WILSON CONNECTIVITY

CIO RESOURCE

IN-BUILDING WIRELESS · EXECUTIVE STRATEGY

Your building has a wireless problem. Here's how to fix it — permanently.

Dead zones, dropped connections, and aging infrastructure are operational risks — not IT inconveniences. This is your executive roadmap to deploying the right in-building wireless solution the first time.

12 MIN READ / EXECUTIVE STRATEGY

72%
of enterprise employees report poor in-building connectivity hurts their productivity

$1M+
estimated hourly cost of wireless-related downtime in high-throughput operations

6
distinct wireless architectures — each purpose-built for a different operational profile

EXECUTIVE SUMMARY

Why in-building wireless becomes a CIO problem

For most CIOs, in-building wireless isn't a headline priority — until it becomes one. A hospital where clinical staff can't reliably reach patient monitoring systems. A distribution center where handheld scanners drop connection mid-pick. A campus where employees rotate between floors with dead zones that make video calls a gamble. A stadium where 40,000 people try to upload the same moment simultaneously.

In every one of these scenarios, the wireless infrastructure failed before the business did. And in most cases, the failure wasn't inevitable — it was the result of deploying a solution that was never designed for the environment it was asked to serve.

This guide is written for the CIO who owns that problem. Whether you're dealing with an active coverage crisis or planning infrastructure for a new build, what follows is a clear-eyed framework for understanding your options, aligning the solution to your operational reality, and making a decision you won't have to revisit in three years.

> **"Most in-building wireless failures aren't technology failures. They're specification failures — the result of deploying a solution designed for a different problem."**

THE STAKES

Why the wrong solution gets deployed — and what it costs

The most common mistake isn't choosing between two similar options. It's deploying a consumer-grade or light-enterprise solution in an environment that demands mission-critical infrastructure — and not discovering the mismatch until operations are already affected. The costs are rarely just technical. They show up as business risk.

Operational downtime

In manufacturing, logistics, and healthcare, wireless connectivity is now load-bearing infrastructure. Unreliable connections to handheld devices, clinical systems, or automated equipment translate directly into stoppages, errors, and lost throughput.

Regulatory & compliance exposure

Buildings above certain size and occupancy thresholds are legally required to maintain in-building signal strength for public-safety communications (NFPA 72, IFC Section 510). Non-compliant facilities face code violations, failed inspections, and — in an emergency — serious liability.

Expensive re-architecture

The most expensive wireless deployment is the one you have to redo. Under-specified infrastructure — installed because it was cheapest at the outset — forces costly retrofits when the building's demands eventually outgrow it. And they always do.

Security vulnerabilities

Shared, public Wi-Fi in environments that handle sensitive data or controlled access creates exposure that a private cellular architecture eliminates by design. Many enterprises relying on Wi-Fi are unknowingly operating outside their own security policies.

THE SOLUTION SET

The six architectures — what they are and who they're for

Six distinct in-building wireless architectures are deployed at scale today. They are not interchangeable — each was designed for a specific operational profile. The right one depends on venue size, user type, security, throughput, and compliance obligations.

ARCHITECTURE 01

Wi-Fi

BEST FOR: SMALL OFFICES · BASIC RETAIL

Familiar, fast to deploy, and cost-effective where shared public internet access is the primary need. Wi-Fi is not a public-safety solution, cannot guarantee QoS, and is not appropriate for mission-critical or compliance-driven environments.

LOWEST COST | NOT E911 COMPLIANT

ARCHITECTURE 02

BDA Passive DAS

BEST FOR: BASIC COVERAGE GAPS · CODE COMPLIANCE

A Bi-Directional Amplifier system that rebroadcasts existing macro cellular signal indoors. Solves coverage gaps in smaller buildings and supports public-safety E911 — the minimum viable solution for buildings that must meet code. Coverage quality depends on the exterior macro signal.

E911 COMPLIANT | MACRO DEPENDENT

ARCHITECTURE 03

BDA Hybrid DAS

BEST FOR: HOSPITALS · UNIVERSITIES · ENTERPRISE

The workhorse solution for complex mid-to-large commercial and institutional buildings. Supports E911, serves both public and private users across multiple carriers, and handles the RF challenges of multi-story, high-obstruction environments that defeat simpler systems.

