
# TRANSFORMING ENTERPRISE WIRELESS: HOW WI-FI 7 AND URWB ENABLE SECURE, SCALABLE CONNECTIVITY IN MISSION-CRITICAL ENVIRONMENTS

*Andrew Spivey, Principal Analyst*

ABIresearch THE TECH INTELLIGENCE EXPERTS™ | CISCO

## CONTENTS



## EXECUTIVE SUMMARY

- Wireless is the key enabler of growth and strategic differentiation within the modern enterprise, underpinning a range of innovative new use cases.
- Competitive advantage can be achieved by adopting an advanced wireless networking platform equipped with future-proof capabilities such as 6 Gigahertz (GHz) Wi-Fi, Ultra-Reliable Wireless Backhaul (URWB), and support for innovative new use cases like location-based services.
- When organizations undertake network upgrades, it is important that they consider not just their needs today, but also the demands of tomorrow.
- Cybersecurity and physical security are two sides of the same coin, and should be addressed with a unified solution.
- We are now in the era of Artificial Intelligence (AI)-driven network management, as the technology is harnessed to improve management effectiveness and efficiency.

# WIRELESS IS THE KEY ENABLER OF MODERN ENTERPRISE

Wireless connectivity is the unsung hero of the modern economy. It facilitates business communications and commercial transactions, underpins security and automation, and is at the foundation of a host of emerging technologies, spanning the Internet of Things (IoT) through to AI. Wireless is now an essential utility for modern organizations, just as vital for operations as water or electricity.

Unfortunately, many organizations today suffer because their wireless networks are not cut out for the needs of their business. Too often they are reliant on outdated technologies that offer insufficient capacity and lack even the capabilities to effectively handle existing applications, let alone innovative new ones. There are four main challenges that organizations with inadequate wireless networks face.

## CHALLENGES TO SCALE AND EXPERIENCE DELIVERY

Organizations are struggling to cope with the ever-rising number of connected devices on their networks, with the resulting higher device densities straining network capacity and available spectrum resources. Highlighting the scale of the challenge is the fact that shipments of chipsets supporting Wi-Fi, the most prevalent wireless technology in the enterprise sector, are projected to expand 53.7% between 2024 and 2030, increasing from 3.7 billion to 5.7 billion. The increase in the sheer volume of devices is straining the ability of organizations to provide consistent experiences for all users and locations across the network, effectively manage the network and troubleshoot issues, handle the large volumes of data that these devices transfer, and rapidly expand or adjust the network to accommodate new demands.

These mounting pressures are becoming an existential crisis for enterprises all over the world, preventing them from realizing their full potential. Faced with these difficulties, enterprises are struggling to achieve acceptable Quality of Experience (QoE) levels for users, witnessing more and more of their resources being drained while attempting to manage an increasingly unwieldy network, and finding themselves incapable of adapting their network to the shifting needs of their business.

Consider also the case of a large sports stadium during a primetime playoff. There will be tens of thousands of visitors entering the stadium simultaneously, all of which expect a seamless, always-on connectivity experience so they can share content in real time, order food, or engage in other activities organized by the home team. If the stadium is unable to handle this high density of dynamically moving devices, then not only will the fan experience be degraded, but the organizers will miss out on valuable revenue opportunities.

Another example is the many hurdles that mine operators face when running their wireless networks. Dependable wireless connectivity is required to connect the thousands of environmental sensors dotted across the entire site, power the numerous Automated Guided Vehicles (AGVs) used for moving material, and ensure that employees have up-to-date safety and task information. Mines often also need to flexibly adjust the scale of their network based on new requirements or shifting work locations. Should the wireless network be unable to meet these needs or if it were to be compromised in any way, downtime costs could be severe and safety at stake.

