OMRON

AMR Wireless Communication

Technical Guide

72503-100 A

Cybersecurity

To maintain the security and reliability of the system, a robust cybersecurity defense program should be implemented, which may include some or all of the following:

Anti-virus protection

• Install the latest commercial-quality anti-virus software on the computer connected to the control system and keep the software and virus definitions up-to-date.

• Scan USB drives or other external storage devices before connecting them to control systems and equipment.

Security measures to prevent unauthorized network access

• Install physical controls so that only authorized personnel can access control systems and equipment.

• Reduce connections to control systems and equipment via networks to prevent access from untrusted devices.

• Install firewalls to block unused communications ports and limit communication between systems. Limit access between control systems and systems from the IT network.

• Control remote access and adopt multifactor authentication to devices with remote access to control systems and equipment.

• Set strong password policies and monitor for compliance frequently.

Data input and output protection

• Backup data and keep the data up-to-date periodically to prepare for data loss.

• Validate backups and retention policies to cope with unintentional modification of input/output data to control systems and equipment.

• Validate the scope of data protection regularly to accommodate changes.

• Check validity of backups by scheduling test restores to ensure successful recovery from incidents.

• Safety design, such as emergency shutdown and fail-soft operations in case of data tampering and incidents.

Additional recommendations

• When using an external network environment to connect to an unauthorized terminal such as a SCADA, HMI or to an unauthorized server may result in network security issues such as spoofing and tampering.

• You must take sufficient measures such as restricting access to the terminal, using a terminal equipped with a secure function, and locking the installation area by yourself.

• When constructing network infrastructure, communication failure may occur due to cable disconnection or the influence of unauthorized network equipment.

- Take adequate measures, such as restricting physical access to network devices, by means such as locking the installation area.

- When using devices equipped with an SD Memory Card, there is a security risk that a third party may acquire, alter, or replace the files and data in the removable media by removing or unmounting the media.

- Please take sufficient measures, such as restricting physical access to the Controller or taking appropriate management measures for removable media, by means of locking and controlling access to the installation area.

- Educate employees to help them identify phishing scams received via email on systems that will connect to the control network.

Contents

Cybersecurity 1

1. Intended Audience 4

2. Principles of Wireless Communication 5

3. Why and How AMRs Use Wi-Fi 10

4. Wireless Network Requirements 11

Communication Standards and Frequencies 12

Signal Strength and Availability 14

Bandwidth 14

Channels 15

Latency 19

Common problems 19

5. Configuring AMRs and IT Infrastructure for Initial Proof-of-Concept 19

Configuration 19

Validation Steps 22

Troubleshooting Flowchart 28

6. Network Planning and Design 29

Site Survey Considerations 30

Bandwidth Calculation 31

Channel Selection and Access Point Layout 33

Network Access and Topology 38

Firewall Access 38

Site Survey Checklist 42

8. Troubleshooting 44

9. Ongoing Monitoring and Maintenance 47

10. Additional Resources 50

1. Intended Audience

This document provides wireless communication guidance for the following groups:

- Technicians
- IT department
- 3rd-party Wi-Fi specialists
- Omron Product Support Specialists

The information covered applies to the phases of the project below:

Phase	Description
Initial sales process	Raise awareness that Wireless Ethernet is a mandatory and critical aspect of a fleet of AMRs
Proof of concept	Testing with single AMR in factory environment for purposes of verifying navigation, tool engagements, and basic Wi-Fi connectivity (Is a Fleet Manager useful and expected at this stage?)
Pre-deployment and network design	Review AMR specifications and network requirements, design and deploy Wi-Fi network
Pilot deployment and acceptance testing	Verify wireless performance of the AMR fleet
Maintenance	Monitor and maintain wireless performance

2. Principles of Wireless Communication

There are several key principles to recognize when working with wireless communication (Wi-Fi):

- Wi-Fi networks are shared resources that require careful design and engineering in order to satisfy all consumers. There are many potential Wi-Fi clients in addition to AMRs, such as cellphones, handheld scanners, PCs, and factory equipment. In addition, it should be designed to accommodate not only current demands, but future needs as well.

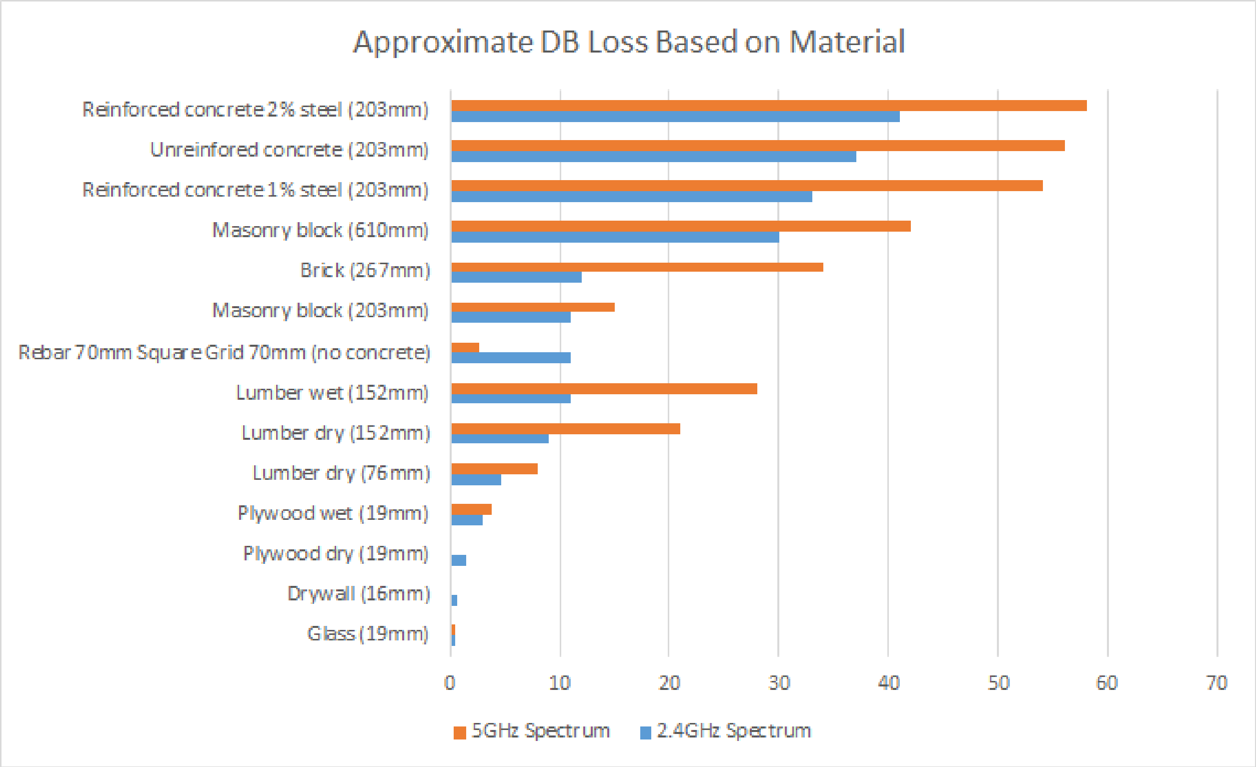
- Signal quality is more important than strength. A signal's quality can be impacted by multiple factors:

Factor	**Description**	**Analogy**
Attenuation	Reduction in strength as the signal passes through materials within the environment	Similar to how sound gets muffled when passing through a wall. Once a sound gets sufficiently muffled then you may no longer be able to interpret what it is.
Multi-path reflectivity	The RF signal can be reflected by materials within the environment, causing the same signal to arrive at the client at slightly different times and with slightly different strengths.	Similar to how sound might echo in an open room. If the echo is loud enough, it can impact how well you can hear it.
Background noise/Noise floor	Many things can emit radio waves on similar frequencies as Wi-Fi devices. Sources of noise are typically referred to as background noise. The level of noise is typically referred to as the noise floor.	Similar to the level of sound in a busy factory or a room full of people. Even if you're not speaking, the room may have a high level of noise.
Co-channel interference	Interference from other Wi-Fi access points. While this is similar to background noise, this type of interference is typically cited as co-channel interfered because it can have a different impact on the Wi-Fi	With co-channel interference, it would be similar to two people talking directly to you at the same time in a language that you understand. This will be more difficult to understand than if one person is talking in a language that

	client than non-Wi-Fi sources of interference.	you do not understand, which would be more similar to background noise.

