WHITE PAPER

PROFINET Over Industrial WLAN Infrastructure

Tony Chen
Product Manager

MOXA®

1. Introduction

With the emerging AIoT and IIoT trends, an increasing number of connected devices are being introduced into industrial operations at a faster pace than ever before. At the same time, wireless connectivity has opened up new doors for many mobile applications and has gained traction in recent years within the industrial sector. We are now seeing more wireless applications which are very difficult or impossible to achieve in conventional wired networks, such as Automated Guided Vehicles (AGVs), Automated Storage and Retrieval Systems (ASRS), and factory automation machinery.

More and more industrial control and automation planners are embracing the benefits of wireless communication and are integrating wireless infrastructure into their system design. This document aims to communicate the protocol requirements, deployment considerations, challenges, and Moxa's solutions to support one of the most popular industrial communication protocols, PROFINET, in wireless networks.

Specifically, this whitepaper provides an overview of the basic PROFINET requirements and configuration variables needed to obtain an acceptable performance margin in a wireless environment. In addition, this paper provides several example scenarios of industrial wireless applications using Moxa's WLAN solutions to serve as a frame of reference for planning out a wireless PROFINET deployment.

Released on June 30, 2020

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things (IIoT). With over 30 years of industry experience, Moxa has connected more than 65 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service. Information about Moxa's solutions is available at www.moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

2. PROFINET Overview

PROFINET is the PROFIBUS International (PI) industrial Ethernet standard designed for automation control communication over Ethernet-based infrastructure. Its modular range of functions and ability to operate in existing Ethernet infrastructure make it a flexible and scalable solution for many automation control applications. PROFINET has since developed into one of the most widely adopted protocols in industrial automation systems and process control networks today. According to PI North America, some 26 million accumulated PROFINET devices were operating in the automation market in 2018. Figure 1 illustrates the growth curve of PROFINET devices in recent years.

https://us.profinet.com/record-year-profinet-node-count/

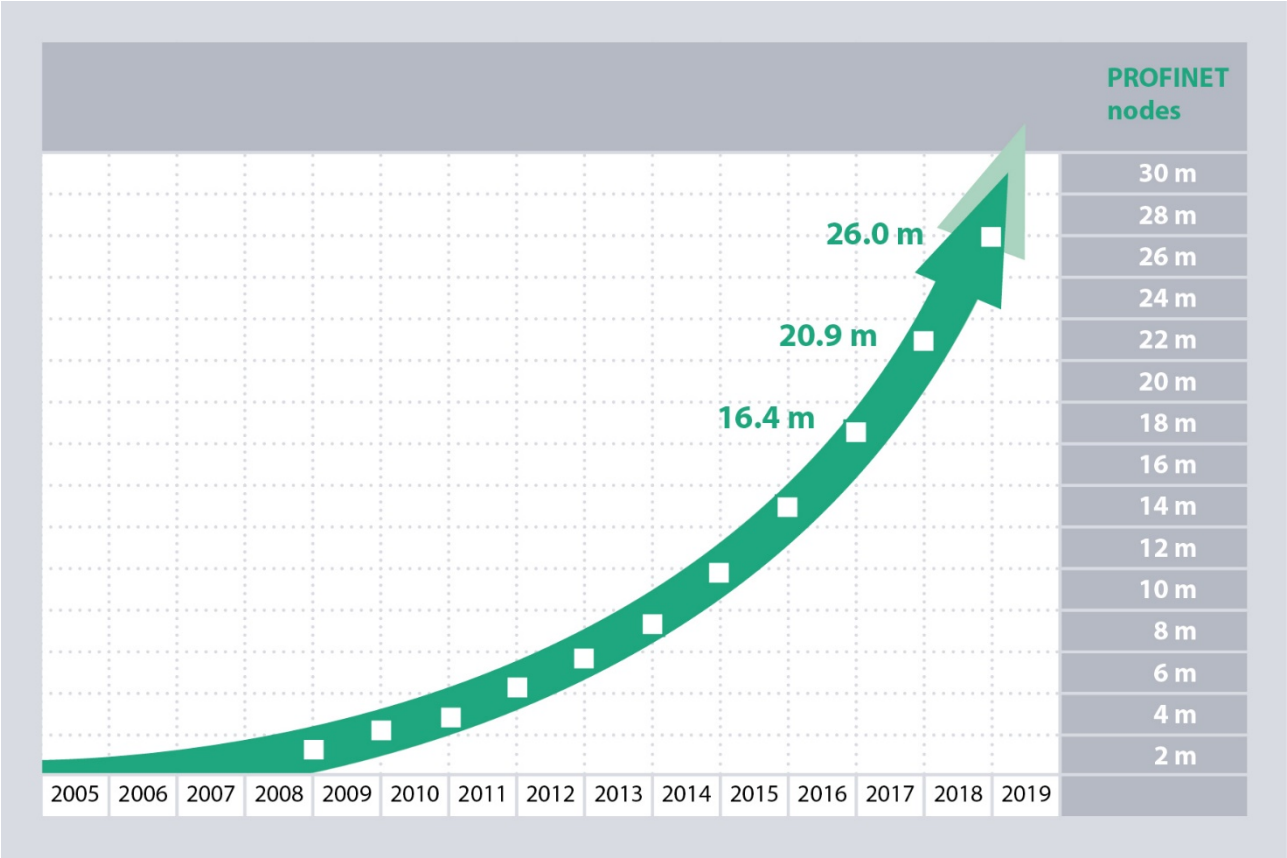


Figure 2-1 – PROFINET growth in recent years

PROFINET devices may require different communication speeds depending on the type of automation process. The PROFINET protocol supports three communication classes, each with a different degree of time sensitivity. These are Non-real-time (NRT), Real-time (RT), and Isochronous Real-time (IRT) communication.

- NRT, sometimes referred to as TCP/IP communication, is acyclic traffic such as sensory, diagnostic, or maintenance data transferred at best-effort speed.
- RT communication is cyclic traffic consisting of high-performance process data transmitted over standard networking infrastructure. This whitepaper mainly focuses on the key aspects of RT communication applications.

- IRT communication is the highest performing type of deterministic traffic within the PROFINET standard. However, this requires hardware-based bandwidth reservation and network-wide clock synchronization to function.

The PROFINET RT and IRT communication classes involve a cyclic data exchange over standard Ethernet and take place directly on Layer 2 without any TCP/IP overhead to minimize latency, as illustrated in Figure 2-2. This means that in an RT/IRT PROFINET environment, data frames are forwarded based on the devices' MAC address. Therefore, it is essential that any underlying network infrastructure deployed to support RT or IRT PROFINET applications is fully Layer 2 transparent to all connected PROFINET devices.

