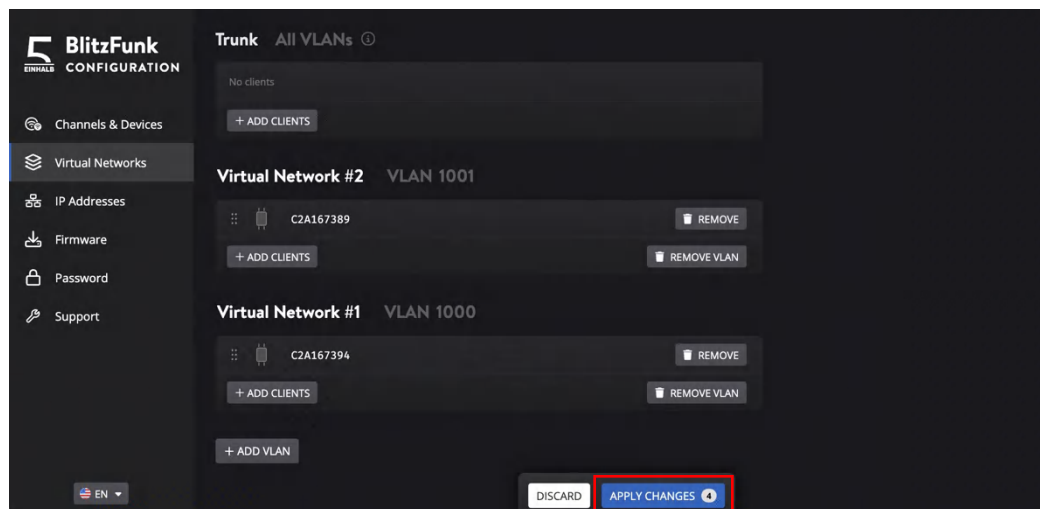
Additionally, the name of the VLAN can be modified in the table header.



Add a client to the first virtual network by clicking the *Add Clients* button or by dragging the client into the virtual network. Repeat the process for the second client and the second virtual network.



After clicking the *Apply Changes* button, the traffic between the two clients is isolated. For traffic from devices connected to access points to reach the respective client, it must contain the corresponding VLAN ID (in this example VLAN ID 1000 or 1001).



To allow the controllers to reach the clients in their VLAN, the managed switch between the access point and the controllers must be configured as follows:

- The port connected to the access point must be configured to transparently forward any VLANs (trunk mode).
- The ports connected to the controllers must each be assigned to one of the previously created VLANs (in this example 1000 or 1001) and configured to apply the corresponding ID to incoming traffic and remove the ID from outgoing traffic (untagged mode).

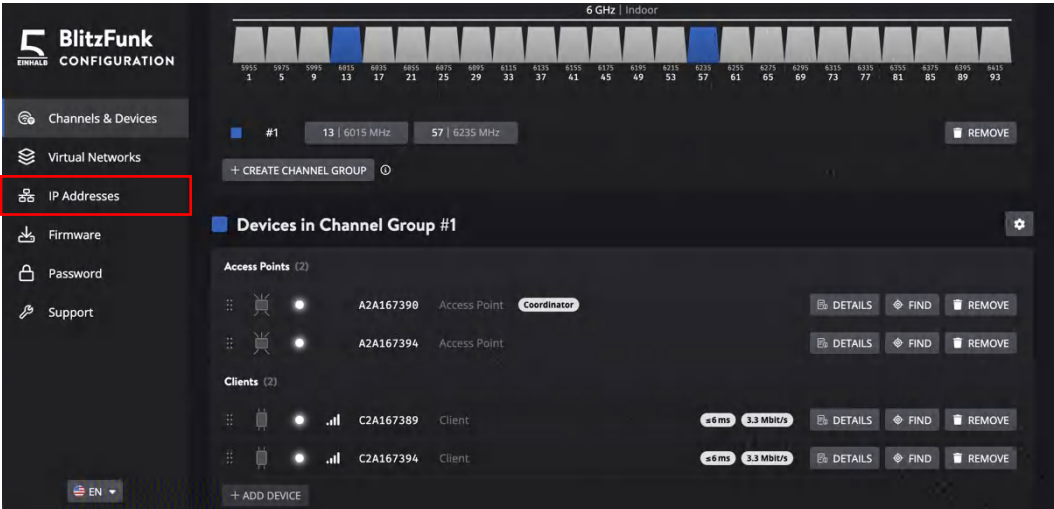
4.7 Changing the IP Address Behavior

Access to the configuration interface requires the coordinating Access Point to have an IP address. In addition, IP addresses can be assigned to individual clients, for example for diagnostic and monitoring purposes.



Tip: Assigning IP addresses to clients is only intended to make the devices themselves reachable, for example for diagnostic purposes. User data transmission through the BlitzFunk network operates transparently on Layer 2 and does not require IP address configuration on client devices.

The settings for the IP address behavior are located in the *IP Addresses* tab of the configuration interface.

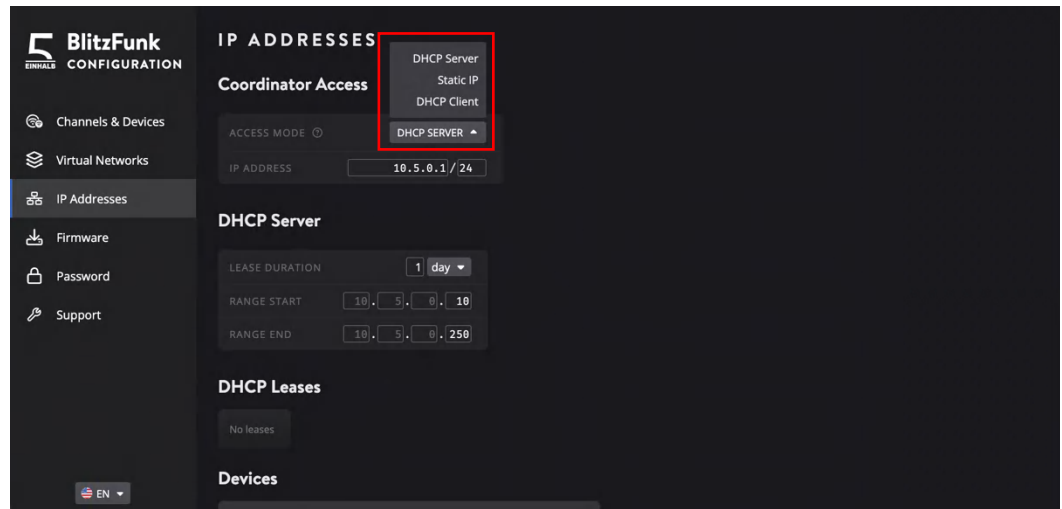


The following options are available for the different device types:

Device Type	Option	Function
coordinating access point (lowest device ID among access points)	DHCP Server (default setting)	The coordinating Access Point operates as a DHCP server and assigns IP addresses to connected network devices within the configured address range.
	Static IP	A fixed IP address and subnet mask are assigned to the coordinating Access Point.
	DHCP Client	The coordinating Access Point automatically requests an IP address from a DHCP server in the network.
client	No IP (default setting)	No IP address is assigned to the client.
	Static IP	A fixed IP address and subnet mask are assigned to the client.

