

OUTDOOR CONNECTIVITY'S CRITICAL ROLE IN NEXT-GENERATION ENTERPRISE NETWORKS

Andrew Spivey, Principal Analyst



CONTENTS

EXECUTIVE SUMMARY	1
THE UNDERAPPRECIATED VALUE OF OUTDOOR CONNECTIVITY	2
THE FOUNDATIONS OF BEST-IN-CLASS OUTDOOR NETWORKS	2
FUTURE-PROOF WI-FI	3
OPTIMIZATIONS FOR THE OUTDOORS	6
AI-DRIVEN CROSS-DOMAIN NETWORK MANAGEMENT	7
INNOVATIVE SERVICES AND PARTNER ECOSYSTEMS	8
REAL-WORLD SCENARIOS	8
STADIUMS/ARENAS	8
HOSPITALITY	10

EXECUTIVE SUMMARY

- Enterprises routinely undervalue and underinvest in their outdoor wireless networks. Doing so limits their ability to fulfill business outcomes and prevents them from harnessing innovative emerging technologies, such as Artificial Intelligence (AI), Internet of Things (IoT), and automation use cases.
- Best-in-class outdoor networks unify all elements of an intelligent wireless platform together in one platform, including connectivity, security, automation, analytics, location intelligence, and multi-wireless capabilities.
- Wi-Fi 7 introduces major advancements in latency reduction, reliability, and spectrum efficiency, all of which are extremely valuable in dense and complex outdoor environments.
- 6 GHz can double the available spectrum capacity for Wi-Fi, whereas the Standard Power 6 GHz operating mode adds support for higher power levels and external antennas, both of which are vital in outdoor environments.
- Cross-domain platforms controlled through a Single Pane of Glass (SPOG) and powered by Agentic AI Ops are crucial for managing sprawling, complex modern enterprise networks that traverse both indoors and outdoors.

THE UNDERAPPRECIATED VALUE OF OUTDOOR CONNECTIVITY

Modern enterprises have strict requirements for their wireless network. Connectivity must be always-on, seamless, and able to provide sufficient bandwidth to support the smooth operation of all the devices and applications within the environment. The network must be adaptable to new use cases and scalable to meet evolving demands. End-to-end visibility is key to ensuring swift troubleshooting and gathering actionable insights for continuous network optimization. Security is increasingly a priority, helping to protect businesses from threats that may jeopardize business operations or lead to stolen data and/or resources. Finally, control and orchestration of the network should be streamlined and automated to reduce the management burden.

All serious organizations consider these connectivity goals non-negotiable. Yet while enterprises invariably place great emphasis on achieving these goals in indoor environments, the connectivity needs of the wider outdoor environment are routinely overlooked. Too often, enterprises view the outdoor network as entirely separate from their indoor one, believing that outdoor connectivity is a nice-to-have, but unworthy of the same investment or attention afforded to the indoor network. This mindset, stemming from the outdated assumption that all significant business value is generated in indoor environments, results in outdoor infrastructure often being substandard, outdated, and ultimately not fit for purpose.

Neglecting outdoor connectivity has serious consequences for modern enterprises. Without reliable, high-performance outdoor connectivity, the full potential of their outdoor environments will remain untapped and go to waste. Business outcomes will suffer from performance gaps between indoor and outdoor network infrastructure, as users and applications are unable to seamlessly traverse the two domains. Moreover, it will not be possible to harness the possibilities enabled by multiple emerging technologies, including AI, IoT, and new automation and mobility use cases. In the long run, organizations that continue to undervalue their outdoor network will suffer operationally and financially, as their peers leverage the benefits of robust outdoor connectivity to their competitive advantage.

THE FOUNDATIONS OF BEST-IN-CLASS OUTDOOR NETWORKS

Robust outdoor connectivity must be a central pillar of any organization's connectivity strategy. Yet simply extending the network outdoors is not enough. Best-in-class outdoor networks combine all elements of an intelligent wireless platform—connectivity, security, automation, analytics, location intelligence, and multi-wireless capabilities—together within one unified platform. This section examines the building blocks required for this intelligent wireless platform, and explores how it can be deployed in enterprise outdoor environments.



