MiR Network and Wifi Guide (en)

Date: 09/2020

Revision: v.2.2

Copyright and disclaimer

Contact the manufacturer:

Mobile Industrial Robots A/S
Emil Neckelmanns Vej 15F
DK-5220 Odense SØ

www.mobile-industrial-robots.com
Phone: +45 20 377 577
Email: support@mir-robots.com

CVR: 35251235

Table of contents

1. About this guide

This guide describes necessary and recommended setup of your WiFi infrastructure for your MiR solution to work optimally. MiR products are highly dependent on the WiFi quality, since WiFi is used by users to interface with the product. A poor WiFi setup will result in:

- Latency between user or fleet commands and robot execution
- Unreliable connection to the robot or fleet interface
- Unreliable connection and slow synchronization between robots and MiR Fleet
- Poor resource management with MiR Fleet
- Poor Collision avoidance coordination between robots connected to MiR Fleet

1.1 Version history

Revision	Release date	Description
0.1	2017-13-09	First edition.
0.2	2017-06-11	Release review.
0.3	2018-21-02	Protocol errors corrected.
0.4	2018-20-08	Full rework + new sections.
0.5	2019-13-02	MiR500 and MiR Fleet added to scope. Changes to sections Network security and Ports.
0.6	2019-23-10	Minor updates and additions to Requirements for WLAN.
0.7	2020-12-02	Protocol requirement note added under Network security section, and subnet note added under IP configuration section.
2.0	2020-15-05	Changed title from *MiR network requirements* to *MiR network and WiFi guide*. Includes sections describing how to evaluate and improve your WiFi network for MiR products.
2.1	2020-05-08	Added ports required for AI camera and HTTPS communication.
2.2	2020-09-15	Added clarification of data rate and bandwidth

Revision	Release date	Description
		requirements. Added recommendation to not use hidden SSIDs. Other minor corrections.

1.2 Where to find more information

At the MiR website, you can find the following resources under the **Manuals** tab on each product page:

- **Quick starts** describe how you start operating MiR robots quickly. This document is in print in the box with the robots. Quick starts are available in multiple languages.
- **User guides** provide all the information you need to operate and maintain MiR robots, and how to set up and use top modules and accessories, such as charging stations, hooks, shelf lifts, and pallet lifts. User guides are available in multiple languages.
- **Getting started guides** describe how to set up products that are mainly software-based, such as MiR Fleet.
- **Reference guides** contain descriptions of all the elements of the robot interface and MiR Fleet interface. Reference guides are available in multiple languages.
- **REST API references** for MiR robots, MiR hooks, and MiR Fleet.
- **MiR network and WiFi guide** specifies the performance requirements of your network and how you must configure it for MiR robots and MiR Fleet to operate successfully.

2. Network requirements

For you MiR solution to function optimally, there are certain configurations and requirements that must be fulfilled. The following sections describe how the network must be set up.

2.1 Requirements for WLAN

For the robots to operate well, it is important that your network fulfills certain requirements. Depending on your setup, the requirements may differ, but for a WiFi setup used by both MiR robots and other devices, it is often suitable to meet the requirements outlined in *Table 2.1*.

Table 2.1.
Guideline for network requirements.

Parameter	Description	Requirement
Signal strength	The signal strength from the robots' perspectives when connected to the best access point.	Min. -67 dBm
Secondary signal strength	The signal strength from the robots' perspectives when connected to the second best access point.	Min. -75 dBm
Signal to noise ratio	Signal to noise ratio from the robots' perspectives.	Min. 20 dBm
Data rate	Rate of data communicated to and from each robot. This is the transfer speed of communications.	Min. 20 Mbps
Channel interference	Number of access points per channel available when signal strength is lowered to -85 dBm	Max. 2 AP/ch at -85 dBm
Latency (round trip time, ping)	Time taken to send and receive messages from robots by for example pinging them.	Max. 200 ms
Bandwidth	The amount of data that can be transmitted over time. Must support 1 Mbps for each robot on the	Min. 1 Mbps/robot

Parameter	Description	Requirement
	network. ⓘ The **data rate** and **bandwidth** requirements should be interpreted as that the network must support robots sending and receiving 1 Mb of data every second with a transfer rate of at least 20 Mbps.	
Packet loss	Percentage of communication packets that can be lost.	Max. 2%

Additionally, your network must fulfill the following requirements:

- There must be full WiFi coverage throughout the traveling path of all robots.
- There must be a WLAN controller to secure that roaming happens at the correct time and without any authentication errors. Make sure that the company network access points are controlled by the same controller.
- The access points must be set up to communicate and share roaming information.
- Make sure that Load balancing on the access points is disabled. The robots must be able to roam freely.
- Airtime Balancing must be disabled if possible. This setting changes how much time a device gets on the network depending on the signal strength. Low signal devices get less time than high signal devices. This means that a robot that is far away will be allowed less data than a robot that is close by.