	DHCP Client	The client automatically requests an IP address from a DHCP server in the network.
--	-------------	--

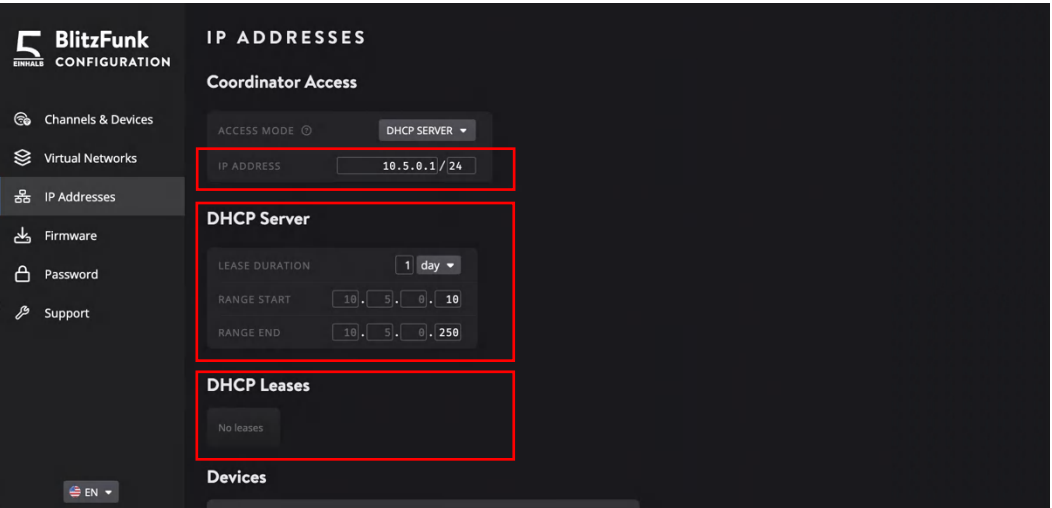
The different options for the coordinating Access Point can be selected from the *Access Mode* drop-down menu in the *Coordinator Access* section.



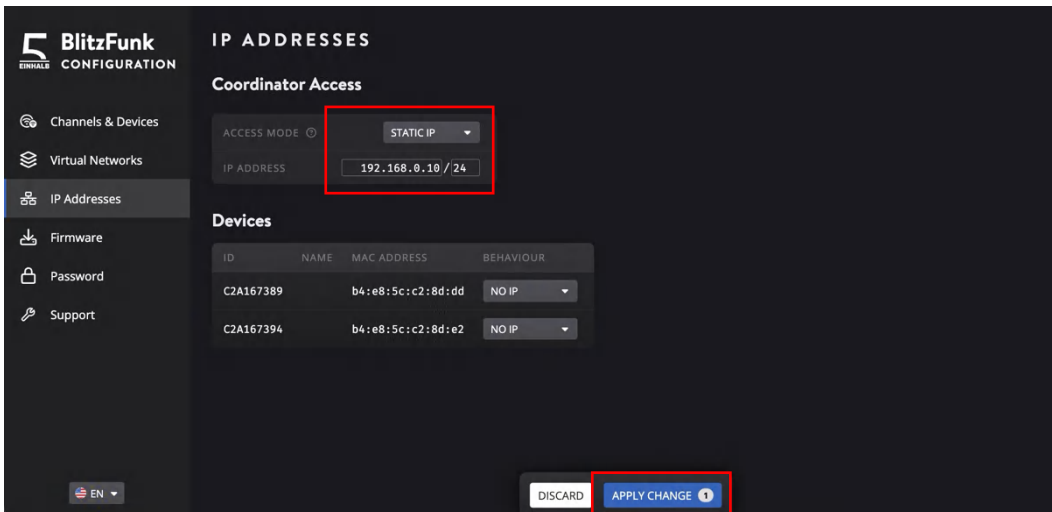
Changing the Coordinating Access Point Behavior

In the default setting *DHCP Server*, the additional sections *DHCP Server* and *DHCP Leases* are displayed. In the DHCP Server section, the address range used by the integrated DHCP server can be configured. Assigned IP addresses have a limited validity period, which is defined by the Lease Duration setting. The address range is defined using the Range Start and Range End settings.

All IP addresses currently assigned by the integrated *DHCP* server are displayed in the *DHCP Leases* section. The IP address and subnet mask of the DHCP server itself are configured using the *IP Address* field.

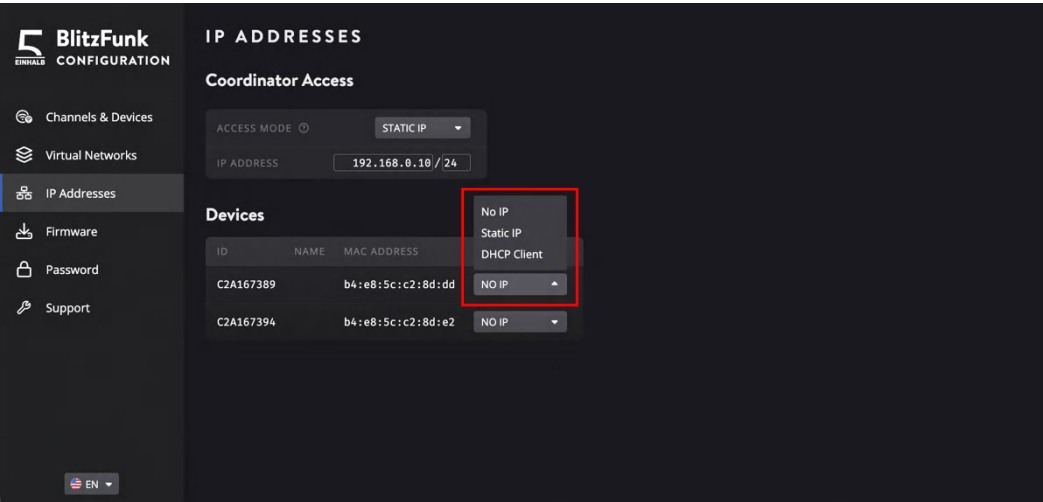


When changing the coordinator access mode to *Static IP* or *DHCP Client* and confirming the change using the *Apply Changes* button, the integrated DHCP server is disabled. The configuration interface is then reachable either via the configured IP address (option *Static IP*) or via the IP address assigned by the external DHCP server (option *DHCP Client*).



