SOLUTION BRIEF

MWL Network Best Practices

This white paper serves as a comprehensive guide to best practices for designing and deploying network architectures in manufacturing wireless LAN (MWL) environments, with a focus on LAN, WLAN, and security. Addressing the inherent challenges and diverse device ecosystems of these settings requires a strategic approach to ensure robust connectivity, seamless operations, and robust security measures.

For LAN, implementing a redundant switch architecture enhances network reliability by minimizing downtime and mitigating the impact of hardware failures. Prioritizing low latency is crucial for latency-sensitive applications such as real-time monitoring and control systems. Quality of Service (QoS) mechanisms ensure that high-priority traffic—such as control signals or video streams for monitoring—receives preferential treatment to maintain performance and reliability. The recommended LAN design features a 2+ multi-unit redundant core with high-speed fiber interfaces and power over Ethernet (PoE) switches, tailored to support extensive Wi-Fi® coverage and capacity.

In terms of WLAN, manufacturing environments often have large, complex layouts with obstacles that can interfere with wireless signals. Designing Wi-Fi networks resilient to outages, interference, and signal blockage ensures consistent connectivity and performance. Network design focused on key performance indicators (KPIs) and meticulous dimensioning exercises are essential to meet predefined performance indicators and ensure optimal network performance and reliability.

Security is paramount in manufacturing networks, which handle sensitive data related to production processes, intellectual property, and proprietary information. Robust security measures, including encryption, access controls, and intrusion detection/prevention systems, are essential to protect against cyber threats and unauthorized access. Typical methods for securing the network include 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. Employee training and awareness programs are also critical to prevent human errors that could lead to security breaches. For endpoint security, RUCKUS Cloudpath® Enrollment System is an excellent solution to secure employees, vendors, and guests on the corporate or guest LAN/WLAN.

Best practices

To ensure all these systems work perfectly, the following network architecture and best practices can be used.

The LAN: Addressing the challenges inherent in MWL environments and accommodating the diverse device ecosystem requires a strategic approach to network design and deployment. Implementing best practices ensures robust connectivity and seamless operations.

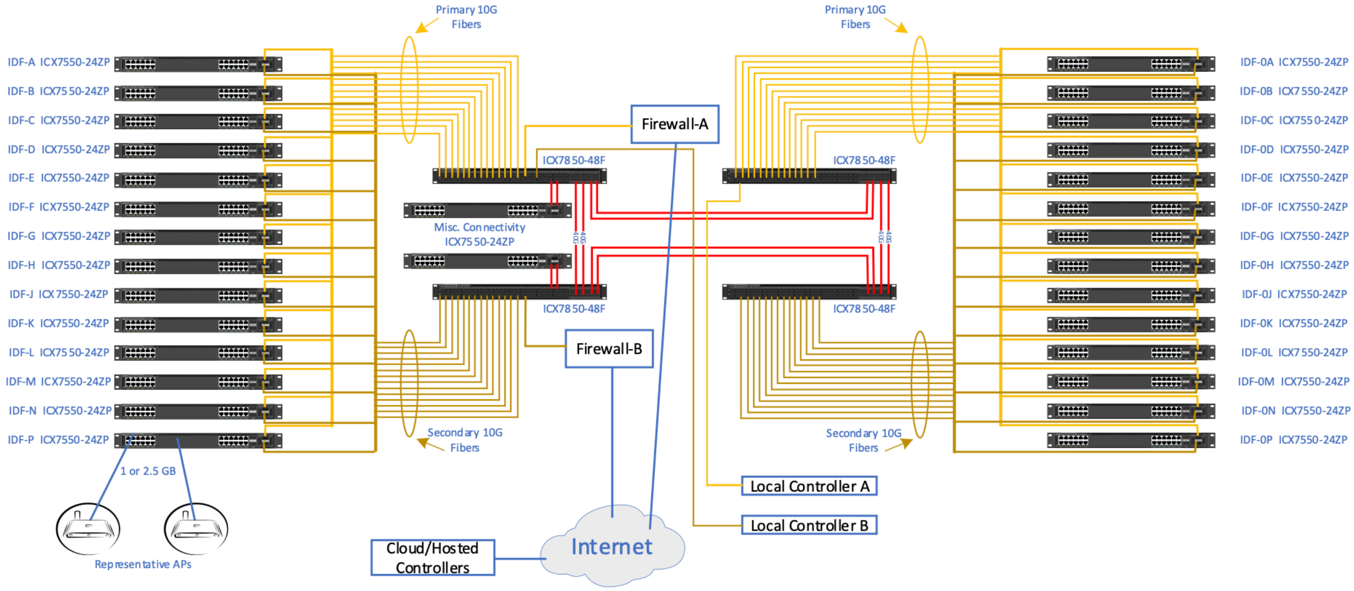
Redundant switch architecture: Deploying redundant switch architectures enhances network reliability by minimizing downtime and mitigating the impact of hardware failures.