- Wi-Fi signals are not immune to interference attenuation, reflections, and obstruction. Impact will vary depending on material, thickness and spectrum. Below is a guideline of expected attenuation for various materials:

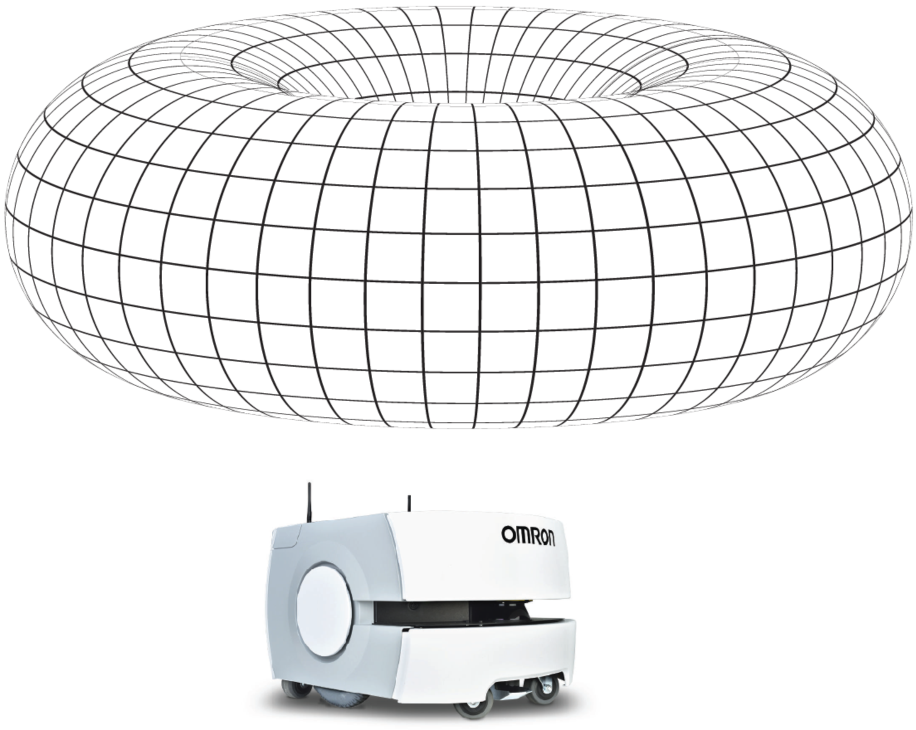
Material (Thickness)	**2.4GHz Spectrum**	**5GHz Spectrum**
Glass (19 mm)	0.4	0.4
Drywall (16 mm)	0.7	0
Plywood dry (19 mm)	1.4	0.2
Plywood wet (19 mm)	2.9	3.9
Lumber dry (76 mm)	4.6	8
Lumber dry (152 mm)	9	21
Lumber wet (152 mm)	11	28
Rebar 70 mm Square Grid 70 mm (no concrete)	11	2.6
Masonry block (203 mm)	11	15
Brick (267 mm)	12	34
Masonry block (610 mm)	30	42
Reinforced concrete 1% steel (203 mm)	33	54
Un-reinforced concrete (203 mm)	37	56
Reinforced concrete 2% steel (203 mm)	41	58



Data courtesy of NIST Electromagnetic Signal Attenuation in Construction Materials

- Antennas have shapes to their coverage. In addition, antennas can be easily damaged. Care should be taken when selecting the location for the antenna on the AMR payload structure.

- LD-series AMRs use a dipole antenna, which is very commonly used. Dipole antennas have a donut-shaped field of coverage, which makes them very well suited to communicating with access points that are on the same elevation as the AMR.



- Channel availability varies by country, and not all channels are available everywhere. Always check with local regulatory authorities. For example, below is a table showing availability of 2.4GHz channels around the world:

Channel	**North America (FCC)**	**Japan**	**World**
1	Yes	Yes	Yes
2	Yes	Yes	Yes
3	Yes	Yes	Yes
4	Yes	Yes	Yes
5	Yes	Yes	Yes
6	Yes	Yes	Yes
7	Yes	Yes	Yes
8	Yes	Yes	Yes
9	Yes	Yes	Yes
10	Yes	Yes	Yes
11	Yes	Yes	Yes
12	---	Yes	Yes
13	---	Yes	Yes
14	---	802.11b only	---

- RF interference and weak signal are the most common causes of poor performance.

- Troubleshooting requires a methodical, layered approach. Recommend working both from top-down and from bottom-up to understand which pieces of the system are working as desired and which piece(s) might be experiencing performance degradation.

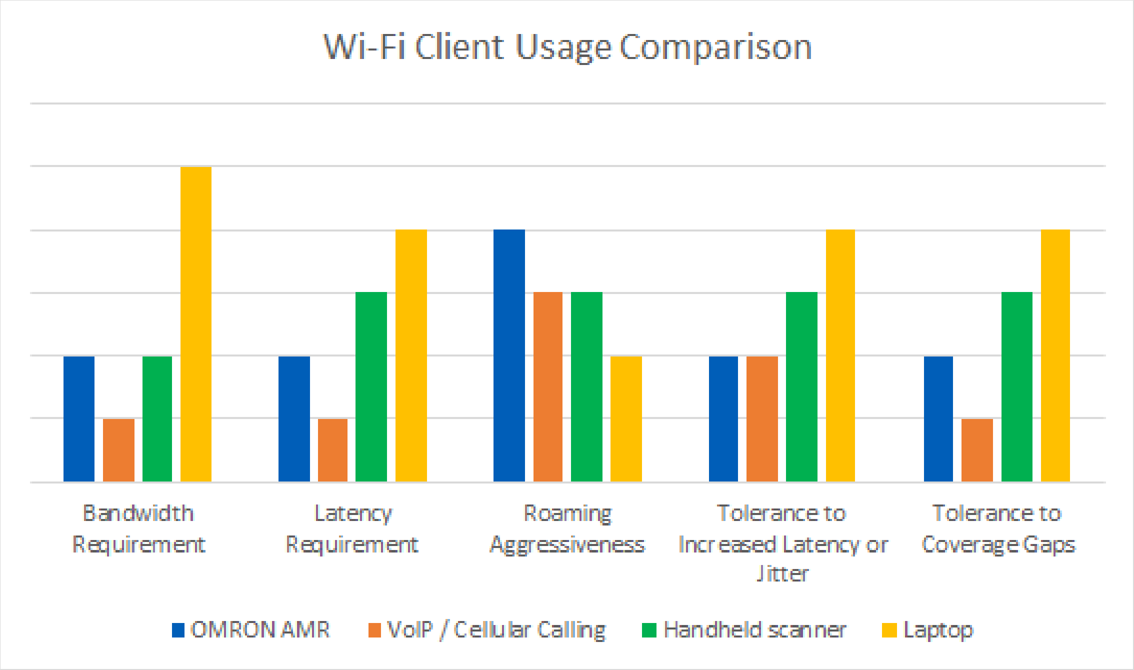
3. Why and How AMRs Use Wi-Fi

AMRs use Wi-Fi for a variety of purposes, as described below:

- Multi-robot traffic behaviors
    - Sharing robot location across the fleet
    - Sharing and coordinating path segments when in close proximity with each other
    - Sending/receiving configuration data
- Command/control
    - Monitoring location, status, and battery state to use in determination of job assignment
    - Dispatching new jobs and sending progress updates
    - Managing charging, standby goals, buffering, and performing IO-handshaking with other factory equipment
- Monitoring and maintenance
    - Updating configuration settings
    - Sending raw sensor data to operator
    - Allowing human override and reset
    - Retrieving log files
    - Applying software updates
    - Performing manual operations calibration routines

Wi-Fi clients can have widely varying usage characteristics. For instance, someone using Wi-Fi on their phone in order to send and receive email will have different requirements than a PC user who is streaming video, and so on. It's important to understand the different characteristics so the network can be designed to properly handle all clients.

Below is a simple overview of how OMRON AMR usage characteristics compare to other common devices:



4. Wireless Network Requirements

Typical AMR communication takes place over wireless Ethernet so it is imperative to have high-quality wireless coverage in the AMR's operating environment. This requires working closely with your IT department throughout the entire development cycle from initial PoC, to network design, deployment, and long-term maintenance.

The table below lists network requirements. The sections that follow provide additional information about each item.

Category	**AMR Requirement**
Bandwidth (per AMR)	50 Kbps average* 500 Kbps when being monitored by MobilePlanner*
Latency	Recommended: <= 10 ms Maximum allowable: 50 ms

Wireless communication standards	802.11a (recommended) 802.11b 802.11g
Signal strength	Ideal case: >= -40 dBm Recommended minimum: -60 dBm
Security methods	Open WPA-PSK WPA2-PSK PEAP-MSCHAPv2 EAP-TLS
Frequency / Channels	2.4GHz / 5GHz Available channels vary by frequency band and region

**Varies depending on exact configuration, as well as MobilePlanner and other client activity.*

Communication Standards and Frequencies

While a device is connected to the wireless network, it communicates using the chosen frequency band for that network (e.g. 2.4 GHz or 5 GHz). It is important to determine which frequency band is suitable for the type of communication needed; each has its own advantages and disadvantages. For example: The 2.4 GHz band is better suited for longer-range communication at a lower bitrate, while the 5 GHz band allows for higher bitrate but its signal will be more easily blocked by objects in the environment.

Each IEEE 802.11 wireless standard has a specified frequency band. The table below describes the supported wireless standards and frequencies available for AMRs.

Wireless Standard	**Speed/Data Rate**	**Frequency Band**	**Notes**
802.11a (Wi-Fi 2)	54 Mbps*	5 GHz Shorter range than 2.4 GHz More susceptible to attenuation from obstructions, like solid walls and other objects Easier to find available channels due to large number of non-overlapping channels	Recommended for AMR networks
802.11b (Wi-Fi 1)	11 Mbps*	2.4 GHz Longer range than 5 GHz Often suffers from congestion and interference due to very small number of non-overlapping channels and large number of 2.4GHz-enabled devices (e.g. microwave ovens, cordless phones, IoT devices, smartphones, PCs, etc.)	802.11b is still supported by OMRON AMRs but is not recommended due to significant performance limitations
802.11g (Wi-Fi 3)	54 Mbps*		Attempts to combine the best of 802.11a and 802.11b Backward compatible with 802.11b network adapters Network slows to 802.11b device speed (if present)

** Theoretical*

Signal Strength and Availability

In order for a wireless device to send and receive data on the network, the signal must be transmitted at an appropriate power level (or strength) in order to be received well. Signal strength is measured in decibels relative to a milliwatt (dBm). OMRON recommends the following for signal strength:

- -40 dBm or greater (ideal)
- -60 dBm (minimum)

The wireless network should provide constant service throughout the workspace. Consider the following for signal availability:

- AMR fleets require constant access; this an operational requirement. For a single AMR or those isolated from others, partial signal coverage might be acceptable in workspace areas where sending commands or receiving status from the AMR is not necessary.
- Do not obstruct the wireless antennas on the AMRs with metal or other objects that can degrade the signal. Refer to the AMR’s user manual for more information about the location of wireless antennas.
- Choosing a 2.4 GHz frequency versus a 5 GHz frequency will depend on the site survey results to account for factors such as existing frequencies, interference, or other objects that can reduce signal strength and coverage.

