HTNG NEXT GENERATION INFRASTRUCTURE TECHNOLOGY GUIDE

Version 1.0
October 2023

About HTNG

Hospitality Technology Next Generation (HTNG), part of the American Hotel & Lodging Association (AHLA), has a mission to foster, through collaboration and partnership, the development of next-generation systems and solutions that will enable hoteliers and their technology vendors to do business globally in the 21st century. HTNG is recognized as the leading voice of the global hospitality community, articulating the technology requirements of hotel companies of all sizes to the vendor community. HTNG facilitates the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hotels, and create a healthy ecosystem of technology suppliers.

Table of Contents

1. Executive Overview

Everyone agrees the pace of evolving technology is staggering. Devices, applications, mobility, and the insatiable need for speed and ubiquitous service places a great deal of pressure on hotels. Guest devices, operations, and other applications in use today were never contemplated when most hotels were being designed. Similarly, to the age of cars and roads, a car built in the 1940s will not do well on modern interstates, and a new EV with rapid acceleration will not perform so well on a road built before it was imagined. It is simply unreasonable to expect past designs to meet future technology developments. This is the challenge the industry faces today; designing and implementing network infrastructure that contemplates and expects more, faster, and fully integrated connected devices.

The goal of this document is to resolve the problem stated above, providing guidance to the industry stakeholders working toward a simplified network design and infrastructure. Through the convergence of faster networks, hotels can support well-designed, managed, and secure networks that will accept almost any device for applications within industry standards. By adhering to this technology guide, hotels should see a reduction in the total cost of ownership over their network's lifetime while improving overall operational efficiency and security. Additionally, by adopting these ideas, hotels will see reduced required physical space, total costs for construction and ownership, improved operational efficiencies and guest experience, more manageable networks, and unified platforms for securely increased revenues.

2. DOCUMENT INFORMATION

This section provides information concerning the document's history, the scope of this guide, its relationship to other HTNG workgroups and standards, pertinent resources and references, the intended audience, and any known limitations to the document.

2.1 DOCUMENT HISTORY

Version	Date	Author	Comments
1.0	23 October 2023	NGI Team	

2.2 SCOPE

Since many hotel types and categories exist, every scenario would be challenging to cover in one concise document. This guide focuses on Greenfield projects (to new construction) and Brownfield projects (on existing properties) that range in size from limited-service hotels to large, full-service resorts. The following information can also help Brownfield properties that need to refresh their current network to support the latest brand standards and technologies. These existing properties would have to consider a significant technology refresh to converge multiple applications onto a single network, or at least do it in phases. In addition, other new construction projects, such as apartments, student housing, and campgrounds, could also benefit from the information in this document.

2.3 RELATIONSHIP TO OTHER HTNG WORKGROUPS AND STANDARDS

Related standards and specifications use or referred to in this Technology Guide:

Workgroup	Deliverables
Fiber to the Room (FTTR)	• Fiber to the Room Day 2 Support • Fiber vs. Copper Cost Comparison Calculator • Fiber to the Room Design Guide • Fiber Deep Alternative Architectures • Passive Optical LAN Power Options
Cellular/Distributed Antenna Systems (DAS)	• Converged Wireless Using Distributed Antenna Systems (DAS) Technology • Hotel Distributed Antenna System (DAS) Reference Document
Device Control Integration	• Device Messaging Structure
New Builds	• New Builds Design Guide
5G for Hospitality	• 5G FAQ
CBRS for Hospitality	• CBRS for Hospitality
Guest Room Entertainment	• Next Generation Entertainment Systems

Internet of Things (IoT)	• Internet of Things (IoT) Fundamentals
Private Exchange Branch (PBX)	• PBX Requirements and Information

2.4 USEFUL RESOURCES AND REFERENCES

Additional available resources:

1. Implementing Web Services Using HTNG Specifications – A Quick Start Guide for Software Developers
2. HTNG Discussion Board – currently available at http://www2.htng.org/discussion
3. Division 27 & Division 28 Construction Standards
   https://www.csiresources.org/standards/masterformat

2.5 AUDIENCE

This document is aimed to assist hotel owners, developers, low voltage consultants, architects and engineering firms, hotel technology integration companies, and the greater ecosystem involved with designing, deploying, and operating a hotel network.

2.6 KNOWN LIMITATIONS

Limitations of this document:

- This document addresses evolving technologies, however, things change over time.
- This document does not address brand standards.
- This document does not address different building codes in various parts of the country.
- This document is primarily U.S.-centric through it anticipates future global adoption.
- The document is vendor-agnostic and readers are encouraged to collaborate with trusted, experienced partners for research and implementation.

3. BUSINESS CASE/NEW AND EXISTING HOTEL APPLICATION REQUIREMENTS

Hotel networks continue to evolve based on new technology and increases in applications required to support hotel guests and staff. Adding new cables, or replacing old cabling, can be quite intrusive to the day-to-day business of a hotel. It is important to pick the correct type of infrastructure that will support today's network as well as networks in the future.

The "triple play," which includes TV (Guest Room Entertainment), High-Speed Internet/Wi-Fi, and phone services, is the standard requirement. Still, more applications are showing up in guest rooms, guest room floors, and common areas throughout the property. In the past, these three services were separate networks, all on different infrastructures, and often even the organizations responsible for seach service were separate with minimal, if any, cross-department communications. TV solutions were mostly Coax-based and phone networks were traditional 2- or 4-wire analog phone systems wired back to a PBX. Additionally, High-Speed Internet and Wi-Fi ran on separate switched networks.

Today, many new hotel buildings have converged these services by utilizing IPTV, VoIP phone systems, and by placing a Wi-Fi Access Point per guest room. Hotel lobbies, fitness rooms, conference spaces, restaurants, and outdoor event areas are becoming more dynamic, requiring more connectivity applications and bandwidth. Over the past five years, more and more applications inside a hotel are converging onto an IP network, turning hotels essentially into "Smart Buildings."

Wireless demand and the number of devices per person have been increasing and will continue to grow every year. Wireless standards, as well as new technologies, will continue to be updated to support this demand.

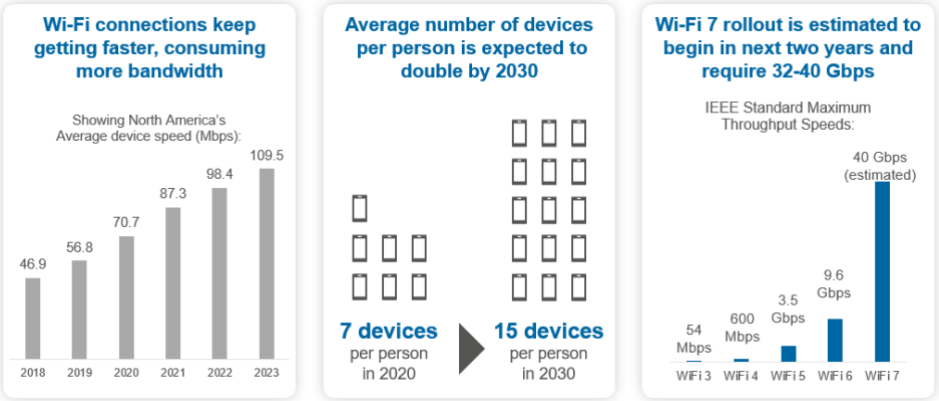


Figure 1

Besides Wi-Fi, other technologies will also continue to place a demand on network infrastructure. These technologies include augmented and virtual reality, 5G, and 6G (plus additional future cellular technologies), Tactile Internet, holographic imaging, and communications.

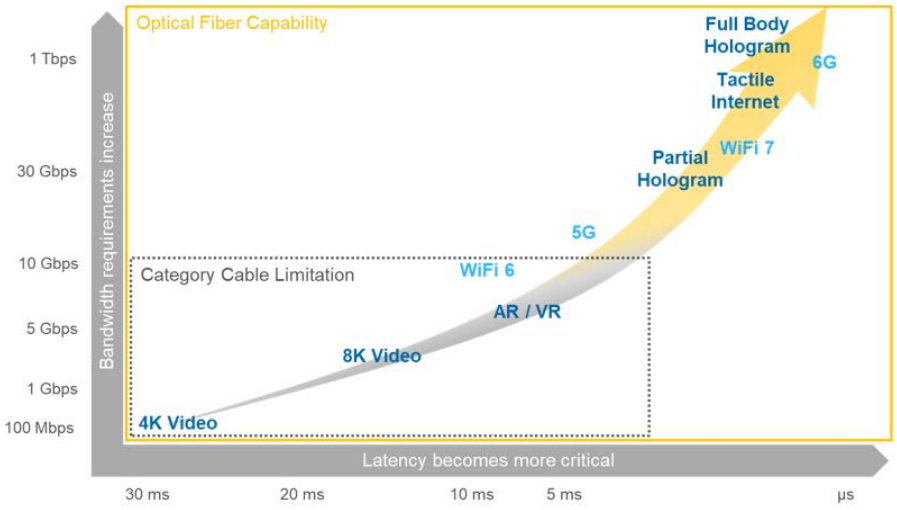


Figure 2

Imagine hotel rooms with the capability to set themes using augmented reality or meeting rooms with full digital walls with teleconferencing capabilities and holographic images. An event space could replay a concert in the same area providing the experience of a live performance. Furthermore, the hardware required for telepresence is getting more economically accessible year after year and has slowly become a staple at major conference events. Implementing these innovations requires a robust wireless network infrastructure to ensure the ever-increasing personal device count can be accommodated in a manner where critical bandwidth is readily available to enhance user experience while still supporting non-client-facing devices in maintaining their Service Legal Agreements (SLAs). Conference areas change daily between customer events and requirements. Can the network infrastructure supporting these areas be disnged in a way to simplify customer needs from one event to another in a timely matter?

Building Management Systems (BMS) and environmental controls can increase a hotel's efficiency and save a property money by keeping HVAC systems and lighting utilized when needed and reduced when not needed. These solutions make an impact in the short term and then become smarter over time as they collect more data points. To assist, sensors can be installed for early detection of water leakage before a problem arises. Location-based services can track employees and hotel assets to improve response time based on the origin point of request. Occupancy and key systems work harmoniously with Property Management Systems (PMS) to help staff stay efficient, providing housekeeping management with optimal cleaning routes and insights on the most effective teams. Additional applications will continue to be discussed throughout this guide.

While we tend to think about multiple applications being managed over one network and infrastructure, we should also consider what it takes to power these devices. Cabling infrastructure, often referred to as low-voltage cabling, can address how these applications are powered.

A converged network design should consider powering applications in the hotel guestroom, Back of House (BoH), admin areas, and hallways. Utilization of Power over Ethernet (PoE) is the most common method to power these different applications. PoE provides DC power to things such as Wi-Fi Access Points, VoIP phones, security cameras, Zigbee controllers, environmental controllers, etc. The amount of PoE these devices require can vary wildly, so the total PoE budget provided by a PoE switch, media converter, Optical Network Terminal (ONT), or Software Defined Access Node (SDAN) must be factored in.

Whether a new hotel is being built or an existing hotel is being updated to the latest technology, decisions need to be made on the most efficient way to build a robust network to support the application requirements of today, but also to be ready for the future.

3.1 THE BENEFITS OF CONVERGENCE

Converging these applications onto one network has benefits to the hotel management company as well as the guest. If you are designing a new hotel from the ground up (e.g. Greenfield), you have an advantage to design a converged network that connects multiple, if not all, applications on the property.