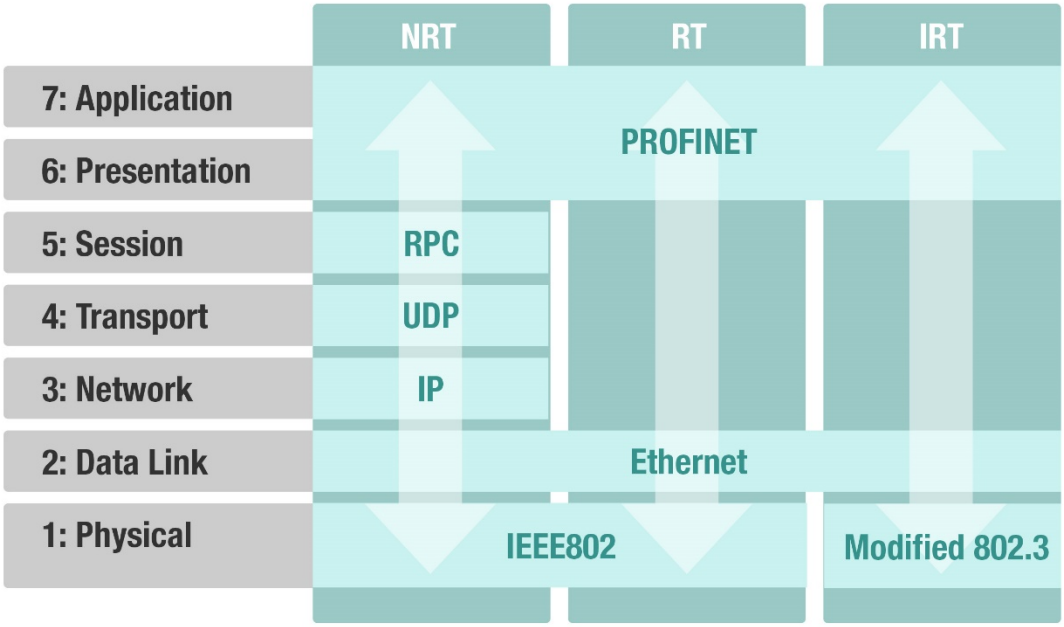


Figure 2-2 – The PROFINET protocol stack

The performance of PROFINET-based communication is limited to the performance ceiling of the underlying network infrastructure. To provide the flexibility to operate reliably over the different network infrastructure components, the cyclic data exchange rate for PROFINET RT communication can be customized to accommodate any infrastructure limitations or to suit the automation context. These configuration parameters are illustrated in Figure 2-3.

In the example below using the Siemens TIA Portal, the **IO cycle > Update time** parameter defines the communication update interval between the PROFINET IO controller and the IO devices. The **IO cycle > Watchdog time** parameter specifies the number of consecutive response failures before reporting a link failure which, depending on the process design, typically triggers the error handling or safe mode, halting the automation process.

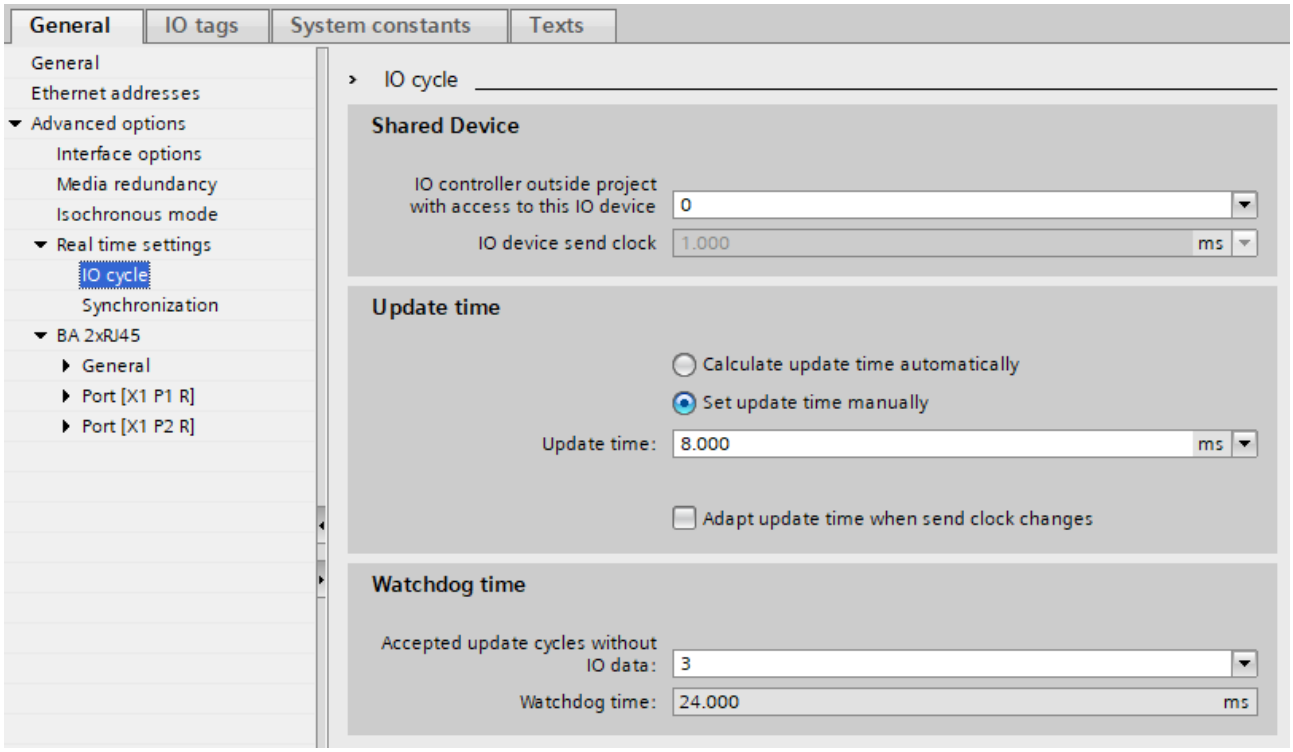


Figure 2-3 – Update time configuration in Siemens TIA portal

3. WLAN Infrastructure Considerations

PROFINET (PN) communication can also be realized over a standard IEEE 802.11 wireless connection. While some PROFINET IO (PNIO) devices have built-in wireless client capabilities, the majority of PNIOs only support Ethernet interfaces. In those cases, system integrators will need to connect the PNIO to a wireless client device that acts as a wireless adapter to communicate with the PN controller.

Even though wireless technology has improved over time with every new iteration of the IEEE 802.11 standard, it is important to note that designing a wireless network is inherently more complex compared to fully wired infrastructure.

In order to design and deploy the right wireless solutions to support PROFINET communication, several key aspects of wireless networking need to be taken into consideration. These include L2 transparency limitations, higher latency, and radio frequency (RF) management to configure the wireless environment for optimal performance.

The following section describes the considerations and challenges integrators need to take into account when designing IEEE 802.11 industrial wireless networks for PROFINET-based applications.

Typical wireless integration scenarios observed in industrial automation and control systems today rely on external wireless devices to serve as the PROFINET IO's wireless adapter. With this in mind, table 3.1 provides an overview of the key focus points associated with evaluating wireless infrastructure components.

Consideration Points	Wired (IEEE 802.3)	Wireless (IEEE 802.11)	Remarks
Layer 2 transparency	Natively supported	Limited	Wireless Layer 2 transparency terminates at the standard Wi-Fi client's interface.
Latency and jitter	Low	High	The RF spectrum is a shared medium that is sensitive to interference from environmental factors. Device mobility and roaming will also cause additional latency and jitter.
Deployment efforts	Cable placement	RF environment	Exercising RF best practices is crucial to optimizing performance and network availability. Activities include site surveys, RF coverage checks, and channel frequency planning.

Table 3-1. Wireless vs wired design considerations

It is important to evaluate these areas systematically when designing wireless networks, in particular when used for critical PROFINET-based control and automation processes. The following sections of this document will outline several typical wireless deployment scenarios, how each of the wireless design considerations relate to different scenarios, and Moxa's solution to address the challenges presented by each scenario.

4. Industrial WLAN Infrastructure Overview

Before evaluating potential WLAN solutions, it is recommended to thoroughly review and map out the requirements of the application first. Since different PROFINET applications require different types of architecture, some variables to consider are:

- The number of PNIO devices to integrate.
- The scale of the wireless network (the number of wireless devices to deploy).
- Device mobility requirements.
- The need to connect standalone Wi-Fi clients such as personnel smart phones, tablets, and laptops.

Different types of wireless deployments such as Point-to-point (P2P) and Point-to-multipoint (P2MP) topologies commonly adopted in the industrial sector fit into one of two main configurations: **AP/Client** or **Bridge** configurations.
The following paragraphs outline the characteristics of both types of configurations.