Bandwidth

All devices that access a wireless network consume bandwidth. Larger AMR fleets will consume more wireless resources. Additionally, bandwidth usage varies by application and can be affected by configuration, monitoring, payload accessories, and other factors.

Consider the following for bandwidth:

- Use a dedicated network to restrict wireless network access to AMRs.
- Use security to prevent other devices from accessing the network.
- Bandwidth consumption may increase or decrease depending on the types of commands and debugging tools that are enabled in MobilePlanner.
- File downloads such as DebugInfo, or viewing log files in SetNetGo are examples of functions that may increase bandwidth usage.
- Port forwarding for attached devices can also affect bandwidth. Refer to *Fleet Operations Workspace Core User's Manual (Cat. No. I635)* for more information.

Channels

Each frequency band is divided into a number of individual channels.

The 2.4 GHz band ranges from 2400 MHz to 2500 MHz, covering a total of 100 MHz. Channels are 20 MHz wide (802.11b) or 22 MHz wide (802.11g). Thus, adjacent channels overlap with each other and can interfere, so it is important to choose channels that do not overlap (such as channels 1, 6, and 11 in the table).

The 5 GHz band ranges from 5150 MHZ to ~5900 MHz, covering a total of roughly 750 MHz. Channel width is also adjustable from 20 MHz to 100 MHz. The 5 GHz band has many more non-overlapping channels than 2.4 GHz. This provides greater flexibility when choosing channels and minimizing channel interference across access points and other networks. This, in part, is why the 802.11a standard is better suited for AMR networks.

Channel numbers and center frequencies for different wireless standards are shown in the tables that follow. Please note that available channels are region-specific, so not all channels may be usable.

Channel #	802.11b (MHz)	Non-overlapping channel sets					802.11g (MHz)	Non-overlapping channel sets			
1	2401–2423	1	2	3	-	-	2402–2422	1	2	3	-
2	2406–2428				4		2407–2427				4
3	2411–2433					5	2412–2432	5			
4	2416–2438	6					2417–2437		6		
5	2421–2443		7				2422–2442			7	
6	2426–2448			8			2427–2447				8
7	2431–2453				9		2432–2452	9			
8	2436–2458					10	2437–2457		10		
9	2441–2463	11					2442–2462			11	
10	2446–2468		12				2447–2467				12
11	2451–2473			13			2452–2472	13			
12	2456–2478				-		2457–2477		-		
13	2461–2483					-	2462–2482			-	
14	2473–2495	14					-				

Channel # (20 MHz)	Frequency Range (MHz)	40 MHz Channels	80 MHz Channels	160 MHz Channels
32	5150–5170			
36	5170–5190	38	42	50
40	5190–5210			
44	5210–5230	46		
48	5230–5250			
52	5250–5270	54	58	
56	5270–5290			
60	5290–5310	62		
64	5310–5330			
68	5330–5350	70	74	82
72	5350–5370			
76	5370–5390	78		
80	5390–5410			
84	5410–5430	86	90	
88	5430–5450			
92	5450–5470	94		
96	5470–5490			
100	5490–5510	102		

104	5510–5530		106	114
108	5530–5550	110		
112	5550–5570			
116	5570–5590	118	122	
120	5590–5610			
124	5610–5630	126		
128	5630–5650			
132	5650–5670	134	138	X
136	5670–5690			
140	5690–5710	142		
144	5710–5730			
-	5730–5735	-	-	-
149	5735–5755	151	155	163
153	5755–5775			
157	5775–5795	159		
161	5795–5815			
165	5815–5835	167	171	
169	5835–5855			
173	5855–5875	175		
177	5875–5895			

Latency

Latency refers to the amount of time that passes between sending a packet to a client and receiving a reply back. A ping test can be used to measure the amount of round-trip time (RTT), in milliseconds. High latency produces a noticeable delay. Obstructions, weak signals, interference, and network congestion can contribute to high latency. OMRON's 10 ms requirement is considered to be very low latency.

Common problems

A low-quality connection can cause problematic AMR behavior such as:

- Frequent disconnections, which may lead to an AMR failing to reconnect and requiring user intervention.
- Network packet loss, leading to unexpected behavior such as failure to perform jobs or failure to move to a Goal.
- Collisions among AMRs when operating in close proximity.
- Inconsistent propagation of configuration parameters.
- Difficulty in monitoring with MobilePlanner, FLOWiQ, or other client software tools.
- Delays in sending job commands or receiving status updates.

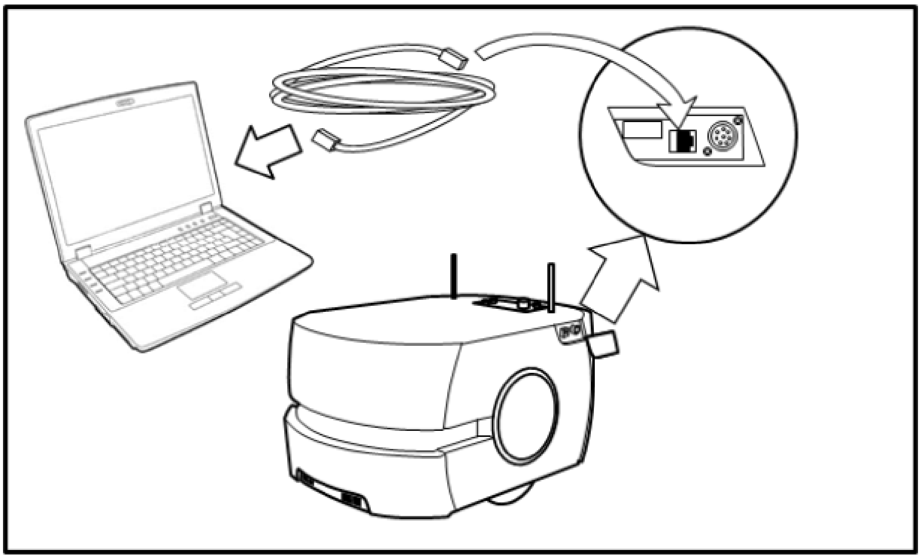
5. Configuring AMRs and IT Infrastructure for Initial Proof-of-Concept

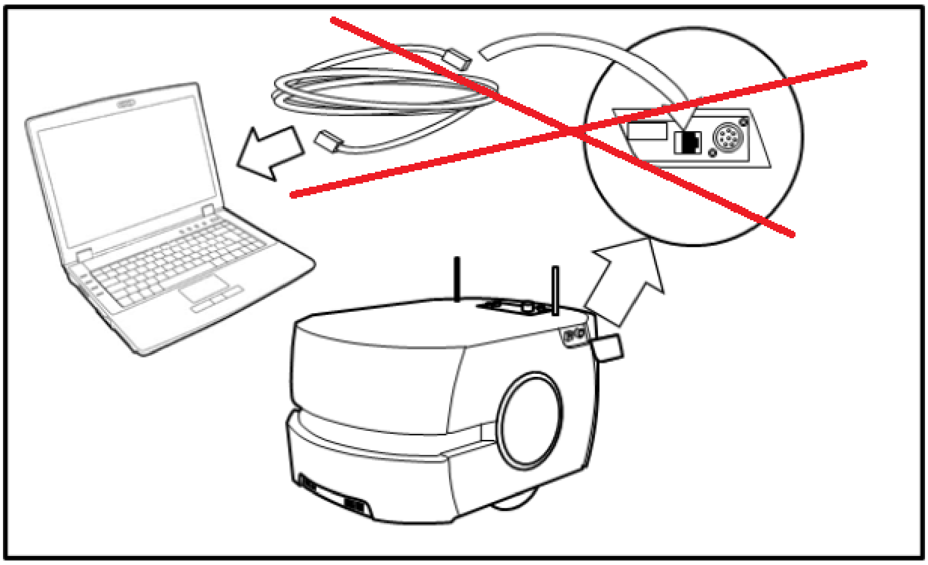
For each phase of the project, actions must be taken to ensure a quality Wi-Fi connection. The sections that follow outline the appropriate steps to take:

- Configuration
- Validation Steps
- Troubleshooting Flowchart

Configuration

The initial sales process (or proof of concept) phase requires a single AMR and operating environment. During this phase, basic configuration takes place. This serves to validate basic functionality. A map of the AMR's environment is also created.

Steps	Description
Connect PC to AMR with Ethernet cable	Configure your PC to use a 1.2.3.x IP for an LD-series AMR, and connect an Ethernet cable to the Maintenance port (as shown below). 
Configure the AMR for wireless communication	Using the SetNetGo tab in MobilePlanner: 1. Click on the Network Tab then the Wireless Ethernet page. 2. Navigate to IP Settings and choose the radio button for the appropriate IP assignment for the network. Input the information for the IP address, netmask, and gateway. Certain IP address ranges are reserved. IP addresses in the range of 1.2.3.x should not be used on LD-series AMRs, and addresses in range 169.254.x.x should not be used on HD/MD AMRs. 3. Under WiFi Network Settings, select your network name/SSID from the list of available networks. 4. Under Security Settings, choose the appropriate encryption and authentication methods for the network. 5. Under Radio Settings, choose the appropriate Radio Mode for the network.

Optionally configure the AMR to connect to a Fleet Manager, if available	Using the Configuration tab in MobilePlanner: 1. Navigate to the AMR's Configuration Tab. 2. Click on the Fleet category. 3. Click on Enterprise Manager Connection. 4. Check the box for *ConnectToFleetManager.* 5. Input the IP address for the Fleet Manager in *FleetManager Address.* 6. Save the configuration.
Test the basic Wi-Fi configuration (Performance is not important at this stage)	Remove network cable, and perform the following tests: 1. Check Wi-Fi association. 2. Run ping test out from AMR. 3. Check ping from PC. 4. Check connection to Fleet Manager (if using one). 5. Test throughput. 6. Watch AMR through MobilePlanner while navigating between points in the facility. See below for validation information. 