If your property already exists and you are updating technologies and your network (e.g. Brownfield), the decision needs to be made upon how many of the applications will ride on the new converged network. The advantages of converged networks can be shown in different ways:

- **Centralized management:** Essentially one network management system can monitor all applications converged onto a single network. This network would be centralized using an IP-based network and would monitor each application down to the port level (including down to the room), receiving alarms specific to different troubles that potentially arise. Note that the team managing this network should be able to keep the network stable and work with any application manufacturer on new hardware/software updates.
- **Ease of tech updates:** Software and system updates can be pushed to the entire network from a central location, providing the latest enhancements and patches as needed. This could be done in a phased approach as well depending on the property requirements.
- **Bandwidth designed for both today and the future:** Guests staying in hotels expect the Wi-Fi to be fast and the guest room entertainment (TV/streaming) to be seamless, giving them similar at-home experiences. Bandwidth on a converged network can be designed to handle the needs of the hotel today but the industry also needs to be ready for what may come years from now.
- **Less refresh on infrastructure:** If designed correctly, the network infrastructure installed can last for over 20 years. It is possible the active components may need an update at some point to meet the latest tech requirements, but the infrastructure could also remain as is. This would save time and is less impactful to the day-to-day business of the property.
- **Less space:** Converged networks typically are a space saver inside a hotel. IDF (i.e. TRs) closet space can be a premium to allocate and build out. If you can reduce these closets, that space and cost can be returned to the owner for other uses. In existing properties, pathways to rooms can be a challenge. Pulling multiple drops (category cables) into a room can be difficult based on existing conduits filled with old existing cables. So, running multiple applications over one cable, for example a hybrid fiber/copper cable, can ease this cabling upgrade.
- **Conduit, core drill, cable tray size reduction:** A converged infrastructure reduces the number of cables required to connect the associated devices. Fewer cables, and, in many cases, smaller cables, reduce the size of the cable trays or may even eliminate them altogether. The reduced size for the cables also reduces the size of conduit and thus the size and/or number of core drilled pathways.
- **Wireless solutions run multiple applications:** Hotel technology is taking advantage of different wireless technologies to connect applications throughout the property. These solutions enable guest Wi-Fi, asset tracking, staff communications, building management controls, mobile key, and many other applications.
- **Carbon footprint reduction:** These days “Going Green” or designing buildings that are more sustainable and efficient has become more important than ever. Converged networks over less cabling infrastructure automatically reduces the carbon footprint. The more applications running over one cable, the more the carbon footprint is reduced. A reduction from three to one cable per room is a common example, but this is more relevant for hotels that require more technology demand per room or may need greater connectivity throughout larger suites.
- **Security policy:** When converging a network, it is important to secure the users, devices, and services that run on the network. This helps keep the network highly available and gives the ability to perform properly while helping secure guest and operational data. For every user and device on the network, a security policy is assigned to limit what they can do within their role on the network. Security policies can identify network segmentation, services available, as well as what other users and devices that can be communicated with. By doing this, guest network services can co-exist with back office and IoT services on the same physical network infrastructure.

Now that we understand some benefits of a converged network, it is important to walk through the decision process of identifying the property type and what applications will be installed on-site.

3.2 PROPERTY TYPES

Identifying your property type is an important step when determining what type of network will be designed. View the options below to see what category your hotel falls into:

- **Limited-Service Hotel:** A property that offers limited facilities and amenities, typically without a full-service restaurant; these hotels are often in the Economy, Midscale, or Upper Midscale class.
- **Standard Branded High-Rise Hotel:** A property that is typically Upscale or Luxury with a wide variety of onsite amenities (e.g. restaurants, meeting spaces, exercise rooms, or spas).
- **Luxury Branded High-Rise Hotel**: An upscale property with high-end amenities and technologies.
- **Luxury Mixed – Uses High-Rise Hotels and Residences:** An upscale property with high-end amenities and technologies; a portion of the property also has permanent residences that may be managed by the same network management company.
- **Small Boutique Hotel (no Brand):** The size and amenities for these properties vary based on locations; buildings may possibly be older or have a unique layout.
- **Historic Hotels or Buildings:** Similar to Boutique-style hotels, size and amenities for these properties vary based on location; building types may have unique pathways or limited space for IT equipment (aesthetics in these properties are typically a high priority).
- **Resort Style:** These properties have a spread-out campus with individual cottages/rooms.

The following property types may also fall under similar technology guidelines:

- Luxury Residential Condo
- Basic Residential Apartment MDU and Student Housing
- Dormitory/Hostel
- Campgrounds and RV Parks

These property types may capture a new project or an existing property. Network decisions will change based on which scenario is chosen below.

3.3 GREENFIELD OR BROWNFIELD SCENARIOS

3.3.1 Greenfield

Greenfield properties are new build properties that need to go through the entire design process. This is an excellent opportunity to design a network that supports convergence. Identifying the property type, MDF, IDF locations/counts, pathways, room types, and associated applications with POE requirements are some important considerations. In addition, be certain to identify any other areas of the property that will include converged applications in scope. These may include back of house (BOH), admin locations, conference and meeting spaces, public areas, parking decks, etc.
Some brands have specific technical design guidelines that are required for networking and applications. It is important to follow these to avoid rework.
To approach a Greenfield converged design for rooms, start with answering the following questions:

- What are the room types?
- What applications will be utilized in the rooms and what are the counts? Where are the ports located?
- What are the POE requirements for the applications per room?
- Where are the IDF closets located in relation to the rooms? Can the IDF counts be reduced based on the type of converged design utilized? (If fiber to the room is used, it is typical that the total IDF count can be reduced up to 50%.)
- What hallway applications and associated POE requirements are needed per floor?

Non-Guest Room Floors/Areas

- What are the plans for the non-guest room floors?
  - IDF locations
  - Applications
  - Cabling requirements
  - Port locations and quantities

3.3.2 Brownfield

Designing networks for a Brownfield (existing property) scenario can bring up different challenges to add the latest technologies to the rooms. Some reasons existing properties need a tech refresh may include:

- Rebranding (for repositioning)
- Conversions (i.e. an office building or a historic building to hotel)
- Refresh of existing property
  - Technology refresh
  - Full or partial property renovation

Some of the same questions still apply for the network design as Greenfield scenarios. In addition, these things need to be considered:

- Where will the new applications be installed in the rooms in relation to the ports or switching devices connecting to these applications?
- Are there applications that will be updated in the near future?
- What are the pathways like from the rooms to the nearest IDF (TR) closet? Do they exist?
- Are the ceilings in the hallways hard ceilings or drop ceilings?
- Are there existing cables in the same pathways that need to be removed or re-used?
- Is there a need for new cabling in the riser pathways? Is there room in these pathways?
- If there is a need for new racked equipment in the MDF and IDFs, is there space available for this equipment?

4. TYPICAL CURRENT HOTEL NETWORK DESCRIPTION

This section contains a high-level description of a typical hotel network. It is important to remember that network standards have been established for some hotel brands. However, since many of their hotels are franchise-managed, franchise owners often choose to only partially follow the standards. Therefore, the information presented in this document will describe the typical network design of many franchise-managed hotels.

4.1 TYPICAL NETWORK DESIGN

Before the demand for high-speed Internet in hotel for hotel associates and guest, there was no need for a converged network. On average, a hotel was able to operate on a small IP subnet (e.g. 254 IP addresses, and a single T1. Guests would typically access email pre-Internet services via a telephone line connected to a modem. In addition, guests did not access streaming services, but requested local TV channels and HBO. Finally, unlike the ability of a guest to easily upgrade devices and Internet speeds in their homes, hotels cannot easily upgrade their infrastructure due to costs and loss of revenue due to the closing of floors to upgrade the network infrastructure (cabling, switching, and Wi-Fi).

Therefore, many hotels continue to utilize flat networks that do not support convergence, bandwidth management, increased security, and limited IP addressing capacity. Many hotels continue to delay the migration to a converged network due to the network outages required to perform a conversion and the cost. However, the need to support increased dependency on the Internet by associates and guests and the frequent changes in the Wi-Fi standard is forcing hotels to consider the need to deploy a converged network architecture.

4.2 BANDWIDTH

Hotels continue to have an issue of keeping up with bandwidth demands of both associate applications and guests' ongoing use of streaming and Internet access. Currently, guests expect to have the same Internet experience at a hotel as they experience at their homes. This has proven to be a challenge for hotels since, unlike a guest at home, the hotel must satisfy many guests simultaneously. Although the cost of higher-speed Internet continues to decrease overall, the current network infrastructure in the hotel may not be able to take advantage of the higher WAN speeds. Finally, many hotels do not have the bandwidth management equipment required to manage bandwidth capping or redeploy unused bandwidth to other users who could take advantage of the extra bandwidth.

Lastly, many hotel owners budget for a known monthly bandwidth fee and thus are unwilling to take advantage of services like burstable bandwidth, which could help when the current purchased bandwidth is exceeded. Hotels are encouraged to look at bandwidth management tools that can effectively bifurcate and dedicate throughput for specific uses. For example, two separate circuits can be sourced and combined into a single service with redundancy. This is referred to as aggregating or bonding circuits. This bonded circuit can then take advantage of management tools to maintain accessibility to network applications and prevent traffic congestion and other potential threats. These tools can allocate dedicated service for back office, conference rooms, and guest rooms with improved services over simple rate limiting. With a common network infrastructure, managing bandwidth becomes easier and more critical.

Therefore, the deployment of a converged network architecture allows a hotel to more effectively manage the bandwidth that is being deployed for both associates and guests.

4.3 SECURITY

As noted above, in the past, security was less of a priority than it is today. Due to PCI requirements for protecting credit card transactions and laws requiring the protection of guests' personal information, hotels must deploy better security infrastructure. As mentioned in the above bandwidth section, deploying a converged network infrastructure would allow a hotel to satisfy current and future security requirements better.

5. HOTEL APPLICATIONS REQUIRING NETWORK CONNECTIVITY

Figure 3 contains a high-level summary of the types of applications and network types required to satisfy current and future hotel guest and hotel staff requirements.

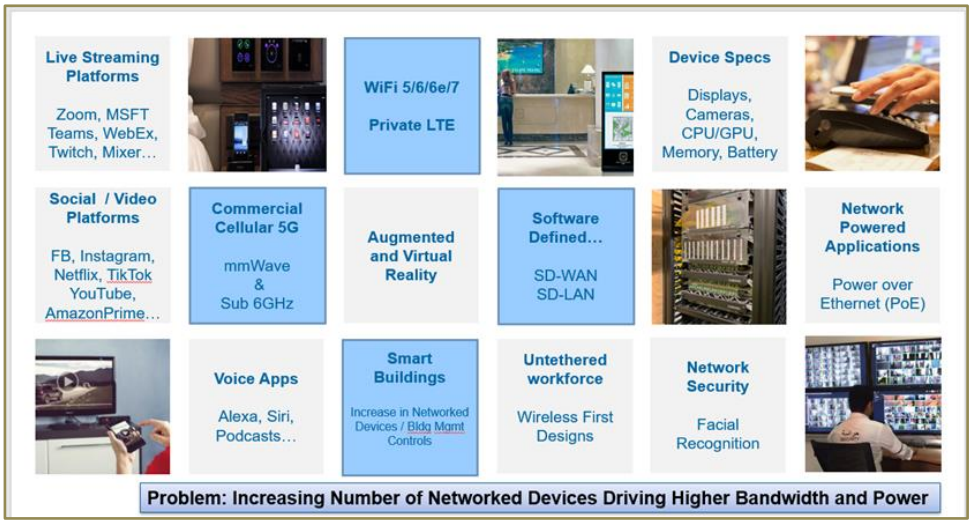


Figure 3

In addition, as hotels migrate to a Smart Building Networking model, the need for a converged network becomes more of a necessity. As shown in Figure 4 below, satisfying the three pillars outlines in the table will require a robust converged network that can be easily configured to support current and future hotel requirements.

