



Secure Room Area Network

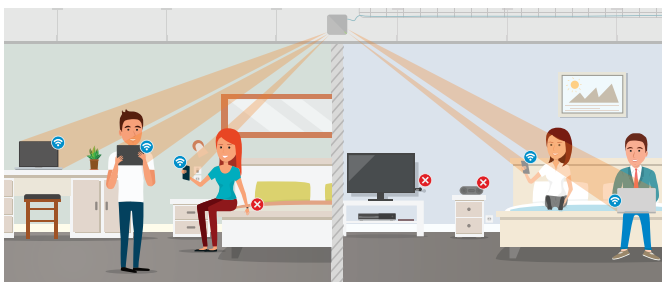
The safest connected room for your guests
to really feel like they're at home

// Connected room infrastructure

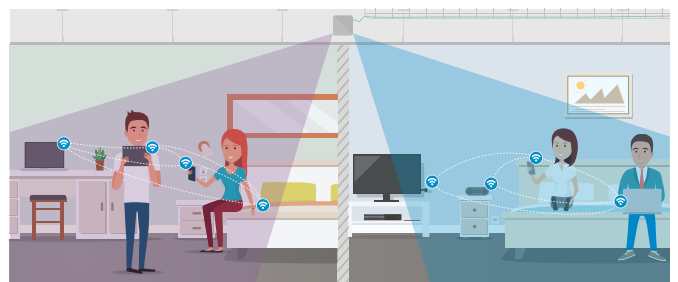
1. Traditional guest Wi-Fi restrictions

Traditional hospitality Wi-Fi is based on an open network with captive portal authentication. The challenge presented by an open network is that it provides malicious users with easy access to illegally obtain data from other devices connected to the network. Typically, wireless service providers will overcome this by configuring the network in a way that avoids devices from being able to see one another. This does, however, cause further challenges and complexities when introducing any form of IoT device into the mix.

Wifirst breaks through this boundary by providing a true home-from-home Wi-Fi experience called Secure Room Area Network. Secure RAN allows guests to easily and securely interact with IoT devices found in their hotel room, and other authorized devices such as a family member in a safe and secure way thanks to WPA2/3 encryption.

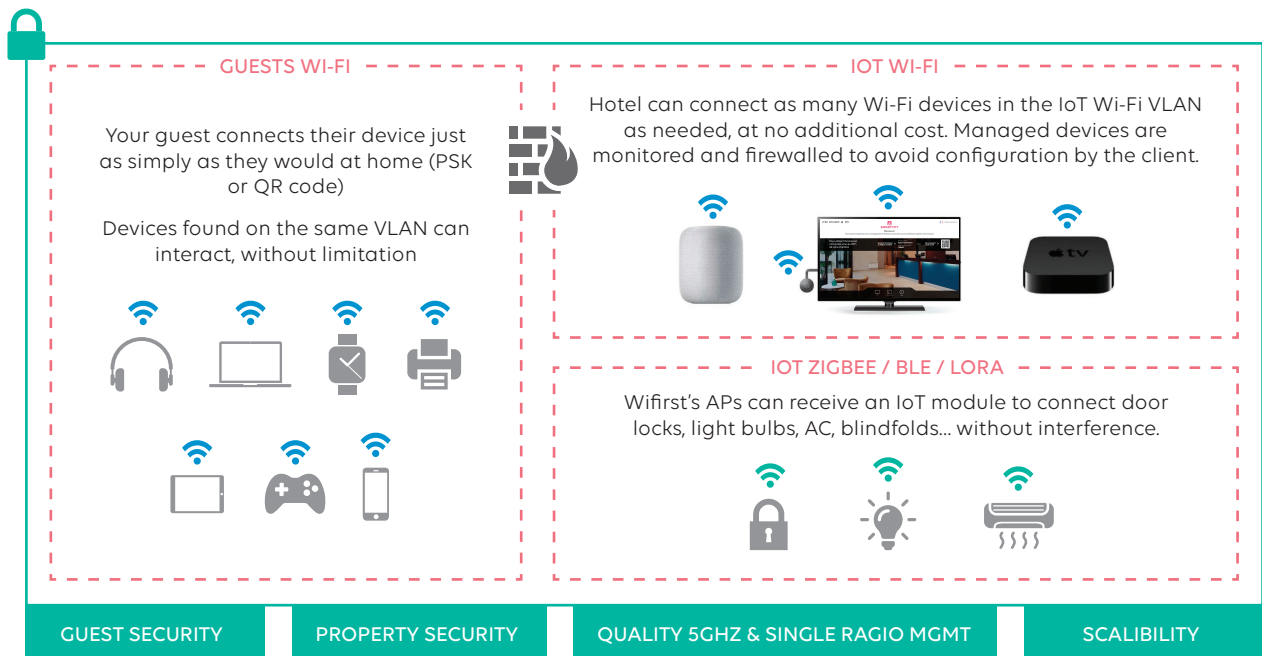


Hotel Guest Wi-Fi without **Secure RAN**



Hotel Guest Wi-Fi with **Secure RAN**

2. What is Secure Room Area Network



KEY STRENGTHS

- Seamless, home-from-home experience for your guests
- Class-leading security for property owned devices
- Converged Wi-Fi + IoT infrastructure to limit interference, complexity and expense
- PMS and Loyalty program integration to create guest's key wherever they check in

// About Wifirst

Wifirst is one of the largest global Wi-Fi Managed Service Providers, having deployed over 200,000 Wireless Access Points, managed and maintained 24/7. We provide Wi-Fi as a service, tailored specifically to the needs of each individual customer. Through the means of site survey, onsite deployment, ongoing service monitoring and proactive maintenance, Wifirst develops custom secure and scalable applications with a strong emphasis on providing users with a seamless experience.

