



TECHNICAL WHITE PAPER

MDU

Managed Wi-Fi for Multi-Dwelling Units

One SSID for the whole property. A private, isolated network for every unit. Onboarding that a resident does once.

The router-per-apartment habit

It looks reasonable. It quietly destroys the airwaves.

Multi-dwelling units have Wi-Fi requirements that blend the public and the private. Tenants expect seamless access, high performance and secure separation between units. Property owners and service providers need simple management, low cost, and the ability to scale across buildings.

Traditionally, Wi-Fi in MDUs has been provided by putting a home router in each unit. Each dwelling gets its own SSID and its own subnet; traffic stays separated. At first glance this makes sense. It does not survive contact with radio physics.

The arithmetic nobody runs. With only four SSIDs present on the same channel, seen by four different access points, **beacons alone consume over 50% of the airtime.** Half the capacity of the network is gone before a single resident has loaded a single page.

And it compounds

- Dozens of SSIDs are visible from any one location — residents cannot tell which is theirs.
- Wi-Fi bleeds between units, next door and floor to floor. A resident often has better signal from their neighbour's AP than their own.
- Common areas need yet another SSID, adding more beacons.
- Give residents poor Wi-Fi and they install their own equipment — which degrades it further for everyone. This is the failure mode that matters, because it is self-reinforcing.

Enterprise approaches are no better. Per-device onboarding and RADIUS-heavy authentication are cumbersome for residents and operators alike. No tenant wants an AAA workflow to connect a television.

One SSID. A key per home.

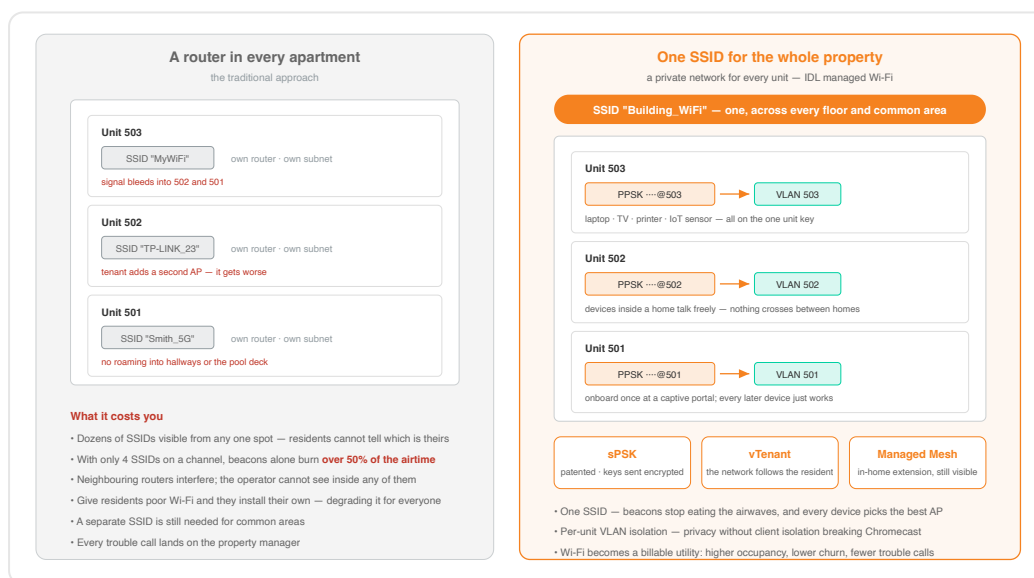
sPSK — IDL's patented answer.

Instead of an SSID per unit, the entire property broadcasts a **single SSID**. Access points placed within units also cover neighbouring ones; devices simply associate with the best available AP, and common areas are covered by the same SSID.

Each tenant gets their own pre-shared key. **sPSK (Sensed PSK)** goes beyond legacy DPSK: keys are securely encrypted during distribution, protecting resident privacy.

How a resident actually experiences it

- They connect once, through a captive portal, and register their unit.
- The controller generates a unique per-unit key, binds it to their VLAN, and pushes it to the access points.
- Every device they own afterwards — laptop, printer, Apple TV, or a headless IoT sensor with no screen at all — joins with that same key. There is no second workflow.
- The key roams with them: the unit's network is available in the laundry room, the lobby, the pool deck.