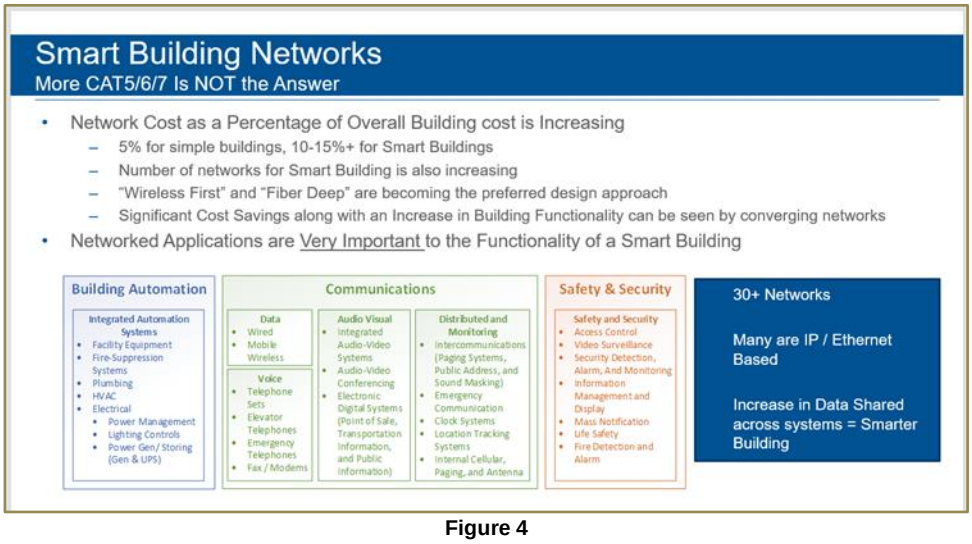
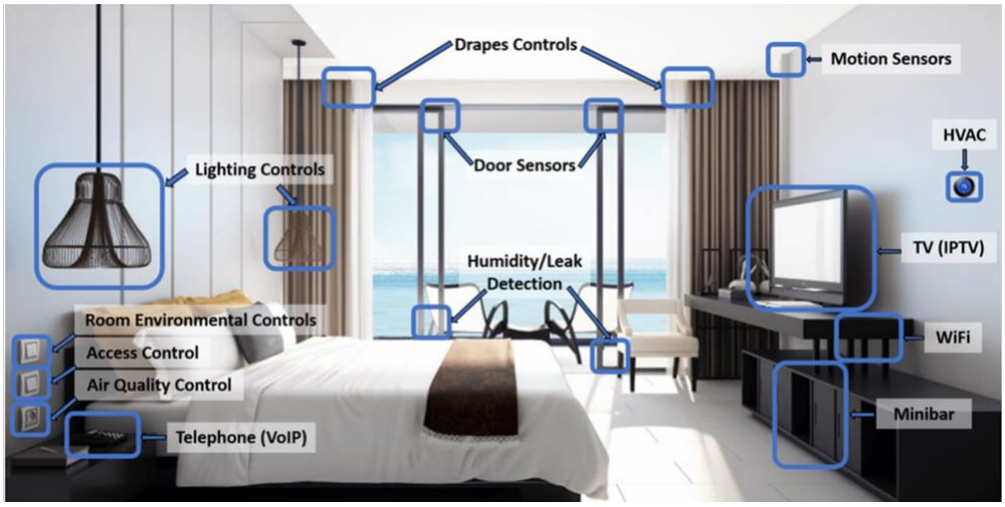


Figure 4

5.1 POTENTIAL HOTEL GUEST ROOM NETWORKING REQUIREMENTS

As noted in the picture below, hotel guest rooms are being configured to support several guest-facing applications that require robust cabling and wireless infrastructure. For example, the guest room shown below has many IoT applications and guest streaming functionality to the guest's device and/or TV.
Each of these applications may need similar or different network protocols but still require a robust network infrastructure to support all network protocols. In addition, deploying some or all the applications and

functionality shown in the following picture could potentially reduce costs using automation and a single vendor support model.



Questions to consider:

- How will these technologies converge with thee existing technologies? For example, could you forego DAS if you could use a CBRS or 5G network?
- Carrier requirements may change when allowing hotels to connect to private networks, so how can the hotelier be more “future-read” for these changes?
- What other questions can hoteliers ask?

Networking as a utility has been a long-term goal. An electrical outlet (with considerations for Amps and Voltage) functions securely and safely regardless of the appliance, which is the same goal of the converged network infrastructure. With considerations for some technical requirements, a converged network can support any IP-enabled devices and multiple wireless protocols. With proper management, security protocols, and planning, a client device and application can be added without pulling additional wires, opening walls, or adding network capacity.

For a more extensive list of potential applications, see Appendix section 14.3.

6.STRUCTURED CABLE SYSTEM OPTIONS

Now that you have considered the type and size of your property, you have also identified the number and types of applications required inside your hotel. Whether building a new hotel from the ground up or updating technology inside an existing property, it is important to understand the media type options available to complete a network design. Multiple cabling and networking options are available to connect through room-based and BOH applications. The following sections will describe these different options. Your final solution may require one or more of these choices below to complete a full design.

6.1 COPPER CATEGORY CABLE (TWISTER PAIR)

Bell invented twisted-pair cabling to connect telephone systems. As telecommunication systems evolved into computer network systems (like Ethernet), so did the twisted-pair cabling. Higher data speeds require unique requirements of twisted-pair cabling, which is why we have category cabling. Standards for category cabling contain many requirements. All of these requirements dictate the ability of the category cabling to support the frequency bandwidth and data speed, translating into an overall allowable distance between network equipment and devices.

Newer technology enables copper cabling to operate beyond the 1 Gbps original design, based on the NBASE-T 802.3bz standard commonly called “Multigigabit.” This recent technology enables specific cables to operate at 2.5 Gbps, 5 Gbps, 10 Gbps, or 25+ Gbps and higher. This is now commonly supported in higher-performing devices, such as Wi-Fi access points that can manage client traffic that exceeds the traditional 1 Gbps limitation.

Now, many of those cables can communicate at these new higher speeds to accommodate the new level of network traffic without needing multiple 1 Gbps cables to support the same level of network traffic.

	Length meters	10 Mbps	100 Mbps	1 Gbps	2.5 Gbps	5 Gbps	10 Gbps	25+ Gbps	Bandwidth MHz
Cat 3	100	Yes							16
Cat 5e	100	Yes	Yes	Yes	Limited	Limited			100
Cat 6	100	Yes	Yes	Yes	Limited	Limited	Limited		250
Cat 6A	100	Yes	Yes	Yes	Yes	Yes	Yes		500
Cat 7	100	Yes	Yes	Yes	Yes	Yes	Yes		600
Cat 7A	100	Yes	Yes	Yes	Yes	Yes	Yes		1000
Cat 8	30	Yes	Yes	Yes	Yes	Yes	Yes	Yes	2000

Table 1

The reason for the limitations of some categories of cabling is because of the introduction of new applications and the desire to reuse installed cabling. The dominant factor causing the limitation is the introduction of unpredictable noise from the higher frequency bandwidth, referred to as alien crosstalk. To mitigate alien crosstalk, one must ensure that the cables are not bundled together to enable Cat 5e and Cat 6 to support 2.5 Gbps and 5 Gbps or reduce the distance between equipment and devices for Cat 6 to 37m.

6.2 BEYOND CATEGORY 6A

Category 6A cables operate up to 500 MHz and easily support today’s 10GBASE-T applications (with Ethernet speeds of 10 Gb/s, a bandwidth of only 400 MHz is needed for 10GBASE-T). The 500 MHz limit of Category 6A cables includes a 20% guard band required by equipment manufacturers.

In parts of Europe where shielded cabling is the standard to support EMC regulations, Category 7 and 7A cabling have been specified with the idea that this would be needed for future applications. The reality is that there are no technology applications that require them, and it only adds unnecessary costs.

Category 8 was developed for data center applications which require a higher bandwidth of 2000 MHz resulting in a reach of only 30 m for 25GBASE-T and 40GBASE-T. But this reach limitation, combined with a large OD, makes Category 8 cable challenging to use—and an upgrade path from 100 m Category 6A to 30 m Category 8 doesn't exist.

In addition, to connect Category 7, 7A, or 8 cables to your network, you'll likely use RJ45 Category 6A connectors. While Category 7 connectors exist (non-split-pair connectors, such as ARJ45), today's equipment (routers, switches, servers, etc.) isn't designed to support this type of connectivity.

When you use Category 6A connectors, you turn a Category 7, 7A, or 8 system into a Category 6A system—and you must measure and test it as such. When lower Category components connect to higher Category components, the system drops to the performance level of the lowest Category used within the system. For example, if you deploy a Category 7 cable using Category 6A components, then you have a Category 6A system—not a Category 7 system.

When selecting the proper cabling to install, consider the data throughput (bandwidth) needed for the supported application and the required reach from the communication room to the end device.

The required bandwidth for video applications can vary significantly by the compression and codec used. The highest bandwidth occurs for uncompressed video and dramatically reduces when compression is introduced. Typical data speeds for video, digital signage, and IP camera applications are given in the following table (compressed codecs using 4:4:4 chroma subsampling, 30 fps, and 8b color depth). Reduction to chroma subsampling, frames per second, or color depth will further reduce the required bandwidth.

Codec	Length meters	10 Mbps	100 Mbps	1 Gbps
Resolution		Required Bandwidth	Required Bandwidth	
720 p	829 Mbps	1.9 Mbps	1.3 Mbps	11.1 Mbps
1080 p	18.66 Mbps	4.3 Mbps	3 Mbps	25.1 Mbps
4K	7465 Mbps	17.3 Mbps	12.1 Mbps	100.2 Mbps

Table 2

The Wi-Fi Alliance gives Wireless Access Point technology the Wi-Fi name. Each name corresponds to the supporting IEEE802.11 technology. The cabling connecting the WAP to the network should be selected to support the technology's maximum backhaul (throughput). The cabling maximum distance for each Wi-Fi type is provided in Table 3. Note that extra cable drops of Cat 6A are needed to fully realize the potential of Wi-Fi 7. Future WAP technologies will likely have a greater backhaul (throughput), making category cabling less practical beyond Wi-Fi 7.

Wi-Fi Type	Max Back Haul	Max Distance						
		Cat5e	Cat 6	Cat 6A	OM3	OM4	OM5	OS2
WiFi 4	**54-600 Mbps**	100 m	100 m	100 m	300 m	300 m	300 m	10 km
WiFi 5	**7 Gbps**		100 m	100 m	300 m	300 m	300 m	10 km

WiFi 6	**10 Gbps**		37 m	100 m	300 m	300 m	300 m	10 km
WiFi 6E	**10 Gbps**			100 m	300 m	300 m	300 m	10 km
WiFi 7	**30 Gbps**			100 m (3 drops)	100 m	150 m	150 m	10 km

Table 3

Power delivery over data cables, or Power over Ethernet (PoE), is designed for use with all category cabling (Cat 5e through Cat 8); for locations that heavily use PoE, the bundle size of the category cabling must be considered. Since the maximum bundle size will vary by power level and gauge size, a recommendation from the cabling manufacturer is needed. Note that 28 AWG cable is not recommended for higher PoE++ power.

PoE Standard	PSE Type	PSE Max Power	PD Max Power	Required Category Cable Conductor Size
PoE	**Type 1**	15.4 W	12.95 W	22-28 AWG
PoE+	**Type 2**	30 W	25.5 W	22-28 AWG
PoE++	**Type 3**	60 W	51 W	22-26 AWG
PoE++	**Type 4**	90 W	71.3 W	22-26 WG

Table 4

6.3 FIBER OPTIC CABLING

Optical fiber has been around since the 1970s connecting countries, cities, campuses, and buildings with high-speed data connections. A single stand of optical fiber close to the length of a human hair is 50,000 times faster than a Cat5 cable and can potentially support 10,000 simultaneous HD video streams. It has a tensile strength 3x stronger than steel and 6x stronger than titanium. There is well over 1 billion km of fiber delivered worldwide, and it is a common part of hotel network infrastructures today. From small boutique hotels to large sprawling resort-style hotels, optical fiber connects guests today. From small boutique hotels to large sprawling resort-style hotels, optical fiber connects guests and staff to wireless data networks, guest room entertainment, and other communication services.

Fiber optics is a medium that allows light to travel long distances between two points, see Figure 5.

Figure 5

The light that is transmitted from the lasers on each side travels within the core. Construction of the fiber is designed with cladding around the core to keep light inside and attenuation low, see Figure 6.

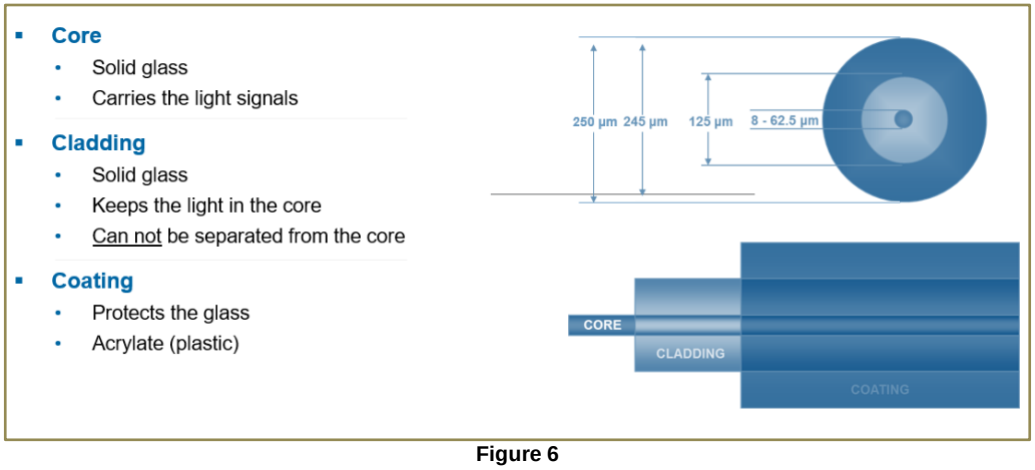


Figure 6

Two main types of optical fiber are used in data and LAN networks: Multi-Mode Fiber (MMF) and Single-Mode Fiber (SMF). Multi-Mode Fiber has four main grades ranging from OM1 (Optical Multimode1) to OM4. There is also a more recent OM5 grade as well. OM1 is older and has a different core size (62.5 microns) than OM2-OM4 (50 microns). Single Mode Fiber, OS2, has a core size of 8-9 microns which allows for less attenuation and can carry more data over longer distances than MMF, see Figure 7.

