



NETWORK SECURITY

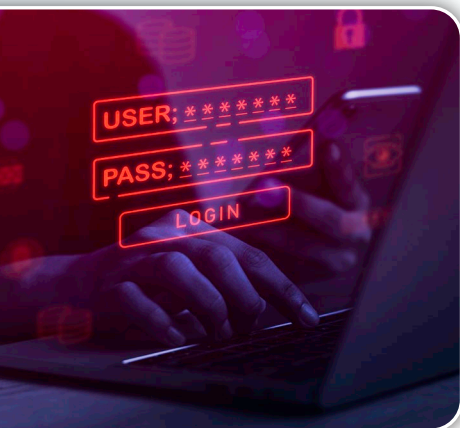
**Why WiFi Security Is Now a Strategic
Asset for Multifamily Owners**

 **Gigstream**
Your network.
Our responsibility.

gigstream.com | 800.747.1830

We've all read the stories. A network gets breached, personal information is exposed, and critical systems go offline. What begins as a quiet vulnerability ends in lawsuits, financial loss, and damaged reputations. As connectivity becomes more deeply

embedded in daily life and business operations, the cost of weak internet security keeps rising.



For multifamily property owners, the risks are compounded.

Connectivity is no longer just an amenity for residents. It underpins smart building systems, supports remote work, and shapes the tenant experience across every square foot of the property. A poorly secured network opens the door to data exposure, tenant distrust, and operational disruption.

In this article, we examine what network security really means in a multifamily environment, why traditional approaches often fall short, and how a purpose-built managed WiFi solution can reduce risk, strengthen resident confidence, and protect the long-term value of your asset.

What Network Security Means for Residents and Property Owners

Owners may not always see the network as part of their risk profile, but residents

already do. The people who reside at your properties expect reliable, secure connectivity throughout, especially as remote work, smart home devices, and streaming define how they live. If the network feels unstable, exposed, or shared in the wrong ways, confidence fades. Security, for residents, means knowing their connection is private, their data is protected, and their experience is uninterrupted.

For property owners, security means something different. It means infrastructure that contains risk by design. It means network segmentation that keeps resident traffic separate from building systems. It means encryption, credential control, and visibility into who's responsible for what. A well-designed managed WiFi system becomes a strategic asset that reduces exposure, supports operations, and strengthens tenant trust.



What Makes a Network Secure? Understanding the Architecture That Protects Your Asset

Secure managed WiFi isn't just "better connectivity." It's engineered infrastructure designed to contain risk, enforce boundaries, and give owners confidence that tenants, systems, and operations are digitally isolated. Here's how that's built.



VLAN: Segmentation That Containment Depends On

A VLAN (Virtual Local Area Network) is the digital equivalent of assigning every tenant their own locked room within a secure building. Although everyone is using the same physical infrastructure, a VLAN ensures each resident's internet traffic is logically isolated from all others.

There's no cross-traffic, digital eavesdropping, or lateral movement of threats. This segmentation is what prevents one compromised device from reaching another tenant or a building system.

Without VLANs, the network is shared. With VLANs, it's isolated by design.



DPSK: Credentials That Tie Identity to Access

DPSK (Dynamic Pre-Shared Key) ensures each resident's access credentials are unique and device-specific. Instead of a shared WiFi password or simple login screen, every tenant is issued a private key that maps to their VLAN. This means:

- No accidental access across units
- No shared credentials floating around the building
- No confusion about who's responsible for what

If a tenant moves out, their credentials are revoked automatically, requiring no hardware to uninstall or passwords to reset. DPSK simplifies onboarding and strengthens accountability.



WPA2: Encryption That Protects in Transit

Even on a VLAN segmented network, data in motion can be vulnerable unless encrypted. WPA2 (Wi-Fi Protected Access 2) is the most deployed WiFi encryption standard for WiFi worldwide. It secures the data moving between a tenant's device and the access point. If someone intercepted the signal, the contents would be unreadable without the key.

WPA2 enhances the integrity of every connection, without requiring any technical steps from the user.



VPN Compatibility: Privacy Beyond the Property

Some tenants, and their employers, require an added layer of encryption and data routing through Virtual Private Networks (VPNs). A secure managed WiFi system must support this without friction.

Properly designed networks allow tenants to run corporate VPNs for compliance and remote work. They can also use personal VPNs for enhanced privacy.

This compatibility reduces tenant complaints and supports a wide range of professional and personal use cases without compromising network security.

Why Managed WiFi Is Safer Than Traditional Approaches

BYO-Router Chaos

In traditional models, each unit contracts separately with an ISP. Tenants install their own routers, often unpatched, unsecured, and misconfigured. Property-wide, this creates a fragmented, unmanaged environment full of interference, rogue devices, and blind spots.

If one tenant's router is compromised, it can:

- Interfere with neighboring connections
- Impersonate legitimate networks
- Act as a bridge to attack building-wide systems
- Become a launchpad for malware within the physical footprint of your property

Worse, owners have no visibility into this environment and no control over how devices behave.



Managed WiFi: Segmented, Monitored, Contained

A well-designed managed WiFi network doesn't just deliver convenience, it:

- Segments traffic from the start (VLAN)
- Locks credentials to users (DPSK)
- Encrypts transmissions (WPA2)
- Monitors infrastructure for threats in real time
- Pushes firmware and security patches without tenant involvement

Managed WiFi shifts security upstream from the tenant's consumer-grade router to enterprise infrastructure with professional oversight. That's how risk is not just reduced, but contained.

How Gigstream Builds Security Into the Network

Most managed WiFi providers talk about speed, simplicity, or basic coverage. Few address security, accountability, and infrastructure designed to reduce risk at scale. Gigstream takes a different approach. From architecture to support, every layer of the network is built to isolate threats, protect tenant privacy, and give owners confidence that their property is secure by default.

Resident Isolation at the Core

Every tenant receives their own VLAN and DPSK credentials. No shared keys or shared traffic. The network is unified, but each user is digitally isolated. This prevents one resident's compromised device or behavior from affecting others, preserving both privacy and network integrity across the entire property.

Enterprise Infrastructure via Ruckus Networks

We deploy enterprise-grade hardware designed for dense multifamily environments—access points with smart antenna technology, load balancing, and real-time threat detection. All infrastructure is monitored and updated remotely. This ensures consistent performance, minimizes signal interference, and reduces the risk of vulnerabilities going undetected or unpatched.

Seamless, Secure Onboarding

Tenants connect in minutes through a self-service portal. No modems, installations, or setup risk. Security defaults are enforced by design. This eliminates common configuration errors and ensures every connection starts with the right protections in place.

Full Support for VPNs

Remote work, high-compliance industries, and high-demand applications are all supported. Residents connect via VPN as needed without adding strain to property management. This gives residents the flexibility they need without compromising the security or stability of the broader network.

Defined Boundaries, Clear Accountability

Gigstream assumes ownership of network security infrastructure. Escalation paths are documented and monitoring is active. If an incident occurs, the line between resident behavior, system integrity, and property impact is clear and contained. This clarity reduces uncertainty, limits liability exposure, and gives property owners confidence in how risk is managed and resolved.

You Don't Need to Be a Security Expert. You Need a Secure Network.

As internet connectivity becomes embedded in building operations, tenant expectations, and investor scrutiny, security can no longer be treated as a secondary concern.

You don't have to master encryption standards or evaluate router firmware yourself, but you do need an infrastructure provider whose solution:

- Protects tenant privacy
- Shields your operational systems
- Clarifies your liability
- Maintains the reputation and stability of your asset

[Reach out to Gigstream](#) to discuss your network security, and how to future-proof it.