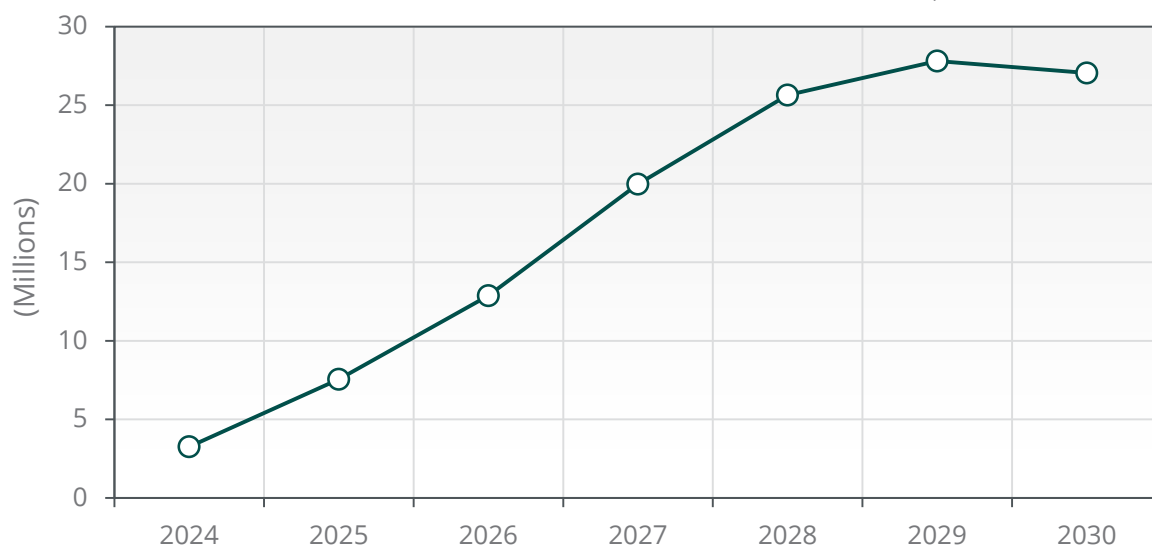
FUTURE-PROOF WI-FI

Wi-Fi 7 is the most advanced Wi-Fi technology currently on the market. The standard was designed to deliver Extremely High Throughput (EHT). In optimal conditions, speeds of up to 46 Gbps can be achieved, over 4X that of the previous generation Wi-Fi 6. Wi-Fi 7 also introduces major advancements in latency reduction, reliability, and spectrum efficiency, through a host of new features, including Multi-Link Operation (MLO), preamble puncturing, and channel widths up to 320 MHz. These enhancements could be extremely valuable in congested and complex outdoor environments, such as campus networks, large public venues, and high-density public spaces in the future.

Illustrating high levels of enterprise demand for Wi-Fi 7 is the rapid level of growth the technology has undergone in recent years. As displayed in Chart 1, shipments of enterprise Wi-Fi 7 Access Points (APs) climbed from 3.3 million in 2024 to 7.6 million in 2025, and are projected to reach a peak of 27.8 million in 2029. While Wi-Fi 6E was the first standard to be compatible with 6 GHz, Wi-Fi 7 was the first standard to be built from the ground up to harness the full potential of the band. Indeed, in many ways, Wi-Fi 7 and Wi-Fi 6 GHz go hand-in-hand, as many of Wi-Fi 7's features were designed on the assumption that the 6 GHz band would be available. Reflecting the additional value 6 GHz adds to Wi-Fi 7, just shy of 99% of all enterprise Wi-Fi 7 APs shipped in North America in 2026 are expected to support the band.