Low latency: In manufacturing, latency-sensitive applications such as real-time monitoring and control systems are common. The network should have low latency to ensure timely data transmission and responsiveness, particularly for critical processes.

Quality of Service (QoS): Different types of traffic may have varying priority levels within a manufacturing environment. Implementing QoS mechanisms helps high-priority traffic—such as control signals or video streams for monitoring—receive preferential treatment to maintain performance and reliability.

The recommended design for the LAN supporting the Wi-Fi system is a 2+ multi-unit redundant core. The core units will be equipped with 10 or 40 GbE fiber interfaces for connectivity to IDF edge/PoE switches. There will be copper 802.3bt PoE switches within each IDF and will connect to the core devices via qty-2 10 GbE fiber. The edge/PoE switches will provide PoE connectivity at 1 or 2.5 Gbps to access points (APs) serviced from that IDF. The "ZP" line of ICX® 7550 edge/access switches has an increased PoE budget and will provide connectivity and power for sensors, cameras as well as APs.

If a switch stack or IDF failure is a major concern, the Wi-Fi network can be split such that one IDF serves half the APs interleaved between the other half served by another IDF. If an IDF or switch stack fails, coverage is ensured in the work environment, although the same performance KPIs may not be assured. Operations may continue while the issue is resolved.

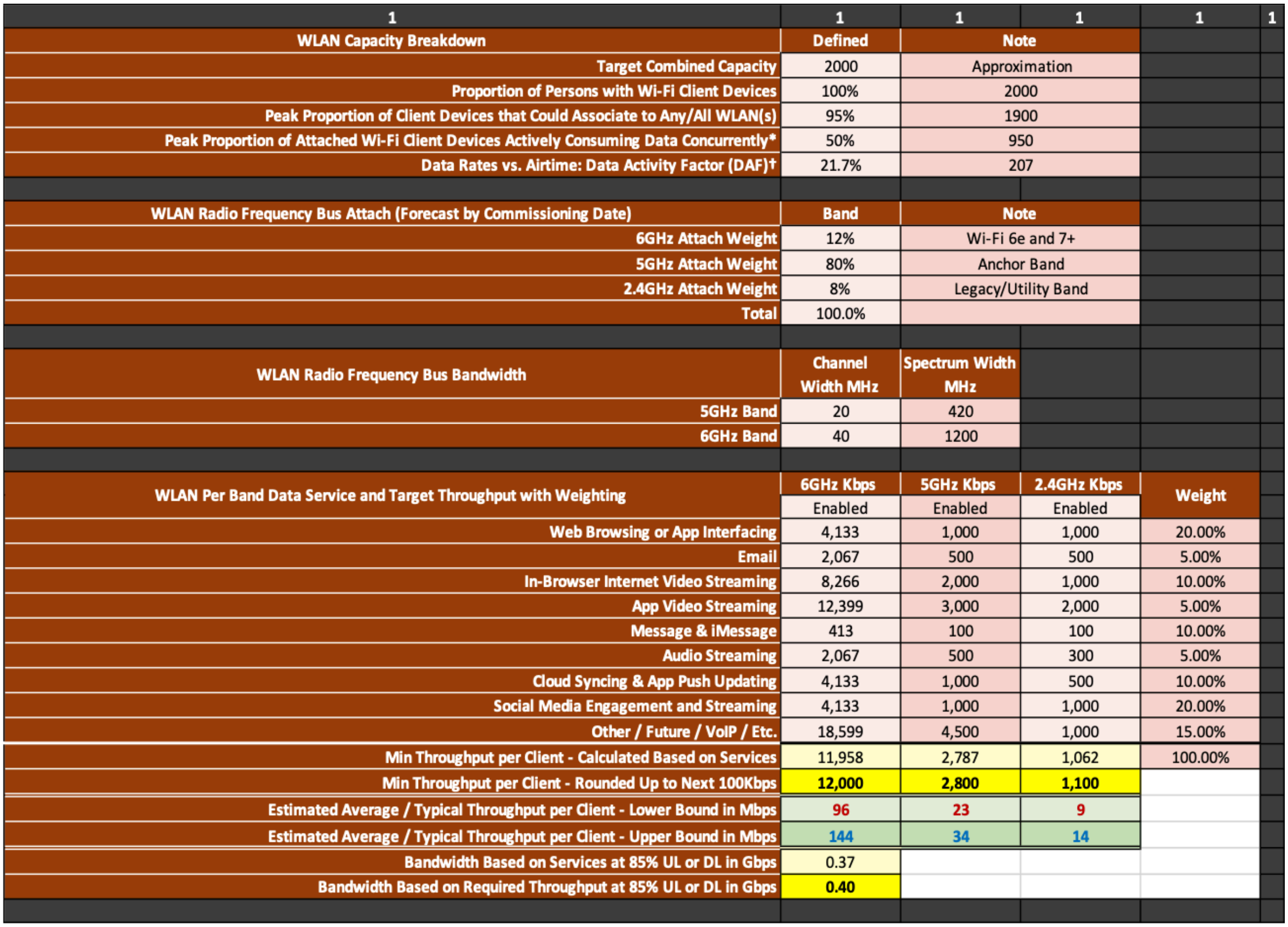


The WLAN

Coverage and capacity: Manufacturing environments can have large, complex layouts with obstacles such as machinery and equipment that can interfere with wireless signals. The Wi-Fi network should provide sufficient coverage and capacity to ensure connectivity across the entire facility, including remote corners and multi-story buildings.
Designing Wi-Fi networks resilient to outages, interference, and signal blockage ensures consistent connectivity and performance in dynamic MWL environments.

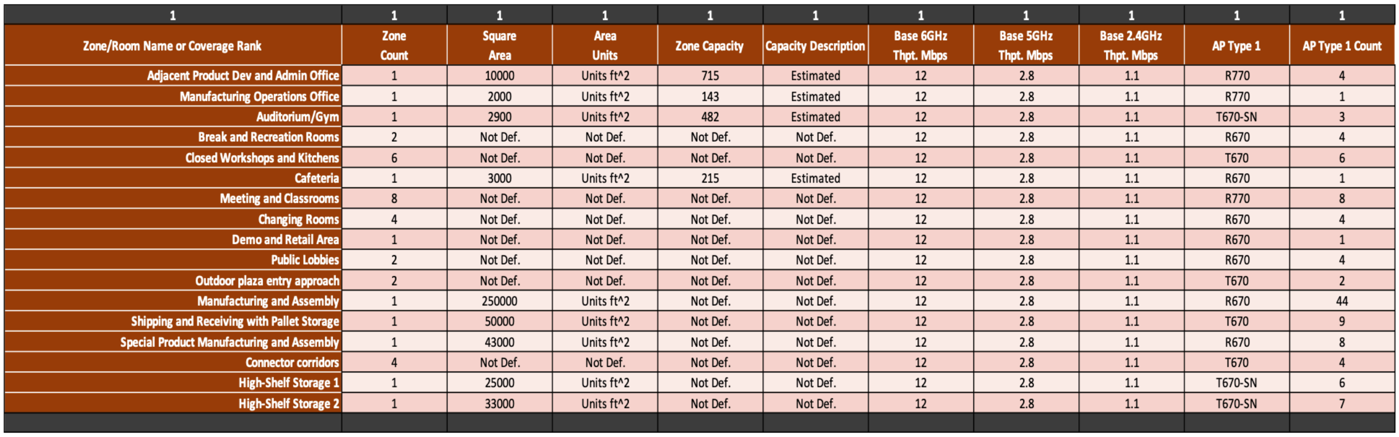
KPI-focused network design: Designing and testing networks to meet predefined KPIs ensures optimal network performance and reliability.