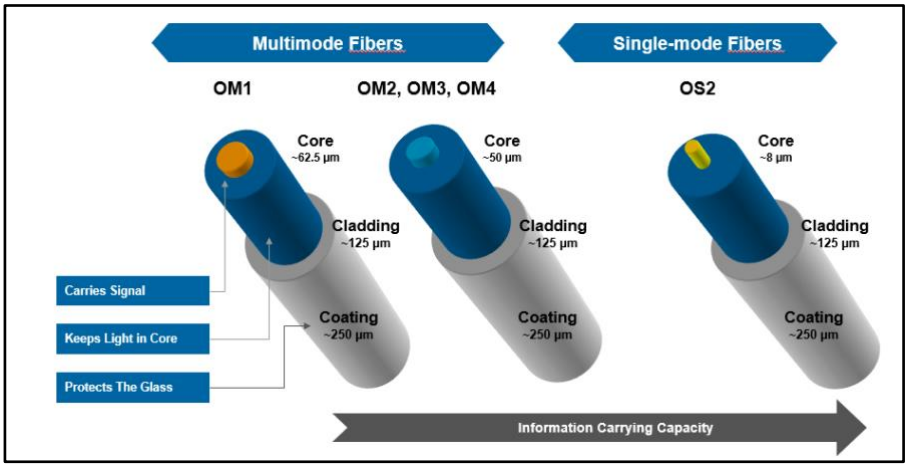


Figure 7

OM4 has been a prevalent optical fiber type used in building LAN infrastructures over recent years connecting switches with 10G and 1G optics in TR closets. From there, it has been traditional copper category cabling to the rooms. Multimode fiber has been used in many cases because distances in many buildings supporting 1G networks up to ~275m for OM1 and ~1100m for OM4. For 10G connections, OM1 can support up to ~33m, and OM4 supports 10G up to ~400m. As you can see, the older OM1 (typically orange jacket) is becoming more limited, whereas the newer OM4/5 supports higher bandwidth at longer distances. Multimode fiber has also been used more often in the past because the transceivers have been more affordable than the Single Mode versions.

As mentioned above, Single Mode (OS2) fiber is highly versatile, supporting 1G, 10G, 40G, and 100G+ connections at distances measured in km vs m. Single Mode fiber is used today in many hotel networks in both the riser and fiber to the room (FTTR) solutions. It is used on Passive Optical Networking (PON) and Active Ethernet designs in smaller hotels to large sprawling resorts. For most new hotel builds and networking upgrades in existing properties, the Single Mode (OS2) option is preferred since it can handle all of the bandwidth needs of today and the future without worrying about longer distances, see Figure 8 comparing Single Mode versus Multimode fiber.

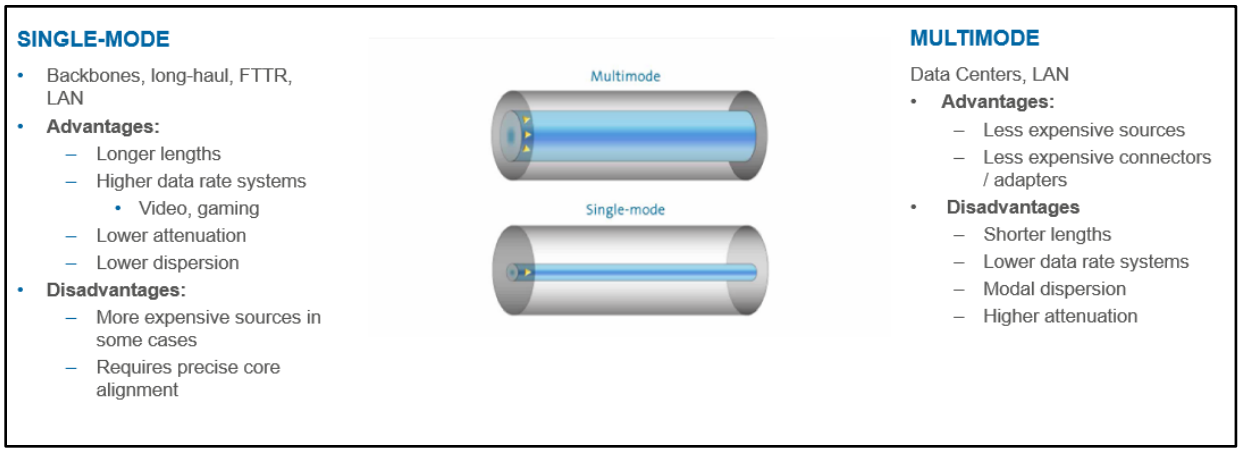


Figure 8

6.4 HYBRID FIBER

Hybrid fiber contains Single Mode fiber and copper conductors in the same jacket and can come in many configurations and jacket types depending on the project requirement. For the guest room, a typical configuration is 2 single-mode fiber/2 copper conductors under one plenum jacket. There are indoor/outdoor rated jackets and armored options for outdoor scenarios. The fiber and copper counts can be increased if needed in specific scenarios. In addition, the copper gauge (AWG), the thickness of the conductor, can very (20AWG – 12AWG are common options). The AWG is typically chosen based on the maximum power draw in the guest room or zone and the maximum distance from the remote power source. Usually, larger hotels will see a max length of 500' or more. There are scenarios where the max distance can reach 2000' or more outdoors. See the examples of hybrid fiber in Figure 9.

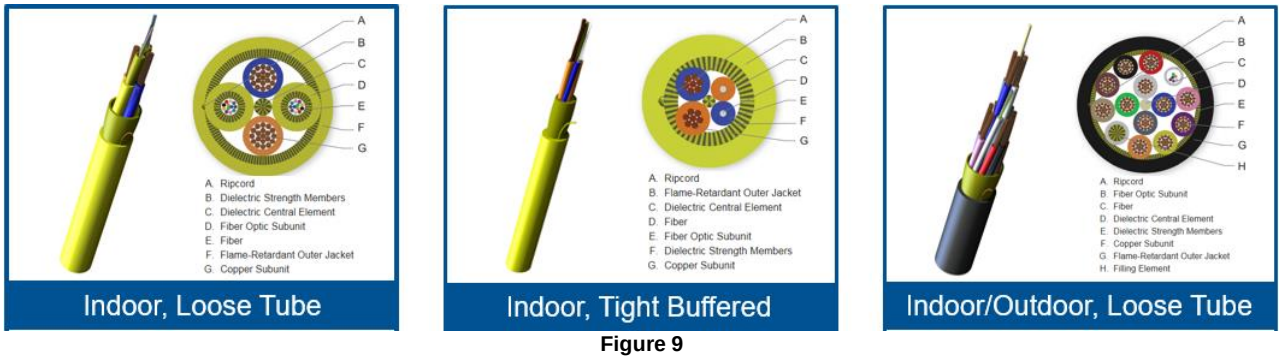


Figure 9

Multiple devices can be connected to hybrid fiber. It is important to understand the inputs for both the media connection and the power inputs. Does the device have an onboard SFP (Small Form-factor Pluggable) cage? What optics and bandwidth does the device support: SFP (1Gb), or SFP+ (10Gb)? Some devices, like ONTs, have embedded SFPs on the device. Common types of endpoints that can receive a hybrid fiber connection include:

- ONT/ONU (Optical Network Terminal/Optical Network Unit)
- SDAN (Software Defined Access Node)
- Fiber Media Converters
- Micro Switches
- Certain Access Points (APs) including future Wi-Fi 7 APs
- 5G Small Cells
- Certain DAS (Distributed Antenna Systems) Remotes
- Certain Surveillance Systems

Designing a converged network using Fiber to the Room or Zone methodology for a hotel property can be done to support many applications. For more details on fiber designs in hospitality, visit the AHLA – HTNG Technical Specifications page or refer to Section 2.4 for links to HTNG's Fiber to the Room technology documents.

6.5 COAXIAL CABLING

Coaxial cable has been used for decades to provide point-to-point or point-to-multipoint radio and video communications. Radio communications generally require higher power over shorter distances, resulting in the predominant use of 50Ω coaxial cable. Video communications generally require lower power over longer distances, resulting in the predominant use of 75Ω coaxial cable.

CATV systems began as an alternative to over-the-air broadcasts, requiring only one-way communication over 75Ω coaxial cable. CATV systems evolved to deliver different content to different customers using technologies providing two-way communication over this same cable. In introductory technologies, communication from the end devices to the provider originally was low bandwidth communication requesting content. Present technologies offer video content and Ethernet over Coax (EoC), such as G.hn, DOCSIS, and MoCA, requiring full-duplex communication.

The changes in technologies have increased the required RF bandwidth of the cable plant. The existing 75Ω coaxial cable, installed to support CATV systems, now must support an RF bandwidth double or triple its originally intended use. This can be done provided the existing cabling plant meets specific criteria. This paper provides general guidance on using existing cabling to support EoC.

6.5.1 Common 75Ω Coaxial Cable Types

Standardization of Coaz cabling initially was under Mi-Specs. The Mil-Spec for Coax began with 'RG' (Radio Guide) followed by an arbitrary number. The Mil-Spec standard is obsolete, but the naming convention has remained. The Society of Cable Telecommunication Engineers (SCTE) realized the importance of an industry standard for numerous reasons. The primary reason is the proper cable to 'F' connector fitting interface ANSI/SCTE 74 2011, Specification for Braided 75Ω Flexible RF Coaxial Drop Cable is the standard that took the universal 'RG' type and standardized it as a 'Series' type.

The dominating characteristics typically include inner conductor diameter and shielding requirements to support the latest video and EoC technologies.

The inner conductor shall be a solid wire that is constructed of copper or copper-clad steel. The dimensions shall meet the requirements of Table 5. Note that the inner conductor tolerances are ±1%.

		Inner Conductor		
Coax Type	Primary Use	Diameter, in	Diameter, mm	AWG
RG59 / Series 59	Video, TV, Headend	0.032	0.81	20
RG6 / Series 6	Video, TV	0.040	1.02	18
RG11 / Series 11	Customer drops, long runs	0.064	1.63	14

Table 5: Inner Conductor Requirements

The outer layers serve as the outer conductor and shield. The first layer of the outer conductor/shield should be a laminated foil bonded to the dielectric, with the foil then being covered with braid wire. The braid wire coverage should be at a minimum of 60%. Additional shield constructions using Tri-shield or Quad-shield are also commonly used in applications requiring greater isolation or installation in noisy environments. The structure of suitable cable constructions is shown in Figure 10.

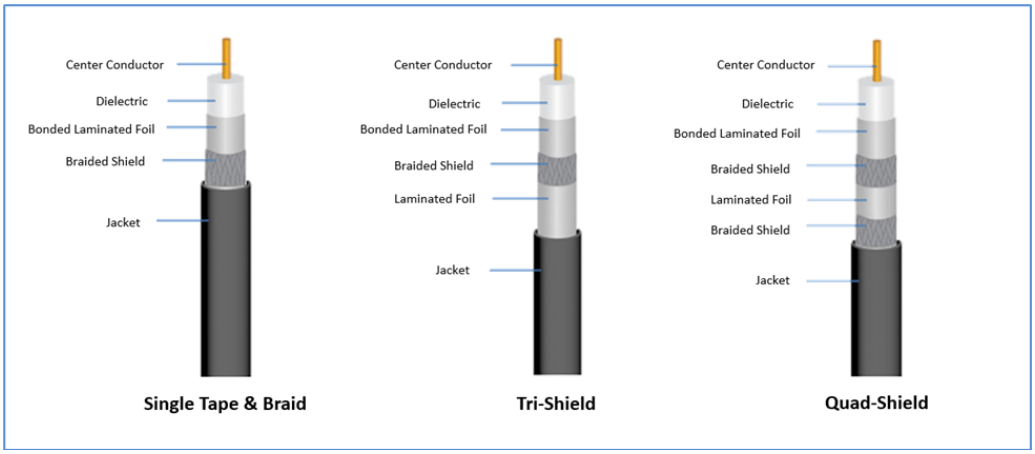


Figure 10: Suitable Cable Constructions for EoC Applications

6.5.2 'F' Type Connectors

'F' type male connectors are standardized as Feed-Through connectors per ANSI/SCTE 123, or Pin-Type per ANSI/SCTE 124 – see Figure 11. The electrical requirements for both types call for an impedance of 75Ω, a frequency range of 5 MHz, and shielding performance levels of an unspliced section of the same cable.