The robots are able to perform some tasks under worse conditions than mentioned above. However, key features in MiR Fleet such as Collision detection, Auto charging and staging, Limit-robots zones, data synchronization between robots, and fleet mission execution will not work optimally.

Network capacity

To meet the aforementioned requirements, you must ensure that your network has the capacity to handle the number of devices connected to it. To establish this you must determine the following:

1. The number of devices that are connected to the network.
2. How much data the devices are transferring at the same time on a busy work day.
3. How many access points are required to ensure that all devices are connected and can transfer data without using over 50% of the access point's capacity.

If anything between 60-70% of the WiFi channel is being used, MiR robots will be affected by latency and packet loss.

With WiFi 5 technology, 60-70% channel utilization is reached when 25-30 robots are connected to a single access point.

2.2 Requirements for MiR Fleet

- MiR Fleet must be connected to the network through Ethernet.
- MiR Fleet must be in the same physical location as the robot. Geographical distance will cause delay between MiR Fleet and robots.

2.3 Wireless network standards

MiR robots can use the following wireless network standards:

- **802.11a**
- **802.11b**
- **802.11g**
- **802.11n**
- **802.11ac**

MiR robots cannot be fixed to 2.4 GHz or 5 GHz. The robots will connect to the best possible connection it has access to. Therefore, the frequency must be controlled by the network / SSID.

2.4 IP configuration

By default, the robot is set up to use DHCP, but the robot also supports setting up a static IP from the robot interface. If you use this option, you can specify the IP, netmask, DNS, and gateway for the robot.

When connected to MiR Fleet, each robot must have a unique static IP or a reserved DHCP assigned IP as MiR Fleet uses the IP to identify the robots.

MiR products only work with IPv4. The system is not compatible with IPv6, which is therefore disabled internally.

Due to the internal network configuration, MiR robots are unable to work on an external network with subnet 192.168.12.0/24.

2.5 Ports

All the listed ports are open on the robot's own network (the internal router). If any of the listed functionalities are to be used on an external network (for example your company network), these ports must be opened.

For MiR products running software version 2.10.0 and higher

Required:

- **Port 443:** used to access the robot interface and for communication through REST protocol (robot and fleet interface actions, MiR Fleet, WISE modules) through HTTPS.
- **Port 9090:** used for ROSbridge. Communication between certain robot functions and the robot interface.

Optional:

- **Port 22:** used for access through SSH (Secure Shell) for MiR personnel.
- **Port 80:** used to access the robot interface though HTTP.

- **Port 8080:** used for communication through the REST protocol (robot and fleet interface actions, MiR Fleet, WISE modules) through HTTP.
- **Port 1908:** used for communication to AI cameras.
- **Ports in range 43001 to 48000:** used for remote access for MiR personnel. The remote connection can be enabled and disabled through the robot interface.
- **Port 502:** required if Modbus is used through the company's network.
- **Port 8888:** used to access the recovery robot interface. This interface allows you to connect the robot to a WiFi network, connect it remotely for technical support, or restore to an old version of the software or the database.

For MiR products running software version 2.9.0.1 and lower

Required:

- **Port 80:** used to access the robot interface.
- **Port 8080:** used for communication through the REST protocol (robot and fleet interface actions, MiR Fleet, WISE modules).
- **Port 9090:** used for ROSbridge. Communication between certain robot functions and the robot interface.

Optional:

- **Port 22:** used for access through SSH (Secure Shell) for MiR personnel.
- **Port 1908:** used for communication to AI cameras.
- **Ports in range 43001 to 48000:** used for remote access for MiR personnel. The remote connection can be enabled and disabled through the robot interface.
- **Port 502:** required if Modbus is used through the company's network.
- **Port 8888:** used to access the recovery robot interface. This interface allows you to connect the robot to a WiFi network, connect it remotely for technical support, or restore to an old version of the software or the database.