Chart 1: Shipments of Enterprise Wi-Fi 7 APs
World Markets: 2024 to 2030

(Source: ABI Research)



6 GHz first became available for Wi-Fi in the United States in April 2020, when the Federal Communications Commission (FCC) made the groundbreaking decision to allocate the band for unlicensed use. The release of the band, which spans the 5925 – 7125 MHz frequencies, more than doubled the available spectrum for Wi-Fi in the United States overnight. Eager to also harness 6 GHz to stimulate economic growth and innovation, other nations worldwide soon

followed the U.S. lead and opened up unlicensed access to the band. Although some nations chose to only assign the lower 5925 – 6425 MHz portion of the band for unrestricted Wi-Fi usage, reserving the upper portion for cellular services, there are growing calls to expand Wi-Fi access to the upper portion, as well as via spectrum sharing models. For example, in early 2026 the U.K. telecommunication's regulator Ofcom released its plans for enabling spectrum sharing between Wi-Fi and cellular in the 6585 – 7125 MHz frequencies of 6 GHz.

6 GHz's introduction heralded a seismic shift in the capabilities of Wi-Fi, providing the requisite capacity and bandwidth necessary to support the increasing number of Wi-Fi devices and to meet the needs of fast-growing data-intensive applications. Furthermore, the migration of 6 GHz-enabled Wi-Fi devices to the new band helps alleviate congestion on the 2.4 GHz and 5 GHz bands, improving performance on these legacy spectrum frequencies. Reflecting the robust enterprise demand for 6 GHz, shipments of enterprise Wi-Fi APs equipped with 6 GHz rose from 11.6% of total shipments in 2023 to 23.1% in 2025, and by 2028 the proportion is projected to rise to 44.0%.

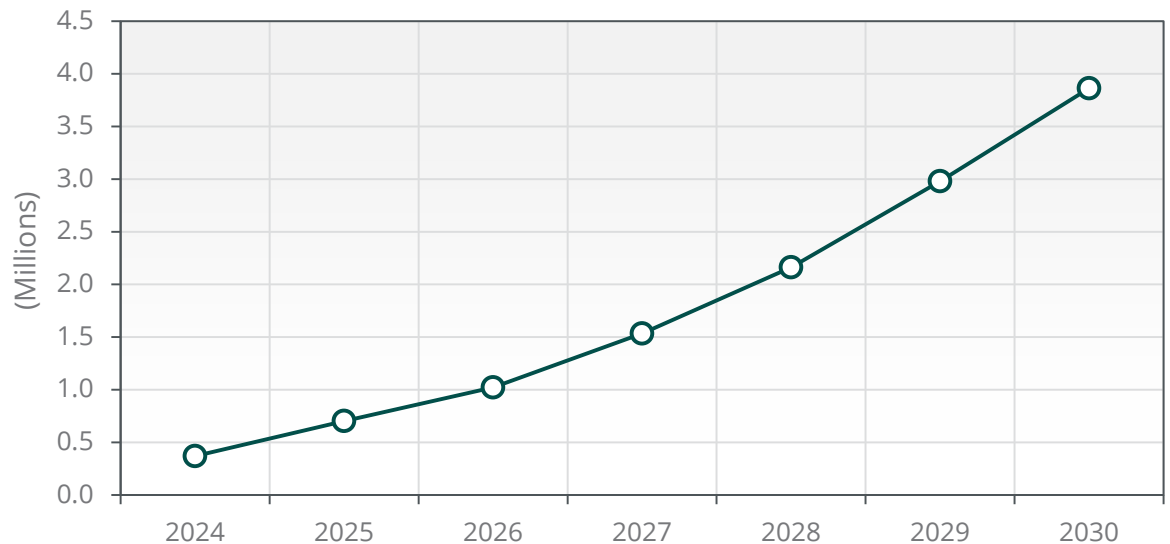
Providing adequate 6 GHz coverage and range in vast and potentially client-dense outdoor environments requires higher power levels than those typically used in indoor settings. This is why the Standard Power 6 GHz operating mode was created for 6 GHz Wi-Fi infrastructure, which permits up to 36 dBm power levels for outdoor transmissions, compared to a maximum of 30 dBm for indoor 6 GHz transmissions. The catch is that Standard Power 6 GHz requires the use of Automated Frequency Coordination (AFC) systems, which are essentially database lookup schemes that first certify the absence of incumbents in the 6 GHz band at any given locality before authorizing transmissions at 36 dBm. For an AP to interact with an AFC system, it must be able to self-locate, and it is for this reason that APs like the Cisco 9177 have a built-in GNSS/GPS receiver, among other mechanisms.

