SOLUTION BRIEF

MWL Onboarding Device Ecosystem

In the dynamic and complex environments of manufacturing wireless LAN (MWL) spaces, onboarding a diverse array of devices into a wireless network is crucial for operational efficiency and productivity. This technical paper explores best practices for integrating various device types, including computer devices, network printers, VoIP phones, scanners, security cameras, and industrial IoT devices, into a robust and secure wireless network. Understanding the unique connectivity requirements and challenges of each device type is essential for designing a network that supports seamless operations and enhances overall performance.

Computer devices such as workstations, laptops, tablets, and AR devices are integral to tasks like inventory management, quality control, and process monitoring. These devices demand seamless Wi-Fi® connectivity to access local or cloud-based applications and network resources. Network printers, while enhancing productivity and convenience, should be connected via LAN to avoid consuming Wi-Fi airtime with broadcast advertising protocols. VoIP phones and barcode scanners, essential for communication and inventory management, require careful Wi-Fi design to ensure reliable connectivity and low latency. Security cameras, typically connected via Ethernet, play a vital role in monitoring and ensuring compliance within the facility. Industrial internet of things (IoT) devices, equipped with sensors and actuators, rely on Wi-Fi connectivity for data transmission and process optimization.

Security is a paramount concern in MWL environments, where networks handle sensitive data related to production processes and intellectual property. Robust security measures—including firewalls, intrusion detection and prevention systems (IDPS), virtual private networks (VPNs), network segmentation, access control systems, patch management, security information and event management (SIEM) systems, endpoint security solutions, and wireless security measures—are essential to protect against cyber threats and unauthorized access. Employee training and awareness programs further bolster security by preventing human errors that could lead to breaches.

Deploying an IoT access network that integrates the diverse ecosystem of standards, devices, and services can be a significant undertaking. However, a converged network simplifies IoT sensor and device onboarding, establishes uniform security protocols, and converges IoT endpoint management and policy-setting. With the RUCKUS® IoT Suite, enterprises can create an IoT access network by reusing existing LAN and WLAN infrastructure, accelerating deployments, reducing costs, and maximizing the benefits of IoT devices.

Diverse device ecosystem in MWL spaces

The operational intricacies of MWL environments necessitate a diverse array of devices requiring connectivity to support various tasks and workflows. Understanding these device types and their connectivity requirements is essential for designing robust wireless networks.

Computer devices (workstations, laptops, tablets, AR devices)

Workers in MWL facilities rely on mobile computers and laptops for tasks such as inventory management, quality control, and process monitoring. These devices require seamless Wi-Fi connectivity to access local or cloud-based applications and network resources. Mobile tablets and AR devices are increasing in popularity as they increase worker efficiency and accountability. As a result, the network demands have increased to sustain the video and AR streams' need for low latency and high performance.

Network printers

Printers connected to the network allow users to print documents from different locations within the facility. They enhance productivity and convenience. Fixed devices, such as printers, should always be connected via the LAN, leaving the Wi-Fi for portable devices. Printers often use broadcast advertising protocols. This type of traffic can be detrimental to Wi-Fi by consuming airtime if allowed to over-propagate. The LAN should be configured to allow these types of advertising protocols to propagate only where needed. Broadcast/multicast rate limiting may be considered—or simply isolating the traffic to specific VLANs.

VoIP phones and scanners

Voice over Internet Protocol (VoIP) phones enable voice communication over the network. They replace traditional landline phones and facilitate efficient communication among employees. Barcode scanners read barcodes on products, inventory, and shipping labels. They quickly retrieve information from barcoded items.

Scanner devices have been used in MWL environments for decades and typically do not impose a heavy data load on the network, yet they must work where and when needed—so the Wi-Fi design must consider where and how these devices are used, including any shadowing caused by the user or the structures around the user.

VoIP devices have increased in popularity, and they typically are used by managers or leads on the shop floor, where communication between staff is critical.

Ensure adequate link budget (always consider the uplink as the governing factor) to overcome the blockage or shadowing. Multiple access points (APs) may be needed to increase the coverage confidence. The VoIP device is more sensitive to latency and will benefit from smaller, higher performance Wi-Fi cells placed closer to device users.

Security cameras

Surveillance cameras enhance security by monitoring the premises. They capture video footage and help prevent theft, monitor safety, and ensure compliance with regulations.

Cameras are typically connected via Ethernet since they are usually fixed in place (leave the wireless to mobile devices and avoid connecting static devices to the Wi-Fi). The LAN used for security is always isolated via VLAN and sometimes by a separate IP domain. In more sensitive security environments, a separate LAN is used for the security cameras, door locks, and badge scanners. The ICX® switches for security may even be placed in separate locked cabinets in the IDF closets.

Industrial IoT devices

IoT devices equipped with sensors and actuators are increasingly deployed in MWL environments for equipment monitoring and process optimization. These devices rely on Wi-Fi connectivity to transmit data for analysis and decision-making.