2.6 DNS

MiR robots can work with company-specific DNS servers. By default, the robots have the Google DNS: 8.8.8.8 and 8.8.4.4.

2.7 Network security

MiR robots support different security protocols for wireless networks. All compatible protocols are listed below:

- **WPA/WPA2 Personal**
- **WPA/WPA2 Enterprise:**
  - LEAP
  - PEAP
  - EAP-TLS: Certificates only accepted in .pem or .p12 format.

WPA/WPA2 Enterprise requires the server to support TLS 1.2 or higher. MiR will not connect to the network using TLS 1.0 or older SSL encryption.

MiR robots can also connect to a hidden SSID. However, you should avoid using them when optimal roaming performance is required.

3. Planning your network

MiR recommends consulting a WiFi specialist to help determine and implement a sufficient wireless network infrastructure for your MiR application. The following sections describe how you can plan and determine a suitable WiFi network setup.

3.1 Site map and access point positions

The position of access points is dependent on multiple factors. The wireless signal can be degraded or lost if there are walls, shelves, or other obstacles in the way.

MiR recommends consulting a map of the entire site, and identifying the positions of current access points, or determining the ideal location for new access points. To help determine where access points would be best positioned, label the map with information such as:

- Infrastructure that may pose issues to the wireless signals, such as concrete walls and metal structures especially.
- For each access point note down:
  - the SSID (or SSIDs) exposed by the access point
  - the channel used
  - the radio mode, such as 2.4 GHz or 5 GHz
- Devices or machinery that generate radio frequency that may interfere with the access point signals, such as microwave ovens, cordless phones, and Bluetooth enabled devices.
- The number of people that are often within each room or building and whether they are likely to have personal devices such as phones or tablets. These devices and the density of people can also affect the wireless signal.

3.2 WiFi heatmap

Consult a WiFi expert to execute a site survey including a heatmap that you can use to identify any area with weak coverage. It is important that there is a strong WiFi signal everywhere across the site where MiR robots operate.

If there are areas that are not covered, see Improving your WiFi network on page 13 for suggestions on how you can improve your WiFi network.

4. Improving your WiFi network

If you have determined that your WiFi network is not sufficient, there are multiple methods to improve your WiFi coverage. MiR recommends consulting a WiFi specialist to identify the best way to improve your network. The following sections outline suggestions that you and the WiFi specialist can consider to improve the WiFi coverage.

If it is only some of your robots that have connection issues in certain areas, try to modify those robots as described in Robot modifications on page 18.

4.1 Radio frequency interference

If you have identified any access points that are located close to devices that generate radio frequency, you should consider the following:

- Do your MiR robots experience issues around the radio frequency source often?
- If they do, try to move the access point further away from the radio frequency source, and see if this improves the performance of the robots in the area.
- Try to arrange access points so they are within direct line of sight of each other.

4.2 Channel planning and overlapping coverage cells

Although radio frequency can interfere with the WiFi signal, the signals are affected more often by other WiFi signals. To minimize this interference, it is important to arrange and configure your access points as follows:

- Make sure that neighboring access points run on different channels.
- Ensure there is only enough overlap between coverage areas to ensure a safe handover when a robot connects from one access point to the other.