Before embarking on the design, doing a proper dimensioning exercise is necessary. This process is also helpful during the pre-sale/budgetary phase to estimate equipment costs. The dimensioning will take into consideration the number of users, the percentage concurrently active on the network, the total number of devices associated to the WLAN, and the services required to be delivered. The result will determine the demand on the network. From the demand, the number of Wi-Fi APs required to meet that demand can be determined. Most of the design tools can do this to some degree; however, most are not sophisticated enough to consider all these factors, so other dimensioning methods are often required to complement the design tool.



1	1	1	1	1	1
WLAN Capacity Breakdown	Defined	Note			
Target Combined Capacity	2000	Approximation			
Proportion of Persons with Wi-Fi Client Devices	100%	2000			
Peak Proportion of Client Devices that Could Associate to Any/All WLAN(s)	95%	1900			
Peak Proportion of Attached Wi-Fi Client Devices Actively Consuming Data Concurrently*	50%	950			
Data Rates vs. Airtime: Data Activity Factor (DAF)†	21.7%	207			
WLAN Radio Frequency Bus Attach (Forecast by Commissioning Date)	Band	Note			
6GHz Attach Weight	12%	Wi-Fi 6e and 7+			
5GHz Attach Weight	80%	Anchor Band			
2.4GHz Attach Weight	8%	Legacy/Utility Band			
Total	100.0%				
WLAN Radio Frequency Bus Bandwidth	Channel Width MHz	Spectrum Width MHz			
5GHz Band	20	420			
6GHz Band	40	1200			
WLAN Per Band Data Service and Target Throughput with Weighting	6GHz Kbps	5GHz Kbps	2.4GHz Kbps	Weight	
	Enabled	Enabled	Enabled		
Web Browsing or App Interfacing	4,133	1,000	1,000	20.00%	
Email	2,067	500	500	5.00%	
In-Browser Internet Video Streaming	8,266	2,000	1,000	10.00%	
App Video Streaming	12,399	3,000	2,000	5.00%	
Message & iMessage	413	100	100	10.00%	
Audio Streaming	2,067	500	300	5.00%	
Cloud Syncing & App Push Updating	4,133	1,000	500	10.00%	
Social Media Engagement and Streaming	4,133	1,000	1,000	20.00%	
Other / Future / VoIP / Etc.	18,599	4,500	1,000	15.00%	
Min Throughput per Client - Calculated Based on Services	11,958	2,787	1,062	100.00%	
Min Throughput per Client - Rounded Up to Next 100Kbps	12,000	2,800	1,100		
Estimated Average / Typical Throughput per Client - Lower Bound in Mbps	96	23	9		
Estimated Average / Typical Throughput per Client - Upper Bound in Mbps	144	34	14		
Bandwidth Based on Services at 85% UL or DL in Gbps	0.37				
Bandwidth Based on Required Throughput at 85% UL or DL in Gbps	0.40				