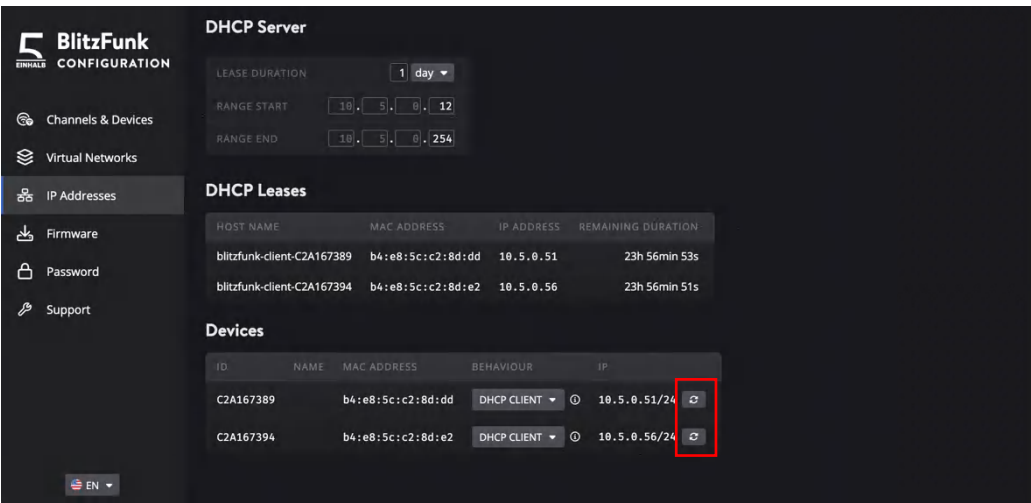
Changing the Behavior of Clients

All clients currently within wireless range are displayed in the *Devices* section. The desired IP address behavior for each client can be selected in the *Behavior* column of the corresponding device entry.



In the default setting *No IP*, a client does not have an IP address assigned. For diagnostic purposes, the options *Static IP*, which assigns a fixed IP address to the client, or *DHCP Client*, where the client obtains an address using the DHCP protocol, can alternatively be used. The IP address of a client can, for example, be used to verify network connectivity to the device using ping.

If a client has obtained an IP address using the *DHCP Client* option, a new IP address can be requested before the current lease duration expires by pressing the button next to the displayed IP address.





Hinweis: When a device (coordinator or client) is operated as a DHCP client, IP addresses are assigned automatically via the network. This generates additional network communication, which may affect real-time communication performance depending on overall network load.

For applications with particularly high real-time requirements, the use of static IP addresses or operation without an IP address is therefore recommended to ensure the most consistent and deterministic communication possible.

4.8 Changing the Device Configuration During Operation

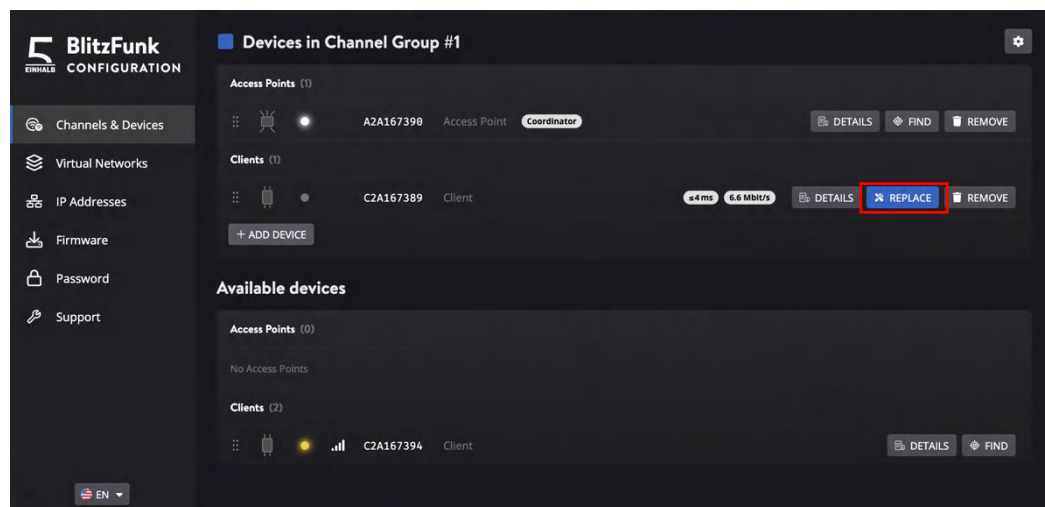
BlitzFunk supports configuration changes at runtime. Applying such changes results in only minimal interruptions, depending on the type of change. The duration of the interruption affects all devices within the configuration:

Device Type	Action	Duration of the Interruption
client	adding device	< 2 ms
	removing device	
coordinating access point (lowest device ID among access points)	adding device	< 5 s
	removing device	< 1 s
non-coordinating access point	adding device	< 50 ms
	removing device	