4.1. AP/Client Architecture

Point-to-point (P2P)

In a P2P AP/Client configuration, a dedicated wireless connection is established between the PN controller and a single PNIO through an access point (AP) and the client's wireless interface. In this scenario, the PN controller and PNIO are connected to the wireless devices

using Ethernet. This type of topology is usually preferred in situations where bandwidth is not shared between clients and where each wireless connection runs on a different, non-overlapping channel.

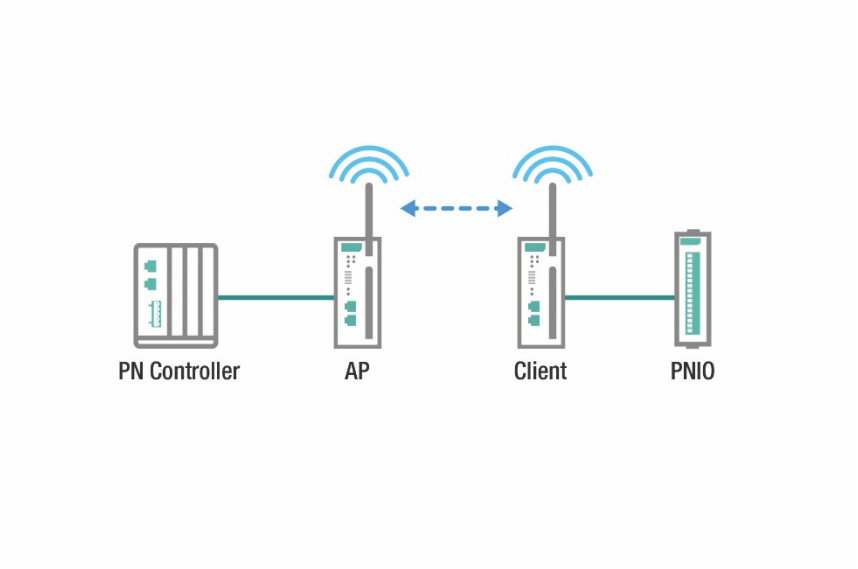


Figure 4-1. Typical P2P AP/Client connection

Point-to-multipoint (P2MP)

In a P2MP AP/Client configuration, a single AP supports multiple clients with each client supporting a maximum of one PNIO connected to it. It is one of the most commonly adopted wireless configurations for connecting multiple clients in a shared bandwidth environment. In some circumstances, the AP will need to serve a combination of PNIO clients and standard Wi-Fi clients such as laptops and tablets.

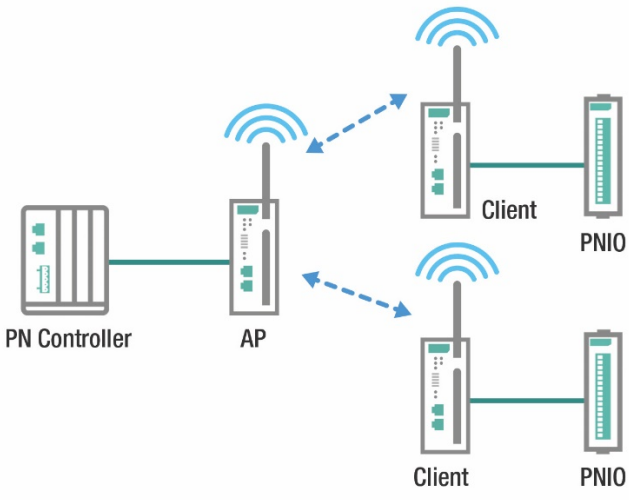


Figure 4-2. Typical P2MP AP/Client connection

4.2. Bridge Architecture

Point-to-point (P2P)

In a P2P bridge configuration, a dedicated wireless bridge between a pair of wireless devices is created to connect multiple PNIOs to a PN controller. Since bridge architecture works at the data link layer (L2) of the OSI model, it allows more than one PNIO to be connected to either wireless device over the same bridge.
This topology can be seen as a wireless extension of a wired backbone, bridging the wired devices on both sides of the wireless connection into a single L2 network. A classic example of a P2P bridge connection is the Wireless Distribution System (WDS).

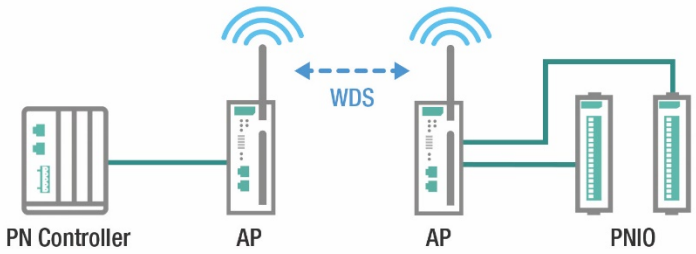


Figure 4-3. Typical P2P wireless bridge connection

Point-to-multipoint (P2MP)

Similar to its AP/Client counterpart, the P2MP bridge topology is a type of deployment that is commonly adopted by system designers that want to integrate multiple mobile PNIOs. In a multi-bridge topology, several wireless bridge connections are established, converging to a single wireless device to connect multiple PNIO systems to a PN controller.

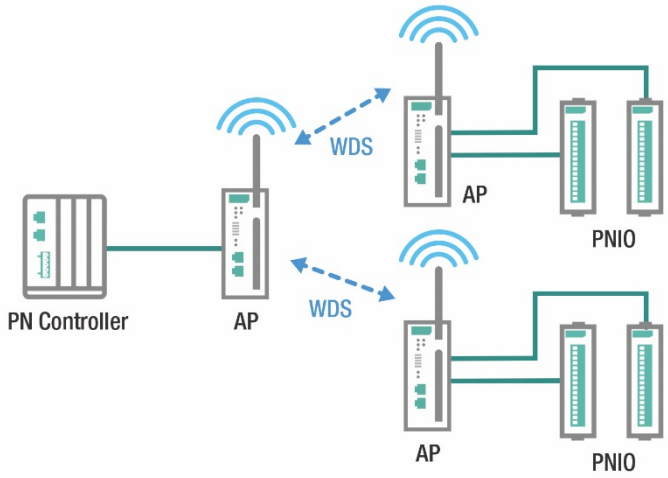


Figure 4-4. Typical P2MP wireless bridge connection

Both the P2P and P2MP bridge topologies are frequently used by AGV machine builders as it allows one wireless device to act as the wireless adapter for multiple PNIOs installed onto the AGV such PLCs for sensors, motors, and cameras.

Whether using an AP/Client or Bridge architecture, PROFINET system designers generally adopt WLAN infrastructure for the benefits of rapid deployment and device mobility. Therefore, candidate wireless solutions are also expected to support seamless roaming to ensure mobile PNIOs can easily move between access points without interrupting the connection.

Once you have identified a suitable WLAN architecture for your PROFINET application, the following sections will explore the challenges presented by each architecture, and the solutions to address these challenges in order to implement a robust industrial wireless network capable of supporting PROFINET WLAN applications.

5. Industrial WLAN Infrastructure Challenges

As wireless solutions gain in popularity, they are gradually becoming an integral part of the industrial network infrastructure designed to support PROFINET-based communication. This section covers the challenges that may arise based on the wireless considerations outlined in section 3 when implementing the industrial WLAN topologies described in section 4.

Below is a quick summary of the key takeaway points from sections 2 through 4:

1. PROFINET real-time (RT) communication requires the underlying network infrastructure to be Layer 2 transparent in order to forward data frames correctly.
2. Wireless infrastructure differs from wired infrastructure. Additional considerations need to be addressed to increase network reliability and availability, such as enhanced functionality to adjust for the additional complications of mobile applications, and RF environment analysis to create a reliable, deterministic wireless network.
3. The most common wireless installations can be categorized into AP/Client or Bridge architectures. Which topology to adopt depends on several factors including the scale of the network and the number of PNIOs that need to be integrated.

