www.ekahau.com

# Understanding Requirements and Constraints

Not All Hospitality Wi-Fi is Created Equal

ekahau
WIRELESS DESIGN

In today's world of online reviews and social media, there is stiff competition for customers, and the quality of the Wi-Fi deployments in hospitality environments is often ranked more importantly than clean sheets and towels.  Good quality Wi-Fi is expected as part of the room rate; if the hotel cannot provide functional Wi-Fi, forget about happy guests, good reviews, or repeat business.

Hospitality environments have unique networking requirements and constraints as compared to other types of properties.  It is therefore important to capture and understand all of the requirements and constraints systematically prior to picking out your AP hardware. Additionally, different hospitality environments cater to different customers and therefore have their own distinct requirements and constraints to contend with.

Every hotel needs to provide guests with the ability to connect wirelessly to the Internet.  The population of devices changes literally on a daily (nightly) basis, as guests check-in and check-out, so the guest network needs to be able to handle an entire *bring your own device (BYOD)* environment.  The number of devices continues to grow. A lone business traveler will virtually always have a smartphone and a laptop, though may have a tablet and e-reader as well.  Families will have multiple phones, laptops, tablets, and gaming consoles.  Guests are also ever-increasing consumers of bandwidth, and expect to be able to stream HD movies and television shows from services like Netflix, instead of relying upon the hotel's entertainment system.

Most hotel chains generally publish a High-Speed Internet Access (HSIA) document for their franchisees, imposing a brand standard of the minimum requirements for the network.  While the intention of such *brand standards* is to provide a consistent Internet quality level expected by guests visiting any hotel in the chain, some HSIA's are written better than others.  Even within a particular chain, not all properties are created equal, and not all of them will have the same facilities and needs.  Additionally, most HSIA's tend to over-constrain the franchisee, sometimes to the extreme level of dictating particular AP vendors and Internet service providers.  Such constraints need to be factored into the design of the network, but may not be optimal for particular properties.

Accordingly, there are a lot of details to be considered when implementing a hospitality Wi-Fi network, and these details can vary widely with different types of properties. It is therefore critical to capture all *usage*, *coverage*, and *capacity* requirements, as well as the *physical* and *organizational* constraints, in order to properly design and implement a particular hospitality network.

*Usage requirements* characterize how the network is going to be used, and by what types of devices, in the hospitality environment. Even within the confines of allowing guests to access the Internet, there are several requirements that can have large impacts on how the network ultimately gets architected, used, and perceived by the guests.

- **Access Control:** Access to the guest network is usually, but not always, restricted to actual guests. In smaller hotels, it is still common to use WPA2 encryption and give guests the passphrase, though posting the passphrase publicly eliminates the whole point of security. Most hospitality environments will not use wireless encryption but instead implement a captive portal for access. The captive portal may be a simple acceptance of terms and conditions (T&Cs), and may require a valid voucher (common for hosted meetings), or require a valid room number and registered guest. Depending on the login method, the captive portal may or may not need to be integrated into the property management system (PMS) for authentication and/or billing. Some hotels will deploy a hybrid model, where T&Cs are used for the lobby, bar, and restaurants for non-hotel guests, a voucher is required for meeting room spaces, and a valid last name and room number are required for access on guest room floors. There usually needs to be a mechanism to on-board devices without browsers (e.g., gaming consoles), usually with temporary MAC authentication.

- **Billing:** While most low-end and mid-range hospitality properties will provide Wi-Fi access for free, some high-end hotels and resorts will still charge for guest access. Some may charge for access unless you are in their frequent guest program, which is a mechanism to get people to enroll.

- **Bandwidth Restrictions:** Almost always, it is desirable to limit the upstream and downstream bandwidth on guest access, to ensure that individual bad actors cannot consume the overwhelming majority of the property's bandwidth. The amount that bandwidth gets restricted is based on how much bandwidth is available at the property and how many simultaneous users are expected.