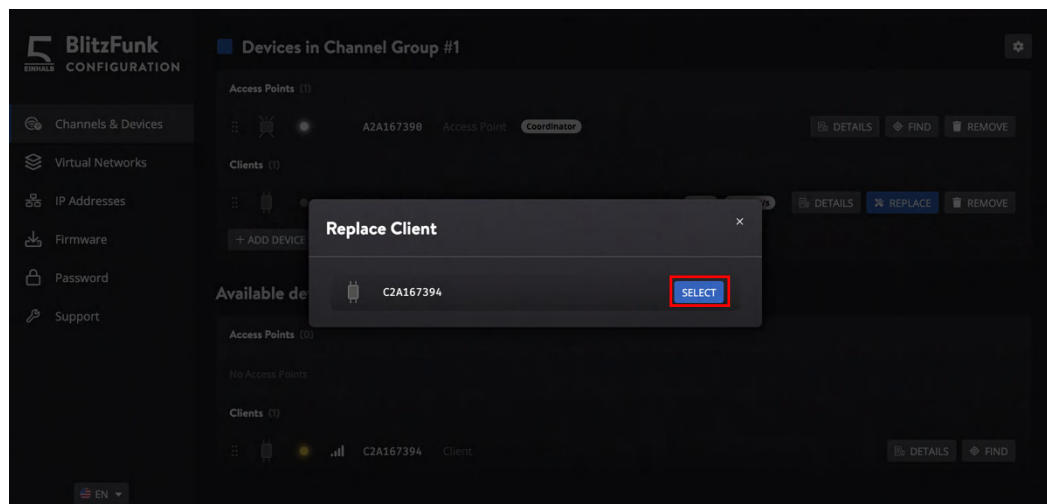
If an access point fails and becomes unavailable, the same interruption duration as when removing that access point applies. After this time, another access point in the configuration can take over, provided the client is within its range.

4.9 Replacing Devices

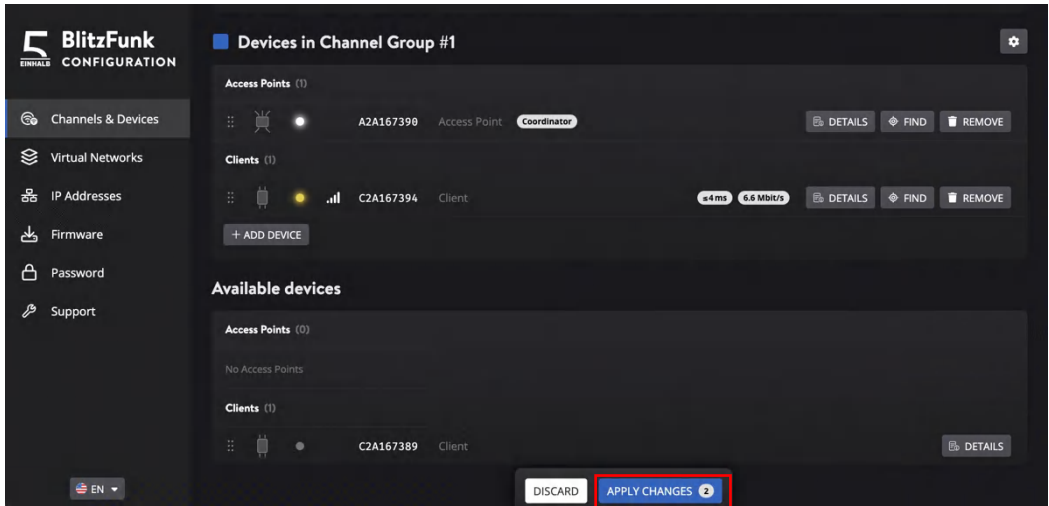
If a configured device is no longer active, it can be replaced with a new one in just a few steps. Devices that are no longer connected to the system display a Replace button, which allows you to select a replacement device.



Select a new device, which replaced the device that is not connected anymore.



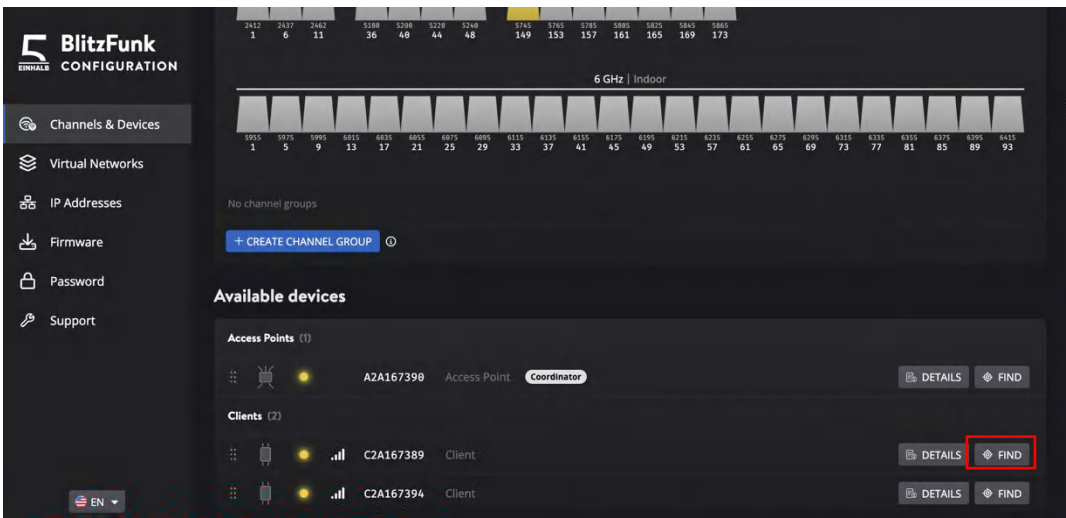
Confirm the replaced device by clicking *Apply Changes*. Changing the configuration causes a brief interruption of all connected devices, depending on the type of device being replaced (ref. *Changing the Device Configuration during*



Operation).

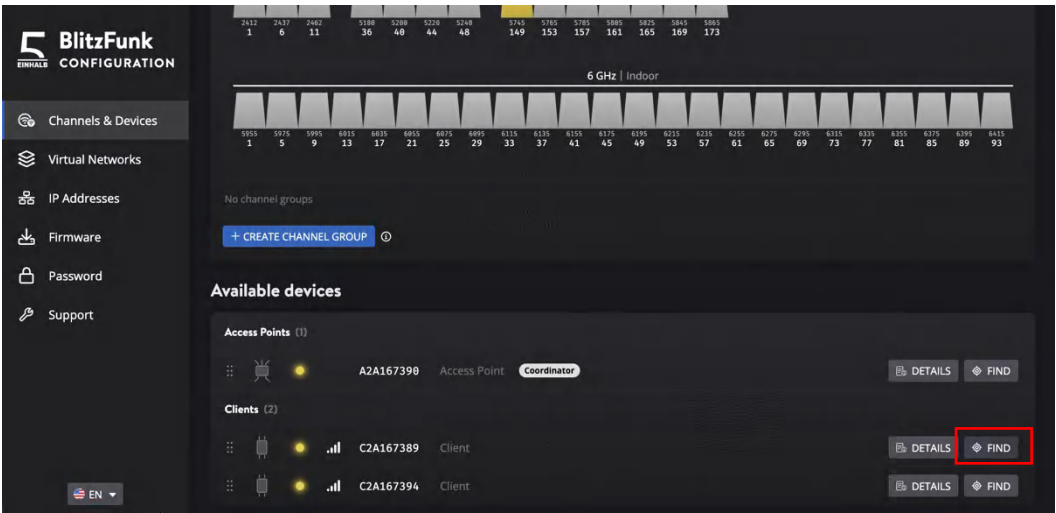
4.10 Locating Devices

If devices are already installed, the device ID on the back may no longer be visible, which can make it difficult to match the entries in the configuration interface to the corresponding physical devices. In this case, press the *Find* button next to the



device entry in the interface. The device's LEDs will flash blue to indicate its location.