Below is an overview of each type of wireless architecture and its requirements for reference.

WLAN Architecture	**Layer 2 Transparency**		**Support Standard Wi-Fi Clients**	**Latency, Jitter, and RF Management**	
	Wireless Links	**No. PNIO/Link**		**Seamless Roaming**	**RF Deployment Best Practices**
AP/Client	≧1	1	Yes	Yes	Yes
Bridge	≧1	≧1	Yes	Yes	Yes

When using standard WLAN solutions in industrial settings, integrators may experience some complications concerning functional requirements. In the following sections, we will explore these specific challenges in more detail.

AP/Client Configurations

In AP/Client P2P or P2MP configurations, when a PNIO is wired to a wireless client, L2 transparency ends at the client device's wireless interface.
This means that when using standard Wi-Fi client connectivity without enhanced functionality, the PN controller will not be able to forward data frames to the PNIO as it cannot identify the MAC address of the connected PNIO. Refer to **Appendix 1** for more details regarding this technical limitation.

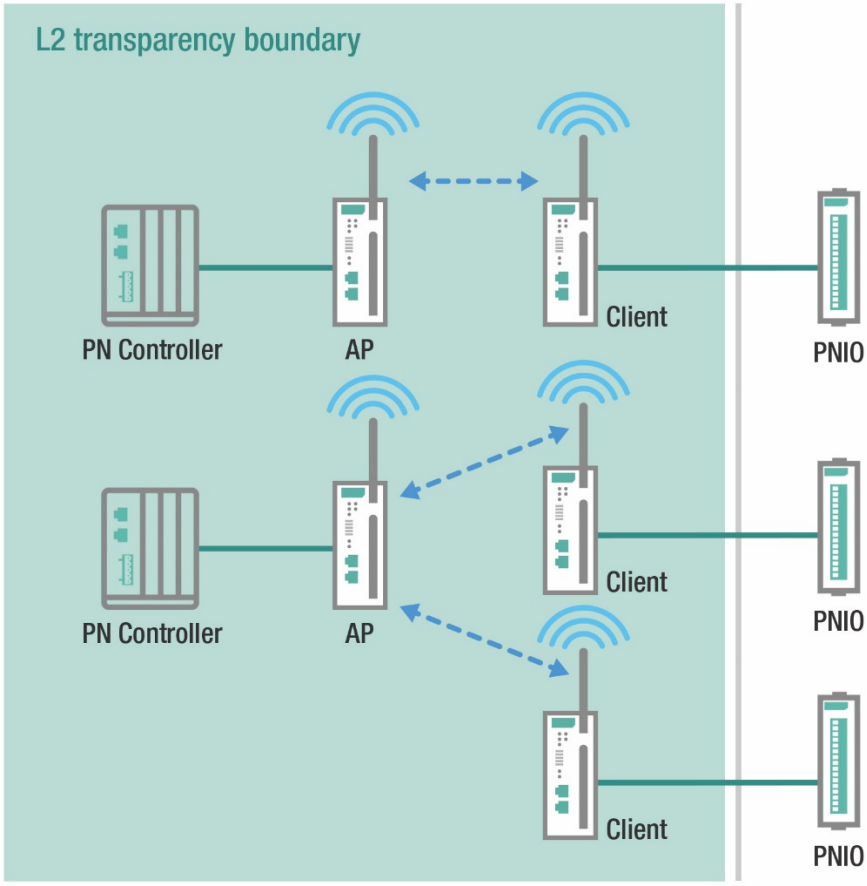


Figure 5-1. Layer 2 transparency boundary in a standard AP/Client setup

Challenge 1: Since the communication between the PN controller and the PNIO happens on the data layer, the boundary of L2 transparency must extend beyond the wireless client's Ethernet interface, while maintaining compatibility with standard AP/Client connections to allow other Wi-Fi devices to connect to the AP.

Bridge Configurations

One example of a typical bridge connection is the Wireless Distribution System (WDS), which, by its technical specification, is a L2 transparent wireless link connecting two APs. A layer 2 wireless bridge setup is preferred in cases where multiple PNIO devices need to be connected to one wireless device.

However, commercial WDS solutions are unable to fulfill the needs of more complex industrial applications. WDS is statically configured and is not designed to support bridge roaming to accommodate moving devices such as AVGs. Furthermore, WDS does not support hybrid bridge/AP functionality by default to serve standard Wi-Fi clients such as laptops and tablets used by on-site engineers.

In cases where multiple wireless bridges are necessary, system designers can set up additional WDS bridge links to create a P2MP configuration. However, each bridge link needs to be configured manually. This makes deploying conventional P2MP wireless infrastructure very time- and resource-intensive and more prone to network issues due to configuration conflicts.

Challenge 2: Commercial wireless solutions have out-of-the-box limitations that make them unable to meet the functional requirements of industrial wireless PROFINET applications. Bridge devices should support multipoint bridge topologies, bridge mobility, and be able to act as a hybrid bridge/AP to connect additional standard Wi-Fi clients.

Latency, Jitter, and RF Management

Wireless connectivity occurs through electromagnetic waves that are sent within an ISM band. This physical characteristic of communicating over a shared medium is inherently susceptible to interference from various devices operating in overlapping channels within that spectrum. As a result, WLAN components are more likely to suffer from latency or jitter. The amount of additional latency compared to a purely wired network depends on the type of WLAN technology, antenna performance, and the channel utilization within the network environment.

Therefore, employing a set of best practices when evaluating and configuring the RF environment and wireless coverage are key to yielding optimal wireless performance and establishing the foundation for a more deterministic WLAN infrastructure.

Outlined below are several important RF best practices for reference.

Wireless spectrum:

- Select the radio bands most appropriate for the application considering the network environment and signal penetration.
  - Reserve the 5 GHz frequency band for critical communication as this band has more channels available and is generally less congested compared to the 2.4 GHz band.
  - Use the 2.4 GHz frequency for farther signal penetration.
- Avoid configuring Dynamic Frequency Selection (DFS) channels on the 5 GHz band (channels 52 to 140) for critical communications to prevent interference from radar signals.
- Perform on-site RF spectrum analysis to identify and allocate devices for different applications to free, non-overlapping channels.

Wireless coverage:

- Maintain an unobstructed line of sight when installing antennas to avoid signal degradation caused by nearby physical objects.
- Select suitable antennas for the environment to ensure a good signal-to-noise ratio (SNR).

However, performing RF analysis and configuration relies on experienced personnel with extensive knowledge of wireless networking. In the industrial sector, it is often difficult to dispatch qualified individuals on a readily available basis.

Challenge 3: RF optimization is a complicated process that relies heavily on highly experienced personnel. Therefore, integrators should look to provide an accessible, easy-to-use solution for on-site personnel with limited WLAN knowledge to perform wireless coverage site surveys and to identify and configure optimal RF channels during installation and maintenance.

Another major benefit of using wireless networks in mobile applications is the ability for wireless clients to roam across different BSSIDs within the network. Roaming involves a client device disconnecting from one access point as it moves out of range and dynamically establishing a new connection with a nearby higher signal quality BSSID. However, this process unavoidably generates additional communication latency as clients constantly transition between APs. Industrial applications can only tolerate a very low margin for latency to ensure smooth and uninterrupted data transmission. As a result, WLAN solution manufacturers are required to optimize their products to mitigate the additional latency generated by the roaming process.

Challenge 4: Wireless mobile applications such as AGV automation and control processes rely on stable and highly responsive networks. Achieving millisecond-level wireless roaming handover times therefore becomes a necessity to minimize latency and avoid impact to operations.

Below is a quick summary of the WLAN scenarios and the challenges (marked C1 to C4) associated with each scenario.