Optional, additional proof of concept steps	1. Create a map of the space using MobilePlanner. 2. Test navigation between sample tools and endpoints. Refer to the AMR's user manual and *Fleet Operations Workspace Core User's Manual (Cat. No. I635)* for guidance.
Perform preliminary Wi-Fi site survey (see *Site Survey Checklist* in *Section 6, Network Planning and Design*)	1. Record Wi-Fi security information. 2. Identify other types of Wi-Fi users such as PCs, handheld scanners, vehicles. 3. Take pictures and identify types of obstacles and building materials, such as metal structures, cement walls, mesh fencing. 4. Identify potential sources of interference such as Wi-Fi devices and non-Wi-Fi emitters (radios, microwave ovens). 5. Get a sense of the overall square footage of the facility.

Validation Steps

The table below provides more information about each step. Each test relies on success of the previous test, so tests should be performed in order listed below. The steps can also been seen in the *Troubleshooting Flowchart* that follows this section.

Step	Description	Indication
Verify boot up	Using MobilePlanner, attempt to connect to SetNetGo at 1.2.3.4. (This is the lowest-level troubleshooting method that allows communication with the AMR. This method should always be attempted if having trouble with Wi-Fi communication).	SetNetGo OS has booted

Verify that FLOW is running	Using MobilePlanner, attempt to connect to Configuration tab and Fleet tab at 1.2.3.4.	• Indicates that FLOW software is installed and running • Note any popups that may indicate configuration or hardware errors. Resolve any errors before proceeding. Refer to AMR user's manual for more information.
Verify Wi-Fi network detection from client	Navigate to Network / Wireless Ethernet section. Check list of available networks.	If the expected SSID never appears in the list then it could indicate: • Incorrect mode or channel settings. Use 802.11a/b/g (auto), and change Channel Setting to use Auto. • Weak signal. Try moving closer to access point. • Failed AMR hardware. Check antenna and antenna cable connections. Try associating with another device to verify proper settings.

Verify Wi-Fi association from client	Navigate to Network / Wireless Ethernet section. Check Status field.	• If Status field indicates Disconnected and remains that way for several minutes, then it likely indicates: o Incorrect SSID. o Incorrect mode or channel. o Incorrect auth type. • If Status field toggles between Disconnected, Connecting, and Connected, then it likely indicates: o Correct authentication type but invalid certificate, passphrase, or user credentials. o Incorrect auth settings or security policy on the access point. o Weak signal. o Hardware problems. • If Status field indicates Connected and remains that way for several minutes then it likely indicates: o Compatible Wi-Fi mode and channel. o Proper SSID. o Compatible encryption and authentication.

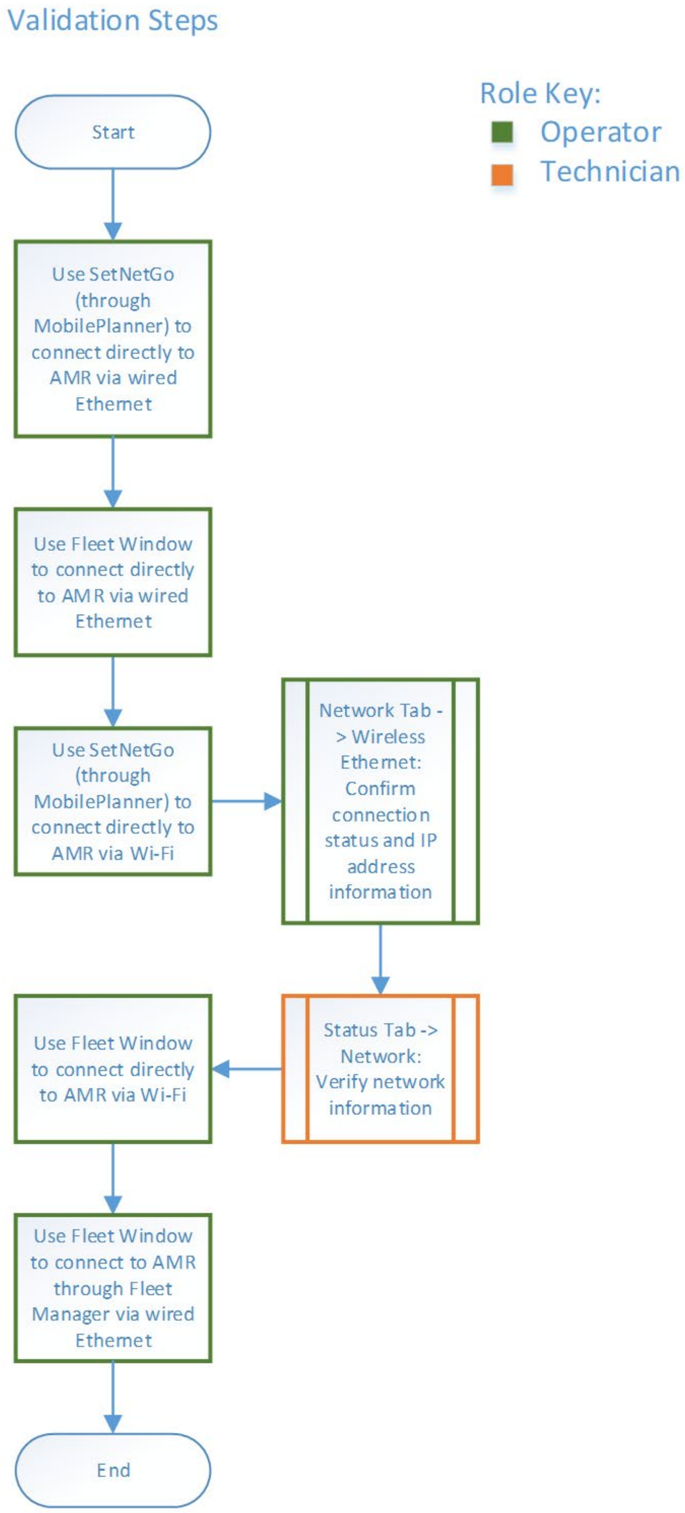
Verify basic Wi-Fi connectivity (client-side) using SetNetGo tab	Navigate to Network / Utilities and perform ping test using IP address of the gateway.	• If ping returns no packets then it likely indicates: o Incorrect IP address. Try pinging from another device. o Weak signal. Try moving closer to the access point. o Bad hardware. Verify antennas and antenna cables. Try pinging from another device. o Incorrect security policy on the access point. Verify with IT. • If ping returns 1-4 packets, then it likely indicates: o Proper Wi-Fi configuration: ▪ Compatible Wi-Fi frequency, mode, and channel ▪ Proper SSID ▪ Compatible encryption and authentication o Proper security policy on the access point.

	Navigate to Network / Utilities and perform ping test to Fleet Manager (optional).	• If ping returns no packets, then it likely indicates: ○ Incorrect IP address of Fleet Manager. Test from another device. ○ Firewall or other network blockage between AMR and Fleet Manager. Check with IT. • If ping returns 1-4 packets, then it likely indicates: ○ Access from AMR to Fleet Manager.
Verify basic Wi-Fi connectivity (network-side)	Using a ping tool on PC, run simple ping test to the AMR's IP address.	• If ping returns no packets, then it may indicate: ○ Incorrect IP address of AMR. ○ Incorrect Wi-Fi configuration on PC. Try pinging other IP addresses on the LAN. ○ Firewall or other network blockage between AMR and Fleet Manager. Check with IT. • If ping returns 1-4 packets, then it likely indicates: ○ Operational Wi-Fi configuration of PC and AMR. ○ Proper network routing (if PC and AMR are on different subnets). ○ No firewall blockage between PC and AMR.

Verify access to Fleet Window on AMR via Wi-Fi	Using MobilePlanner, connect to the AMR's IP address and open the Fleet tab.	If tab opens, then it likely indicates: • Proper Wi-Fi configuration on AMR. • Proper Wi-Fi configuration on PC. • FLOW running on AMR.
Verify that AMR is connected to Fleet Manager, and Fleet tab is accessible via Wi-Fi	• Using MobilePlanner, connect to the Fleet Manager’s IP address and open the Fleet tab. • Check to see that the AMR is displayed.	If tab doesn't open, then it may indicate: • Incorrect IP address for Fleet Manager. • Incorrect network access between PC and Fleet Manager. • Fleet Manager not operational. If tab opens but AMR is not displayed, then it could indicate: • Fleet Manager is booted and accessible from PC. • Potential network blockage between AMR and Fleet Manager. • Incorrect Fleet Manager configuration on AMR. If tab opens and AMR is displayed, then it indicates: • Both Fleet Manager and AMR are properly booted. • Proper Wi-Fi configuration on the AMR and PC. • Fleet Manager and AMR can access each other across the network.