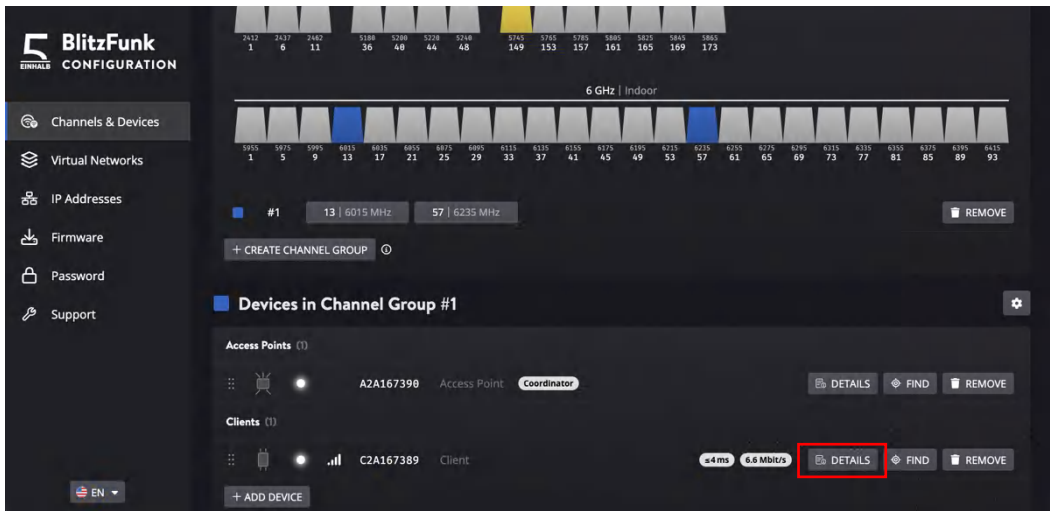
To stop the locate animation on the device press the button again.



5 System Diagnostics

5.1 Link Status Monitoring

For configured clients, detailed status information about the wireless connection can be viewed in the configuration interface (ref. *Accessing the Configuration Interface*). Click the client’s *Details* button to open it.

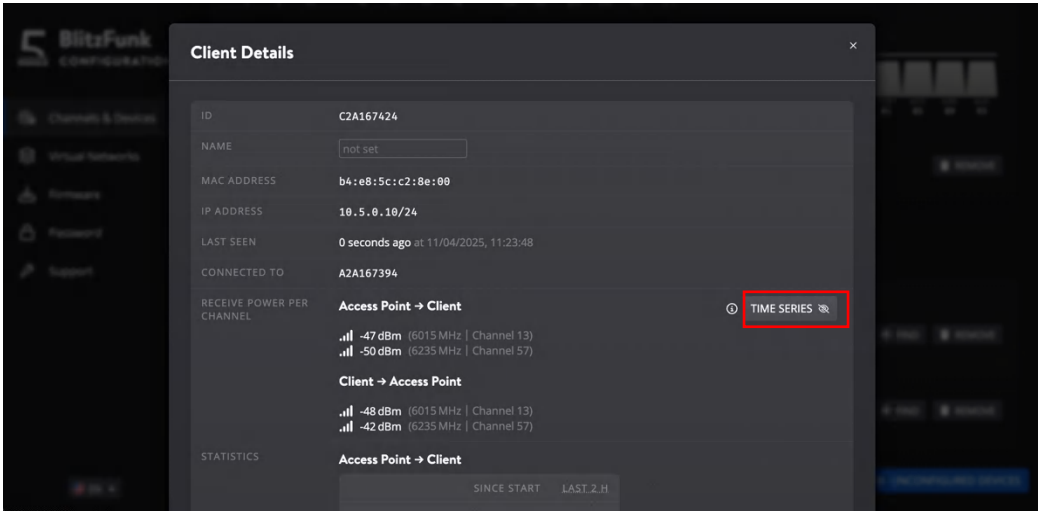


The menu gives detailed status information about:

Reported Metric	Meaning
ID	Serial number of the client
Name	User-defined device name
MAC Address	MAC address of the Ethernet interface
IP Address	Displays the IP address and subnet of the client. The displayed IP address can, for example, be used to check the network connection to the client (e.g., using a ping).
<i>Started</i>	Duration since the client was started.