WLAN Architecture	Layer 2 Transparency		Service Standard Wi-Fi Clients	Latency, Jitter, and RF Management	
	Wireless Links	No. PNIO/link		Seamless Roaming	RF Deployment Best Practices
AP/Client	≧1	1[C1]	Yes	Yes[C4]	Yes[C3]
Bridge	≧1[C2]	≧1	Yes[C2]	Yes[C4]	Yes[C3]

6. Moxa's WLAN Infrastructure Solutions

The following section describes how Moxa's AWK Series WLAN products and features help address each of the challenges defined in the previous section.

6.1. MAC Cloning

Challenge 1: Extend Layer 2 transparency beyond the client's Ethernet interface in an AP/Client configuration so that the connected PNIO is addressable by the PN controller.

The Moxa AWK Series' proprietary MAC Cloning feature is designed to extend L2 transparency to a single PROFINET IO device connected to the wireless client by cloning the MAC address of the PNIO to the client it is connected to. By doing so, the PN controller is able to communicate with the PNIO through the client using its cloned MAC address. MAC Cloning can be used in either **Auto** or **Static** mode, depending on the application.

- **Auto**: The AWK client automatically copies the MAC address of the PNIO device connected to its Ethernet interface. Only one device should be connected to the client when using this method to avoid MAC address translation conflicts.
- **Static**: The MAC address of the AWK client is manually configured to use the MAC address of the PNIO. This is useful in cases where multiple devices need to be connected to the same client. While this method supports more than one device to be wired to the client, only one PNIO device can be connected to one client at any given time.

6.2. Master/Slave Bridge

Challenge 2: Bridge devices should support multipoint bridge topologies, bridge mobility, and be able to act as a hybrid bridge/AP to connect additional standard Wi-Fi clients.

Master/Slave mode is a variation of the wireless bridge mode exclusively available on Moxa's AWK Series that allows multiple bridges from a single Master device to several Slave client devices, with each Slave client supporting multiple PNIO devices. Moxa's Master/Slave bridge configuration is simple and intuitive, adopting a configuration process similar to setting up an AP/Client connection. This eliminates the complicated and issue-prone setup procedure that plagues conventional bridge setups such as WDS.

In addition, Virtual Access Point (VAP) functionality can be enabled on the designated Master AWK Series device, enabling it to broadcast its SSID to concurrently support additional standard Wi-Fi client connections.

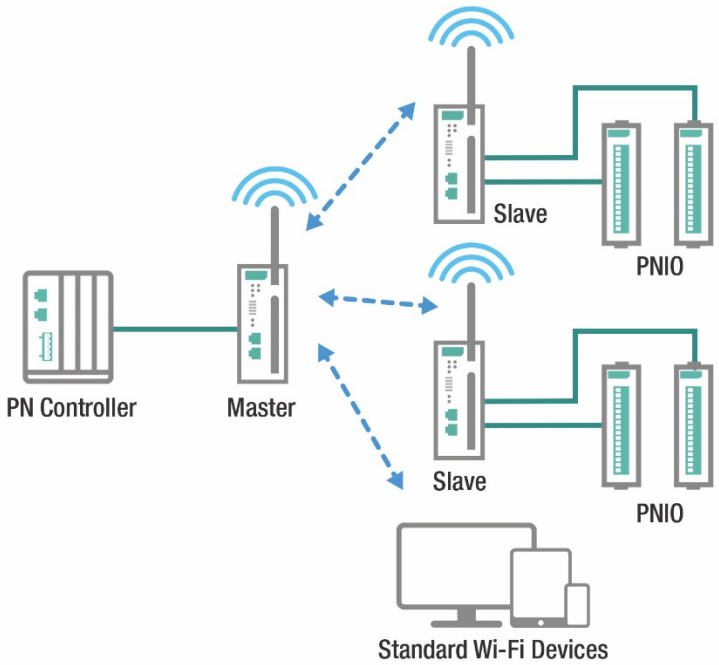


Figure 6-1. P2MP bridge supporting standard Wi-Fi devices using Moxa Master/Slave

6.3. AeroMag

Challenge 3:
RF optimization is a large and complex activity that requires experience and knowledge to execute. Accessible tools should be available to enable less experienced on-site personnel to 1) perform wireless coverage surveys to determine optimal deployment and antenna density, and 2) analyze the wireless spectrum to determine the best wireless bands and channels.

Moxa's AWK Series features AeroMag technology, which helps alleviate the complexity of RF optimization by automatically configuring basic Wi-Fi settings and performing RF spectrum analysis to identify optimal bands and channels. AeroMag is a useful tool throughout the entire Wi-Fi network lifecycle. During the installation phase, AeroMag helps streamline network operations by dynamically analyzing and adjusting radio channels depending on your current operating environment. When configuring network devices, AeroMag's one-step setup establishes Wi-Fi connections quickly, significantly reducing deployment times.

Moxa's AWK Series industrial WLAN AP/Bridge/Clients support AeroMag functionality in AP/Client mode. Once the RF and channel settings are configured using AeroMag, the device can be switched to bridge mode and will automatically carry over the RF and channel settings.

While AeroMag simplifies the RF optimization process, it does not substitute a full analysis of the wireless environment. To ensure maximum availability and deterministic performance, a complete independent site survey should still be conducted to generate the best wireless coverage and most suitable RF configuration for the target environment.

6.4. Turbo Roaming

Roaming behavior is configured on WLAN clients. Standard WLAN clients without any roaming enhancements usually maintain an established connection regardless of changes in environment or signal quality. This often results in the device disconnecting before attempting to find the next available BSSID. As industrial applications require seamless communication to avoid interruptions to operations, conventional WLAN client roaming solutions are inadequate.

Challenge 4: Establish millisecond-level wireless roaming to avoid any impact to industrial operations.

Moxa's WLAN Client products support Moxa's proprietary Turbo Roaming feature. This function actively scans the wireless environment to identify and roam to nearby APs with optimal signal quality before the original connection deteriorates beyond a predefined threshold. By constantly monitoring and connecting to the best available AP, Moxa's Turbo Roaming feature increases WLAN reliability and availability through fast millisecond-level roaming handover times.

Turbo Roaming is available in both AP/Client and Master/Slave bridge topologies. A customizable AP signal quality indicator or roaming threshold can be set to cater to different environmental conditions. In addition, the intuitive Turbo Roaming Analyzer utility tool is available to help network designers visualize and confirm that the roaming logic behaves as intended within the set performance margins.

Detailed information on how to use AeroMag can be found in the Moxa AWK Series user manual. The wireless installation scenarios, challenges, and Moxa's solutions are consolidated in the following summary table.

WLAN Architecture	Layer 2 Transparency		Service Standard Wi-Fi Clients	Latency, Jitter, and RF Management	
	Wireless Links	No. PNIO/Link		Seamless Roaming	RF Deployment Best Practices
AP/Client	≧1	1[C1]: MAC Cloning	Yes	Yes[C4] Turbo Roaming	Yes[C3] AeroMag
Bridge	≧1[C2] Master/Slave	≧1	Yes[C2] Master/Slave	Yes[C4] Turbo Roaming	Yes[C3] AeroMag

7. Moxa's Reference WLAN PROFINET Solution

This section aims to provide process owners with a frame of reference when evaluating their own applications. The recommended PROFINET update times are based on a test scenario using SIEMENS PROFINET devices communicating over a Moxa-powered WLAN infrastructure.

Most PROFINET scenarios categorically fall into static or mobile applications. Common static applications involve wirelessly connecting stationary devices in environments where hard-wiring is difficult. An example of a static PROFINET application would be a wireless connection between an onshore PROFINET controller and a PROFINET IO installed inside an offshore wind turbine. In contrast, mobile applications connect constantly moving PROFINET devices such as in automated factories, where PROFINET IOs installed on AGV vehicles are moving around the facility.
Based on the typical WLAN architectures described in the previous sections, the following deployment scenarios will be covered utilizing Moxa's proprietary devices and functions.