Troubleshooting Flowchart

See below for a visual representation of the validation steps:

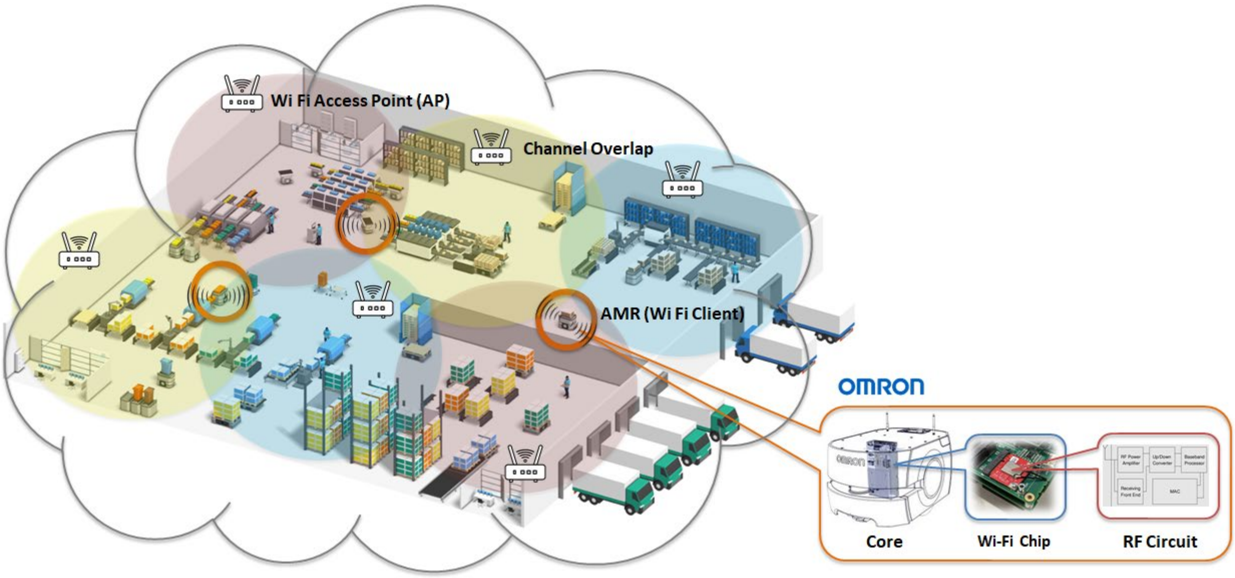


Validation Steps
Role Key:
🟩 Operator
🟧 Technician
Start
Use SetNetGo (through MobilePlanner) to connect directly to AMR via wired Ethernet
Use Fleet Window to connect directly to AMR via wired Ethernet
Use SetNetGo (through MobilePlanner) to connect directly to AMR via Wi-Fi
Network Tab -> Wireless Ethernet: Confirm connection status and IP address information
Status Tab -> Network: Verify network information
Use Fleet Window to connect directly to AMR via Wi-Fi
Use Fleet Window to connect to AMR through Fleet Manager via wired Ethernet
End

6. Network Planning and Design

The following takes place during this phase:

- Site survey considerations
- Bandwidth calculation
- Channel selection and access point layout
- Network access and topology
- Firewall access
- Site survey checklist



Site Survey Considerations

It is important to collect information about the current wireless network and environment in order to understand how it can be better suited for AMRs. Document the following and evaluate:

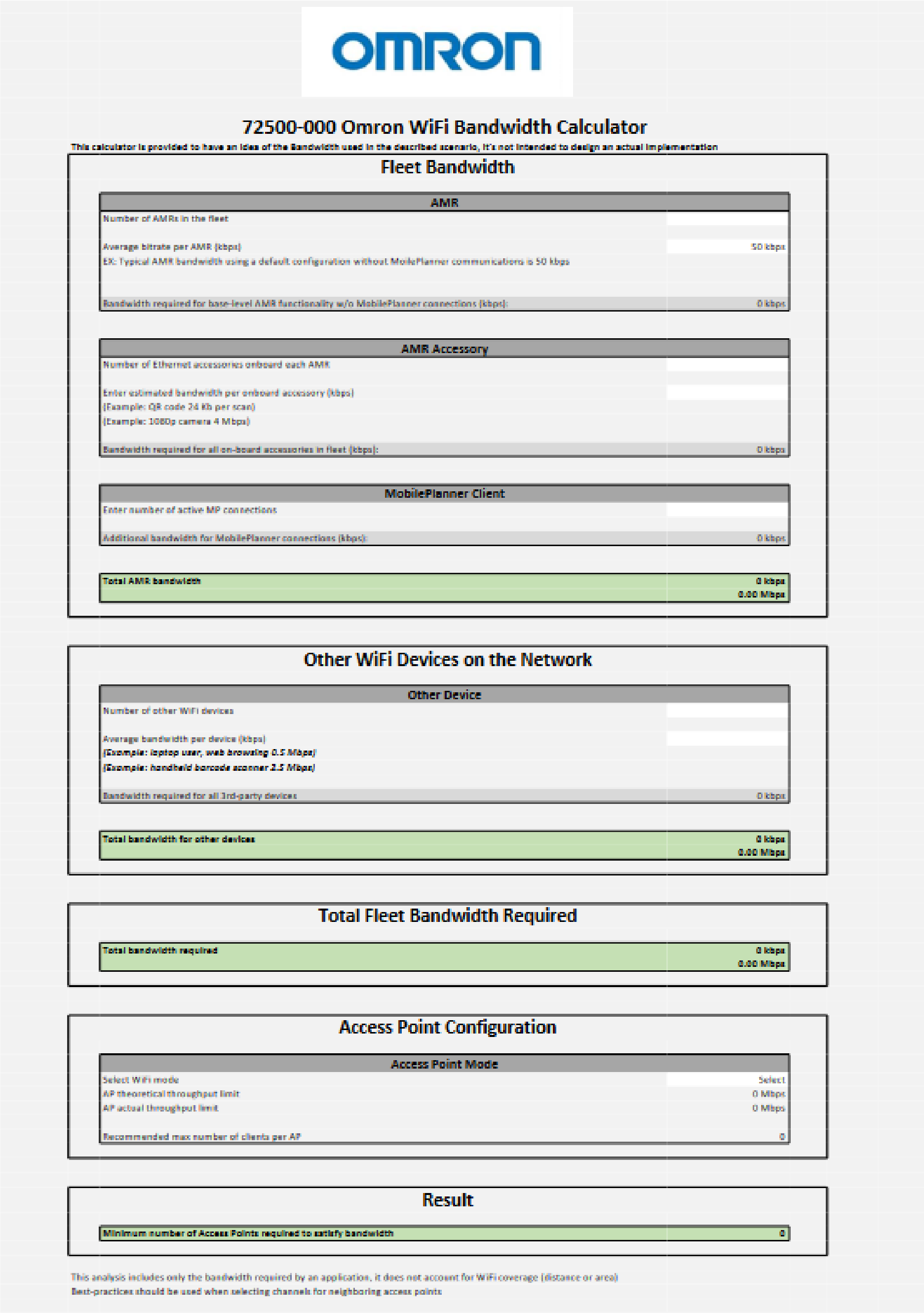
Physical Environment	• Items that may obstruct wireless signals: Walls, doors, windows, and other objects (especially if they are constructed of metal or concrete) • Items that also generate radio frequencies, such as microwave ovens, cordless phones and radios, Bluetooth-enabled devices such as PCs or tablets • Number of people typically in the area who may be carrying personal devices
RF Environment	• Access point locations • SSID(s) associated with the access points • Radio frequencies and channels used • Channels used
Wi-Fi Clients	• Type of clients • Approximate bandwidth requirements • Roaming characteristics • Wi-Fi mode and security requirements
Predicted Roam Locations	• Transitional spaces, such as passing through metal or block walls • Entry into tools where metal tooling and machines may cause dramatic fluctuation in signals
Wireless Coverage	• Heatmap showing signal strength, channel overlap, and gaps in coverage (site survey generated by IT professional)

Bandwidth Calculation

OMRON provides a simple bandwidth calculator to help account for overall requirements (OMRON PN: 72500-000). The table below can also be used.

Line #	Description	Sub-total
1	Number of AMRs in the fleet	
2	Average bitrate per AMR	
3	**Multiply lines 1 and 2.** **This is the total bandwidth for AMR → Fleet Manager connections.**	
4	Number of Ethernet accessories onboard each AMR	
5	Estimated bandwidth per onboard accessory (kbps)	
6	**Multiply lines 1, 4 and 6.** **This is the total bandwidth for onboard devices.**	
7	Number of active MP connections	
8	**Multiple line 6 by 450kbps.**	
9	Number of other Wi-Fi devices on the network	

10	Average bandwidth per other Wi-Fi client	
11	**Multiply lines 9 and 10.** **This is the total bandwidth for other Wi-Fi clients.**	
Total		
12	**Add lines 3, 6, 8 and 11.** **This is the total estimated bandwidth required for your Wi-Fi network.**	



72500-000 Omron WiFi Bandwidth Calculator

This calculator is provided to have an idea of the Bandwidth used in the described scenario, it's not intended to design an actual implementation

Fleet Bandwidth

AMR	
Number of AMRs in the fleet	
Average bitrate per AMR (kbps)	50 kbps
EX: Typical AMR bandwidth using a default configuration without MobilePlanner communications is 50 kbps	
Bandwidth required for base-level AMR functionality w/o MobilePlanner connections (kbps):	0 kbps

AMR Accessory	
Number of Ethernet accessories onboard each AMR	
Enter estimated bandwidth per onboard accessory (kbps)	
(Example: QR code 24 Kb per scan)	
(Example: 1080p camera 4 Mbps)	
Bandwidth required for all on-board accessories in fleet (kbps):	0 kbps

MobilePlanner Client	
Enter number of active MP connections	
Additional bandwidth for MobilePlanner connections (kbps):	0 kbps

Total AMR bandwidth	**0 kbps** **0.00 Mbps**

Other WiFi Devices on the Network

Other Device	
Number of other WiFi devices	
Average bandwidth per device (kbps)	
(Example: laptop user, web browsing 0.5 Mbps)	
(Example: handheld barcode scanner 2.5 Mbps)	
Bandwidth required for all 3rd-party devices	0 kbps

Total bandwidth for other devices	**0 kbps** **0.00 Mbps**

Total Fleet Bandwidth Required

Total bandwidth required	**0 kbps** **0.00 Mbps**

Access Point Configuration

Access Point Mode	
Select WiFi mode	Select
AP theoretical throughput limit	0 Mbps
AP actual throughput limit	0 Mbps
Recommended max number of clients per AP	0

Result

Minimum number of Access Points required to satisfy bandwidth	**0**

This analysis includes only the bandwidth required by an application, it does not account for WiFi coverage (distance or area)
Best-practices should be used when selecting channels for neighboring access points

Once you have calculated the total overall bandwidth, you can compare that to the expected throughput from a single access point. Then select the number of access points that exceeds the required bandwidth, accounting for a margin due to expected versus theoretical throughput.