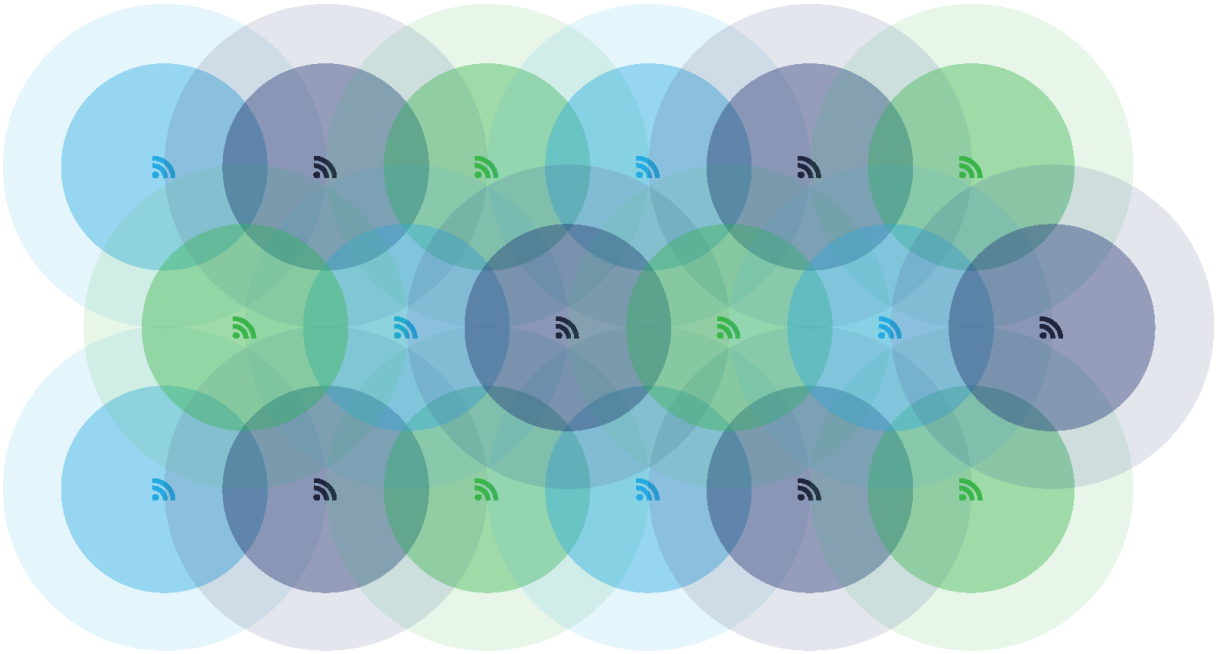

Figure 4.1. Illustration of a simplified scenario where access points cover a circular area in a site without any interference from structures or other devices. In this case three WiFi channels are used, and the access points are configured so there is the greatest distance possible between access points on the same channel.

Figure 4.1 shows a simplified case where only three frequencies are used. It is often better to use more frequencies so there is a greater distance between coverage areas on the same channel. This makes it possible to get better signal strength in the coverage area and less interference, meaning a better signal to noise ratio so higher data rates can be achieved.

Channel planning 2.4 GHz

When you are using a 2.4 GHz band, always use a channel width of 20 MHz per access point and avoid using channels where the frequencies overlap. Since channels are divided by only 5 MHz, you should only use channels with four or five channel intervals to avoid channels interfering.

In principle, 802.11n allows assigning two channels (40 MHz) per access point, but that interferes with too many channels and is only useful in simple cases with few access points.

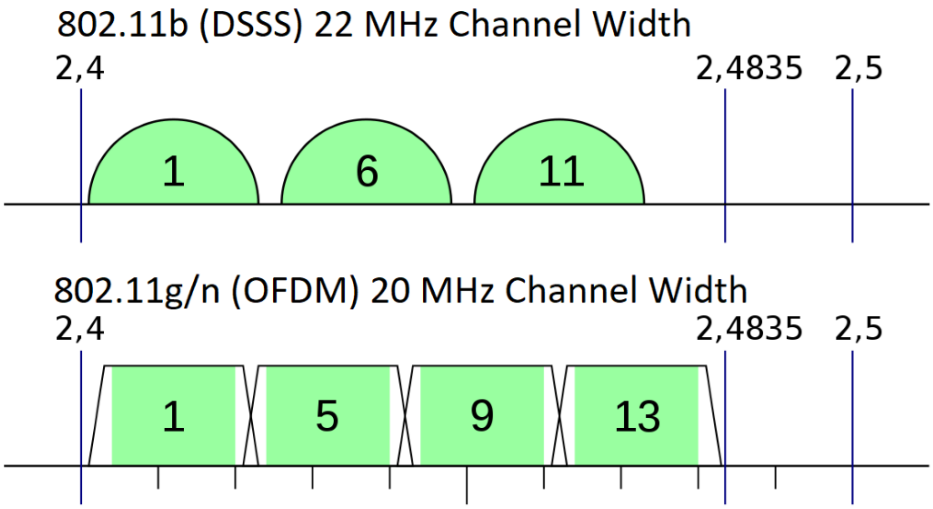

Figure 4.2. Channel separations on 802.11b and 802.11g/n standards.

There are two possible channel selections:

- If you are within the North American region, there are 1-11 channels available. To avoid interference between channels, only use channels 1, 6, and 11.
- If you are using 802.11b, the channels have a width of 22 MHz. To avoid interference between channels, only use channels 1, 6, and 11.
- If you are outside of North America and are not using 802.11b, there are often 1-13 channels available. To avoid interference between channels, only use channels 1, 5, 9, and 13.