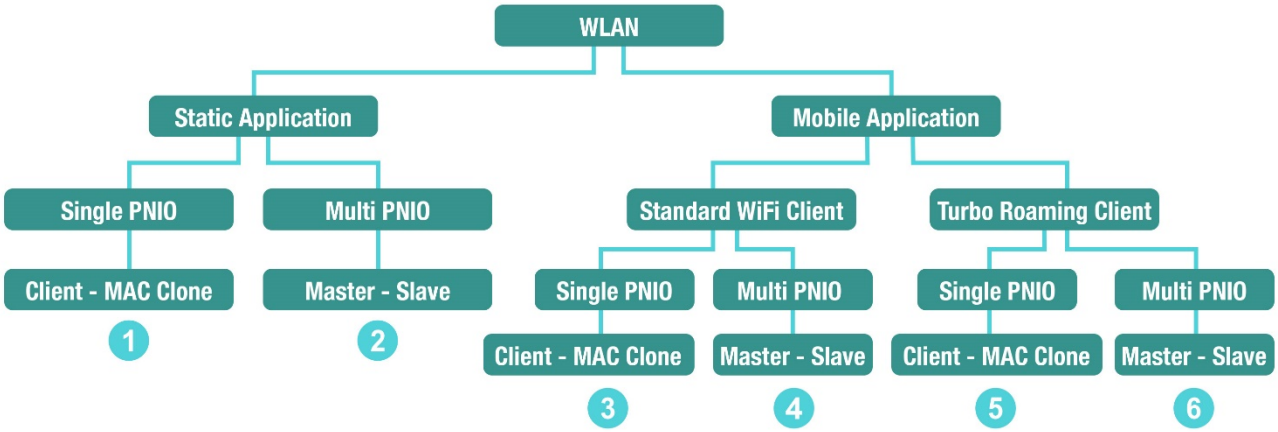


Figure 7-1. Reference scenarios

7.1. Scenario Setup Overview

The diagrams below illustrate the PROFINET test configurations using the following devices:

- PNIO controller: SIEMENS SIMATIC ET200SP CPU
- Control software: PC running SIEMENS TIA Portal
- Wireless AP/Client/Bridge devices: Moxa AWK Series
- PNIO: SIEMENS SIMATIC ET200SP Distributed I/O