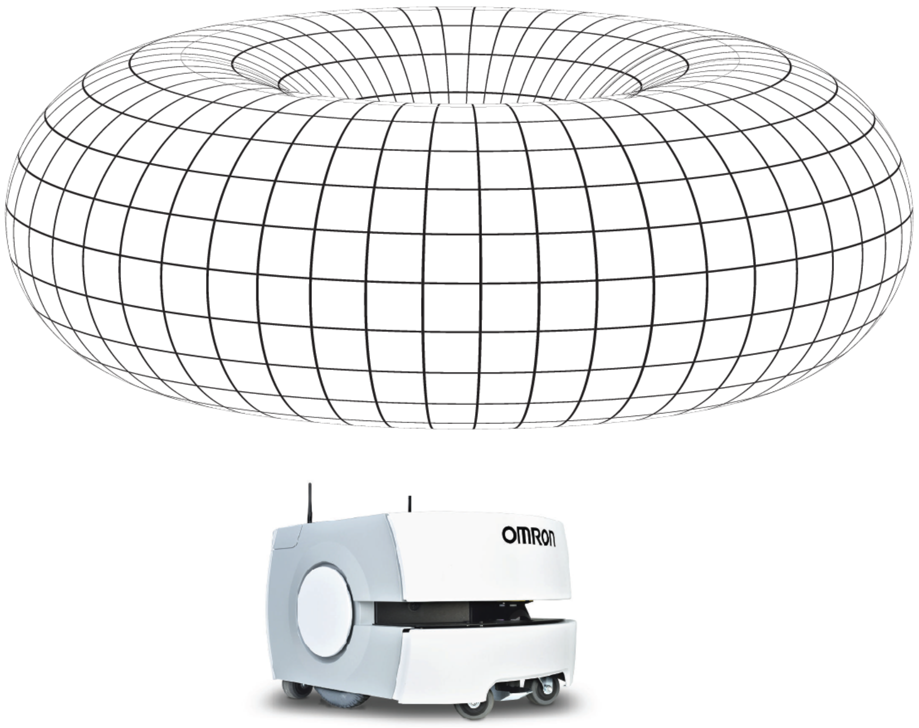
In addition, it is important to consult manufacturer's documentation for limitations of number of clients per access point.

Channel Selection and Access Point Layout

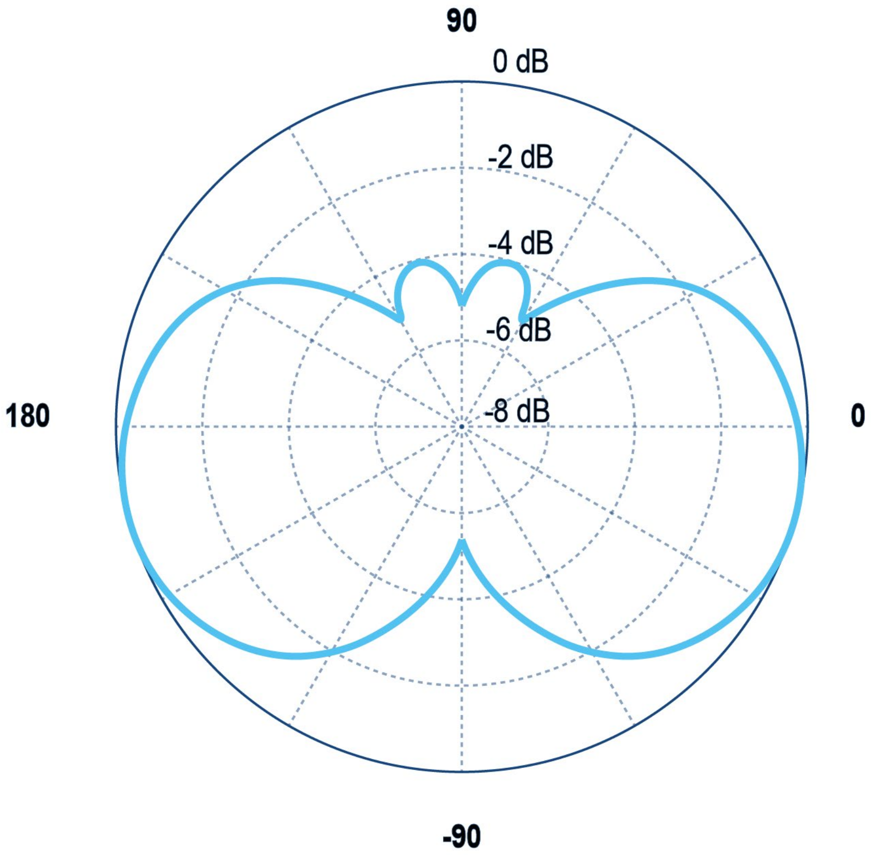
The two most important steps for a Wi-Fi network are to ensure adequate signal strength in all target locations, and minimize background noise and co-channel interference. If these steps are overlooked then the symptoms can range from minor inconvenience to complete factory shutdown. Thus it is imperative to take access point placement and channel selection into account when designing the network.

Access Point Placement

Antennas have different shapes of radiation. Most access points come with either external dipole or internal, integrated antennas. In both cases the field of coverage is similar to the standard dipole antenna, which is a full 360 degrees in the horizontal direction, and roughly 60-90 degrees in the vertical direction. The images below show the dipole antenna over an LD-series AMR and the cross-section of the dipole coverage pattern.



Shape of dipole antenna coverage over an LD-series AMR.



Cross-section of dipole antenna coverage. In this image, the access point would be positioned horizontally at the bullseye.

Most access points are designed to be ceiling-mounted so the dipole shape is well-suited to providing coverage to clients that are on the same floor. As a result, the access point should typically be located ~20-30 feet from the floor. Consult the manufacturer's specifications to select and mount the access points according to their design.

In certain cases, different antennas can be selected. For instance, if the access point is located at the end of a long, narrow corridor, then it may be advantageous to select a directional antenna (or patch antenna). This will focus the energy in a narrower beam through the length of the hallway. In other cases it might be appropriate to install higher-gain antennas, depending on the type of cabling that is used between antenna and access point.

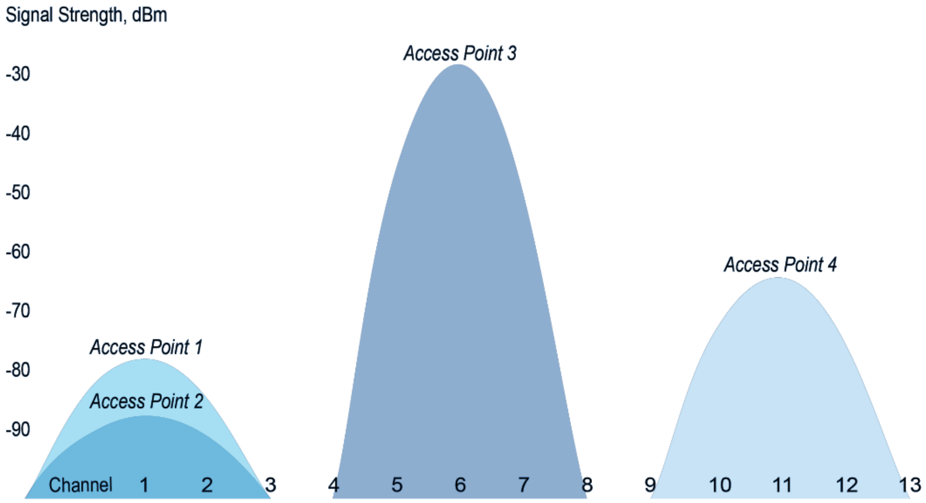
Using different antennas or antenna cables may cause the device to operate outside of regulating specifications. Always consult manufacturer's specifications and country regulations to ensure compliance.