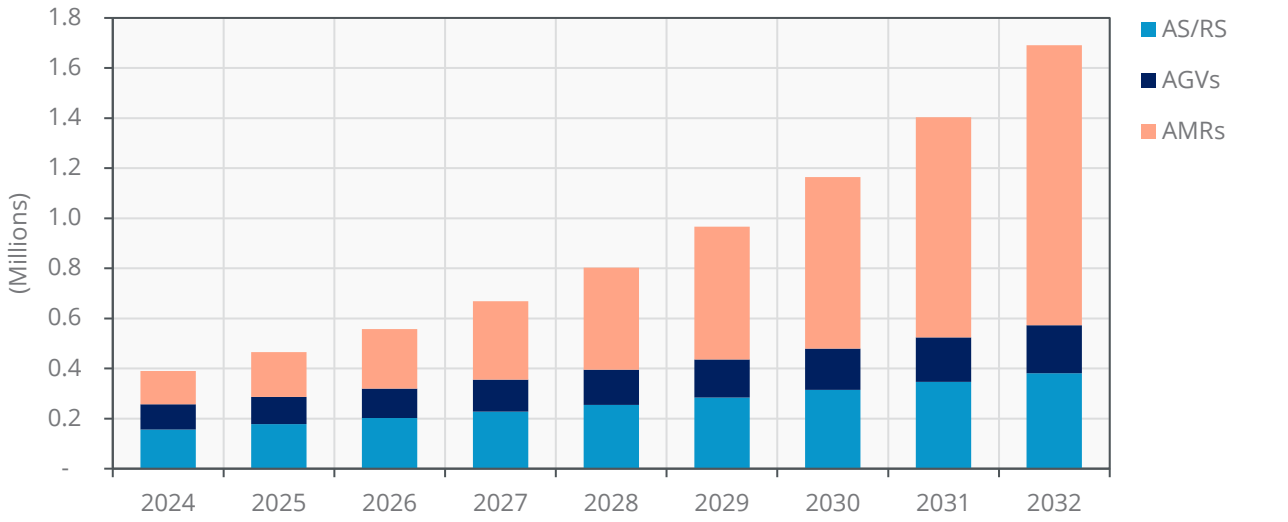
## CHALLENGES IN ENABLING NEW USE CASES

Businesses must innovate to survive, which involves harnessing the latest technologies that give them the edge. Although often underappreciated, wireless is more often than not at the heart of many of the most disruptive new innovations, providing the reliable connectivity underpinning their operation.

Take autonomous robotics as an example. It is not feasible to connect these mobile machines by physical cables, which would be restrictive and prone to failure due to the high levels of wear and tear they face. Thus, wireless is the only possible enabler. The number of warehouses leveraging autonomous robotics is set to skyrocket from 76.6 million in 2024 to 210.8 million by 2032, driven by warehouses' push for greater efficiency, cost savings, and the need to compensate for a lack of skilled workforces. As illustrated in Chart 1, much of this increase will be spurred by the exponential growth of Automated Storage and Retrieval Systems (AS/RSs), AGVs, and Autonomous Mobile Robots (AMRs). Autonomous forklift adoption will likewise continue to increase, with annual shipments projected to gradually grow from 2.0 million in 2024 to 2.3 million in 2032. Organizations that wish to leverage these autonomous robotics will require advanced wireless networks that offer high bandwidths, low latencies, and support for seamless roaming.

***Chart 1: Installed Base of Autonomous Robotics Within Warehouses World Markets: 2024 to 2032***

*(Source: ABI Research)*



Another transformative technology enabled by wireless is AI. Implementing AI can help streamline processes, automate operations, and facilitate the most efficient allocation of resources, boosting an organization's overall productivity. Yet none of this is possible if wireless is not in place to collect data from every connected device, sensor, and application within the network, providing valuable input for both AI inferencing and the continuous training of models. The sourcing of this information inevitably drives up network traffic, as does the operation of autonomous Agentic AI agents across the network. Furthermore, whereas in the past, network traffic has primarily been downlink in nature and often intermittent, AI traffic has a higher uplink distribution and requires the constant transfer of data. These increased uplink demands are driven by the need to continuously gather and upload network data for AI inferencing, whereas the continuous operation of and interaction with AI agents and AI workloads means traffic will be more constant. Enterprises lacking infrastructure built to handle these increased loads and new traffic patterns will be unable to leverage AI for their business.