Channel planning 5 GHz

There are significantly more channels available on a 5 GHz band. The available channels are region dependent. To determine which channels you can use in you region, consult a WiFi specialist.

All channels on a 5 GHz band have a frequency width of 20 MHz or a multiple of 20 MHz. Channels on a 5 GHz band are also divided by 5 MHz intervals, meaning that only every four channels are defined to ensure there is no overlap between channel frequencies.

If a sufficient number of channels is available to avoid interference , it can be advantageous to use two channels (40 MHz) per access point. When an access point uses two channels, it is able to transfer data twice as fast to and from the connected robots. Keep in mind, if each

access point uses two channels, the number of available frequencies is halved. You must ensure that you can keep the coverage area of access points that are using the same channels separated—see *Figure 4.1*.

For access points where the channel utilization is especially high, you can also use four channels (80 MHz) per access point. This can be efficient if only a few clients with high bandwidth requirements are connected. This is often not required for MiR products.

Increasing WiFi capacity with channel planning

To improve the WiFi capacity you cab adjust your channel configuration as follows:

- If there are a sufficient number of available channels, you can add more access points that are not using interfering channels, or increase the bandwidth used by each access point.
- If all available channels are in use, you can minimize the area of interference by reducing the power per access point. This will also decrease the signal strength and signal to noise ratio. Make sure these do not drop below the required value.
- To focus the signal strength within the coverage areas without increasing the signal strength in interference areas, you can use more directional antennas.
- Do not use access points connected to both the 2.4 GHz and 5 GHz band. Choose which of the bands you want to use, and make sure all access points are using that band. If significant bandwidth is required, use the 5 GHz band.

4.3 Minimum data rate

Setting the minimum data rate can improve a robot's ability to roam well between access points and improve the utilization of the WiFi capacity. The default minimum data rate for legacy 802.11b is 1 Mb/s and for newer standards it is 6 Mb/s. The following points describe why you may want to change the minimum data rate:

- Access points transmit beacons at the lowest available data rate per SSID. With a low data rate, a significant percentage of the capacity is wasted on transmitting beacons. With a high data rate, the beacons are transmitted faster and utilize less of the network capacity.
- Increasing the minimum data rate will make robots search for access points where they can transfer data faster. Many WiFi clients stick to an access point for as long as possible before changing, even if they can connect to access points with a stronger signal.

- The WiFi utilization is also improved, since robots do not spend as much time transferring data at low rates through access points where their connection is poor. With better roaming, the robots will spend more time transferring data through access points with a faster data rate.

At sites with good and stable WiFi coverage, it can be an advantage to increase the minimum data rate to 12-24 Mb/s. High density 5 GHz deployments may have an even higher optimal minimum data rate.

On sites where the WiFi coverage often varies, for example in warehouses where the WiFi is affected by changing inventory, it may be necessary to keep the minimum data rate low, to ensure that robots are always able to connect to an access point.

4.4 SSID and roaming considerations

If you are using multiple SSIDs, you should consider the following:

- Access points can transmit multiple SSIDs where each SSID provides a logical separation between different networks. All SSID's and access points on the same frequency share the same physical channel. Traffic on one SSID will degrade the performance (latency, packet loss, and data rate) on other SSIDs on the same channel. For this reason, critical SSIDs should therefor use their own channel, while secondary SSIDs can use another.
- Each SSID broadcasts a beacon at the minimum data rate. If the minimum data rate is high, adding additional SSID's does not impair the capacity significantly, but at low minimum data rates, the number of SSIDs should be limited to the ones you really need.

When configuring roaming (changing to an access point with a better signal), you should consider the following:

- For roaming to work, the access points must use the same SSID, use the IP addresses of the same network segment, and be in the same VLAN.
- To ensure the robots transition to other access points smoothly, there must be good secondary coverage. In other words, when a robot moves away from one access point, the signal strength from the next access point must be good before the signal quality from the first degrades—see Network requirements on page 6.

- The network should support fast reauthentication to other access points. You can limit the security measures to very basic WPA2-PSK to increase the authentication speed, but there are also other options for caching the keys for authentication which are just as fast and don't sacrifice security.
- Hidden SSIDs should be avoided when stable and optimal roaming performance is desired. Hidden SSIDs don't broadcast their name in beacons, making it impossible for robots to construct a list of possible access points to roam to in advance. As a result, the roaming behavior is negatively impacted when using hidden SSIDs.