Channel Selection

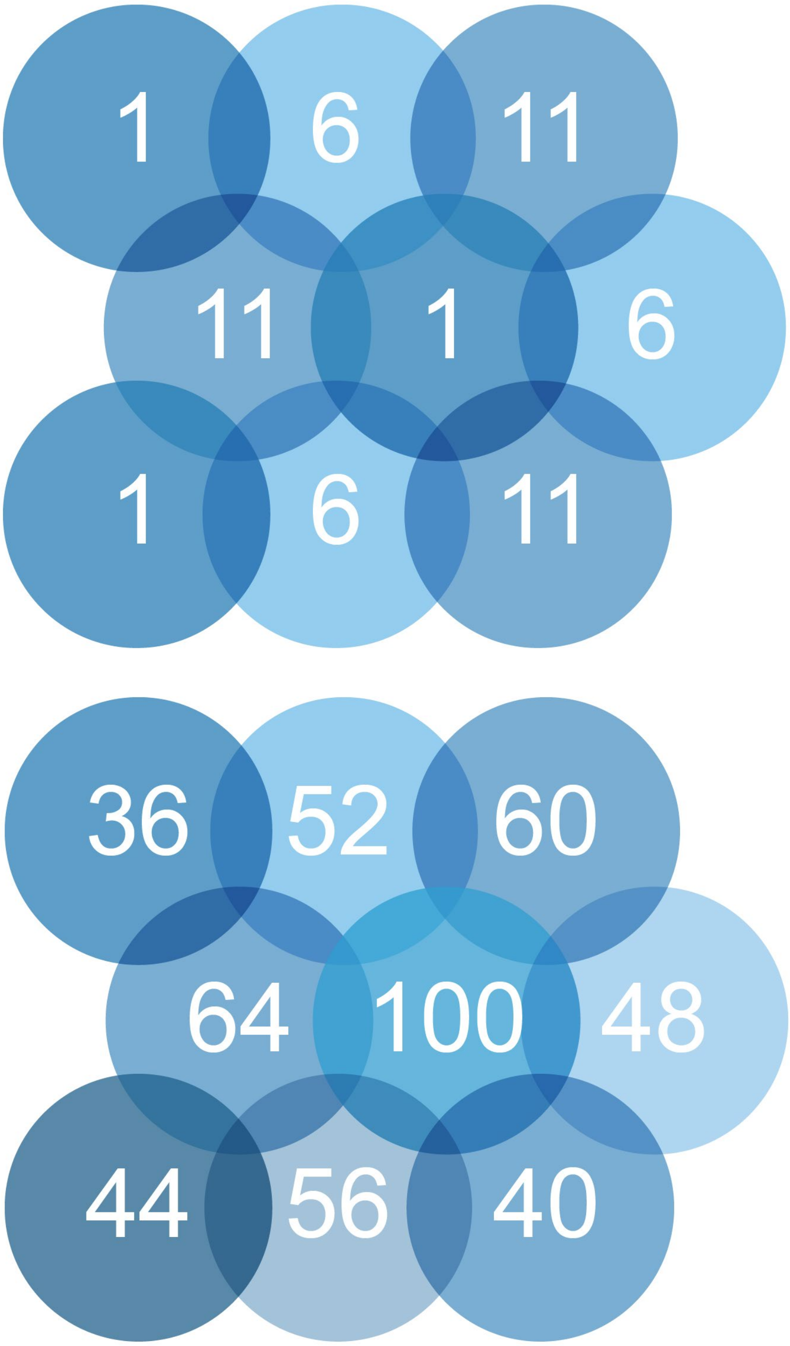
As noted previously, different bands of Wi-Fi have different channel widths. In some cases neighboring channels in a spectrum can directly overlap, such as with 802.11b/g in the 2.4 GHz range. In other cases the channels are unique from each other, as in 802.11a with 5 GHz range.

Always select channels for your access points that allow adjacent access points to be on different channels. Alternatively, enable the automatic channel selection feature of your access points. However, automatic channel selection works best when one single wireless controller is managing all Wi-Fi access points in the environment. If there are multiple controllers being used (such as for neighboring companies or manufacturing lines), then it may be necessary to use manual channel assignment to avoid conflict and unexpected changing of channel assignments.

Prior to selecting channels, it is recommended to perform a site survey to understand the noise floor and the channel utilization of any existing equipment. Perform the scan during normal operating hours to ensure that it is a representative sample.



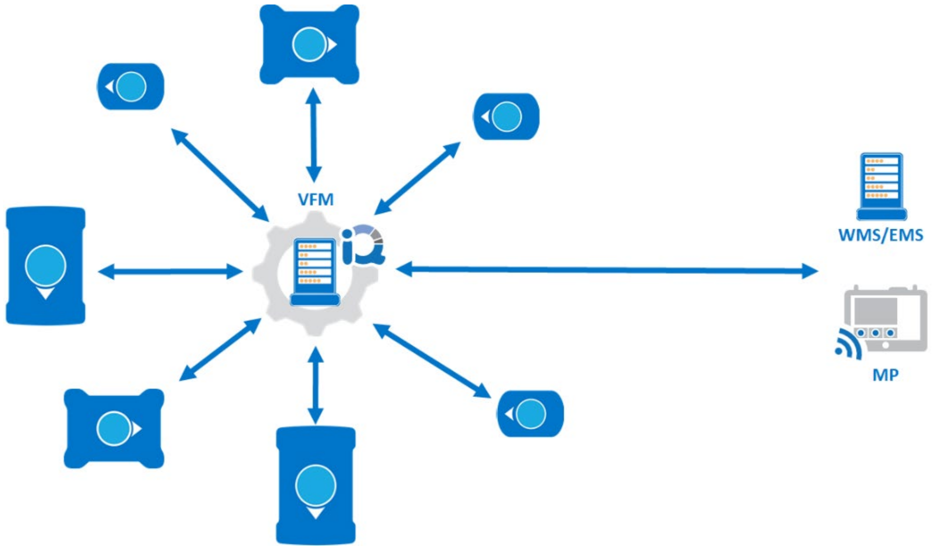
Example showing Wi-Fi channel scan for 802.11g (2.4 GHz). Note the overlap into neighboring channels.



Sample channel layout for 802.11g (2.4 GHz) shown above, and 802.11 (5 GHz) shown below.

Network Access and Topology

The OMRON AMR fleet uses a star network topology. Each AMR communicates with the Fleet Manager, and the Fleet Manager shares information with each AMR in the fleet, as well as with other servers and clients (as shown below).



Depending on the application, it is possible for the AMRs to also have direct communication with factory tools for purposes of handshaking.

Firewall Access

OMRON AMRs communicate with the Fleet Manager using several different ports. It is important to ensure that bidirectional communication is allowed on all required ports between the Wi-Fi infrastructure and the AMRs. Failure to provide adequate firewall access can lead to inability to operate the fleet.

In addition, any other equipment or servers that communicate with the Fleet Manager will need access to ports listing here. This includes WMS/MES and MP clients.

Below is a listing of required TCP and UDP network ports.

Port	Protocol	Category	Initiator to Recipient	Details
37	TCP	Intra-fleet Communications Ports Used to broadcast configuration updates to AMRs, to dispatch job commands, and to share position and trajectory updates throughout the fleet	AMR to Fleet Manager	Maintenance, Management, and Fleet ports use this.
5000	TCP/UDP			Fleet port uses this.
Range 10000 and up	UDP			For UDP Range 10000 connections and up, such as an AMR connecting to a Fleet Manager, this protocol grows with the number of AMRs. For best results, allocate at least twice as many UDP ports as there are AMRs in the fleet. For instance, a fleet of 20 AMRs should have an allocated range of 10000-10039.
7272	TCP/UDP			
1884	TCP			
5672	TCP	Integration Toolkit TCP Ports Excludes dynamically allocated port numbers	RabbitMQ AMQP	
8443	TCP		ITK REST	
5432			PostgreSQL	
443	TCP	Configuration and Monitoring of Fleet	Client PC to Fleet Manager	Maintenance and Management ports use this.

Range 7272 and up	TCP/UDP	Used for MobilePlanner connections to the Fleet Manager and AMRs for monitoring and configuration	Client PC to Fleet Manager	This protocol uses as many ports as there are AMRs. Each AMR that connects uses the next available port >= 7272. For best results, allow a large number of ports, such as 7272-7999.
7272	TCP/UDP		Client PC to AMR*	
Range 10000 and up	UDP		Fleet Manager to Client PC	This protocol uses as many ports as there are AMRs. Each AMR that connects uses the next available port >= 10000. For best results, allow a large number of ports such as10000-10999.
10000	UDP		AMR to Client PC*	
7171	TCP	Job Monitoring and Submission (ARCL Interface) Used for managing jobs on the Fleet Manager, typically submitted from a Warehouse Management System (WMS) or Manufacturing Execution System (MES)	WMS/MES to Fleet Manager	If ARCL Server is enabled in the configuration (Robot Interface -> ARCL Server Setup), then this port is open on the Fleet Manager and accepts unlimited incoming connections. The port number is configurable. This port may or may not be available on the AMR, depending on the application.

Configurable port #	TCP		Fleet Manager to WMS/MES	If Outgoing ARCL Connection is enabled in the configuration (Robot Interface -> Outgoing ARCL Connection Setup), then the Fleet Manager initiates an outgoing connection to the specified hostname and TCP port number.
123	TCP	Optional	Fleet Manager to NTP server	If you enable an NTP client Fleet Manager (SetNetGo -> System -> Date/Time), the Fleet Manager attempts to set its clock from the NTP sever at the specified IP address. This function is available on the AMR if you do not use a client Fleet Manager.
Range 1000 - 65535	TCP/UDP		Offboard devices to AMR	If RS232 or Ethernet Port Forwarding is enabled on the AMR (SetNetGo -> Network), then the configured TCP ports are open on the AMR for incoming connections.

** Optional - Only if connecting directly to AMR with MobilePlanner on a client PC.*

Site Survey Checklist

See below for the site survey checklist, originally contained in *LD-Series Integration Guide (Cat. No. I680).*

Wi-Fi bandwidth requirements for all devices
AMR: __________ Kbps
Controller: __________ Kbps
HMI: __________ Kbps
Other devices:
______________________: __________ Kbps
______________________: __________ Kbps
______________________: __________ Kbps
______________________: __________ Kbps
______________________: __________ Kbps
Network information
Wireless network name: ____
Type of network (Production, Administrative, etc.): __________________________
Explanation (if this is not an exclusive network): ______________________________
____
Devices using this network
Controllers: ____

PCs: ____

Material Tracking: ____

EMS/WMS: ____

IoT: ____

Available Wi-Fi technology in the plant (Check all that apply)

802.11a _________

802.11b _________

802.11g _________

802.11n _________

802.11ac _________

AMR Wi-Fi configuration

Static IP address: ___________________________

Subnet mask: ___________________________

Gateway: ___________________________

DNS server(s): ___________________________

SSID for AMR network: ___________________________

Network mode: Must be set to “Infrastructure.”