## CHALLENGES TO SECURITY

Cybersecurity is a growing threat for organizations, with potential network vulnerabilities increasing at the same time that the threats themselves are becoming more varied and sophisticated. If exploited, security vulnerabilities can be crippling for a business. A recent example of this danger is provided by the cyberattack on Jaguar Land Rover in the United Kingdom, with the 5 weeks of halted production and ensuing months of recovery projected to cost a total of £1.9 billion.

Yet security concerns are not limited solely to the cyber realm—ensuring the physical security of products, facilities, and employees is equally as challenging for organizations. Too often, organizations suffer because they have blind spots in their surveillance infrastructure or are unable to effectively act based on the captured footage, and employee safety is endangered due to inadequate protections. There is also the perpetual challenge of balancing security against convenience, with initiatives improving the former regularly coming at the expense of the latter.

## CHALLENGES TO OPERATIONS

The increasing scale and complexity of networks is testing the ability of organizations to effectively and efficiently manage them. The problem is further compounded by the need to integrate diverse services and assets, or deal with multi-vendor environments where solutions do not work together seamlessly. This operational complexity often prevents organizations from proactively addressing issues, leaving them in a constant state of crisis as they attempt to put out fires once they are already raging.

The repercussions of ineffective management are myriad and serious, including degraded user experiences, delayed troubleshooting, greater instances of tickets, a lack of network visibility, exacerbated security vulnerabilities, and inhibited flexibility. Network inefficiencies also inevitably result in wasted resources, both in terms of manpower and with regard to network capacity and capabilities, and ultimately lead to heightened operating expenses and significant opportunity costs.

# HOW TO HARNESS WIRELESS INNOVATION FOR A COMPETITIVE EDGE

If organizations are to advance their competitive differentiation, improve their efficiency, and increase revenue, all while protecting their employees and customers from security threats, they must take into account the following when planning their next network upgrades.

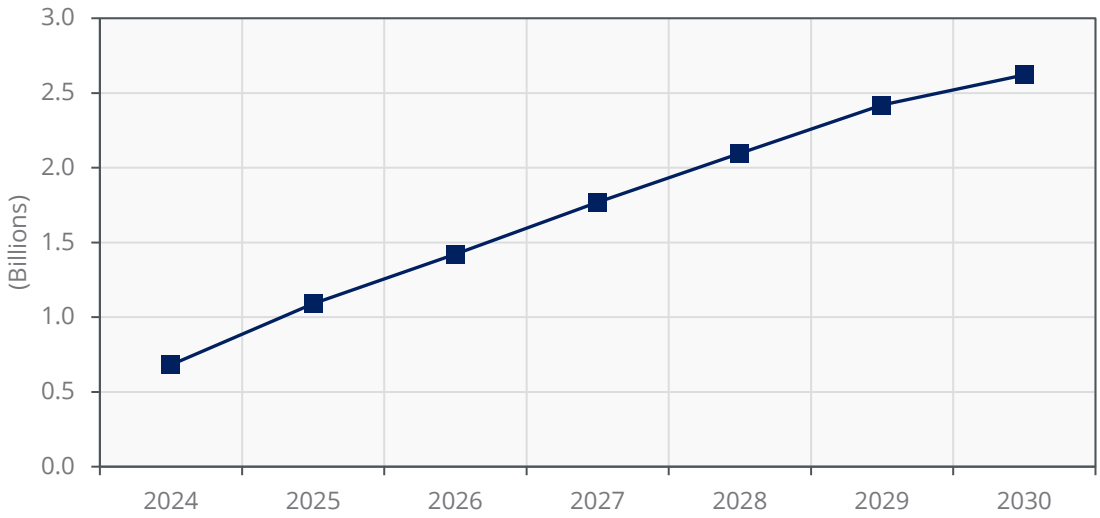
## ENSURE YOUR NETWORK IS FUTURE-PROOFED

It is important that when organizations undertake their network upgrades, they consider not just their needs today, but also the demands of tomorrow. This means building in adequate capacity to account for the future growth in device volume and density, as well as their individual bandwidth requirements. It also means preparing the network for high-value new applications that can help advance their competitive differentiation further down the road.