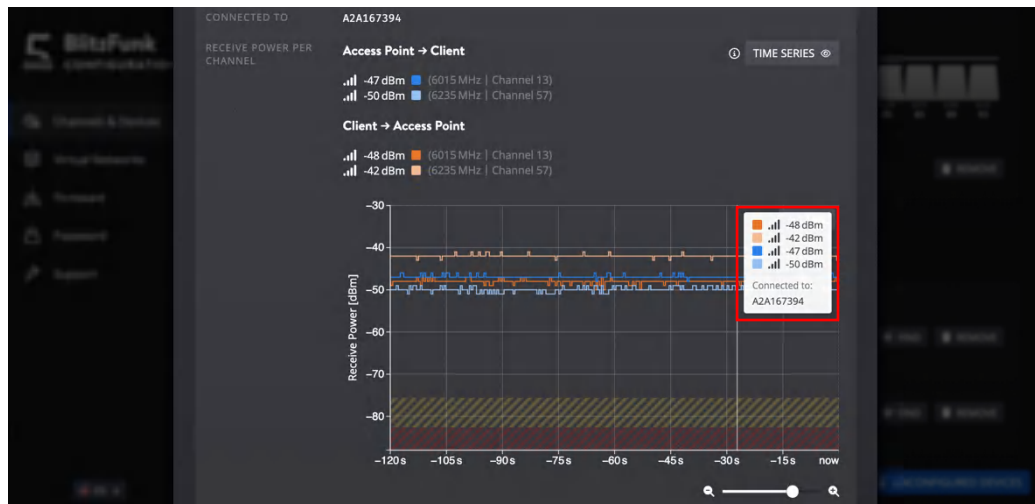
Last Seen	Duration since the client last connected to an access point.
Connected To	Displays the access point the client is currently connected to.
Receive Power per Channel	Displays the wireless signal strength of each wireless link used during operation between the client and the currently connected access point. A low receive power indicates coverage issues due to a large distance from the access point, an improperly mounted antenna, or a setup in which the antenna is obstructed by metal.
Transmitted Frames (Transmit Direction / Receive Direction)	Displays the number of Ethernet payloads that the devices received for transmission.
Dropped Frames (Transmit Direction / Receive Direction)	Displays the number of packets that have been dropped. When the system is overloaded with more data than can be transmitted, packets are dropped to ensure real-time performance for newer packets. A value greater than zero indicates that more data is being generated than the wireless system can handle. Overloading is expected for short periods when using the transport control protocol (TCP).
Losts Slots (Transmit Direction / Receive Direction)	Displays the number of packets lost over the wireless link. A value greater than zero indicates coverage issues or strong interference from other wireless networks on the operating channels.
Custom Antennas	Allows adjustment of the antenna gain when antennas other than the default ones are used.

Firmware	• Version: Firmware version number. This field is not displayed for development versions. • Commit: Unique identifier of the device firmware. • Date: Creation date of the firmware.
System	• Version: Operating system version number. This field is not displayed for development versions. • Commit: Manufacturer identification of the operating system. • Fingerprint: Unique identifier of the device's operating system. • Date: Creation date of the operating system.



In addition to the displayed metrics, the *Time Series* button allows the reception power per channel to be displayed over time. The time series is only recorded while the browser window remains open. Reloading the browser window resets the displayed time series.

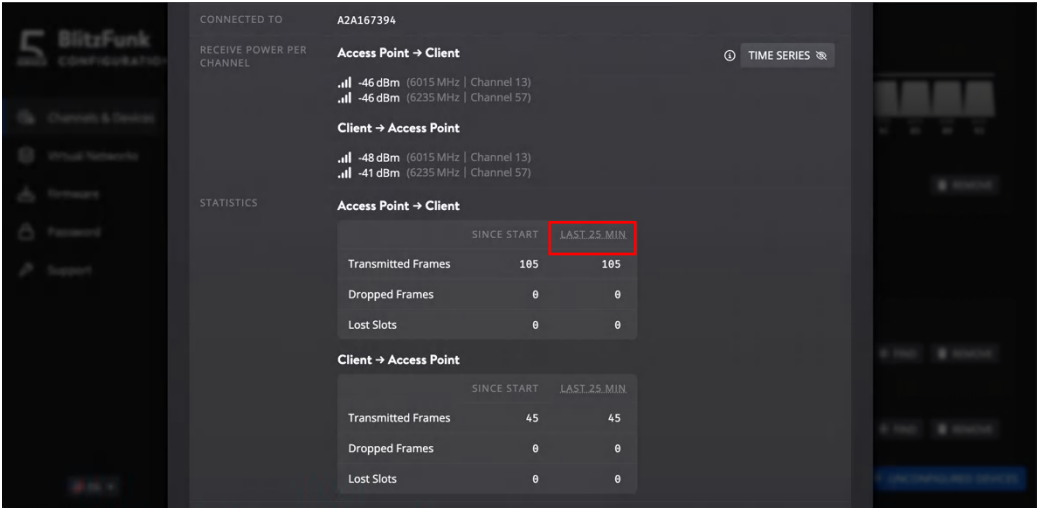
To obtain detailed information for a specific point in time, move the mouse to the desired position in the chart.



To mark specific points in the chart (e.g., to indicate the client's location at that time), a label can be added for a selected point in time using the *Label* button.



When troubleshooting an installation, the counters in the table entry statistics can be reset by clicking the table head with a dotted underline.



6 Device Maintenance

6.1 Firmware Updates

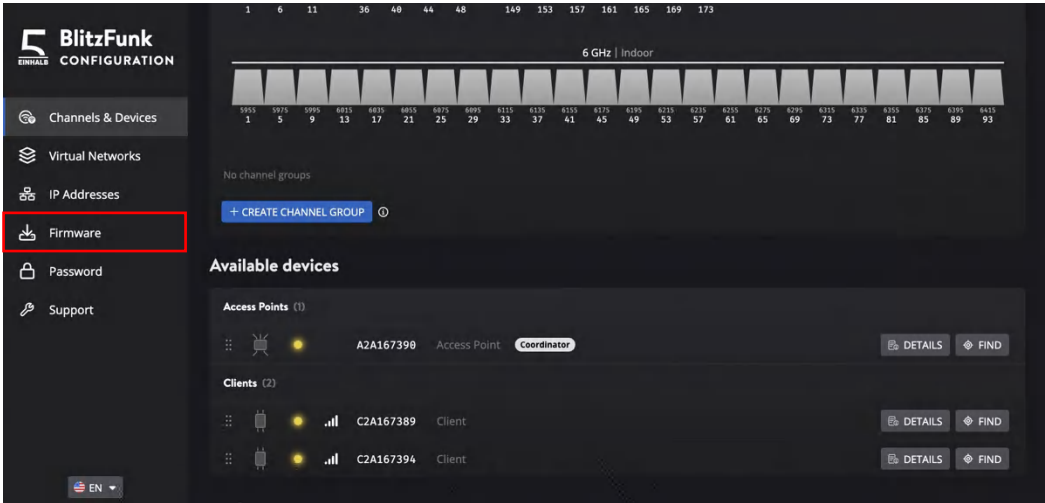
Devices can be updated via the configuration interface (ref. *Accessing the Configuration Interface*). Updating devices while they are configured may fail and should preferably be performed in the unconfigured state (devices with a yellow PWR LED).