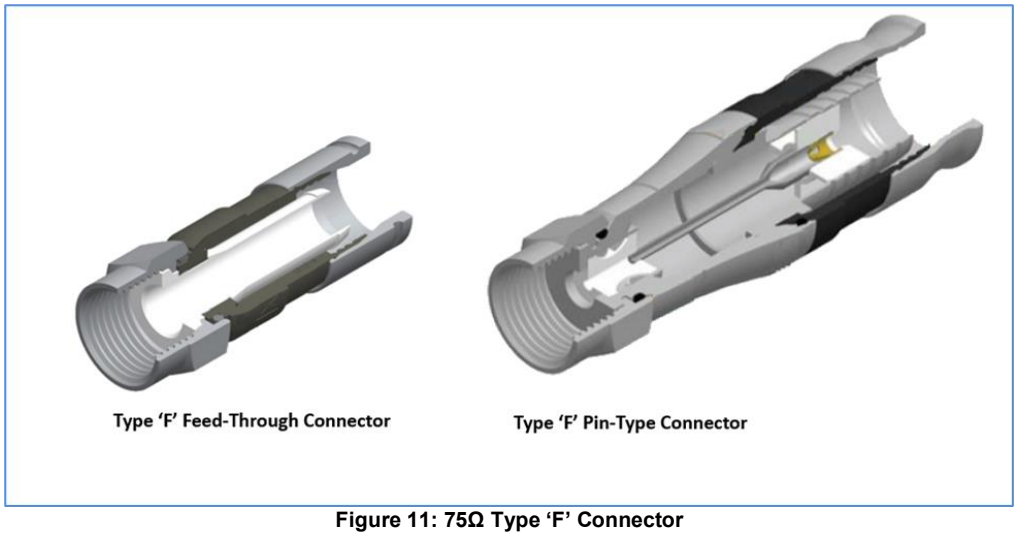


Figure 11: 75Ω Type 'F' Connector

The Feed-Through connector allows for an inner conductor diameter, as shown in Table 6. Only cables with an inner conductor gauge size of 18 AWG and 20 AWG can use Feed-Through connectors. Cables with other gauge sizes must use Pin-Type connectors.

	Diameter, in		Diameter, mm	
	Min	Max	Min	Max
Inner Conductor Diameter	0.025	0.042	0.64	1.07

Table 6: Male 'F" Feed-Through Dimension

6.5.3 Typical EoC Cable Plant

Ethernet over Coax technologies have roots in CATV systems. Initial systems only needed to work up to

around 850MHz; but, as the need for additional data services rose, other technologies (such DOCSIS, MoCA, G.hn, etc.) overlayed the data services utilizing different spectrum ranges, ranging from 5-200 MHz for G.hn to 1 GHz or higher for DOCSIS and MoCA. Additional devices were added at the end of the Coax lines to provide CATV services and data connection to in-room Ethernet, see Figure 12.

When conducting coaxial cables within a building, placing them in air ducts or passageways sometimes makes sense. According to Article 800 of the National Electrical Code, plenum cables must be used in these cases. This code states that plenum cable should ALWAYS be used in plenum airspaces and air ducts to slow the spread of flames and reduce smoke and toxic fumes from circulating throughout the building.

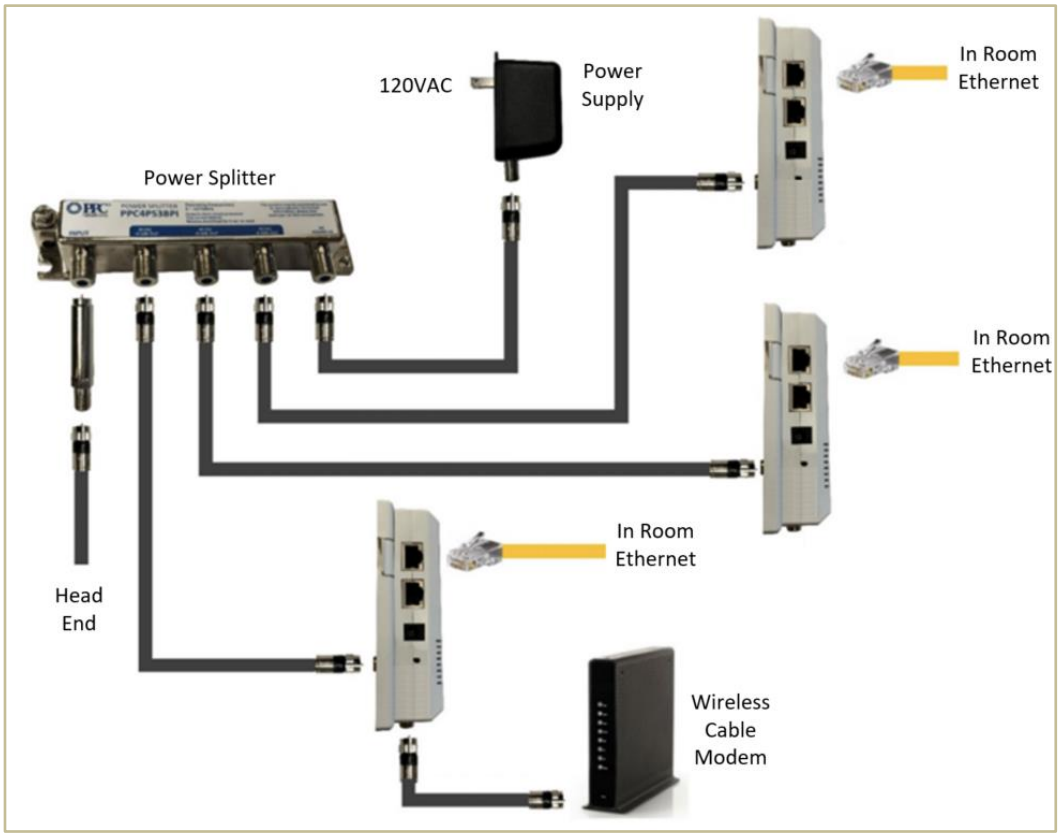


Figure 12: Typical Modification to CATV system to include data services

The cable plant's bandwidth will vary depending on the complexity (number of services and nodes) within a given installation. Please refer to Section 6.6.3 for an overview of DOCSIS, G.hn, and MoCA.

6.5.4 Recommendations

The existing cable plant must be inspected for acceptable use in upgrades for Ethernet over Coax applications. Acceptable coaxial cable, see Figure 13, shall be 75Ω with a foil shield that is bonded to the dielectric and has a fine braid shield with at least 60% coverage.

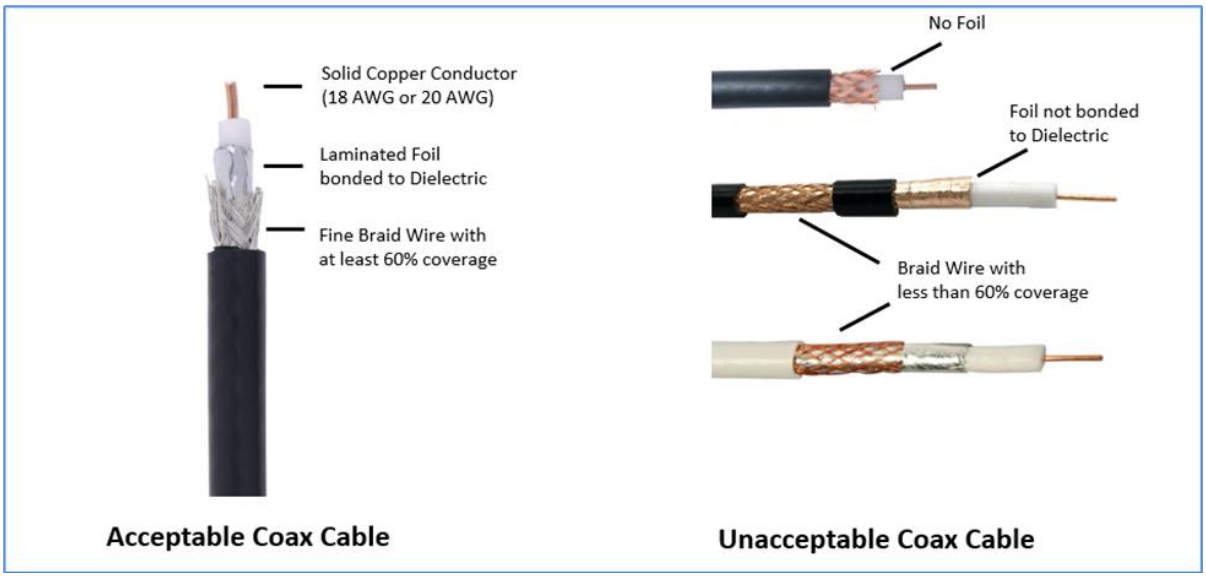


Figure 13: Cable Plant Coax

To best achieve the shielding requirements, 'F' type connectors shall have compression-type mating to the cable. Compression connectors offer superior RF shielding, both for ingress and egress, when compared to hexagonal crimped connectors due to the 360 degrees of contact between the rear of the connector and the cable braid/foil screen, see Figure 14.

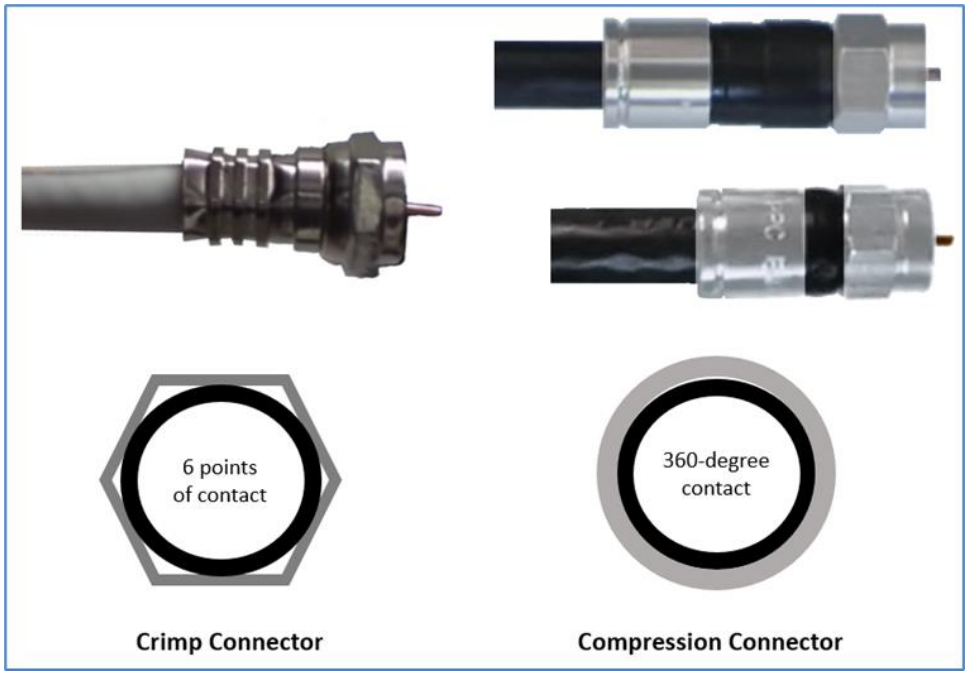


Figure 14: Connector Termination Methods

Other cable plant passive devices (such as splitters and taps) must have sufficient RF bandwidth, see Figure 20 to match the designed complexity of the network upgrade.

Figure 19: Cable Plant Passive Devices

These recommendations are intended to offer guidance when using existing coaxial cabling for EoC applications, do not necessarily indicate the best infrastructure to use, and do not guarantee performance. Other parameters, such as application, distance, and transmission rate or frequency, should be considered. Consult with your network designer to ensure the existing cable plant can support all data and CATV services.