Adoption of the new 6 GHz spectrum band is non-negotiable for any forward-looking network refresh. The 6 GHz spectrum, first released for Wi-Fi by the Federal Communications Commission (FCC) in the United States in 2020, represents 1200 Megahertz (MHz) of additional fresh spectrum for Wi-Fi to utilize. To put this into context, this is over twice the previously available spectrum from the 2.4 GHz (60 MHz) and 5 GHz (500 MHz) bands in the United States. This expanded capacity will prove invaluable toward supporting the expanded number of Wi-Fi devices and their higher bandwidths demands. The 6 GHz band is also unique in that, unlike 2.4 GHz and 5 GHz, it alone provides the space for the wider 320 MHz channels introduced with Wi-Fi 7, which are important for advanced high-throughput, low-latency demanding applications. Another benefit of 6 GHz worth noting is that the migration of Wi-Fi devices to the 6 GHz band will help alleviate congestion on the 2.4 GHz spectrum, indirectly improving the reliability of IoT devices relying on the band. Finally, the rapid expansion of 6 GHz-enabled devices on the market over the next couple of years, as illustrated in Chart 2, means that networks lacking 6 GHz support will quickly become outdated.

***Chart 2: Shipments of Wi-Fi Chipsets Supporting 6 GHz World Markets: 2024 to 2030***

*(Source: ABI Research)*



End-to-end visibility across the entire network is another must for future-proofed networks. Armed with this insight, organizations can swiftly identify and resolve network issues, optimize the network in real time, and collect the data necessary for actionable AI. Wireless is a key element of this observability, as it connects the end clients, IoT sensors, and other connected devices like cameras dispersed throughout the environment.

Highlighting the importance of both adequate capacity and end-to-end visibility within a network is the example of BottleRock Napa Valley, an annual festival with up to 45,000 visitors. After switching to Cisco Wi-Fi 7 infrastructure with 6 GHz, data usage jumped from 31 Terabytes (TB) the previous year to 44 TB, and there was zero downtime throughout the event. Onboarding onto Wi-Fi was also seamless for visitors, with Cisco Spaces OpenRoaming providing secure, automatic, and password-free Wi-Fi access. Splunk, on the other hand, delivered customizable dashboards to aggregate and visualize data sourced from sensors, cameras, and applications, providing the organizers with a real-time view of network health and performance.

URWB can also play a pivotal role in future-proofing a wireless network. In the past, organizations had to rely on separate wireless backhaul systems, creating additional complexity and cost. Now, thanks to the integration of URWB into many Cisco Wi-Fi 7 and 6E Access Points (APs), the deployment of scalable, resilient backhaul networks is simplified and more cost-effective. URWB offers ultra-low latencies (<10 Milliseconds (ms)) with seamless handover, coupled with Multipath Operation (MPO) for enhanced reliability. These attributes make the technology ideal for supporting applications that standard Wi-Fi struggles to serve, such as mission-critical mobile applications like AGVs or AMRs. It was for this reason that Brazilian infrastructure conglomerate Aterpa chose to leverage the technology instead of Wi-Fi for its dam decommissioning project between 2022 and 2025. Aterpa used unmanned heavy equipment due to the project's inherent dangers, and between September 2022 and April 2025, roughly 2.2 million cubic feet of waste was removed via teleremote operations over Cisco URWB. URWB is also extremely versatile, equipped with an ultra-reliable mesh topology that offers a quick, low-cost, and reliable method of expanding the wireless network to new areas, potentially into outdoor or harsh environments.

## EMBRACE INNOVATIONS UNDERPINNED BY WIRELESS

Simply having wireless alone is not sufficient to retain a competitive edge and meet the demands of tomorrow. If organizations wish to enable a host of innovative applications and experiences that improve outcomes and create new revenue streams, they must ensure that their networks are equipped with advanced, next-generation wireless networking features. This includes capabilities such as Wi-Fi 7, 6 GHz, Cisco AI-Enhanced Radio Resource Management (AI-Enhanced RRM), and Ultra-Reliable Wireless Backhaul (URWB).