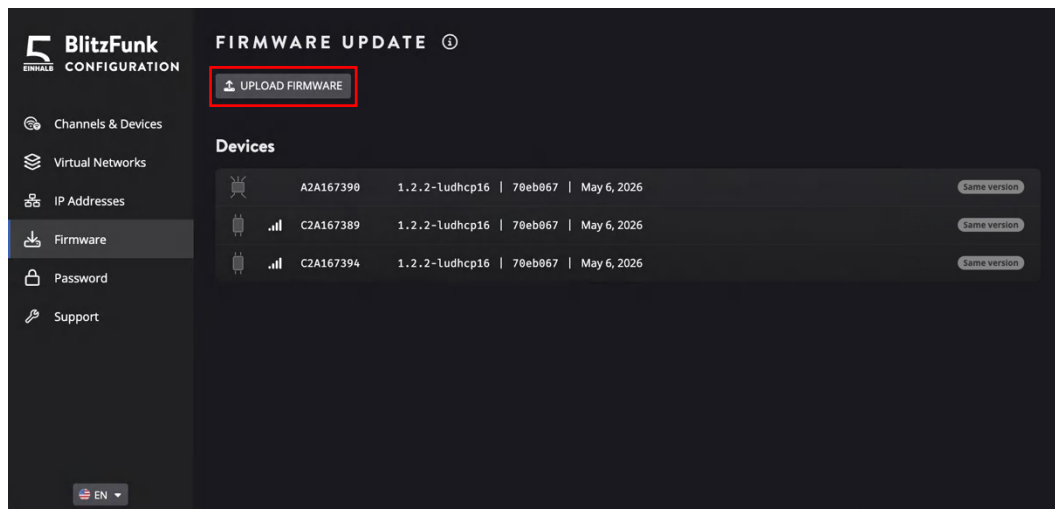
WARNING: When performing an update or a firmware synchronization on a configured system, data transmission will be interrupted. Due to the additional load on the system, interruptions may also occur even if only devices outside the configuration are being updated. All devices must be reconfigured after the update.

To update the devices, switch to the firmware tab in the configuration interface.

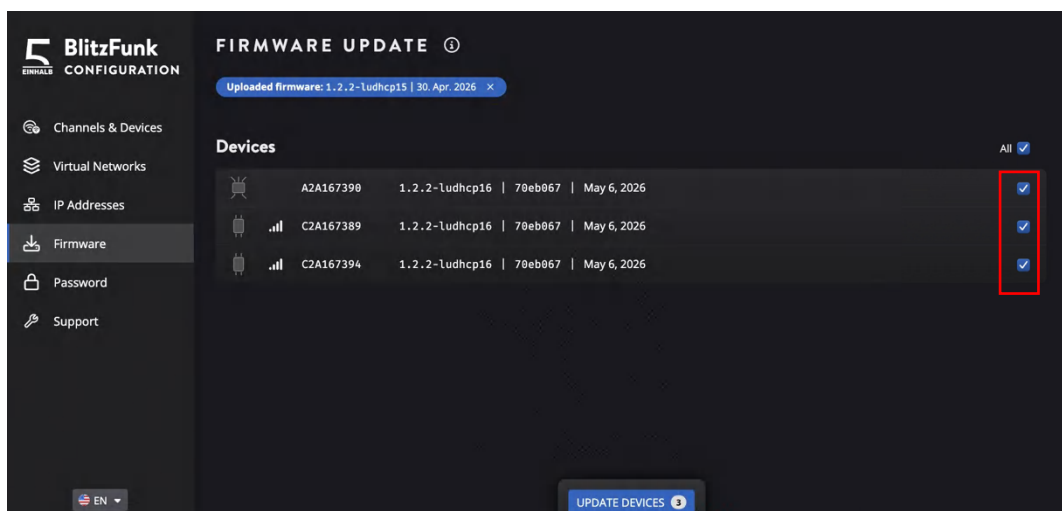
To upload a new firmware, select a firmware file from your computer using the



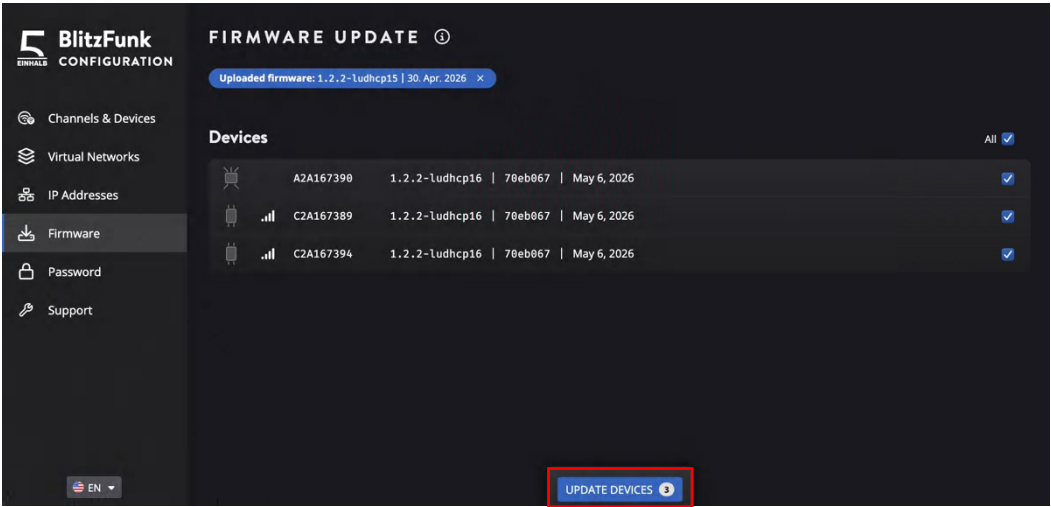
Upload Firmware button or drag a firmware file into the window.