In addition to higher power levels, Standard Power 6 GHz also sanctions the use of external antennas, which can be fine-tuned to extend range and avoid interference between multiple APs. While the majority of Standard Power 6 GHz-enabled Wi-Fi APs are deployed in outdoor environments, the device class is also used in industrial settings to optimize performance for mission-critical applications.

Demand for Standard Power 6 GHz has risen rapidly from enterprises, particularly in the United States. This is highlighted in Chart 2, which shows shipments of Standard Power 6 GHz APs almost doubling between 2024 and 2025, from 0.37 million to 0.70 million. Standard Power 6 GHz AP shipments are forecast to continue increasing going forward, approaching 4 million annually by 2030.

Chart 2: Shipments of Enterprise Wi-Fi APs Supporting Standard Power 6 GHz World Markets: 2024 to 2030

(Source: ABI Research)



A key characteristic of a future-proof outdoor wireless network is convergence of Wi-Fi with private 5G capabilities. While 5G is not well suited to indoor environments, its unique attributes have a lot to offer outdoor environments. These include wider coverage, advanced roaming capabilities, reduced interference due to its use of licensed spectrum, and support for up to 1 million devices per km² via Massive Machine-Type Communication (mMTC). Because 5G's capabilities are complementary to Wi-Fi's, an increasing number of organizations with outdoor connectivity requirements are deploying converged Wi-Fi/5G networks, in which the benefits of both technologies are leveraged for the achievement of optimal performance. Platforms that create competitive integrations between Wi-Fi and 5G provide agnostic access at the service layer, ensuring that management of both technologies is unified and seamless, and that they have a common authentication and policy enforcement framework, meaning that the user experience will be consistent regardless of the technology.

A particularly innovative wireless technology that is highly optimized for outdoor environments is Ultra-Reliable Wireless Backhaul (URWB). This ultra-low latency mesh technology supports Multiprotocol Label Switching (MPLS) for deterministic reliability, Multipath Operation (MPO) for enhanced reliability, and zero-loss handoffs, making it the perfect choice for connecting fast-moving mobile applications in outdoor environments, such as Autonomous Guided Vehicles (AGVs) or Autonomous Mobile Robots (AMRs). A large number of Cisco Wi-Fi 7 APs come integrated with URWB as standard, simplifying and reducing the cost of deployment for scalable, resilient backhaul networks.



OPTIMIZATIONS FOR THE OUTDOORS

Outdoor environments are naturally harsh and inhospitable, with potential hazards including extreme temperatures and exposure to water and dust. Equipment and devices that must operate outdoors need to be engineered to withstand these conditions. The Ingress Protection (IP) rating is an industry standard benchmark used to help organizations understand and measure the resilience of each outdoor device, including enterprise Wi-Fi APs. IP ratings consist of two numbers—the first signifies the degree of protection against solids, and the second protection against liquids.

Due to the potential for high volumes and density of dust in virtually all outdoor environments, it is critical that an outdoor Wi-Fi AP is completely sealed for full shielding against dust. An IP number that begins with 6 offers this level of protection. High levels of water exposure are also a given in outdoor settings, so an outdoor AP must have at least a second IP number of 6, denoting protection against strong water spray from all directions. Yet this is often not sufficient, and for maximum reliability it is recommended that an outdoor AP supports a second IP number of 7, which ensures the ability to withstand up to 30 minutes of water immersion between 15 cm and 1 m. The recently released Cisco 9177 is an example of an outdoor Wi-Fi AP with an IP67 rating, signifying that it is built for operation in harsh and unpredictable outdoor environments.