It was only by harnessing URWB that DP World Evyap Körfez, one of Türkiye's major ports, was able to achieve ultra-reliable coverage across its 265,000 Square Meter (m2) site. This was thanks to URWB's unique ability to offer seamless handover for roaming assets—essential for cane and AGV operation—and mesh technology that effectively eliminated coverage dead zones. Zero downtime and enabling real-time tracking further improved the port's operational efficiency, and therefore global competitiveness.

Location-based services (LBS) are another series of disruptive technologies underpinned by wireless. LBS can enable numerous innovative applications, ranging from asset tracking, indoor navigation, and occupancy analytics. Yet industry adoption of LBS solutions is currently hampered by an extremely fragmented market, leading to limited scalability and an increased Total Cost of Ownership (TCO). Many suppliers offer only siloed point solutions that rely on proprietary hardware and software, and are typically deployed as custom-built shadow networks, creating additional security vulnerabilities and management complexity.

Cisco has taken a fundamentally different approach toward LBS. Whereas point solutions introduce location capabilities late in the deployment lifecycle, Cisco has embedded location capabilities directly into the core network deployment journey. This is achieved by integrating the precise positioning technologies Ultra-Wideband (UWB) and Bluetooth® Low Energy (LE) into Cisco Wi-Fi 7 APs, and through the Cisco Spaces platform. Because organizations can seamlessly enable LBS on their Wi-Fi 7 infrastructure, network deployments are simplified and greater long-term value can be realized on network investments. Key drivers of Cisco Spaces adoption are indoor navigation (turn-by-turn directions on AI maps), occupancy analytics, seamless Wi-Fi onboarding, and device and asset tracking, with customers using the platform's insights to inform real-estate consolidation, space utilization, and long-term portfolio decisions.

One example of a company leveraging Cisco's LBS solutions is Nutrien, a world-leading producer of crop fertilizer. Nutrien utilizes Cisco Spaces and Cisco Wireless to track assets and personnel in its mines, helping to enhance worker safety and achieve operational enhancement. Similarly, Frankfurt University Hospital deployed Cisco Spaces to track healthcare assets and patients, improving safety, efficiency, and the overall patient experience.

## PROTECT YOUR ORGANIZATION FROM VIRTUAL AND PHYSICAL THREATS

A strong, resilient security posture is formed from a range of key elements. First, security must be simple to deploy, easy to scale, and seamlessly integrated across the entire technology stack. All users and devices wishing to access the network must be met with a zero-trust approach, with continual verification to guarantee compliance, and permissions must dynamically adjust based on posture, behavior, and real-time risk. Policy enforcement must be consistent across all network domains, spanning wireless, switching, and the Software-Defined Wide Area Network (SD-WAN). To minimize vulnerabilities, the network must be micro-segmented, preventing the lateral movement of threats. Unified visibility is also crucial, as this provides a comprehensive, end-to-end view of all threats across the network, at the same time allowing for effective threat neutralization. Such a security posture is provided by Cisco's Identity Services Engine (ISE), an industry-leading Network Access Control (NAC) platform.

Although the proliferation of wireless has brought with it myriad benefits and new capabilities, wireless has also increased security vulnerabilities, as there are more entry points into the network and a greater number of devices to exploit. This necessitates introducing advanced security measures at the Radio Frequency (RF) level. Features developed by Cisco to address this include Cisco's advanced Wireless Intrusion Prevention Systems (aWIPS), CleanAir technology, and Rogue AP detection capabilities.

Finally, organizations must not neglect physical security when protecting their critical infrastructure, enabled by cameras and sensors connected to the network. For maximum efficiency and effectiveness, the physical security platforms should be integrated with the broader network management system, as is the case with Cisco's portfolio of physical security products. This range includes Cisco Meraki MV Smart Cameras, which can be managed and configured directly from the Meraki dashboard. From the Meraki Dashboard, you can reach the Vision portal, which provides access to review or scrub footage, and to locate a person of interest across a camera deployment with a feature called cross-camera tracking. Also included in the range are Cisco's broader suite of Cisco Meraki MT sensors for environmental monitoring or simply monitoring the temperature, humidity, and water leaks of an Intermediate Distribution Frame (IDF) closet.