ENTERPRISE-GRADE | E911 COMPLIANT

ARCHITECTURE 04

Private Cellular Network

BEST FOR: MANUFACTURING · LOGISTICS · INDUSTRIAL IOT

A dedicated LTE or 5G network owned and operated by the enterprise. The only architecture that delivers deterministic QoS — connections don't degrade under load. Essential where connectivity directly drives operational output and cannot be shared with a public network.

DETERMINISTIC QOS | IOT EXCELLENT

ARCHITECTURE 05

Private Cellular + Hybrid DAS

BEST FOR: AIRPORTS · LARGE CAMPUSES · PORTS

The most capable enterprise architecture — a private cellular core layered with Hybrid DAS to serve both enterprise operations and public multi-carrier access simultaneously. Supports E911 at scale, guaranteed QoS for private users, and open carrier access for guests.

MISSION CRITICAL | VERY HIGH SCALE

ARCHITECTURE 06

Radio Source + Fiber DAS

BEST FOR: STADIUMS · CONVENTION CENTERS · MEGA-FACILITIES

The gold standard for very large, very dense venues. Fiber-fed distributed antenna systems with dedicated radio sources deliver carrier-grade throughput for tens of thousands of simultaneous users across all carriers, with full public-safety compliance. Built for extreme density.

FULLY E911 | CARRIER-GRADE

MAKE THE CALL

The CIO's decision framework

The right architecture emerges quickly once you work through the following questions in order. Most environments fall clearly into one or two categories by question four.

01

Is public-safety (E911) compliance a legal requirement for this building?

If yes — and for most commercial buildings above a certain size, it is — Wi-Fi is eliminated immediately, and a standalone Private Cellular Network also cannot meet this requirement without a DAS layer. Your solution set is BDA DAS, Hybrid DAS, PCN + Hybrid DAS, or Fiber DAS. Start your evaluation there.

02

Is this environment operational-critical — do wireless failures directly stop business processes?

If yes, best-effort QoS is not acceptable. Only Private Cellular or PCN + Hybrid DAS deliver guaranteed, deterministic throughput. If your environment is manufacturing, logistics, healthcare operations, or port/airport ground operations, this requirement alone narrows the field significantly.

03

Who are the wireless users — your employees only, the public, or both?

Private enterprise environments (factories, warehouses, restricted campuses) can own and control the entire network layer. Public-facing venues (hospitals, malls, airports) need solutions that support visitors' own carrier SIMs across all networks. Mixed environments point directly toward PCN + Hybrid DAS or Fiber DAS.

04

What is the venue size and peak user density?

Small offices and retail: Wi-Fi or BDA Passive. Mid-size enterprise and institutional buildings: BDA Hybrid DAS. Large industrial sites and campuses: Private Cellular. Very large public venues: Fiber DAS. If you're unsure, the rule is simple — size up, not down. Retrofitting a more capable system always costs more than specifying it correctly at the outset.

The compliance deadline most CIOs don't know about

Many jurisdictions are actively enforcing — or moving to enforce — NFPA 72 and IFC Section 510 requirements for in-building public-safety wireless coverage. These are not recommendations. Buildings that fail minimum signal-strength requirements for first-responder communications can be cited, fail occupancy inspections, or face permit delays on renovations.

If your building doesn't have a current RF survey confirming E911 compliance, that assessment should happen before anything else.

SIDE BY SIDE

Full comparison: ten criteria across all six architectures

Criteria	Wi-Fi	BDA Passive	BDA Hybrid	Private Cellular	PCN + Hybrid	Fiber DAS
Venue size	Small	Small–Med	Medium	Med–Large	Med–Large	Very Large
User type	Public	Public	Public / Private	Private	Private / Ent / IoT	Public / Private
Security level	Low–Moderate	High	High	Mission Critical	Mission Critical	Mission Critical
Access control	Open	Public	Public	Controlled	Private + Multi-carrier	Multi-carrier
Data throughput	Med–High (shared)	Macro dependent	Macro dependent	Guaranteed QoS	Guaranteed QoS	Carrier-grade
E911 / public safety	Not compliant	Supported	Supported	Handset only	With DAS layer	Full
User capacity	Small–Med	Small–Med	Med–Large	Med–Large	Med–Large	Very Large
IoT suitability	Limited	None	Limited	Excellent	Excellent	Excellent
Scalability	Limited	Limited	Moderate	High	Very High	Very High
Relative cost	$	$$	$$$	$$$	$$$$	$$$$$

Ratings reflect the intended operational profile of each architecture. Actual performance depends on building RF characteristics, carrier agreements, and deployment design.