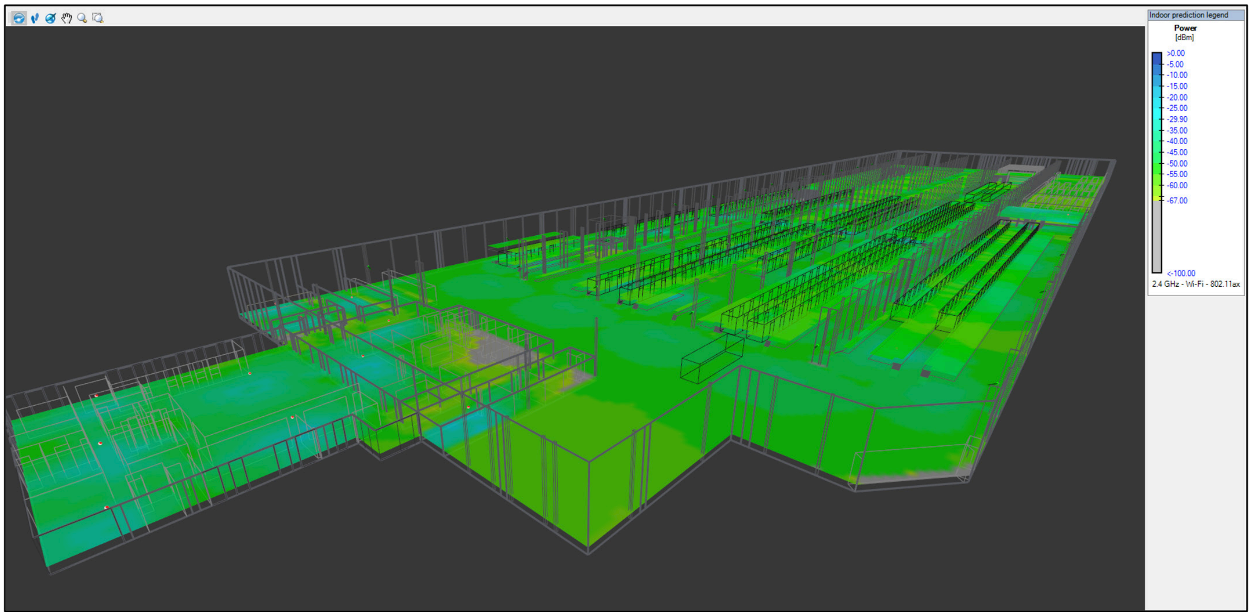
Example of dimensioning for capacity demand



1	1	1	1	1	1	1	1	1	1	1
Zone/Room Name or Coverage Rank	Zone Count	Square Area	Area Units	Zone Capacity	Capacity Description	Base 6GHz Thpt. Mbps	Base 5GHz Thpt. Mbps	Base 2.4GHz Thpt. Mbps	AP Type 1	AP Type 1 Count
Adjacent Product Dev and Admin Office	1	10000	Units ft^2	715	Estimated	12	2.8	1.1	R770	4
Manufacturing Operations Office	1	2000	Units ft^2	143	Estimated	12	2.8	1.1	R770	1
Auditorium/Gym	1	2900	Units ft^2	482	Estimated	12	2.8	1.1	T670-SN	3
Break and Recreation Rooms	2	Not Def.	Not Def.	Not Def.	Not Def.	12	2.8	1.1	R670	4
Closed Workshops and Kitchens	6	Not Def.	Not Def.	Not Def.	Not Def.	12	2.8	1.1	T670	6
Cafeteria	1	3000	Units ft^2	215	Estimated	12	2.8	1.1	R670	1
Meeting and Classrooms	8	Not Def.	Not Def.	Not Def.	Not Def.	12	2.8	1.1	R770	8
Changing Rooms	4	Not Def.	Not Def.	Not Def.	Not Def.	12	2.8	1.1	R670	4
Demo and Retail Area	1	Not Def.	Not Def.	Not Def.	Not Def.	12	2.8	1.1	R670	1
Public Lobbies	2	Not Def.	Not Def.	Not Def.	Not Def.	12	2.8	1.1	R670	4
Outdoor plaza entry approach	2	Not Def.	Not Def.	Not Def.	Not Def.	12	2.8	1.1	T670	2
Manufacturing and Assembly	1	250000	Units ft^2	Not Def.	Not Def.	12	2.8	1.1	R670	44
Shipping and Receiving with Pallet Storage	1	50000	Units ft^2	Not Def.	Not Def.	12	2.8	1.1	T670	9
Special Product Manufacturing and Assembly	1	43000	Units ft^2	Not Def.	Not Def.	12	2.8	1.1	R670	8
Connector corridors	4	Not Def.	Not Def.	Not Def.	Not Def.	12	2.8	1.1	T670	4
High-Shelf Storage 1	1	25000	Units ft^2	Not Def.	Not Def.	12	2.8	1.1	T670-SN	6
High-Shelf Storage 2	1	33000	Units ft^2	Not Def.	Not Def.	12	2.8	1.1	T670-SN	7