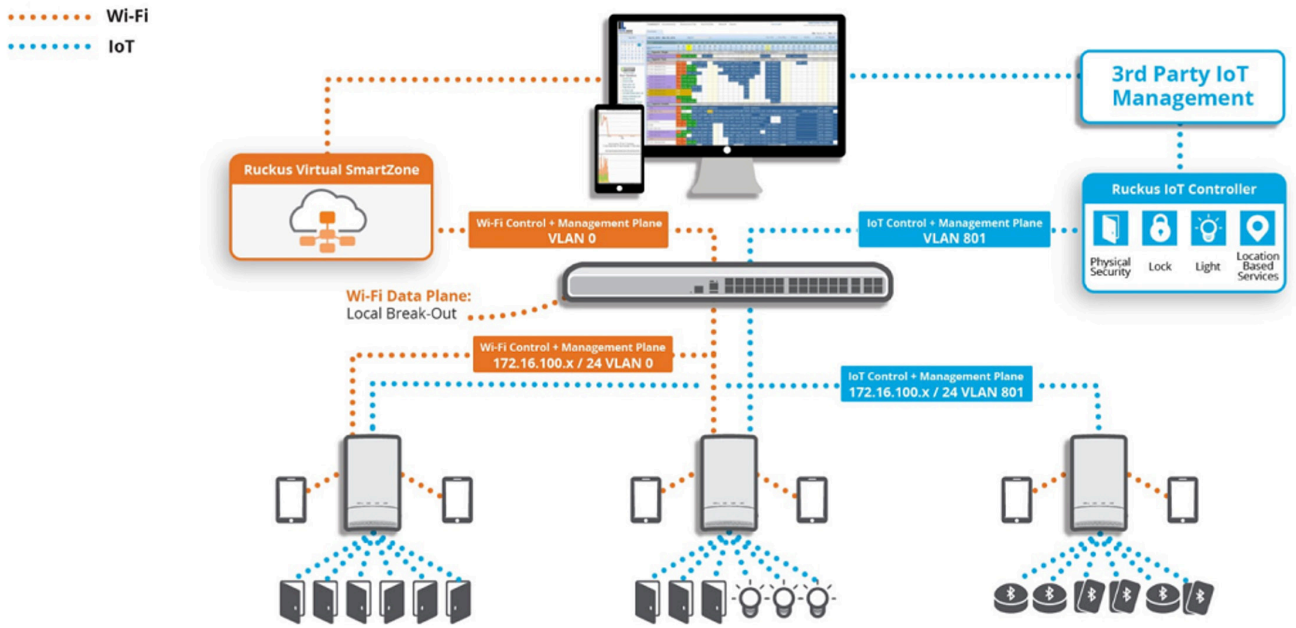
The organization needs to assess the types of endpoints required to support their solution. An IoT endpoint encompasses a wide array of computing devices that can communicate with other machines without human interaction. The considerations include the computing power necessary for the task, the required battery life for communication frequency and network, device cost, and the availability of skilled staff to develop applications for these devices. The organization must consider various factors, including a diverse range of connectivity types used in IoT deployments, including Wi-Fi, cellular, satellite, and Zigbee®. Questions—such as whether the endpoint resides in a predefined area, requires real-time connectivity, consumes significant power, or needs high bandwidth—must be addressed.

Handling network complexity presents another obstacle for the organization. Every instance of incorporating a device utilizing a distinct communication protocol—like Wi-Fi, Zigbee®, or Bluetooth® Low Energy—necessitates constructing a supporting network, which is both expensive and time intensive.

Furthermore, integrating IoT data with essential systems and engaging stakeholders from various departments within the company are imperative for high-adoption IoT projects. Deliberating from technological, human, and procedural angles is pivotal in safeguarding technology selections for the future and adapting to prospective applications beyond the primary use case.

Deploying an IoT access network that ties together the complex, fragmented ecosystem of standards, devices and services can be a large undertaking. But a converged network can simplify IoT sensor and device onboarding, establish uniform security protocols, and converge IoT endpoint management and policy-setting.

With RUCKUS IoT Suite, enterprises can create an IoT access network by reusing LAN and WLAN infrastructure. This accelerates deployments, reduces costs and increases the benefits from IoT devices.



A RUCKUS IoT network enables organizations to aggregate and backhaul IoT traffic over their new or existing RUCKUS Wi-Fi infrastructure. Plus, RUCKUS Networks can help create a converged edge network that brings together wireless, wired and IoT networks into a shared network architecture.

Successfully onboarding a diverse array of devices into a wireless network in manufacturing wireless LAN environments requires a strategic approach that addresses connectivity, performance, and security challenges. By understanding the unique requirements of computer devices, network printers, VoIP phones, scanners, security cameras, and industrial IoT devices, organizations can design robust networks that support seamless operations and enhance overall productivity. Implementing best practices for

network architecture—such as redundant switch designs, low latency, and Quality of Service (QoS) mechanisms—ensures reliable and efficient connectivity. Additionally, robust security measures such as firewalls, IDPS, VPNs, and endpoint security solutions are essential to protect sensitive data and prevent unauthorized access.

Organizations should conduct a thorough assessment of their current network infrastructure and device ecosystem to identify areas for improvement. Engaging with stakeholders from various departments will ensure that all connectivity and security needs are addressed. Leveraging solutions like the RUCKUS IoT Suite can simplify the integration of IoT devices by reusing existing LAN and WLAN infrastructure, thereby accelerating deployments and reducing costs. Regularly updating and testing the network to meet predefined key performance indicators (KPIs) will help maintain optimal performance and reliability.

By following these best practices and taking proactive measures, organizations can build resilient networks that support their operational goals and drive future growth.

About RUCKUS Networks

RUCKUS Networks builds and delivers purpose-driven networks that perform in the demanding environments of the industries we serve. Together with our network of trusted go-to-market partners, we empower our customers to deliver exceptional experiences to the guests, students, residents, citizens and employees who count on them.

www.ruckusnetworks.com

Visit our website or contact your local RUCKUS representative for more information.

CO-119203-EN (01/25)

RUCKUS®
COMMSCOPE