- **Content Filtering:** A hospitality property generally wants to prevent access to? BitTorrent and other illegal web sites while on their properties. In public areas such as pools, bars, and restaurants, further restrictions may be required to block pornography and other offensive content.

- **Client Isolation:** This is generally considered a "best practice" and is usually easy to enable with most enterprise-grade Wi-Fi equipment, yet all too often this does not get implemented. While all guests should get on the Internet, client isolation mechanisms - both within and between access points - are needed to prevent guest devices from intercommunicating with each other. This is to protect guests against deliberate hacking and from malware attacks from infected devices put on the networks by guests.

The hotel may need to leverage the wired and/or Wi-Fi network for several other uses as well. Some typical examples are as follows:

- **Staff / Back-of-House:** This would be for staff laptops, tablets, and smartphones for use by the cleaning and maintenance staff, restaurant and banquet staff, as well as for the front desk.

- **Point of Sale (PoS):** For hotels with restaurants / bars / gift shops, PCMCIA compliance usually requires any point-of-sale systems to be on dedicated VLANs that are isolated from all other networks. Such systems may be wired or wireless.

- **Surveillance:** It is common to see cameras installed in lobbies, meeting rooms, elevators, guest room hallways, restaurants, back-of-house areas, etc. While these are usually wired vs. wireless, they still need to be accounted for in the overall network design, especially if only certain staff is allowed access to these video feeds.

- **In-Room Guest Services:** There are many in-room devices / services that will use either the wired Ethernet or Wi-Fi to access the Internet

  o VoIP / VoWiFi: While some hotels have actually stopped putting phones in the guest rooms, most hotels are still providing in-room phones, but are using VoIP-hosted providers for such services.

  o IPTV: Many hotels have switched over to IPTV services instead of conventional cable / satellite to control costs.

  o Mini-Bar: Many mini-bars have the technology to immediately detect which items a guest has taken from the mini-bar and notify the PMS for billing.

  o Smart Room / IoT: Some hotels have started deploying sensors and other "smart room" devices, both for the benefit of the guests, such as lighting and entertainment control, but also for the benefit of the property, to adjust the temperature in the room and shut off lights when the room is unoccupied — to minimize wasted energy costs.

- **Panic Button:** In New York City, the hotel must provide all staff with a panic button that will locate them down to the specific room, in case of emergency or incident. This is usually implemented directly with Wi-Fi or with various indoor location technologies (e.g., BLE beacons) that will use Wi-Fi as the backhaul.

*Coverage requirements* capture the areas of the property that will need Wi-Fi coverage. For guest access, obviously all guest-facing areas in the front-of-house (FoH) need coverage, including guest rooms, lobby, restaurants, pool, exercise room, etc., need to be covered. For hospitality environments that also do a lot of catering / entertainment events in high density areas, such as conference rooms and banquet halls, these areas also need to be explicitly identified, and may have different capacity needs. If the network is also being used by the staff to support operations, then all back-of-house (BoH) areas also need to be covered, including kitchens, offices, loading docks, service areas, etc.

The design will also be different if it is a motel environment (i.e., external room doors) vs. a hotel environment (i.e., internal room doors).

*Capacity requirements* focus on what devices, and in what quantities, are going to be on the network. Unlike other environments, the client device population is literally changing on a daily (nightly) basis, as guests check-in or check-out. Guest rooms will generally have one set of requirements (an average of 2-3 devices per room), whereas conference rooms and other high density areas may have hundreds of devices in a relatively small area. If the network is also being used for back of house, surveillance, IoT, etc., those devices are more fixed in type and quantity, but need to be accounted for.

