



IMMUNITY NETWORKS · eBOOK

# High-Density Wi-Fi 6 Deployment Guide

How to design, size and run Wi-Fi 6 networks that actually perform under load — for campuses, venues and enterprises.

**A Make-in-India OEM guide**

immunitynetworks.com · +91 91367 90819

## Contents

1. Wi-Fi 6 vs Wi-Fi 5 vs Wi-Fi 6E
2. Designing high-density Wi-Fi for airports & venues
3. Powering your access points: PoE explained

Compiled from the Immunity Networks knowledge base. For tailored design help, contact our engineers.

# 1. Wi-Fi 6 vs Wi-Fi 5 vs Wi-Fi 6E

Wi-Fi standards are marketed on headline speed, but for a business the real question is different: how many devices can connect at once, how does it behave in a crowded room, and is it worth upgrading? Here is a practical comparison of Wi-Fi 5, Wi-Fi 6 and Wi-Fi 6E.

## The quick version

Wi-Fi 5 (802.11ac) was built for speed in a world of fewer devices. Wi-Fi 6 (802.11ax) was built for density — many devices sharing the air efficiently — which is what modern offices, campuses and public venues actually need. Wi-Fi 6E is Wi-Fi 6 extended into the new 6 GHz band, adding clean spectrum where regulators (and your country) permit it.

## Capacity, not just speed

The biggest real-world gain in Wi-Fi 6 is how it handles many clients. OFDMA lets one transmission carry data to several devices at once, instead of serving them one after another. MU-MIMO increases the number of simultaneous streams. BSS colouring reduces interference between overlapping access points. Together these mean a hall full of phones stays usable, not just “connected.” If you have crowded spaces, this matters far more than peak megabits.

## Battery life and latency

Wi-Fi 6 introduced Target Wake Time (TWT), which lets devices schedule when they wake to transmit — saving battery on phones and IoT sensors. Combined with more efficient scheduling, Wi-Fi 6 also lowers latency under load, which helps video calls, cloud apps and real-time systems.

## What Wi-Fi 6E adds

Wi-Fi 6E opens the 6 GHz band: a large block of fresh spectrum with no legacy Wi-Fi 4/5 devices crowding it. In dense environments that translates to wider channels and less congestion. The catch is that 6 GHz has shorter range and requires 6E-capable client devices and regulatory approval in your market, so it complements rather than replaces good 5 GHz design.

## Do you actually need to upgrade?

Upgrade to Wi-Fi 6 if any of these are true: your spaces are dense (offices, classrooms, clinics, retail, venues); you’re adding lots of IoT; users complain during busy periods; or your access points are several years old. If you run a sparse environment with few devices, Wi-Fi 5 may still be adequate — but new deployments should standardise on Wi-Fi 6 for headroom.

## Designing for density the right way

A Wi-Fi 6 logo on a box doesn’t guarantee good Wi-Fi. Capacity comes from design: estimating concurrent clients, planning access-point placement and channels, and tuning continuously. Immunity’s Lotus Alpha Wi-Fi 6 access points are built for high density, and Net Cloud includes a WiFi Planner to model coverage and capacity before you buy, plus automatic RF optimisation after. See our guide to high-density Wi-Fi for airports and venues.

## 2. Designing high-density Wi-Fi for airports & venues

Airports, stadiums and large campuses are the hardest Wi-Fi environments there are: thousands of devices in a small area, constant roaming, and zero tolerance for downtime. Coverage alone is not the goal — capacity is. Here is how we approach high-density Wi-Fi 6 design.

### Plan for capacity, not just coverage

A single access point can “cover” a large hall, but it cannot serve a thousand simultaneous clients. High-density design starts from client count and application mix, then works out how many radios you need and where. Our built-in WiFi Planner models coverage and capacity on your floor plan before any hardware ships.

### Why Wi-Fi 6 matters here

Wi-Fi 6 (802.11ax) was designed for density. OFDMA lets one transmission serve many clients efficiently, MU-MIMO increases parallelism, and BSS colouring reduces interference between overlapping cells. In a terminal full of phones, these features are the difference between “connected” and “usable.” The Lotus Alpha access points are built for exactly this.

### Seamless roaming across a large footprint

Passengers walk the length of a terminal without dropping a session. Fast roaming and a well-designed channel plan keep handoffs invisible. This is where a planned RF layout — not ad-hoc AP placement — pays off.

### Isolation and compliance

Public passenger Wi-Fi must never touch operational or security systems. We segment guest traffic onto isolated VLANs on NetForce switches, enforce client isolation, and log public access centrally for compliance.

### Operate it from one screen

At airport scale you cannot manage APs one by one. Net Cloud gives you live telemetry, automatic remediation and one-click rollout across every terminal — and across multiple airports — from a single console.

We run exactly this for passenger and public Wi-Fi across major Indian airports. Read the aviation case study or discuss your venue.

## 3. Powering your access points: PoE explained

Power over Ethernet (PoE) lets a single network cable carry both data and electrical power. It's what powers your access points, IP cameras, phones and door controllers without a separate electrician-installed socket at each device. Here's what the different PoE types mean and how to plan for them.

### Why PoE matters

Without PoE, every ceiling access point or wall camera needs a nearby power outlet — expensive, ugly and inflexible. With PoE, you run one Ethernet cable from a PoE switch, and the device gets both connectivity and power. You can place devices exactly where coverage needs them, and back the whole network with a single UPS in the comms room.

### The PoE standards, simply

PoE (802.3af) delivers up to about 15.4 W at the switch port (~12.95 W at the device). Fine for basic access points, VoIP phones and small cameras.

PoE+ (802.3at) delivers up to about 30 W per port (~25.5 W at the device). This is the practical default today — enough for Wi-Fi 6 access points, PTZ cameras and most devices.

PoE++ (802.3bt) comes in Type 3 (up to ~60 W) and Type 4 (up to ~90–100 W) for power-hungry devices like high-end APs with multiple radios, video phones, displays and some IoT gateways.

### What is a “power budget”?

A PoE switch has a total power budget shared across its ports. A switch might support PoE+ on every port individually but not be able to deliver maximum power on all ports at once. When specifying a switch, add up the wattage of every powered device and confirm the switch's total budget comfortably exceeds it — with headroom for growth. This is a common and costly oversight.

### Planning PoE for a real deployment

Count your powered devices and their class: access points (often PoE+), cameras (PoE or PoE+), phones (PoE), door controllers and IoT (varies). Sum the worst-case draw, add ~20–30% headroom, and choose access switches whose budget covers it. For a campus, distribute powered devices across multiple switches rather than overloading one. Immunity's NetForce switches offer PoE/PoE+ across the access range, with budgets sized for dense access-point and camera deployments — see PoE adapters & mounts for standalone injectors and mounting.

### PoE and your wireless rollout

Because access points are almost always PoE-powered, your switching and wireless plans are linked. Size the PoE budget alongside your Wi-Fi 6 design so every planned access point has guaranteed power. Managing both from Net Cloud means you can see per-port power draw and spot problems early.