While a high IP rating will protect an AP from the elements, physical knocks to the hardware could still push the AP and its finely tuned external antennas out of alignment, disrupting its operation. The challenge is that many organizations would be unaware and even unable to verify if the AP has been struck or tampered, preventing them from addressing the issue. To ensure that organizations are alerted when a knock to their AP occurs, Cisco has introduced an accelerometer into its advanced enterprise APs, including the Cisco 9177. This embedded accelerometer helps organizations continuously monitor and validate the orientation, pitch, and roll of their Cisco AP after deployment, enabling them to detect any physical interactions with the AP and to maintain optimal antenna alignment.

Utilization of outdoor environments may often be intermittent, meaning that connectivity is not required 24/7. For example, consider an outdoor hospitality venue that closes overnight. To help reduce unnecessary power consumption during these off-hours, advanced Wi-Fi APs now come equipped with power saving modes that intelligently deactivate radios during periods of inactivity. In power saving mode, the AP is still aware of the client environment and can automatically reactivate the disabled radios should the need arise. This feature helps not only with lowering electricity costs for an organization but can also contribute toward sustainability and net-zero initiatives.



AI-DRIVEN CROSS-DOMAIN NETWORK MANAGEMENT

Modern enterprises operate sprawling, increasingly complex networks that span multiple domains. This is especially the case for organizations that traverse both indoor and outdoor environments. In the past, each domain of the network may have been managed by siloed teams using isolated dashboards and a separate set of tools. This approach was not only extremely inefficient but also prevented organizations from achieving their business outcomes and exposed them to security vulnerabilities.

This outdated mode of operation is now being consigned to history with the arrival of cross-network platforms. These provide unified end-to-end visibility across multiple domains, enable the collection of cross-domain telemetry, and offer centralized control via an SPOG. This gives administrators a complete picture of network status, accelerates Root Cause Analysis (RCA), and ensures uniform policy enforcement and a consistent operating model throughout distributed environments, from campus, branch, data center, cloud, and security domains.

AI-driven analysis, automations, and assistance are likewise transforming how enterprises manage their network. There are now myriad different applications for AI within enterprise networks, from AI-enhanced Radio Resource Management (RRM) and network assurance, to AI-driven automation and natural language assistants. These AI capabilities are essential for managing and orchestrating increasingly unwieldy modern enterprise networks.

It is also important to note that AI progress is occurring at an exponential rate, and that the AI of today is far more advanced than that of even just a few years ago. We are no longer in the era of Generative (Gen) AI, in which AI analyzed data with deep learning to generate personalized original content for a specific user. The most widespread application of this form of AI within enterprise networking has been Large Language Models (LLMs), which allow chatbots to engage in natural language conversations with humans. Rather, today we are in the era of Agentic AI, which is characterized by its proactive and autonomous nature, power to execute multi-stage strategies, cross-domain operation, and capacity for inter-agent collaboration.

Security elements must also be integrated throughout the complete technology stack of the platform to guarantee enhanced protection. Key requirements of a resilient security posture include centralized Zero-Trust Access and Role-Based Access Control (RBAC) for all users and devices, consistent policy enforcement across all network domains, micro-segmentation, and Agentic AI for threat detection with human-in-the-loop remediation.

Cisco's Cloud Control platform is an industry-leading cross-domain management platform powered by AgenticOps and unified network and security operations. Control is centralized within a single operational surface, with one login, one inventory, and one topology. AgenticOps capabilities include the natural language AI Assistant (which answers questions

and resolves issues across domains), AI Canvas (a collaborative workspace for teams and AI agents to work together), and Cloud Studio Control (that helps to integrate third-party tools and custom agents optimized for the specific needs of an organization). These AI capabilities are powered by the industry's most powerful LLM purpose-built for networking, the Deep Network Model, which can draw upon over 40 years of Cisco Certified Internetwork Expert (CCIE) data, and that is continuously learning from new Technical Assistance Center (TAC) and Customer Experience (CX) insights.