Example of the different service areas common in an MWL environment

Manufacturing operations often rely heavily on real-time data and communication. Therefore, network reliability is paramount. The network should be designed to minimize downtime and ensure consistent connectivity to support critical operations. Modeling in 3D is always recommended because of the size of the MWL space and the fact that the location of the machinery and structures is not constant in the space. Being able to create a digital twin of the facility, calibrate the propagation, and pre-optimize the design is critical to ensuring the design will work as needed and prevent costly changes after the installation.



Security: Manufacturing networks handle sensitive data related to production processes, intellectual property, and proprietary information. Robust security measures, including encryption, access controls, and intrusion detection/prevention systems, are essential to protect against cyber threats and unauthorized access.

Typical methods for securing the network include:

1. Firewalls, which act as a barrier between the internal network and external networks—monitoring and controlling traffic based on security rules.
2. Intrusion detection and prevention systems (IDPS), which continuously monitor network traffic for suspicious activities—aiming to detect and block malicious actions in real time.
3. Virtual private networks (VPNs), which create secure, encrypted connections over public networks—enabling remote access to the manufacturing facility's network.
4. Network segmentation, which divides the network into smaller, isolated segments to limit the flow of traffic between different parts—thereby containing potential security threats.
5. Access control systems, which regulate access to specific network resources through authentication mechanisms and role-based access controls.
6. Patch management, which involves regularly updating and patching network devices to mitigate known vulnerabilities and reduce the risk of exploitation.
7. Security information and event management (SIEM) systems, which collect, analyze, and correlate security event data from various sources across the network—providing real-time monitoring and threat detection capabilities.
8. Endpoint security solutions, which protect individual devices from malware, unauthorized access, and other threats through antivirus software, intrusion detection systems, and endpoint detection and response solutions.
9. Wireless security measures for wireless networks, which include implementing strong encryption protocols, disabling unnecessary services, and educating employees about security best practice
10. Employee training and awareness programs, which educate employees about cybersecurity best practices, aiming to prevent human errors that could lead to security breaches.

Key benefits of secure onboarding

Hassle-free wired and wireless network access

RUCKUS Cloudpath® Enrollment System simplifies BYOD and secure guest access with easy, secure self-service network onboarding. Employees, students, partners, and guests onboard their devices once and then automatically re-authenticate in the future—in a process that is entirely transparent. They no longer have to repeatedly re-enter credentials on subsequent network connections. You can also easily onboard headless devices like gaming consoles, printers and IoT devices.

Automated device onboarding and network authentication

Our system lets you automate network onboarding and authentication, so the IT help desk doesn't need to intervene. Easily create customized workflows to support any user. Customize the onboarding portal to reflect your organization's brand identity. You'll no longer see a mountain of trouble tickets for every new device type, and you'll gain the freedom to focus on higher-value activities.