Unlike requirements, which should be related yet technically independent from each other, constraints are what the network designer needs to work around. Constraints ultimately limit the ability of the network designer to satisfy all of the requirements. *Physical constraints* outline the constraints imposed by the physical property itself. For wireless networking, the biggest physical constraint is the existing (or lack of potential for installing a new) wired infrastructure, and thus will dictate whether the wireless access points are mounted in the rooms vs. in the hallways. It is virtually always desirable to place APs in the guest rooms, so as to have the APs as close as possible to the client devices and to place as much physical structure as possible between APs to minimize co-channel interference. However, many hotels, especially older properties or poorly planned newer properties, often don't have the cabling infrastructure necessary to support this, and thus the APs can only be placed in the hallways, which will compromise coverage in at least some rooms and will increase co-channel interference, meaning that the overall performance of the network will degrade as more client devices use it simultaneously. For multi-building environments, lack of cabling between buildings may also necessitate the use of wireless backhaul links to interconnect different parts of the property.

There are also several common *organizational constraints*, which are imposed by the owner of the hospitality property or its franchiser. Some common constraints in this category are as follows:

- **Budget:** This will often limit the choice of AP vendor or the choices in having an adequate number of APs to satisfy coverage requirements.

- **Aesthetics:** This will generally limit the placement of APs so that they are invisible, and may force the placement of APs in non-optimal or even highly undesirable locations (e.g., above duct work in the ceiling). The impact on aesthetics can be minimized by painting the APs or using skins to disguise the APs.

- **Legacy Systems:** Most hotels don't have the budget to upgrade their entire infrastructure at once, so support for legacy back-of-house systems and legacy IoT client devices may need to be accounted for. This may lead, for instance, to a dedicated SSID that still supports WEP or WPA-TKIP, and prevent disabling of lower data rates.

- **AP Vendor Selection:** Many AP vendors have managed to write themselves into HSIA specifications, meaning that a franchise owner must use APs from that vendor, even if another vendor's product would be more appropriate from a cost and/or functionality standpoint.

- **Service Provider Selection:** Many hotel chains will have a "short list" of approved HSIA service providers, so the franchisee is not free to necessarily pick the best vendor for his particular needs. Ironically, the constraints for using particular service providers often is linked to the constraint to use specific AP vendors, leading to the service providers competing with each other to offer the exact same design.

Wi-Fi is not a commodity, and there is no one-size-fits-all solution for hospitality Wi-Fi. The variation in a particular property's requirements and constraints require having an adaptable solution that can fit various profiles and use cases.

Author: Jason D. Hintersteiner, CWNE #171

## What Can Ekahau Do for Your Organization?

Today, 35% of Fortune 500 companies run their networks with Ekahau Wi-Fi planning and measurements solutions.

We are recognized for delivering the easiest-to-use, most reliable solutions for Wi-Fi planning, site surveys, troubleshooting and optimization.

Our solutions minimize network deployment time and ensure sufficient wireless coverage – across all industries, project sizes, building infrastructures and level of complexity.

Our enterprise tools are ideal for wireless professionals designing and deploying small to large Wi-Fi networks and troubleshooting Wi-Fi issues.

## About Ekahau

Ekahau is the global leader in solutions for enterprise wireless network design and troubleshooting. More than 15,000 customers, including 35% of Fortune 500 companies, run their networks with Ekahau's Wi-Fi planning and measurement solutions. Our software and hardware solutions design and manage superior wireless networks by minimizing network deployment time and ensuring sufficient wireless coverage across all industries, project sizes, building infrastructures and levels of complexity. We are recognized for delivering the easiest-to-use, most reliable solutions for Wi-Fi planning, site surveys, troubleshooting and optimization. Whether a corporate office, hotel, hospital or university – if the Wi-Fi works well, it has likely been built using Ekahau's Wi-Fi Design solutions.

Ekahau is headquartered in Reston, Virginia and has much of its R&D and product related functions in Helsinki, Finland.

**www.ekahau.com**

Schedule a demo today to see the complete Ekahau Wi-Fi toolkit in action.

ekahau
WIRELESS DESIGN