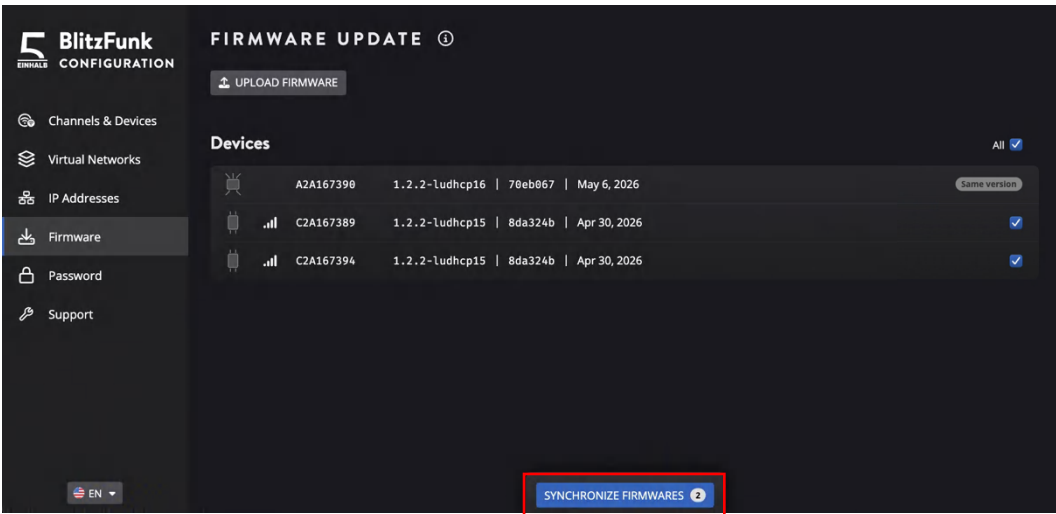
By default, all devices in the list are preselected to receive the uploaded firmware. By clicking the corresponding checkbox, the device can be removed from receiving the update.



By clicking the *Update Devices* button, the firmware will be distributed to all devices showing a activated checkbox in the list.



If there is a firmware mismatch between devices, they can be synchronized to the same firmware using the *Synchronize Firmwares* button. The button is only displayed in case of a firmware mismatch. All devices are updated to the firmware version of the coordinating access point. If devices are to be updated to a different firmware version than that of the coordinating access point, the corresponding firmware version must be uploaded using the *Upload Firmware* option.



After a firmware update or a firmware synchronization, the configuration is deleted, and the devices restart into setup mode. Then, the devices need to be reconfigured (ref. *Device Configuration*).



Tip: Send an email to contact@fuenfeinhalb.de with subject line „Update Notification“ to be informed about new firmware updates.

6.2 Factory Reset

To perform a factory reset, power off and on the device exactly three times within the first two seconds of startup. When all three LEDs light up blue, allow the device to continue booting. During startup, the device will delete its configuration and briefly flash all LEDs yellow to indicate the reset. It will then restart in setup mode.



Figure 12 Visualization of how the device displays the number of power cycles performed at the beginning of its startup phase. This also applies to access points.

7 Technical Data

Mechanical Data		
Width	Client	100 mm
	AP	160 mm
Height (without antennas)	Client	130 mm
	AP	140 mm
Depth	Client	36 mm
	AP	39 mm
Mounting	Wall mounting	

Environmental Conditions	
Operating temperature	-20 °C to 60 °C
Degree of protection	IP65 (CW32R), IP6X (AW32R)

Connections		
Power Supply	Client	12 – 48 V DC; 4.1 W average; 10 W peak
	AP	14 – 48 V DC or PoE 802.3af mode A / mode B; 4.8 W average; 15 W peak
DC	M12, 5-pin, A-coded	
Ethernet	Client	M12, 4-pin, D-coded; 100 Mbit/s
	AP	M12, 8-pin, X-coded; 1000 Mbit/s
Antennas	RP-SMA female, 50 Ω (CW32R), Integral (AW32R)	

Quality of Service	
Maximum one-way latency	4 ms for 1 Client
	+2 ms per additional client
Additional roaming latency	0 ms
Data rate	6 Mbit/s shared between clients
Payload per Ethernet frame	1500 Bytes
Reliability	99.999999 % for specified latency and data rate

Wireless Features	
Center frequencies	2412 MHz – 2462 MHz 5180 MHz – 5240 MHz 5745 MHz – 5865 MHz 5955 MHz – 6415 MHz 6435 MHz – 7115 MHz (USA / Canada)
Bandwidth	2 × 20 MHz

8 Troubleshooting and Support

8.1 Troubleshooting

Problem: Web interface not accessible

It takes about 30 seconds after powering on an access point before the web interface becomes available. When devices are in setup mode, which is indicated by a yellow PWR LED, the interface can only be accessed through access points, not from client devices. Make sure the URL in your browser is `http://10.5.0.1` and not `https://10.5.0.1`. If another DHCP server is active on the network, locate the access point's IP address in the DHCP lease list.

Problem: New client does not appear or disappears occasionally (grey status indication or device is completely missing in the web interface)

This is likely caused by low signal strength. Verify that all antennas are properly mounted on both access points and clients. Antennas should be tightened hand tight or using a torque of 0.9 Nm. Try moving the client closer to the nearest access point or install another access point nearby. Avoid shielding antennas with metallic objects like control cabinets or machine housings. For devices mounted in metal enclosures, use low-loss RP-SMA cables rated up to 7 GHz to position the antennas outside.

Problem: Additional access point does not appear in the web interface

For coordination between the access points, VLAN ID 512 is used. If you are using managed Ethernet switches to connect the access points, ensure that VLAN ID 512 is forwarded by the switch.

Problem: Occasional communication errors and outages

This may be due to system overload, weak signal strength, or interference from other wireless networks operating on the same channels. In the web interface, open the client's status and check the reported values (ref. *Link Status Monitoring*). If buffer overflows are rising, the system is overloaded and must be supplied with less data. If the receive power drops below -80 dBm and packet loss increases, refer to the signal strength tips above. If receive power is good (above -60 dBm) but packet loss is still high, interference is likely. Try using different channels with at least 80 MHz spacing.

Problem: Unexpected continuous activity on TX and RX-LEDs in combination with communication errors and difficulties accessing the web interface

The system is likely overloaded. If you do not expect high traffic from the application, check your network for loops. Ensure that none of the clients are connected to the access points using a wired connection.

Problem: Otherwise inexplicable behavior

Unexpected behavior can occur during undervoltage conditions. If the device is powered through the DC connector, ensure that the supply voltage does not drop below 10 volts. When using Power over Ethernet (PoE), make sure the PoE source (e.g. a PoE switch) is compliant with at least IEEE 802.3af and is capable of supplying sufficient power. Note that not all switches can power every port simultaneously at full load.

Do not power off the device during firmware updates or configuration changes. In rare cases, unexpected behavior may also result from software bugs. You can always recover from invalid configurations by performing a factory reset (ref. *Factory Reset*).

8.2 Support

For technical assistance, troubleshooting, or product inquiries, please contact our support team at contact@fuenfeinhalb.de or call +49 351 8966 5590.

fünfeinhalb Funksysteme GmbH

Chemnitzer Straße 78A

01187 Dresden, Germany