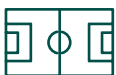
INNOVATIVE SERVICES AND PARTNER ECOSYSTEMS

Few enterprises today fully appreciate the breadth and depth of possible wireless innovations available to them for their outdoor environments. This lack of understanding puts them at a competitive disadvantage, as those who embrace these additional services are able to increase the efficiency and effectiveness of their operations. The range of use cases that these innovations can address is extensive, with solutions optimized for the unique requirements of each vertical's outdoor environment. For example, the need for asset tracking is high in healthcare and logistics, whereas for outdoor retail and hospitality (think of garden centers or outdoor food stalls) Electronic Shelf Labels (ESLs) are in high demand. Again, in the Operational Technology (OT) vertical, enabling the Industrial Internet of Things (IIoT) can help collect valuable data, such as on machinery performance or environmental conditions in outdoor spaces, which can be leveraged for predictive maintenance and operational optimization.

Most of these potential additional services can be deployed from the same wireless infrastructure used for Wi-Fi connectivity. For example, Cisco has embedded Bluetooth® Low Energy (LE) radios into its recently released 9177 series of enterprise Wi-Fi 7 APs, which are designed to support the enablement of a range of innovative applications for outdoor environments. These include Location-Based Services (LBS) like asset tracking, seamless onboarding, and proximity analytics. These LBS can be managed directly through the Cisco Spaces platform.

REAL-WORLD SCENARIOS

For an understanding of how the innovations discussed above can impact outdoor enterprise environments, we do a deep dive in this section into several of the largest campus verticals—stadiums/arenas, education, and warehousing.



STADIUMS/ARENAS

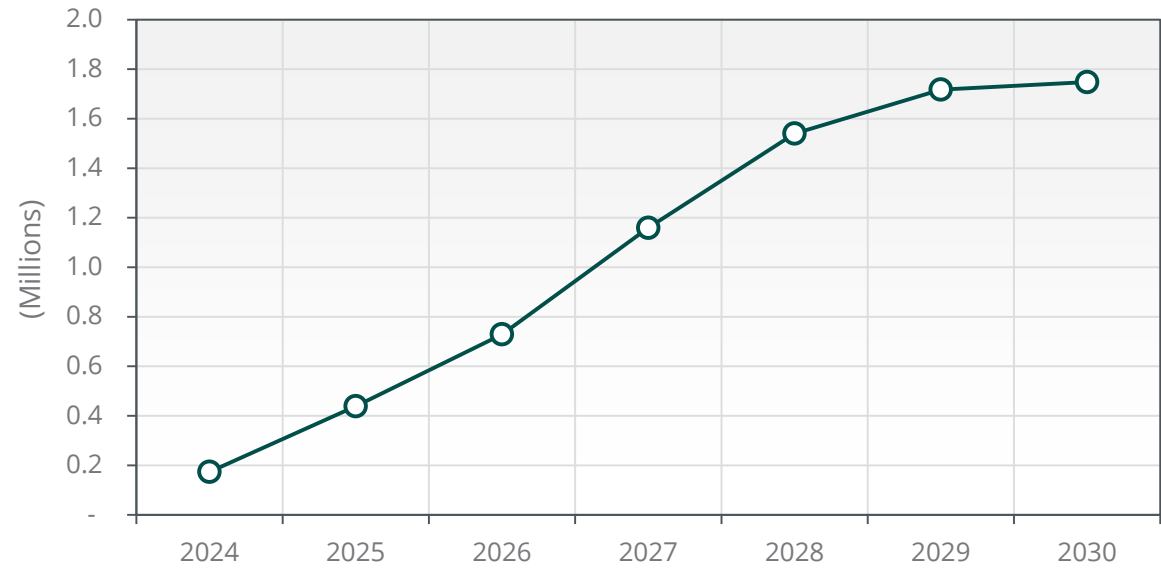
Resilient, high-capacity Wi-Fi has now become indispensable to modern stadiums and arenas. Visitors have come to expect constant connectivity so they can stay connected with friends and family, live-stream footage, and engage with on-site activities such as quizzes or special promotions. Event organizers, on the other hand, now depend on Wi-Fi for essential

communications, tasks such as real-time digital ticketing, and for enabling new interactive services that increase customer satisfaction and boost revenue. Wi-Fi can also be harnessed to provide valuable data on visitor traffic, which through analysis can be used for crowd management, targeted sales promotions, and network optimization.