7. WIRED CONVERGED NETWORK TECHNOLOGY OPTIONS

Media types can vary and are important in the design and network selection process. It is critical to ensure the correct core technologies supporting convergence are also selected to match the capabilities and connectivity of the selected infrastructure. The selection process typically goes hand in hand, but options can exist. The following section will describe these options and how they correlate to the cabling infrastructure.

7.1 STRUCTURED CABLING / ETHERNET

Network convergence refers to the use of a single, physical network to connect multiple applications and technologies to that network. The alternative is to deploy separate, disparate networks for those applications and technologies. Examples of where disparate networks have traditionally been deployed in hotels are back-office administrative systems, guest Wi-Fi, telecom systems, guest key lock systems, and many others. In the past, network security and integration complexities drove the adoption of disparate networks in hotels. However, the advancement of logical networking technologies such as Virtual Local Area Networks or VLANs has enabled the technical possibility and even preference to implement converged networks.

There are several advantages to converged networks:

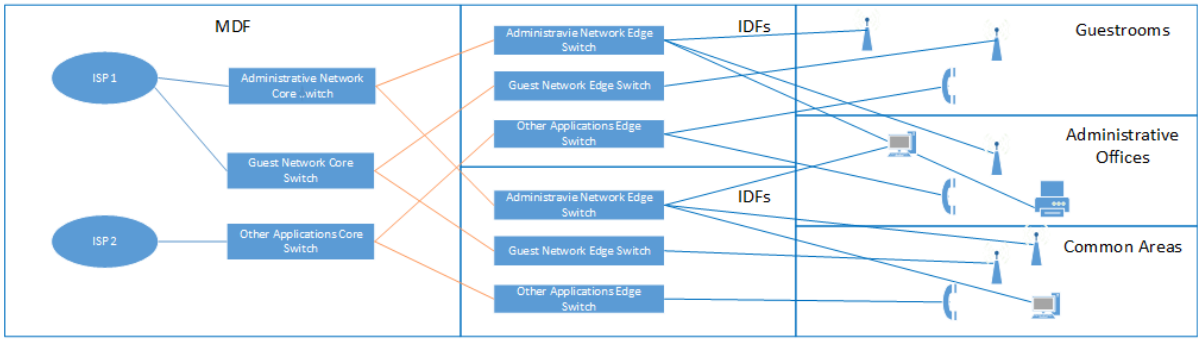
- Simplification of the network cabling plant
- Reduction of the number of active components such as routers, switches, or access points
- Cost reduction
- Fewer support and maintenance suppliers
- Remote network configuration and support enablement
- Single network security strategy
- Consistent network performance experience

There are however a few challenges to be aware of:

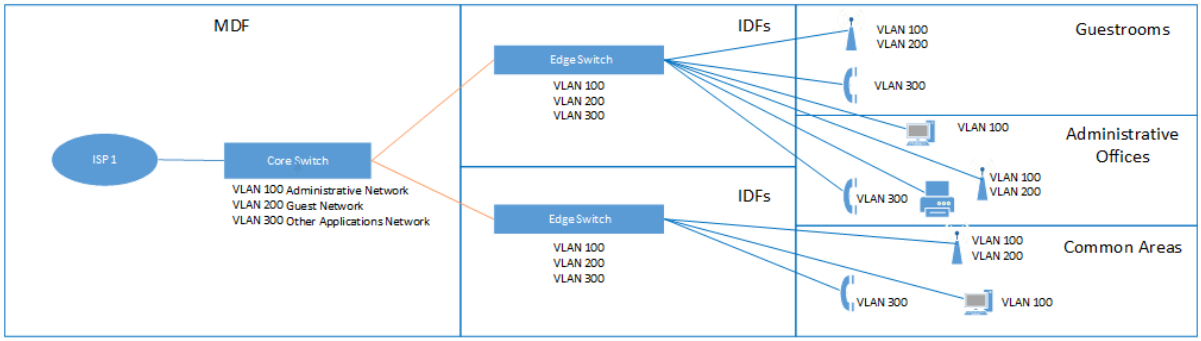
- Physical complexity reduction is traded for additional logical complexity (documentation and configuration rules become critical)
- Network security strategy must be robust since all applications rely on a single network
- Redundancies should be built into a converged design to ensure network stability

As you can see from the diagram (Figure 20) below, many duplications result from separate physical networks. Hotels requiring back-office applications in guest rooms or common spaces may have to duplicate wired and wireless networks. This drives the need for duplicate cabling, network switches, and even wireless access points or security appliances to support this configuration, which is inefficient. Properly designed and implemented converged networks can use the same equipment to connect multiple applications using the same physical network equipment. This simplifies the physical design, lowers up-front costs, and enables a better remote support experience for a hotel.

Siloed Networks



Converged Network



7.2 FIBER-OPTIC BASED (FTTR) NETWORKS

As mentioned above in Section 6.3, the two most common FTTR technologies includes Passive Optical Networking (PON) also known as Point to Multi-Point and Active Ethernet which is also known as Point to Point.

7.2.1 FTTR Using Passive Optical Networking (PON)

PON technologies have been around for a long time and have evolved from supporting fiber-to-the-room (FTTR) or fiber-to-the-home solutions to in-building data networks. PON utilized a centralized management headend called an Optical Line Terminal sized to the property. It then connects to passive optical splitters that utilize one single-mode fiber and split into many.

Typical sizes of splitters used in hotels are 1x16 and 1x32. These splitters can be located at the head end or in IDFs (TRs) throughout the property. Less fiber will be used if distributed around the property. From the splitter, one of the splitter legs will be connected to a single-mode fiber that makes its way typically to the guest room.

A device called an Optical Network Terminal (ONT), or Software Defined Access Node is placed in the guest room. This device typically has multiple Ethernet ports with POE enabled as needed to connect to devices like Wi-Fi APs, VoIP Phones, and IPTV. Gigabit Passive Optical Networking (GPON) is a common solution for many hotels today as it provides 1Gb speed to the room. A single GPON port out of the OLT supports speeds of 2.5Gb down and 1.2Gb up. This bandwidth is shared across the optical splitters. See typical split ratios in Figure 21 for simple FTTR PON Topology:

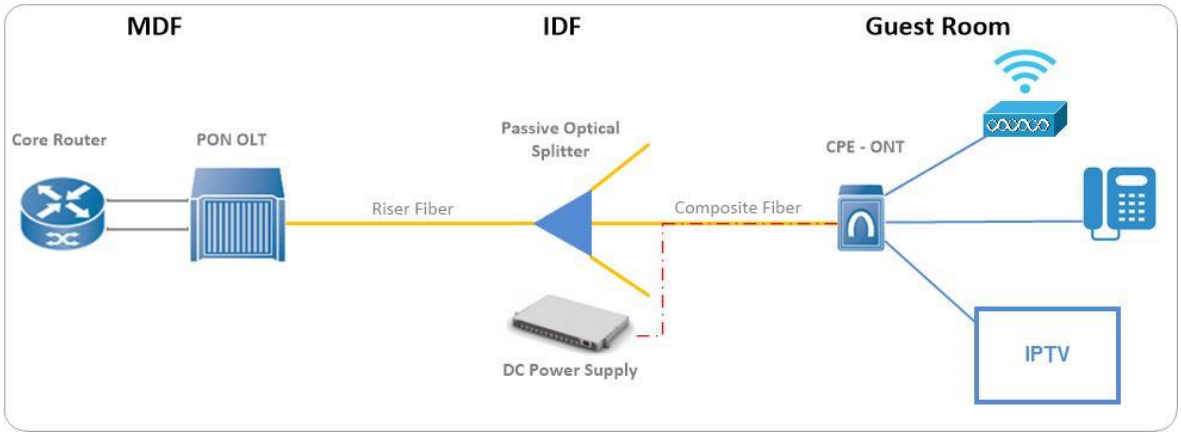


Figure 21

7.2.2 XGS PON

XGS-PON (X-10, G=Gigabit, S=Symmetric) is a passive optical networking standard (ITU-T G.9807.1) that provides 10G symmetrical bandwidth. Like GPON, XGS-PON utilizes a single fiber from the OLT (Optical Line Terminal) to ONTs (Optical Network Terminal) in a point-to-multi-point topology using passive splitting of the optical signal for distribution. The splitter is a device with flexible installation applications that is relatively small and does not require power or cooling. XGS-PON and GPON differ because XGS-PON provides a 10G symmetrical (10G downstream and 10G upstream) capacity, and GPON provides asymmetric rates at approximately 2.5G downstream and 1.2G upstream).

XGS-PON was defined to use different wavelengths than GPON, which makes the two standards compatible and enables them to co-exist on a single fiber. Figure 22 shows the wavelengths of the upstream and downstream transmissions of GPON and two different XGS-PON signals. In essence, this diagram provides for two 10G symmetrical signals co-existing with GPON.

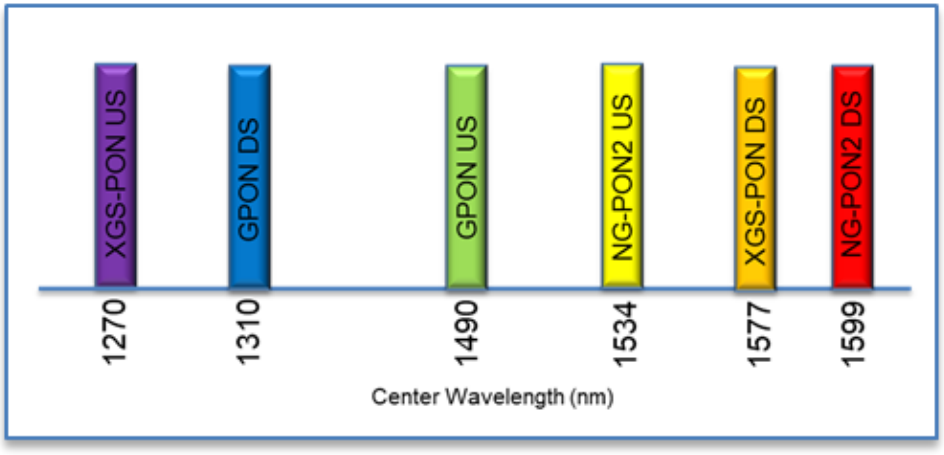


Figure 22

Right-sizing 10-gigabit connectivity inside buildings and across a campus starts at the OLT. The OLT can be equipped with either 2.5 G-PON (ITU-T G.984) or symmetrical 10G XGS-PON (ITU-T G.9807) ports by choosing the corresponding XFPs (pluggable optics). Given that XGS-PON and GPON are compatible and can coexist, it's possible to optimize a deployment's capacity requirements or to grow and transition a GPON network to a XGS-PON network.

Combining XGS-PON and GPON to co-exist on a single fiber uses a Wave Division Multiplexer (WDM). It is depicted in the following diagram where the XGS-PON and GPON, from the same or different OLTs, interface

with the WDM (combiner) device. The signals co-exist over the same fiber and utilize the same splitter. From the splitter, individual fibers go to ONTs, which are specific to being XGS-PON or GPON compatible.

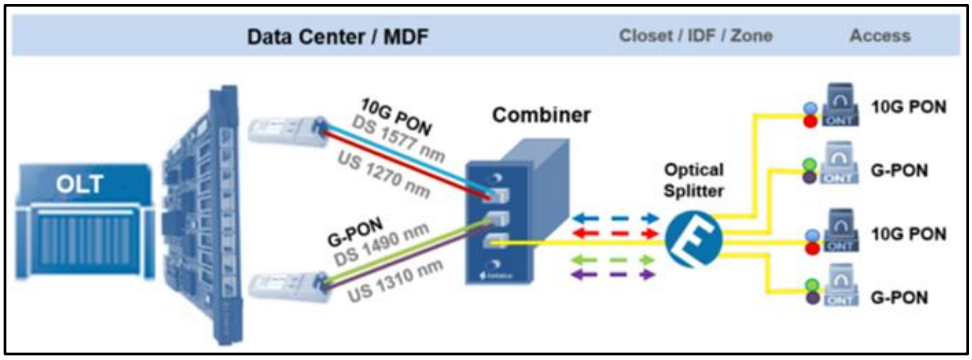


Figure 23

Higher capacity PON standards will be market-available in the future. Specifically, the NG-PON2 (ITU-T G.989) standard is defined to provide 40G symmetrical capacity using four wavelengths of 10G each and using the same WDM concept, as noted earlier. NG-PON2 is defined to be compatible with GPON and XGS-PON, so there are no foreseen wavelength conflicts; thus, it's possible to grow network capacity and transition to, or cap-and-grow, networks with PON over today's fiber infrastructure to ensure that as bandwidth requirements increase, no rip-and-replace will be necessary.