Static Application

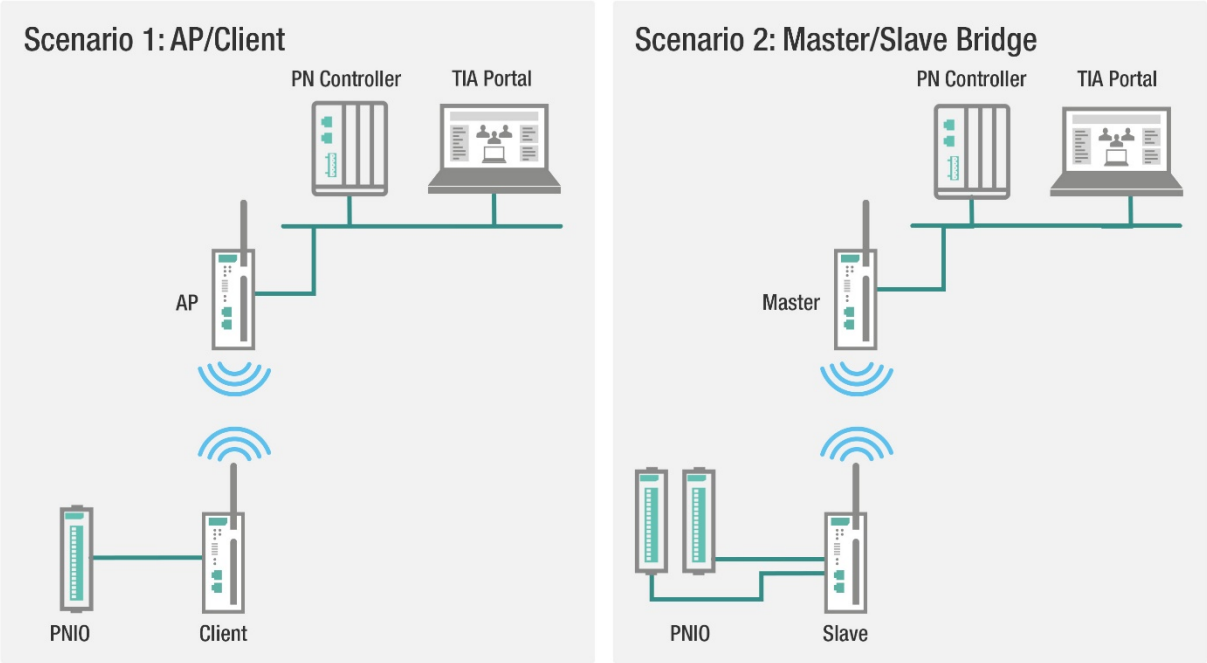


Figure 7-2. Static AP/Client and Bridge scenario

Mobile Application: Standard Client Behavior

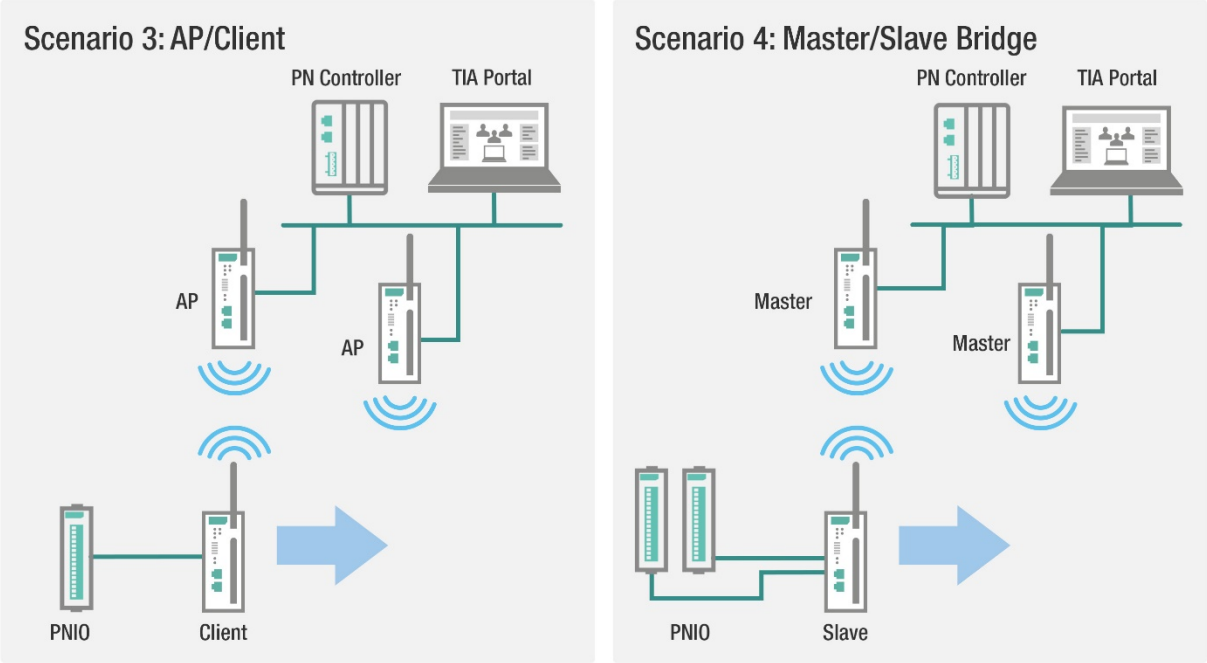


Figure 7-3. Mobile AP/Client and bridge scenario with standard client behavior

Mobile Application: Turbo Roaming Client

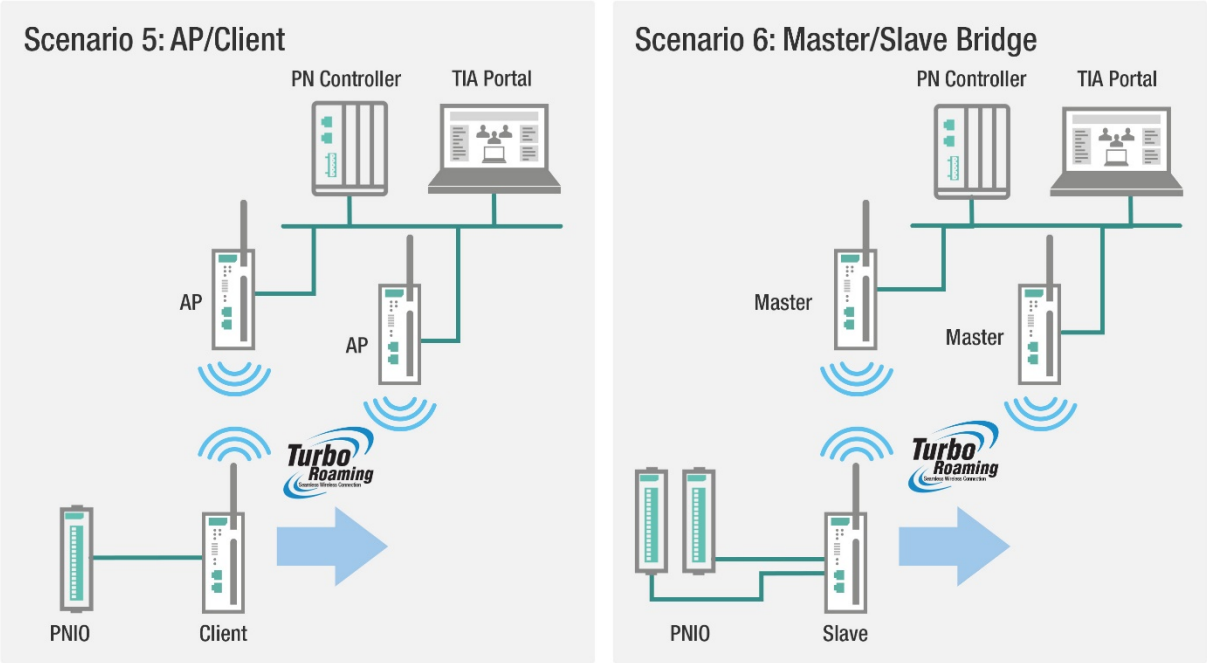


Figure 7-4. Mobile AP/Client and bridge scenario with Turbo Roaming

7.2. Generic WLAN Settings

In the table below are the WLAN settings of the AWK Series used in the reference scenarios.

Band	5 GHz (N only)
Channel	Interference-free, non-overlapping channel
Channel Width	20M
Encryption	WPA2-Personal
Roaming Threshold	Default

Table 7-1. AWK Series test scenario settings

When deploying your wireless network, adhere to industry best practices to identify the appropriate WLAN settings for the intended deployment environment. You can leverage the AeroMag function to automatically perform an RF spectrum scan and identify the optimal operation channels. In addition, it is recommended to employ other RF optimization practices to ensure a stable and reliable industrial wireless communication system, including:

- Selecting the radio bands most suitable for the environment
- Selecting a free, non-overlapping channel based on the AeroMag RF spectrum analysis
- Avoiding environmental interference and maintain a clear line of sight for antennas
- Selecting suitable antennas for the environment to ensure a good signal-to-noise (SNR)

7.3. Reference Test Results

The PROFINET communication latency can be customized to accommodate the requirements of the application. Thus, process owners need to derive the optimal PROFINET update time based on the deployed WLAN infrastructure. The following test result data serves as a reference point to evaluate PROFINET latency when using Moxa’s WLAN solutions.

Tables 7.2 through 7.4 show the reference PROFINET update times configured in the TIA portal for all six scenarios.

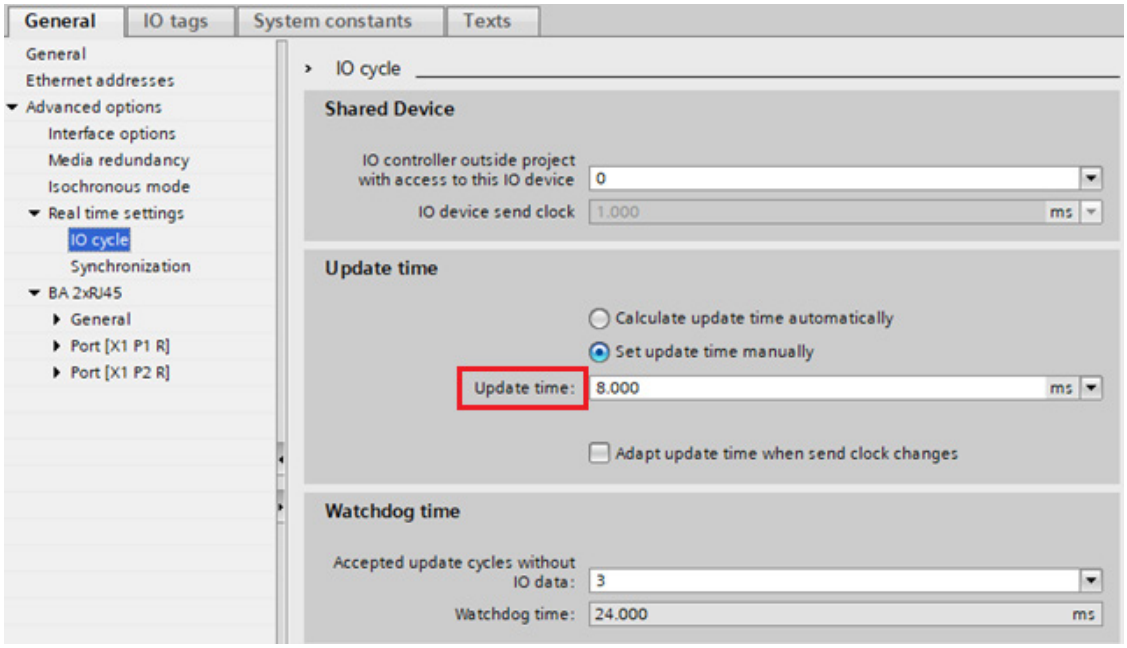


Figure 7-5. PROFINET update time in TIA portal

7.3.1. PROFINET Update Time Reference

Scenario	Architecture	L2 Transparency Function	No. PNIO	Min. PNIO Update Time
1	AP/Client	Client: MAC Clone	1	32 ms
2	Bridge	Master/Slave	2	32 ms

Table 7-2. Static scenario

Scenario	Architecture	L2 Transparency Function	Turbo Roaming	No. PNIO	Min. PNIO Update Time
3	AP/Client	Client: MAC Clone	No	1	N/A (4s ~ 5s reconnect)
4	Bridge	Master/Slave	No	2	N/A (4s ~ 5s reconnect)

Table 7-3. Mobile scenario with standard Wi-Fi clients

Scenario	Architecture	L2 Transparency Function	Turbo Roaming	No. PNIO	Min. PNIO Update Time
5	AP/Client	Client: MAC Clone	3 channels	1	128 ms
6	Bridge	Master/Slave	3 channels	2	128 ms

Table 7-4. Mobile scenario with Turbo Roaming

8. Executive Summary

There are two key challenges to address when attempting to build a stable PROFINET application over a WLAN infrastructure. 1) The selected WLAN solution must support L2 forwarding in different configurations. 2) Wireless latency and jitter need to be minimized to meet the requirements of the PROFINET application.