This explosion of new, data-intensive applications for Wi-Fi, alongside the steady increase in the sheer number of connected client devices, is driving the need for greater network capacity and more advanced Wi-Fi technologies within the stadium/arena vertical. To meet this demand, stadiums/arenas the world over are migrating to Wi-Fi 7 infrastructure with Standard Power 6 GHz support, which provides much needed additional range in the vertical's vast open spaces. This network upgrade is leading to a robust shipment expansion of enterprise Wi-Fi 7 APs to the stadium/arena vertical, as illustrated in Chart 3.

Chart 3: Shipments of Enterprise Wi-Fi 7 APs to the Stadium/Arena Vertical
World Markets: 2024 to 2030

(Source: ABI Research)



At the same time, stadiums/arenas are extremely vulnerable to cyberattacks. In part, this is due to the staggering amount of connected wireless devices throughout the environment, ranging from staff and visitor devices, cameras, and media systems to digital signage, Point of Sale (POS) terminals, access systems, IoT sensors, and more. This diversity and density of devices create a plethora of potential entry points for malicious actors. Therefore, it is vital that outdoor networks in the stadium/arena vertical pair high-performance connectivity with best-in-class security.

A strong example of a tight integration between networking and security within stadiums/arenas is the Cisco network at Levi's® Stadium, the home of the San Francisco 49ers. A Wi-Fi 7 with 6 GHz upgrade was completed at the stadium in advance of Super Bowl LX in

February 2026, which vastly expanded capacity and performance in time for the game. The new infrastructure makes it possible to upload over 35 Terabytes (TB) during the event, which is an immense jump from the approximately 300 Gigabytes (GB) total upload seen at the 2012 Super Bowl. This massive jump in bandwidth was able to provide seamless connectivity experiences for the more than 70,000 visitors to the Super Bowl, and power new applications and devices, such as the world's largest outside 4k video board. This connectivity was integrated with end-to-end security gathering insights from a range of Cisco sources, including Splunk, Cisco ThousandEyes, Cisco Talos Intelligence Group, Cisco Umbrella, Cisco Secure Firewall, and Cisco Meraki.