BY SECTOR

What CIOs in your sector are deploying

Healthcare

RECOMMENDED: BDA HYBRID DAS

Hospitals require E911 compliance, multi-carrier support for patients and visitors, and reliable coverage across complex, RF-challenging multi-story buildings. Larger health systems adding clinical IoT or RTLS are layering in Private Cellular for those networks.

Manufacturing & logistics

RECOMMENDED: PRIVATE CELLULAR

Guaranteed QoS for machine-to-machine communication, autonomous equipment, and real-time telemetry is non-negotiable. Private cellular (LTE/5G) delivers the deterministic performance Wi-Fi cannot. Many facilities now deploy 5G private networks to enable next-generation automation.

Stadiums & arenas

RECOMMENDED: FIBER DAS

The only architecture that handles tens of thousands of simultaneous users across all carriers, meets public-safety compliance, and supports modern event operations — cashless payments, mobile ticketing, broadcast, and live video — is Radio Source + Fiber DAS.

Enterprise & multi-tenant

RECOMMENDED: BDA HYBRID DAS

BDA Hybrid DAS provides cellular coverage across all carriers without requiring tenants to join a private network. Enterprises that need guaranteed QoS on specific floors or zones are increasingly adding a Private Cellular layer for those areas.

K-12, higher ed & MDH

RECOMMENDED: BDA HYBRID DAS

University housing, K-12 schools, and multi-dwelling residential properties need reliable cellular coverage for all residents and visitors without complex private-network management. BDA Hybrid DAS delivers E911 compliance, multi-carrier support, and the scalability to serve medium to large building populations.

Airports, ports & campuses

RECOMMENDED: PCN + HYBRID DAS

These environments must simultaneously serve public visitors and all carriers, enterprise operations teams with guaranteed QoS, and dense IoT infrastructure — a combination no single-layer solution can address. Private Cellular + Hybrid DAS is the only architecture built for this requirement.

THE ECONOMICS

What the right infrastructure costs — and how to think about it

The relative cost scale runs from a single dollar sign for basic Wi-Fi to five for full Fiber DAS. But the more important cost conversation for a CIO isn't comparing solutions against each other — it's comparing the cost of the right solution against the cost of getting it wrong.

An under-specified BDA Hybrid DAS that must be torn out and replaced with a Private Cellular architecture two years later costs multiples of what the correct solution would have cost at the outset. A Wi-Fi deployment in a building that legally required E911-compliant DAS isn't a savings — it's a liability that hasn't been discovered yet.

The framework for CIOs is straightforward: define your operational requirements and compliance obligations first. Then find the lowest-cost architecture that reliably meets them — for today's requirements and the operational roadmap three to five years out. That is the cost-optimized decision. Everything else is false economy.

> **"The most expensive wireless deployment is the one you have to redo. Specify for your actual requirements — including where the business will be in five years."**

NEXT STEPS

Getting to the right answer for your building

The framework in this guide will get you to the right category of solution in a single conversation with your team. Getting to the right specific system — the right equipment, architecture, carrier agreements, and coverage model for your floor plan — requires a proper RF site survey, propagation modeling, and an integrator with experience across all six architectures.

The highest-risk path is engaging a vendor who only sells one or two of the six solutions. The recommendation you receive will reflect their inventory, not your requirements. An independent, multi-platform integrator will model your building, assess your compliance obligations, and present options across the full solution set.

Wilson Connectivity has deployed in-building wireless across all six architectures and every major vertical — healthcare, manufacturing, higher education, hospitality, stadiums, and government facilities. Our starting point is always your operational requirements, not a product catalog.

TALK TO AN ENGINEER

Ready to solve your building's wireless problem?

WILSON CONNECTIVITY

Wilson Connectivity will assess your facility, map your compliance obligations, and recommend the architecture that fits your operations — not our product line.

WEB
wilsonconnectivity.com

EMAIL
sales@wilsonconnectivity.com

PHONE
1-800-871-1612

ST. GEORGE HQ — 1444 E VENTURE DR, ST. GEORGE, UT 84790