7.2.3 FTTR Using Active Ethernet

A Fiber to the Room (FTTR) Active Ethernet (AE) design is like the PON example above. The main difference from the PON scenario is that the simplex or duplex fiber connects an SDAN (Software Defined Access Node) similar switch (or AP with switch ports) in the guest room to a larger switch that receives a Small Form Pluggable (SFP) back in the IDF or MDF. The typical connection is 1Gb dedicated to the guest room endpoint but could be a 10Gb or multi-gigabit port. It is important to identify the type of fiber connection or SFP that the switch in the gues will use. See Figure 24 for a simple FTTR AE Topology.

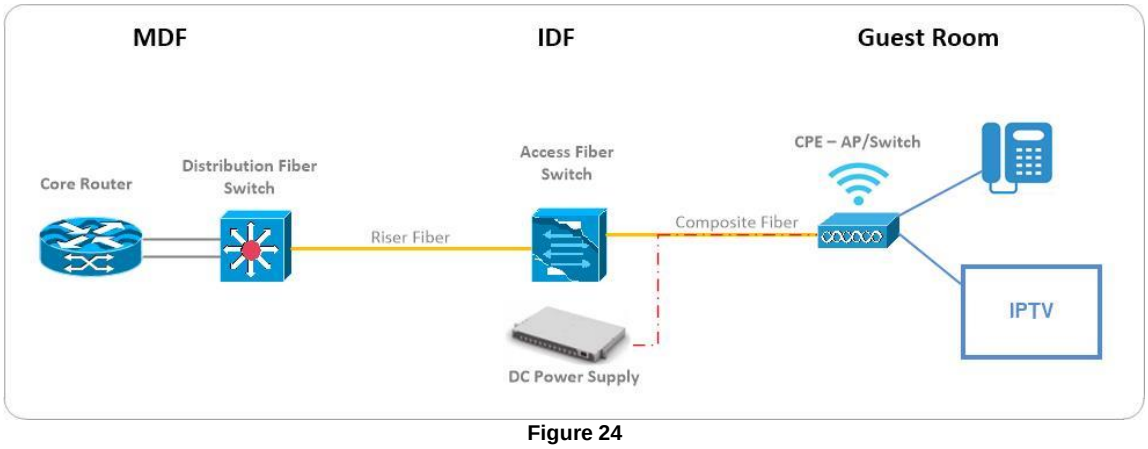


Figure 24

In both cases, the number of rooms served out of each IDF should be considered to identify total rack space requirements. It is important to identify the following:

- The number of optical splitters (for PON) or the number of fiber switches (for AE)
- Pathway availability/routing
- Supporting fiber management and fiber jumper requirements
- Remote powering: available power, power supplies, and UPS

7.3 COAX-BASED

Traditionally, the use of Coax for connectivity has been synonymous with DOCSIS from CableLabs. Over recent years, newer Ethernet over Coax technologies have been introduced. G.hn and MoCA are both ITU-T standards that achieve multi-gigabit Ethernet connectivity.

G.hn and MoCA are particularly well-suited to offer a converged Ethernet infrastructure that can serve multiple uses, from HSIA Guest Wi-Fi to IPTV, Casting, and IoT.

Re-using Coaxial cabling offers a unique cost-saving opportunity compared to rewiring a property with fiber or structured cabling. Just like Passive Optical Networking (PON), a Coaxial cabling infrastructure uses passive Coax splitters or taps to connect multiple guest rooms over a single Coax cable segment and ultimately a single port of a G.hn Access Multiplexer (GAM), MoCA headend or DOCSIS CMTS.

Another significant benefit is that the Coaxial cabling already terminates in the back of the TV set and is ready to be used for IPTV services when ready to transition away from QAM-based Free-to-Gues entertainment.

Coaxial cabling has a long useful life remaining and will be ready to offer 10 Gigabit services by the 2025-2026 timeframe with the next generation of G.hn and MoCA. Even DOSIS 4.0 bears the promise of 10 Gigabit services.

When considering the reuses of the Coaxial cabling, it is important to understand how each technology operates and whether amplifiers are required, how the bandwidth is managed, and the spectrum used, and therefore the overall distance/reach achievable.

A summary of each of these technologies follows.

7.3.1 DOCSIS

Data Over Cable Service Interface Specification (DOCSIS) is an international telecommunications standard defined and managed by CableLabs that permits the addition of high-bandwidth data transfer to an existing cable television (CATV) system. Many cable television operators use this to provide cable Internet access over their existing Hybrid Fiber-Coaxial (HFC) infrastructure. The early versions of DOCSIS (no longer used) offered limited performance.

DOCSIS 3.1 is now the dominant version and offers a shared capacity of 1-5 Gbps downstream and 200 Mbps to 1.2 Gbps upstream. A DOCSIS CMTS is usually deployed to serve an upward of 100 rooms per Coax port.

Figure 25 is a summary of various DOCSIS standards and their evolution over time.

	DOCSIS 1.0	DOCSIS 1.1	DOCSIS 2.0	DOCSIS 3.0	DOCSIS 3.1	DOCSIS 4.0
Highlights	Initial cable broadband technology: high speed internet access	Added VoIP service, gaming, streaming	Higher upstream speed, capacity for symmetric services	Greatly enhances capacity, channel bonding, IPv6	Capacity and efficiency progression, DFDM, wideband channel	Symmetrical streaming and increased upload speeds

Downstream Capacity	40 Mbps	40 Mbps	40 Mbps	1 Gbps	5 Gbps	10 Gbps
Upstream Capacity	10 Mbps	10 Mbps	30 Mbps	200 Mbps	1-2 Gbps	6 Gbps
Upper RF Frequency	860 MHz	860 MHz	860 MHz	1002 MHz	1218 – 1794 MHz	1794 – 3000 MHz
Initial Issue Date	1996 *Obsolete*	1999 *Obsolete*	2001 *Obsolete*	2006 *Obsolete*	2013 *Widely used*	2019 *Limited Deployment by Cable COs begun in 2022-23*

Figure 25: The Evolution of DOCSIS

7.3.2 G.hn

G.hn is an ITU-T standard (G.9960 family) to deliver Gigabit Ethernet services over multiple media: coaxial cabling, copper (CAT-3/telephone wiring or better), and even powerlines. G.hn is primarily used over coaxial cabling in the hospitality market, with properties electing to use technology over copper in some cases.

G.hn is also widely used in the residential market as a fiber extension technology. A G.hn installation uses a G.hn Access Multiplexer (GAM) based on a Multi-Gigabit Ethernet switch architecture. G.hn Endpoint devices terminate the G.hn links and provide one or more Gigabit Ethernet ports to connect devices such as Wi-Fi Access Points and smart TVs.

The current version of G.hn (referred to as Wave-2) was ratified in March 2016. It expanded the standard to include signaling over telephone wire and coaxial cabling to provide data rates of up to 2 Gbps, achieving an aggregate Ethernet bandwidth of 1.7 Gbps. This aggregate bandwidth is managed via a flexible Dynamic Transmit Allocation (cDTA/iDTA) technique that provides unparalleled real-time Upstream/Downstream Gigabit performance verified by network speed tests such as OOKLA.

When operating over coaxial cabling, G.hn operates in a Point-to-Multipoint (P2MP) mode where each port of a GAM device serves up to sixteen (16) G.hn links (rooms or TV set) by re-using existing coaxial splitters or tap devices already used for the Free-to-Guest Entertainment. Since GAM units usually come with multiple ports, they can easily serve upward of one hundred (100) G.hn links at a time where each port is capable of 1.7 Gigabit speeds, ensuring plenty of upstream and downstream bandwidth for each guest. When operating over copper/telephone wiring, each port of a GAM device serves one G.hn endpoint (Point to Point). The uplink (backhaul) connectivity of GAM devices is typically achieved by one or two 10-Gigabit ports (usually SFP+ fiber).

Other benefits are:

- G.hn uses the 5-200 MHz spectrum, allowing for seamless co-existence with Free-to-Guest (QAM-encoded) TV. Where necessary, it is possible to configure one or more notches that G.hn will free up to enable support for other services such as Pay-Per-View (PPV) signaling. This allows FTG (Free to Guest) content to begin at channel 30 (258 MHz), as it is already often the case in most FTG installations. The spectrum used is less susceptible to attenuation over distance when compared to DOCSIS and MoCA and allows for Gigabit performance at an attenuation level of 42 d8 (about 2600 feet/800 meters over RG-6 Coax cabling).
- G.hn does not need amplification or regeneration. Unlike DOCSIS, G.hn does not require the use of amplifiers that require fine tuning during their installation and regular maintenance over time.

- G.hn dynamically allocates bandwidth to each link based on their actual demands and the service profile defined. This approach ensures that each guest obtains the necessary bandwidth for their needs.
- G.hn is 100% compatible with the Ethernet standards, including VLAN support (Q-in-Q), Quality of Service (QOS), 802.1x authentication, and more.

In March of 2020, the ITU-T updated the G.hn standard to allow performance of 10 Gigabit on Coaxial cabling and 5 Gigabit over CAT-3/telephone wiring. Chipsets and new GAM devices are anticipated to be available in 2025.

Figure 26 summarizes the evolution of the ITU-T G.hn standard.

	G.hn (Wave 1)	G.hn (Wave 2) COAX and Twisted Pair	G.hn (Wave 3) COAX and Twisted Pair
Physical Medium	Coax Copper (CAT-3 or better) Powerline	Coax Copper (CAT-3 or better) Powerline	Coax Copper (CAT-3 or better) Powerline
MAC Throughput	1 Gbps	2 Gbps	COAX -10 Gbps Twisted Pair – 5 Gbps
Operating Mode	Copper: PTP COAX: P2MP (16 links per port) Powerline: P2MP / MESH	Copper: PTP COAX: P2MP (16 links per port) Powerline: P2MP / MESH	Copper: PTP COAX: P2MP (16 links per port) Powerline: P2MP / MESH
RF Frequency Range	2 - 100 MHz	2 - 200 MHz	2 - 1200 MHz
Initial Date Issue	2009 No longer widely used	2016 Widely used	2020 Anticipated availability in 2025

Figure 26

7.3.3 MoCA

The Multimedia over Coax Alliance (MoCA) is an international standards consortium that publishes specifications for networking over Coaxial cable. The technology was initially developed to distribute IP television in homes using existing cabling. It is now used as a general-purpose Ethernet link where replacing existing Coaxial cable with optical fiber or twisted pair cabling is inconvenient or undesirable.

MoCA 1.0 was approved in 2006, MoCA 1.1 in April 2010, MoCA 2.0 in June 2010, and MoCA 2.5 in April 2016. The most recently released version of the standard, MoCA 2.25, supports speeds of up to 2.5 Gbps.

	MoCA Home 2.0	MoCA Home 2.5	MoCA Home 3.0	MoCA Access 2.5	MoCA Access 3.0
MAC Throughput	500 Mbps	2.5 Gbps	10 Gbps	2.5 Gbps	10 Gbps
RF Frequency Range	500 - 1650 MHz	500 - 1650 MHz	500 - 3000 MHz	400 - 1650 MHz	400 - 3000 MHz
Initial Issue Date	2010	2016	2018	2017	2023 *Deployment expected by 2025*

Figure 27: The Evolution of MoCA

8. INDOOR WIRELESS CONVERGED NETWORK TECHNOLOGY OPTIONS

These wireless technologies are typically aggregated on the converged fixed (wired) network infrastructure. Figure 28 shows the list of Wireless Protocols and the following sections will describe these options.

Protocol	Common/Best Use Case(s)
Wi-Fi	Building and campus-wide LAN, guest wireless
Bluetooth	Location services, mobile key, mobile and wearable devices
ZigBee	Building control and automation
Z-Wave	Home automation
Mobile Networks	Mobile phones, devices in isolated locations
SigFox	Asset tracking, utility monitoring, environmental sensors
LoRaWAN	Asset tracking, smart metering, door sensors
BacNet	Building automation and control systems
Thread	Building automation and control systems

Figure 28: Summary of Current Wireless Protocols

In addition to providing support for Ethernet, most hotels currently require support for wireless connectivity for both associate and guest use and various IoT (Internet of Things) devices. Therefore, to provide the reader with additional information on the wireless requirements that may be needed to support the next-generation hotel network requirements, a summary of the currently supported wireless protocols and their intended use is presented in this section.