Radio mode: ___________________________

Channel set: ___________________________

Wireless watchdog IP address: ___________________________

Wireless watchdog max count (0 disables): ___________________________
Security encryption: ___________________________
Authentication method: ___________________________

8. Troubleshooting

Below is a list of potential root causes of Wi-Fi issues, along with potential indicators and mitigations.

Cause	Indicators	Mitigation
Inadequate signal coverage	• Weak signal strength reported by one AMR (see wifiLog.txt, iQ, MP) • Strong signal strength reported in third-party survey tool	• Confirm unobstructed antennas on AMR payload structure. • Confirm proper antenna extension cables for AMR payload structure. • Replace antennas and antenna cables. • Replace AMR hardware.
	• Weak signal strength reported by multiple AMRs (see wifiLog.txt, iQ, MP) • Weak signal strength reported by third-party survey tool	• Install additional access points. • Relocate existing access points to avoid barriers.

Co-channel interference	• Multiple access points appearing on overlapping channel (see wifiScanLog.txt) • Overlapping or channel re-use reported in third-party survey tool	• Adjust channels on neighboring access points. • Adjust transmit power-level on neighboring access points. • If using 802.11g, switch to 802.11a.
General RF interference	• Noise reported in third-party survey tool • Overlapping or channel re-use reported by third-party tool • Sporadic and intermittent failure to associate or remain associated • Sporadic and intermittent throughput problems as reported by AMR (MobilePlanner, download testing) and/or third-party ping tool or bandwidth test (such as iPerf)	• Change frequency band (5GHz instead of 2.4GHz). • Change channels. • Locate source of interference and relocate or shield.
Incompatible or misconfigured security	• AMR displays the proper SSID in list in SetNetGo Network page • AMR logs the expected access point(s) in wifiScanLog.txt • AMR never reports association for 10+ minutes after booting up And: • AMR reports failure to associate in SetNetGo Network page, or: • wpa_supplicant logs reports failure to attempt to associate due to incorrect auth type (see wpa_supplicant log reference)	• Review wpa_supplicant logs and access point logs. • Ensure AMR and access point authentication types match. • Ensure AMR and access point security credentials (certificate username, password) match. • Test with another security type on a different network.

Incompatible or misconfigured channels	• AMR does not show expected access point in SetNetGo / Network / Wireless Ethernet / Available Networks list • AMR works in one part of facility but not in another	• Verify that channels for all access points are in the configuration for the AMR. • Try using different channels, and/or try Auto.
Failed AMR hardware (antenna, cables, card)	• Connectivity or performance issues that are specific to one AMR in the fleet but not others And: • Weaker signal than other AMRs when in same location • Intermittent and sporadic failure, sometimes requiring a reboot	• Confirm unobstructed antennas on AMR payload structure. • Confirm proper antenna extension cables for AMR payload structure. • Replace antennas and antenna cables. • Replace AMR hardware. • Confirm LD failed Wi-Fi card (AC7260).
Incorrectly configured access point	• AMR can connect to Fleet Manager without problems when associated to other access points And: • AMR reports "Connected" but is able to ping out, and is unable to be pinged when connected to one particular access point	• Verify access point configuration with IT.

Incorrect security policy	• AMR is normally able to connect to Fleet Manager, for hours or days at a time And: • AMR will periodically lose connectivity from Fleet Manager but will report that it is connected when viewed through SetNetGo Network / Wireless / Status • AMR will regain network connectivity after specific duration (such as 180 minutes) • Pattern repeats itself with same frequency	• Possible misconfiguration on access point security policy. • Possible interoperability issues between AMR and APR infrastructure.

9. Ongoing Monitoring and Maintenance

Once a fleet reaches a production status, FLOW iQ and MobilePlanner are used to monitor and maintain the fleet, along with third-party tools.

FLOW iQ is an analytical tool that tracks, stores and displays a fleet’s operational status and performance using a graphical format. It provides current and historical data to plan and take preemptive actions for fleet optimization purposes. The FLOW iQ application and associated database are included in the Fleet Operations Workspace Core package. This application runs on the Fleet Manager.

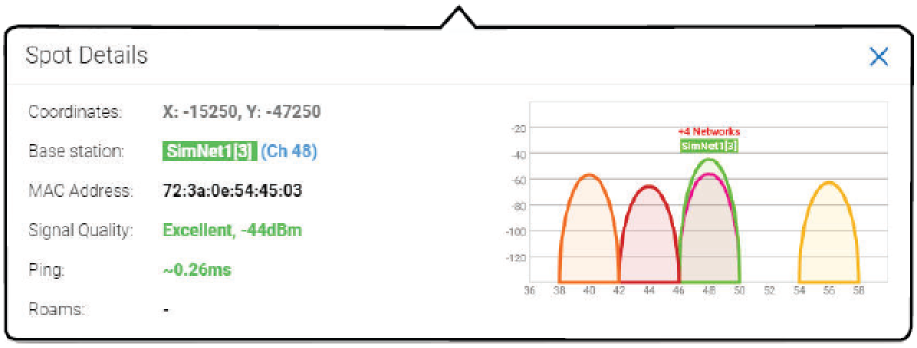
FLOW iQ includes the following graphics. Each graphic can be filtered to display operational data for the entire fleet or a specific AMR. Refer to Section 3, *Operation* for more information about accessing these areas.

Metric	**Description**
Robot Status	This indicates how the fleet or a single AMR is utilized over a 24-hour period as a percentage.
Job History	This indicates the jobs and job segments performed for the selected time period.
Battery Info	This indicates the battery performance for the fleet or individual AMRs for the selected time period.
Position Density Map	This indicates how often the fleet or a single AMR visits different parts of the fleet map as a total count.
Localization Map	This provides the localization score as a percentage for areas of the map.
Wireless Quality Map	This provides wireless signal strength by map location as a percentage.
Robot Fault Map	This provides the distribution of AMR faults over selected time intervals on the fleet map. This area also provides details about each fault and can be sorted for the entire fleet or a specific AMR.

Of particular note, the Wireless Diagnostics area is used to analyze wireless network performance and functionality, using the following metrics:

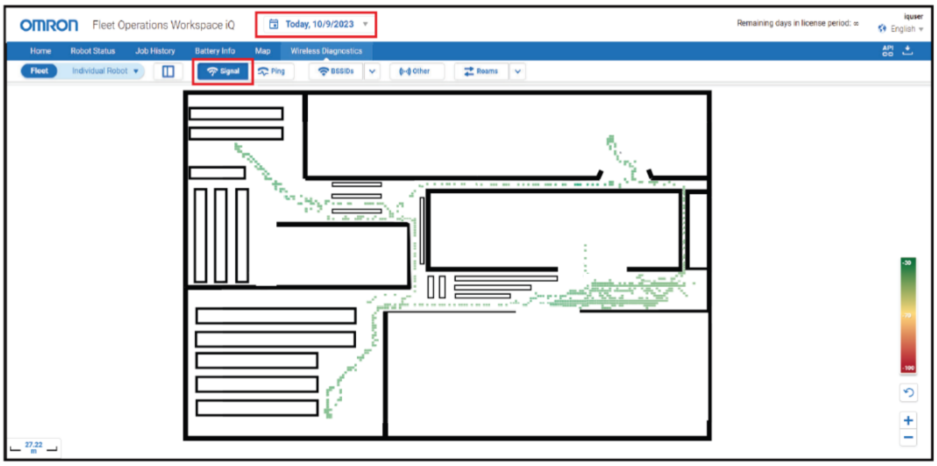
Values	Description
Coordinates	X and Y coordinates of that map point
Base Station	Wireless access point and channel
MAC Address	Device MAC address alias generated from the SSID and a number, used for system identification
Signal Quality	Quantitative and numeric value (dBm) of signal at that point, when available
Ping	Ping time, if available
Roams	BSSID connection switch, at that access point

Wireless Diagnostics collects data and displays it as Spot Details when the point is clicked in the Signal, Ping, BSSIDs, and Roams maps. Spot Details shows the fleet signal level, not an individual AMR, even when Individual Robot is selected.


Spot Details

Coordinates:	X: -15250, Y: -47250
Base station:	SimNet1[3] (Ch 48)
MAC Address:	72:3a:0e:54:45:03
Signal Quality:	Excellent, -44dBm
Ping:	~0.26ms
Roams:	-

The details can be displayed in a map view, helping to quickly identify potential areas of signal loss, or performance degradation:



In addition, there are a wide variety of tools available to enterprise IT departments to monitor items such as:

- Health and online status of network switches, servers, access points, and other infrastructure.
- Proactive monitoring of service availability for outage, degradation, or other blockage.
- Monitoring of software versions and availability of security updates.

10. Additional Resources

- Omron Mobile Robotics Document Library
- Contact your local OMRON representative.

OMRON Corporation **Industrial Automation Company**

Kyoto, JAPAN **Contact : www.ia.omron.com**

Regional Headquarters

OMRON EUROPE B.V.
Wegalaan 67-69, 2132 JD Hoofddorp
The Netherlands
Tel: (31) 2356-81-300 Fax: (31) 2356-81-388

OMRON ASIA PACIFIC PTE. LTD.
438B Alexandra Road, #08-01/02 Alexandra
Technopark, Singapore 119968
Tel: (65) 6835-3011 Fax: (65) 6835-3011

OMRON ELECTRONICS LLC
2895 Greenspoint Parkway, Suite 200
Hoffman Estates, IL 60169 U.S.A.
Tel: (1) 847-843-7900 Fax: (1) 847-843-7787

OMRON ROBOTICS AND SAFETY TECHNOLOGIES, INC.
4225 Hacienda Drive, Pleasanton, CA 94588 U.S.A.
Tel: (1) 925-245-3400 Fax: (1) 925-960-0590

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower, 200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-6023-0333 Fax: (86) 21-5037-2388

Authorized Distributor:

1124 (1124)