4.5 Robot modifications

There are a few modifications you can apply to robots to improve their connection to the network:

- Robots are equipped with internal antennas —see the user guide for your robot for the antenna locations. If your robot is carrying a payload that obscures the antenna radiation pattern (often dense and large objects), consider applying the following actions to improve the connection:
  - Reposition the payload to be at least 4 cm from the antenna.
  - If your top module enables it, mount an external antenna where interference from the payload is minimized. Refer to the *Optional features* list under **Hardware** on the Distributor site for antennas provided by MiR.
- The internal antennas used by the robot do not have a powerful gain and are designed for 2.4 GHz. It can be beneficial to replace them with an antenna more suited for your wireless network.
- Each robot has a wireless access point enabling you to connect to its web-interface. This access point can interfere with other access points. Consider applying the following actions to improve the connection:
  - Turn off the access point on the robot to eliminate the interference. If you need to access the web-interface of that robot for either maintenance or to control it manually, you will need to connect to it via an Ethernet cable.
  - Dedicate a frequency to the robot access points that only they can use.

To modify the robot access points, contact MiR Technical Support for assistance.

5. Evaluating the network performance

If you meet the network requirements outlined in Network requirements on page 6 and are still experiencing issues with the WiFi connection to your MiR robots, you can contact MiR Technical Support for an analysis of your network from the robots' perspective. MiR Technical Support can retrieve network heat maps and MiR Fleet data logs to help you evaluate the performance of your wireless network.

6. Check list

To summarize the content of this guide, when planning or modifying your WiFi network it is recommended to do the following:

1. Ensure your network meets the requirements in Network requirements on page 6, or a set of network requirements determined by a WiFi specialist for your setup.
2. If possible, disable Load balancing and Airtime balancing on your access points.
3. Determine if your network capacity is suitable for the number of devices connected to your network.
4. If you are using MiR Fleet, make sure that:
   - MiR Fleet is connected to the network through Ethernet.
   - MiR Fleet is in the same physical location as the robot. Geographical distance will cause delay between MiR Fleet and robots.
5. Make sure your network uses one of the following network standards:
   - 802.11a
   - 802.11b
   - 802.11g
   - 802.11n
   - 802.11ac
6. If you are configuring the IP value, make sure to use IPv4.
7. Make sure you are not using subnet 192.168.12.0/24 with MiR robots.
8. Make sure the following ports are open:
   - Port 80
   - Port 8080
   - Port 9090
9. Make sure you are using one of the following security protocols:
   - WPA/WPA2 Personal
   - WPA/WPA2 Enterprise:
     - LEAP
     - PEAP
     - EAP-TLS: Certificates only accepted in .pem or .p12 format
10. If you are using WPA/WPA2 Enterprise, make sure the network server supports TLS 1.2 or higher.
11. Determine if there are areas in your site where there is high interference from the structure, personnel, and other devices.

12. Generate a WiFi heatmap to view the coverage of your access points to determine if there are areas where you need more access points, or the existing ones need to be reconfigured.
13. Check that devices generating radio frequency are not interfering with the signal from nearby access points.
14. Set up your access points so access points using the same channel do not have overlapping coverage areas.
15. Use either a 2.4 GHz or 5 GHz band.
16. Use every four channels to avoid interference.
17. Use directional antennas to focus the signals from the access points.
18. Reduce the power per access point to reduce the area of interference, but make sure the signal strength does not drop below the required value.
19. If your site has a stable and good WiFi coverage, increase the minimum data rate 12-24 Mb/s.
20. If you have a low minimum data rate (around 1-6 Mb/s), reduce the number of SSIDs.
21. Make sure all access points the robot uses are on the same SSID and VLAN and use IP addresses within the same network segment.
22. Avoid using hidden SSIDs on your network.
23. Make sure the network supports fast reauthorization to other access points.
24. Make sure the payload of the robot is not interfering with the antenna signal by:
    - Mounting an external antenna.
    - Repositioning the payload at least 4 cm from the antenna.
25. Consider replacing the internal antenna with one with a stronger gain and better support for 5 GHz.
26. You can turn off the access points on the robots to eliminate interference, or dedicate a channel that only the robot access points can use.