The limitation of L2 transparency terminating at the client level can be overcome by using Moxa's proprietary MAC Clone and Master/Slave bridge features.
The remaining challenge that comes with designing a stable PROFINET application over WLAN Infrastructure is to account for the impact of additional latency from wireless communication and roaming activities. Moxa's AeroMag functionality simplifies RF configuration by performing automatic spectrum analysis and channel optimization while Turbo Roaming enables millisecond-level roaming capability.

In terms of the overall WLAN network latency in relation to the PROFINET update time requirements, the AWK Series reference results suggest that PROFINET communication stabilizes with a minimum IO Cycle Update Time of 32 ms in static applications. Mobile scenarios without seamless roaming are not feasible as the reconnection time significantly exceeds the typical PROFINET update time window, which would interrupt or halt the PROFINET communication altogether. Enabling Moxa's Turbo Roaming feature can mitigate roaming overhead down to milliseconds, allowing stable PROFINET communication with a minimum IO Cycle update time of 128 ms.

We recommend using the aforementioned PROFINET update times as a starting point for process owners to evaluate update intervals that work best for the intended network design. Since wireless communication occurs over a public transmission medium, it is important to consider a large enough time margin to account for any external interference. Furthermore, we highly recommend incorporating an error handling or recovery mechanism into the PROFINET control logic to handle unexpected interference that may cause the PROFINET communication to time out.

Appendix 1 - WLAN Layer 2 (L2) Addressing Overview

As PROFINET RT and IRT operate on L2, we need to take a closer look at the L2 addressing mechanism of standard WLAN technology to fully understand the technical requirements of using PROFINET over WLAN.

The IEEE 802.11 MAC frame can have up to four address fields in the MAC header. 802.11 frames forwarded over a standard AP-to-client connection use only three of the MAC address fields, whereas frames transmitted over a bridge such as a WDS (Wireless Distribution System) connection use all four MAC address fields. This is illustrated in Table 1 below.

The number of MAC address fields used will affect L2 transparency. Depending on the type of wireless connection and the direction of the traffic, the content of these address fields (fields 1 to 4) can include the following:

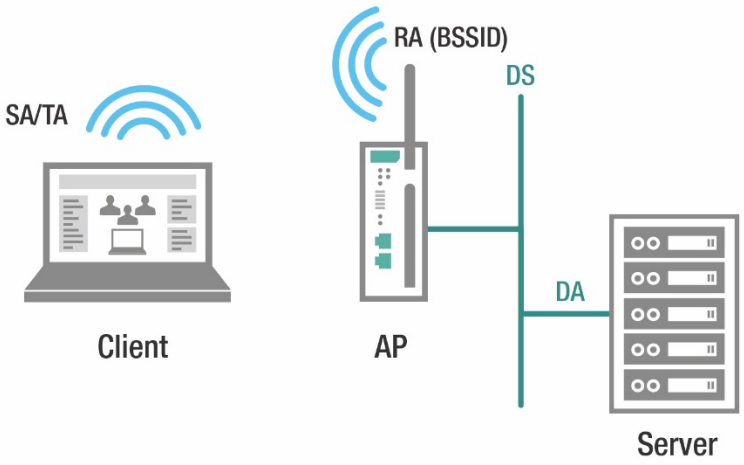
1. Receiver Address (RA)
2. Transmitter Address (TA)
3. Basic Service Set Identifier (BSSID)
4. Destination Address (DA)
5. Source Address (SA)

Function	ToDS	FromDS	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
IBSS	0	0	DS	SA	BSSID	N/A
To AP (infra.)	1	0	BSSID	SA	DA	N/A
From AP (infra.)	0	1	DA	BSSID	SA	N/A
WDS (bridge)	1	1	RA	TA	DA	SA

Appendix Table 1. IEEE 802.11 data frames

Depending on how the **To DS** and **From DS** fields are set in the control frame, the definition of each MAC address field will change, as shown in Appendix Table 1.

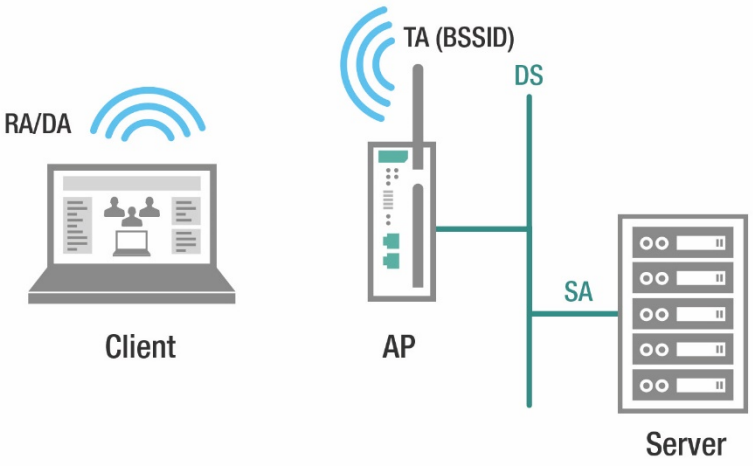
A standard AP/Client scenario where traffic is moving from the wireless client towards the wired network is illustrated in Appendix Figure 1 below. This scenario corresponds to the **To AP (infra.)** function in Appendix Table 1, which only uses 3 MAC address fields. Devices connected at the AP side are L2 transparent and addressable by the client.



Appendix Figure 1 – Client-to-AP communication

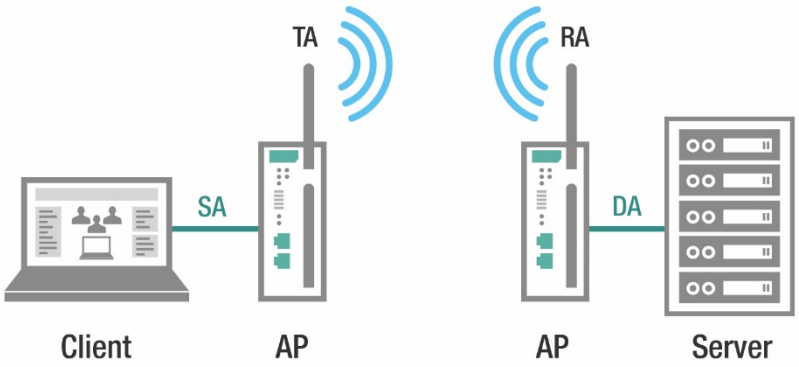
The figure below shows AP/Client communication moving in the opposite direction, from the AP to the wireless client.

This scenario illustrates the **From AP (infra.)** function in Appendix Table 1, which also only uses 3 out of 4 available MAC address fields. However, devices connected on the AP side would only be able to address the client's MAC address, meaning any devices wired to the client would not be transparent or L2-addressable by devices on the AP side.



Appendix Figure 2 – AP-to-Client communication

Contrary to AP/Client configurations, WDS (Wireless Distribution System) bridges wirelessly connect two LANs, using all 4 MAC address fields. Therefore, in a WDS connection, traffic in both directions is L2 transparent and devices connected to each side of the WDS connection can address one another, as shown in the figure below.



Appendix Figure 3 - WDS bridge communication

The most important takeaway here is to remember that in an AP/Client wireless setup, the client itself is a wireless device where its own MAC address is either the source or the destination address. Since only 3 MAC address fields are used in AP/Client configurations, devices connected to the client are not L2 transparent to devices on the other end of the connection and are therefore not addressable. For deployments where wired devices are connected to both sides of the wireless device, all 4 MAC address fields are necessary to correctly forward L2 data frames to end devices across the wireless bridge.