Powerful wireless security and policy for users and devices

WPA2/WPA3-Enterprise enables secure connectivity, with powerful encryption for data in transit over the air. An up-front posture check with remediation means that every device employs baseline security measures before it connects. Authentication based upon digital certificates increases network and data security. You can define and manage granular policies to govern the level of access, plus gain visibility and control over devices on the network—with the ability to revoke access at any time.

For endpoint security, the RUCKUS Cloudpath Enrollment System is an excellent solution to secure employees, vendors and guests onto the corporate or guest LAN/WLAN. For IT-owned assets, Cloudpath can provision devices with a certificate automatically so those MWL devices reside on a secure network, without any end user intervention.

Interoperability: Manufacturing facilities often utilize a diverse range of devices and systems from different vendors. Ensuring interoperability between devices is critical—and ensuring that functionality is maintained before any firmware upgrades, LAN or WLAN upgrades or migrations is important. Assuming that functionality will be maintained can lead to lost time during critical maintenance windows or possible outages during operations. Furthering the point, testing interoperability between LAN (local area network) and WLAN (wireless local area network) devices is crucial to ensure seamless communication and compatibility within a network environment. Several methods can be employed for this purpose:

Functional testing: This involves verifying the basic functionalities of LAN and WLAN devices, such as connectivity, data transmission, and network discovery. Test cases may include checking the ability to establish a connection, transfer data between devices, and detect other devices within the network.

Protocol conformance testing: This type of testing ensures that LAN and WLAN devices adhere to standardized network protocols, such as Ethernet (for LAN) and IEEE 802.11 (for WLAN). Test cases evaluate the devices' compliance with protocol specifications, including packet formatting, addressing schemes, and error handling mechanisms.

Interoperability testing: Interoperability testing focuses on verifying the ability of LAN and WLAN devices to communicate and work together effectively. Test scenarios may involve connecting devices from different vendors or with varying configurations to assess compatibility and interoperability across the network.

Security testing: Security is a critical aspect of network interoperability. Testing methods include assessing the effectiveness of encryption algorithms, authentication mechanisms, and access control policies implemented by LAN and WLAN devices to protect data confidentiality and integrity.

Performance testing: Performance testing evaluates the speed, throughput, and latency of data transmission between LAN and WLAN devices. Test scenarios simulate various network conditions, such as heavy traffic loads or interference, to measure the devices' performance under different circumstances.

Roaming testing: For WLAN devices, roaming testing is essential to ensure seamless handoff between APs as mobile devices move within the network coverage area. Test cases assess the speed and reliability of the roaming process and verify that network connectivity is maintained without interruption during device transitions.

Load testing: Load testing evaluates the scalability and resilience of LAN and WLAN devices under high network traffic conditions. Test scenarios simulate heavy usage scenarios to determine how well the devices handle increased data loads and maintain network performance without degradation or failures.

Compatibility testing: Compatibility testing assesses the ability of LAN and WLAN devices to work with various operating systems, network protocols, and hardware configurations commonly found in the target environment. Test cases verify that the devices can function correctly across different platforms and configurations without compatibility issues.

By employing a combination of these testing methods, organizations can thoroughly assess the interoperability of LAN and WLAN devices, identify potential issues or vulnerabilities, and ensure the reliability and performance of their network infrastructure.

Ensuring interoperability between devices is critical in manufacturing facilities that utilize a diverse range of devices and systems from different vendors. Testing interoperability between LAN and WLAN devices is crucial to ensure seamless communication and compatibility within a network environment. Methods such as functional testing, protocol conformance testing, interoperability testing, security testing, performance testing, roaming testing, load testing, and compatibility testing are employed to thoroughly assess the interoperability of LAN and WLAN devices, identify potential issues or vulnerabilities, and ensure the reliability and performance of the network infrastructure.

By following these best practices, manufacturers can build resilient networks that ensure consistent connectivity, robust security, and operational excellence.

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.

RUCKUS®
COMMSCOPE