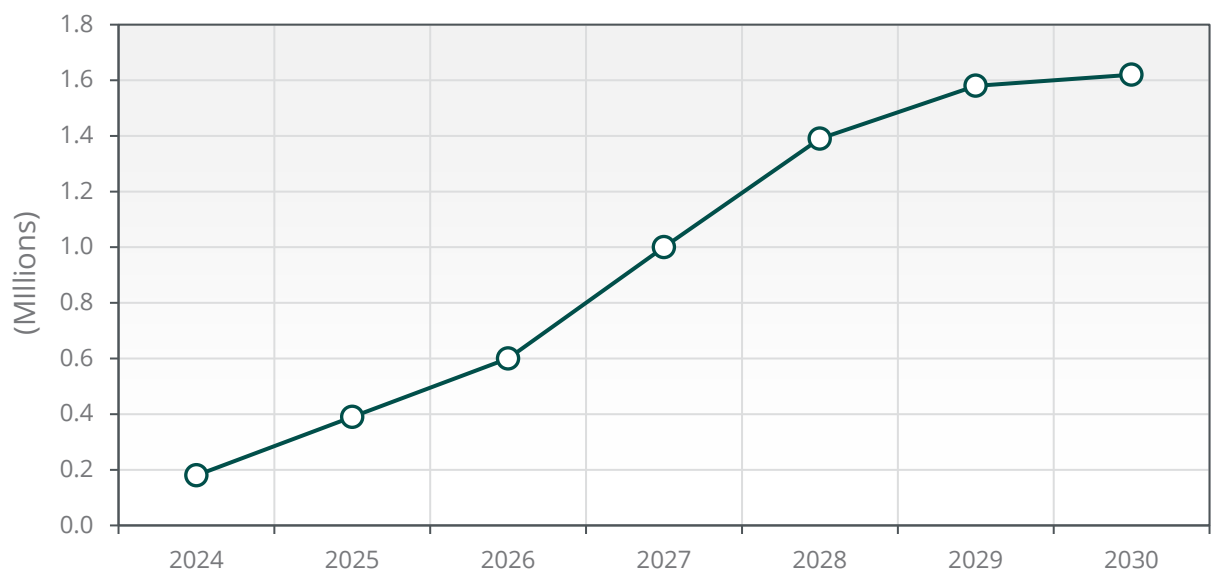


HOSPITALITY

Hospitality is a diverse vertical encompassing a multitude of different sectors, including food & beverage (e.g., cafés, restaurants, etc.), accommodation (e.g., hotels, resorts, etc.), and entertainment (such as wellness packages or immersive events). Each has a unique set of connectivity requirements, but one constant across them all is the need for reliable connectivity that extends to the outdoor domain. For example, to maintain high guest satisfaction and facilitate the smooth operation of additional services like LBS or digital keys, hotels need to ensure that connectivity spans all the outdoor spaces in their environment. Uninterrupted connectivity becomes even more of a critical requirement for a hotel if it is frequented by business travelers or there are business conferences held at the venue. Similarly, restaurants are increasingly relying on Wi-Fi to collect granular data on traffic and customer behavior, which they can then use to refine their own service offerings and introduce new targeted products and services. Yet these insights are only useful if the data are complete and can cover all guests, including those that choose outdoor seating. The growing need for reliable connectivity in the hospitality sector is driving increased demand for Wi-Fi 7 in the vertical, as highlighted in Chart 4.

**Chart 4: Shipments of Enterprise Wi-Fi 7 APs to the Hospitality Vertical
World Markets: 2024 to 2030**

(Source: ABI Research)



As discussed above, hospitality is a diverse sector, encompassing food & beverage, accommodation, and entertainment. Yet in the case of a cruise ship, all the above are combined to offer travelers maximum enjoyment and relaxation throughout their vacation. Reliable connectivity is essential aboard cruise ships for both operational purposes and guest satisfaction. However, cruise ships are some of the most challenging networking environments, due to their scale, harsh conditions, diversity of requirements, and physical isolation. Furthermore, the window for network installation and maintenance is typically exceedingly tight, given that cruise ships spend most of their time on the high seas and rarely dock for extended periods of time.

Cisco drew upon its extensive experience supplying the hospitality sector to support AIDA Cruises in meeting this challenge. To guarantee network reliability and allow network deployment to be completed within a 14-day window, a digital twin of the network was built prior to deployment with Cisco Solution Validation Services (SVS), through which configurations were validated and integrations were rigorously tested. To ensure that guests were provided a seamless connectivity experience across the entire cruise ship, ruggedized APs were deployed in outdoor environments, and wireless OpenRoaming was enabled to allow guests to roam freely on the Wi-Fi network without the need for re-authentication. RFID and Bluetooth® LE integrations in Cisco APs were also leveraged to support critical safety features, such as automated fire patrol monitoring, safety compliance tracking, and emergency scenarios like mustering and evacuation assistance.



Published September 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.

©2026 ABI Research. Used by permission. Disclaimer: Permission granted to reference, reprint or reissue ABI products is expressly not an endorsement of any kind for any company, product, or strategy. ABI Research is an independent producer of market analysis and insight and this ABI Research product is the result of objective research by ABI Research staff at the time of data collection. ABI Research was not compensated in any way to produce this information and the opinions of ABI Research or its analysts on any subject are continually revised based on the most current data available. The information contained herein has been obtained from sources believed to be reliable. ABI Research disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.