An example of a company that has successfully leveraged Cisco solutions to tackle both cybersecurity threats and physical theft is the Danish fashion brand SAMSØE SAMSØE. Regarding the former, SAMSØE SAMSØE deployed the end-to-end Cisco Security Suite, with Meraki MX SD-WAN and physical security appliances to provide cutting-edge integrated cybersecurity protections. Centralized management within the Meraki dashboard also ensured swift security patching and updates, while the use of configuration templates helped minimize security vulnerabilities during network deployments. Physical security, on the other hand, was provided by Cisco Meraki MV Smart Cameras. This included the MV84X multi-imager, a 4-cameras-in-1 hardware camera solution, with a single cable deployment for scalable simplicity, 4 TB of storage, and infrared illumination up to 98 feet.

## SUPERCHARGE YOUR NETWORK MANAGEMENT

While advanced capabilities hold transformative potential, they are irrelevant if they cannot be effectively and efficiently managed and orchestrated by users. This is why management simplicity is the final crucial component of a modern network.

We are now in the era of AI-driven network management, when the majority of organizations are leveraging AI technology across the ecosystem to streamline operations and accomplish more with fewer resources. These AI capabilities are powered by advanced Large Language Models (LLMs), the quality of which is inherently dependent on the data that they are trained upon. Drawing from over 40 years of Cisco Certified Internetwork Expert (CCIE) data and continuously learning from new Technical Assistance Center (TAC) and Customer Experience (CX) insights, Cisco has created the industry's most powerful LLM purpose-built for networking, named the Deep Network Model.

The Deep Network Model has been leveraged to develop a range of innovative AgenticOps technologies, in which networking is "agent-first" with agents operating with greater autonomy. One example is Cisco AI Canvas, a Generative User Interface (UI) designed for cross-domain Information Technology (IT) operations, which provides teams with a unified workspace to visualize real-time telemetry, synthesize insights, and accelerate troubleshooting. The Deep Network Model also underpins the Cisco AI Assistant, a natural language assistant that offers continual support to help accelerate workflows and expand proactive capabilities: increasing staff efficiency and effectiveness.

# THE FUTURE OF ENTERPRISE WIRELESS CONNECTIVITY

We are currently living in an era of great innovation within wireless networking. The 6 GHz spectrum is vastly expanding network capacities, Wi-Fi 7 is facilitating immense boosts to wireless speeds and resilience, and URWB is finally enabling the ultra-reliable, seamless connectivity that mission-critical applications demand. Advanced zero-trust NAC platforms are helping organizations defend themselves against the growing sophistication of cybersecurity threats, whereas AI-enhanced cameras are extending protections into the realm of physical security. AI, on the other hand, is delivering a wholesale transformation of what is possible with wireless networking, as the technology is implemented across the entire technology stack. This spans the use of AI-Enhanced RRM to optimize wireless configurations, to the powering of AgenticOps and dynamic AI Canvas for simplified, streamlined network management.

Organizations that harness these innovations will be equipped to thrive in the modern economy, greatly improving their operational efficiencies, providing adequate protection for staff and customers, and creating competitive differentiation through the adoption of disruptive new technologies. In contrast, those that neglect these developments and try to make do with legacy infrastructure will find themselves unprepared to meet the growing challenges of modern networking. For this reason, ABI Research recommends that organizations make an informed, forward-looking network plan when embarking on their next wireless upgrade, so that they are in a position to derive the maximum benefit from these latest innovations.

Published February 2026

ABI Research
157 Columbus Avenue
New York, NY 10023
Tel: +1 516-624-2500
www.abiresearch.com

**WE EMPOWER TECHNOLOGY INNOVATION AND STRATEGIC IMPLEMENTATION.**

ABI Research is uniquely positioned at the intersection of end-market companies and technology solution providers, serving as the bridge that seamlessly connects these two segments by driving successful technology implementations and delivering strategies that are proven to attract and retain customers.