One SSID across the property; per-unit PPSK mapped to a per-unit VLAN

Isolation without breaking things

Privacy that doesn't stop a resident casting to their own TV.

Traffic is separated into a unique VLAN per dwelling — Unit 501 lands on VLAN 501. Every device in one household shares that VLAN, so a resident can print, and cast to their own TV. Nothing crosses between homes.

This distinction matters: you cannot simply enable client isolation as you would on a guest network, because residents legitimately need their devices to discover each other over protocols like Bonjour. Per-unit VLANs give privacy *and* keep Chromecast working — which is the difference between a solution and a support ticket.

vTenant

vTenant supports both centralized and per-unit local forwarding, so deployment can match the property rather than the other way round. It aligns with how residents actually move — the network follows the user — while SLA monitoring and failover keepalive maintain availability and a consistent experience.

Managed mesh

In-home coverage extension has to be effortless or residents will improvise. Each household can extend coverage with EasyMesh, and third-party access points are supported. Critically, those meshes remain integrated into the central system — combining sPSK authentication, dynamic VLAN assignment and user-to-unit binding — so the operator never loses visibility of a network running inside their own building.

Built for

Apartments

The highest user density, and the most signal bleed between units.

Student housing

The heaviest usage and highest device density of any MDU type; residents change constantly.

Senior & assisted living

Often overlooked. Wi-Fi is now a basic utility here, with more common areas and more guest access.

Townhouses

Larger units, fewer of them, less bleed-through — closer to single dwellings.

Wi-Fi as a billable utility

Take back control of the building.

Like water, electricity or maintenance, the building becomes responsible for the aggregate supply and distribution of connectivity to its tenants. Different service levels can be offered, and the service can be written into the lease.

Revenue

- Increase net operating income and property value by bundling Wi-Fi into the lease, or offering it as a paid upgrade.
- Offer tiered performance and pricing, producing a continuing revenue stream rather than a one-off fit-out cost.
- Increase occupancy and reduce churn — properties that deliver excellent online experiences retain tenants.

Tenant satisfaction

- Tenants onboard every device within minutes of arrival.
- Managed Wi-Fi eliminates the RF conflicts caused by bring-your-own equipment — performance improves for *everyone*, including the residents who were the problem.
- Seamless roaming across the entire property.
- A service that is genuinely better than the mobile signal in an urban building.

Operating cost

- A single managed service simplifies infrastructure oversight.
- The same network, segmented, carries both tenant traffic and building operations — access control, surveillance, door locks, climate, sprinklers. One network, not two.
- Trouble calls fall, because the causes of them have been removed rather than managed.
- A tenant's service can be enabled or disabled digitally, as a matter of billing rather than a site visit.

In summary. sPSK distributes per-unit keys securely under one SSID. Per-unit VLANs isolate traffic while letting devices inside a home talk freely. vTenant makes the network follow the resident. Managed mesh keeps in-home extension under central control. Together they turn Wi-Fi in a multi-dwelling property from a liability into a utility — and into revenue.

About Ignition Design Labs

Ignition Design Labs (IDL) is a market leader in next-generation carrier-grade convergent Wi-Fi and 4G/5G wireless access technologies.

IDL has distinguished itself in the telecommunications sector most notably through its partnership with a Tier-1 operator in East Asia serving over 100 million subscribers — a collaboration that produced one of the world's largest integrated Wi-Fi and cellular systems, with over 400,000 access points across the capital area.

Beyond convergence, IDL addresses the user-experience problems of large-area Wi-Fi coverage: scalability, cognitive radio management, and integration with 4G/5G. It applies AI to network management and IoT security so that customers gain a better experience while spending less on maintenance.

IDL is headquartered in Silicon Valley, with R&D in Taiwan.

Related solutions

- **SD-WiFi** — carrier Wi-Fi offload inside the 3GPP core
- **SD-Edge** — vCPE and uCPE: a fully virtualized, software-defined carrier edge
- **SD-Access** — a zero-trust campus fabric without replacing your switches
- **SD-Branch** — networking, security and SD-WAN converged into one gateway
- **MDU** — one SSID for the whole property, a private network for every unit
- **AIOps** — from reactive monitoring to a network that explains itself
- **Security** — secure gateway and DPI engine

Learn more at ignitiondl.com/solutions