Wireless protocols work in the OSI model's physical layer, layer 1. This layer carries the signal from device to device or from device to the network. Devices on a wireless network can connect to each other (peer-to-peer) or can connect to an access point (most common). An access point, in turn, connects to the larger network, typically the LAN, which may connect to the Internet. Each device must have a transceiver (transmitter and receiver combined) and must implement and use the appropriate communication protocol to communicate with the other devices on the wireless network. Most wireless connections and all the protocols covered here use radio waves as the medium that carries the signal.

Some devices, such as laser or infrared, may use light to carry the signal instead of radio waves This isn't common but has been used to connect printers to networks in office settings. While Near Field Communications (NFC) is technically a wireless protocol, it is not an Internet protocol, and its range is too short to be useful in an IoT world when not paired with another device, so it is not covered in this document.

Except for Wi-Fi, most protocols outlined in the above table perform backhaul communication via either a wireless mesh between similar devices or utilize a wired gateway. In the case of a gateway, the cabling required to support egress from the gateway can be CAT 3 or higher. The reason for this is that, except for Wi-Fi, the bandwidth requirements are minimal.

However, in the case of Wi-Fi, the Ethernet backhaul requirements would require either CAT 6/6E or higher or using a fiber connection. Several of the current AP vendors support a fiber connection to the APs.

In addition, most of the current AP vendors provide either a built-in Bluetooth beacon or an external USB port that can be used for Bluetooth or any other protocols listed above that provide a USB-capable device.

Lastly, as you can see in the list of wireless protocols currently being used in hospitality, there is a definite need to provide a converged network infrastructure to support these protocols and business requirements.

8.1 WIRELESS PROTOCOL SUMMARY

Contained in the following section is a high-level summary of the various wireless protocols.

8.1.1 Wi-Fi

Wi-Fi has become critical to the hospitality industry. With reliable Wi-Fi, hotels can satisfy guests and maintain loyalty. Signal quality and throughout must be good enough for a home-like or office-like experience. Additionally, business travelers rely on quality Wi-Fi to do work while traveling.

As of 2020, Wi-Fi uses two main radio frequency spectrums: 2.4 GHz and 5 GHz. To clarify, 5 GHz Wi-Fi is not related to 5G, which is the latest cellular communication standard. 802.11a in 1997 leveraged 5 GHz, but since it was a more expensive enterprise solution, it didn't take off as well as 802.11b, which leveraged the 2.4 GHz spectrum also used in 802.11g. The latest Wi-Fi standard, "Wi-Fi 6" (802.11ax), recognized the trend and benefits of 2.4 GHz for IoT and designed the standard with features to improve the handling of the limited spectrum for the growing number of devices. Below are five benefits of Wi-Fi 6 for IoT devices:

- Improved battery performance: The battery life of IoT devices is increased with Target Wake Time (TWT) mode, enabling IoT devices with low transmission requirements to remain in sleep mode for extended periods of time
- Airtime opportunities: Small packets of IoT device data can be aggregated with OFDMA (Orthogonal Frequency-Division Multiple Access), enabling increasing numbers of IoT device connections with minimal bandwidth impact, providing more bandwidth to more data-intensive applications.
- Improved co-existence with other IoT technologies: Utilization of the 2 MHz channels allows for an improved co-existence with other 2.4 GHz technologies.
- Provides for a simple cost-effective design: Optionality for cost-effective radios, with simple BPSK, modulation is enabled by bandwidth as low as 2 MHz and rates of 375 bit/s.
- Improved link budget without battery impact: With bandwidth for 802.11ax clients as low as 2 MHz, a narrower bandwidth can be utilized to concentrate the transmit energy, resulting in longer range.

An extension of the Wi-Fi 6 (802.11ax) standard is Wi-Fi 6E. This is an expansion of Wi-Fi 6 into the new 6 GHz frequency band. This new band will open two to three times more bandwidth than is available today with 2.4 GHz and 5 GHz. This will add significant capacity to Wi-Fi networks for guests, including operational and IoT technologies. This will also result in 80 megahertz (MHz) and 160 MHz channels being viable for the first time, making the new Wi-Fi 6E standard ideal for supporting digital transformation efforts and use cases like high-definition video and X Reality (XR). Much of this will depend on the regional country's approval of utilizing this new band. Wi-Fi 6E also brings new security models with WPA3 and Enhanced Open. Consumer devices are just beginning to support 6E but will continue to come to market on phones, tablets, laptops, and wireless cards.

Wi-Fi 7 (also known as 802.11be) will use the 2.4, 5, and 6 GHz bands like Wi-Fi 6E, but its most significant selling point is Extremely High Throughput (EHT). This will allow Wi-Fi 7 routers to reach speeds of up to 46 Gbps. Another advantage of the latest Wi-Fi standard over existing ones is that it will have several multi-link options to significantly increase throughput while reducing latency. Traditional Wi-Fi devices use just a single link to transmit data. Still, Wi-Fi 7's Multi-Link Operation (MLO) allows devices to simultaneously send and receive data across different frequency bands and channels.

Whether or not it will be worth upgrading to a Wi-Fi 7 router depends on current equipment. If you have older Wi-Fi 5 access points installed, then it will be worth it, as you'll likely see a significant performance boost. However, if Wi-Fi 6E access points are installed, you might want to hold off a bit before upgrading. Regardless, one of the best things about introducing new Wi-Fi standards is that they are always backward compatible with existing ones.

8.2 IoT – Internet of Things Wireless Protocols

Internet of Things (IoT) is a catchall phrase describing physical objects (or groups of such objects) which sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over a common IP network. Below are several wireless IoT technologies utilized in the hospitality environment.

8.2.1 Bluetooth

Bluetooth is a wireless point-to-point technology standard for exchanging data between fixed and mobile devices over short wavelength Ultra High Frequency (UHF) radio waves.

8.2.1.1 Current Standards and Roadmap

Bluetooth is managed by the Bluetooth Special Interest Group (SIG). The IEEE initially standardized Bluetooth as IEEE 802.15.1 but no longer maintains the standard. The Bluetooth SIG now oversees the development of the specification, managers the qualification program, and protects the trademarks. A manufacturer must meet Bluetooth SIG standards to market as a Bluetooth device.

8.2.1.2 Current Adoption in the Hospitality Industry

While seeing significant growth, Bluetooth technologies have not historically carried a substantial audience in the hospitality space. Figure 29 lists some of the most popular historial and future uses.

Current	Future
• **Mobile connectivity to in-room speakers** • **Mobile entry to guestroom doors**	• Employee tracking and safety technology • Wearable payment technology • Marketing metrics

Figure 29

8.2.1.3 Key Considerations for Hoteliers

There are several factors to consider when choosing whether to deploy a Bluetooth network as part of, or the entire architecture for, technology solutions in hospitality. To properly consider all applicable variables, the following questions should be answered by prospective users:

- Which technology products will be implemented now or in the future as part of the technology/automation deployment?
- Are those products available with Bluetooth connectivity built-in?
- How does the pricing of these Bluetooth products compare to those with other built-in networking capabilities?
- Which existing networking infrastructures are already available with with property?
- What speed is required for communication?
- What is the proximity of the individual devices?
- What is the breadth of choices among products necessary to meet each of the required abilities?

8.2.2 Zigbee

Zigbee is a specification for a suite of high-level communication protocols used to create local area networks with low-power digital radios. Zigbee is used for home and building automation and other low-power, low-bandwidth needs.

The technology defined by the ZigBee specification is intended to be simpler and less expensive than other wireless networks such as Bluetooth or Wi-Fi. ZigBee devices can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones. Zigbee is typically used in low data rate applications that require long battery life and secure networking (Zigbee networks are secured by 128-bit symmetric encryption keys). Zigbee has a defined rate of 250 kbit/s and is best suited for intermittent data transmissions from a sensor or input device.

Zigbee builds on the physical layer and media access control defined in IEEE standard 802.15.4 for low-rate wireless networks (WPANs). The specification includes four additional key components: network layer, application layer, Zigbee Device Objects (ZDOs), and manufacturer-defined application objects. ZDOs are responsible for some tasks, including keeping track of device roles, managing requests to join a network, and device discovery and security.

ZigBee devices may be configured and controlled remotely using a ZigBee gateway or central control device (hub), which also acts as the portal connection to the public Internet. ZigBee provides the application layer interoperability between home control systems of different manufacturers and products.

8.2.2.1 Current Standards and Roadmap

Established in 2002, the Zigbee Alliance is a group of companies that maintain and publish the Zigbee standard. Zigbee is a registered trademark of this group, not a single technical standard. This alliance publishes application profiles that allow multiple OEM vendors to create interoperable products. The relationship between IEEE 802.15.4 and Zigbee is like that between IEEE 802.11 and the Wi-Fi Alliance.

Zigbee protocols are intended for embedded applications requiring low power consumption and tolerating low data rates. The resulting network will use very little power – individual devices must have a battery life of at least two years to pass Zigbee certification.

ZigBee-style self-organizing ad-hoc digital radio networks were conceived in the 1990s. The IEEE 802.15.4-2003 Zigbee specification was ratified on December 14, 2004. The Zigbee Alliance announced the availability of Specification 1.0 on June 13, 2005, known as the ‘Zigbee 2004 Specification.’

8.2.2.2 Current Adoption in Hospitality

Zigbee has historically enjoyed the most prolific coverage across products and technology when considering automation and sensing technology. Zigbee’s longevity in hospitality is unmatched, from sensing, building control, and product integrations to the breadth of products available, existing product and platform integrations, and proven deployments. Figure 30 is a listing of some of the most popular current and potential future uses.

Current	Future
• **Lighting** • **HVAC** • **Sensing (temperature, humidity, light level, air quality, noise, smoke, security)** • **Door lock** • **Window treatments** • **Room signage** • **Voice**	• **Mobile key** • **Wearables** • **Tracking** • **Payment** • **Elevator call** • **Concierge call** • **Window tinting** • **Load shedding**

• **Media** • **Tablet**	

Figure 30

8.2.2.3 Key Considerations for Hoteliers

There are several factors to consider when choosing whether to deploy a Zigbee network as part of, or the entire architecture for, technology solutions in hospitality. To properly consider all applicable variables, the following questions should be answered by prospective users:

- Which technology products will be implemented now or in the future as part of the technology/automation deployment?
- Are those products available with Zigbee connectivity built-in?
- How does the pricing of these Zigbee products compare to those with other built-in networking capabilities?
- Which existing network infrastructures are already available within the property?
- What speed is required for communications?
- What is the proximity of the individual devices?
- What is the breadth of choices among products necessary to meet each of the required abilities?

8.2.3 Z-Wave

Z-Wave is a wireless communication protocol used primarily for home automation. Z-Wave is a mesh network using low-energy radio waves to provide low-throughput communication from device to device. These devices may be configured and controlled remotely using a Z-Wave gateway or central control device (hub), which also acts as the portal connection to the public Internet. Z-Wave provides the application layer interoperability between home control systems of different manufacturers and providers.

Year Released	1999
Standard	N/A
Frequency Range	800-900 MHz (varies worldwide)
Physical Range	100 ft (depending on various factors and radio types)
Data Rates	40 kb (depending on various factors and radio types)
Network Connectivity	Mesh

Figure 31

Z-Wave's Interoperability at the application layer ensures that devices can share information, allowing all Z-Wave hardware and software to work together. Its wireless mesh networking technology enables any node to talk to adjacent nodes directly or indirectly, controlling any additional nodes. Nodes that are within range communicate directly with one another.

If they aren't within range, they can link with another node that is within range both to access and exchange information. In September 2016, certain parts of the Z-Wave technology were made publicly available when then-owner Sigma Designs released a public version of Z-Wave's interoperability layer, with the software added to Z-Wave's open-source library. The open-source availability allows software developers to integrate Z-Wave into devices with fewer restrictions. Z-Wave's S2 security, Z/IP for transporting Z-Wave signals over IP networks, and Z-Ware middleware, are all open source as of 2016.

Z-Wave is designed to provide reliable, low-latency transmission of small data packets at data rates up to 40 kbit/s. The communication distance between two nodes is about 30 meters (40 meters with a 500 series chip), allowing the message to hop up to four times between nodes.

Z-Wave uses the Part 15 unlicensed industrial, scientific, and medical (ISM) band. It operates at 868.42 MHz in Europe, 908.42 MHz in North America, and other frequencies in other countries, depending on federal regulations.

This band competes with some cordless telephones and other consumer electronic devices but avoids interfaces with Wi-Fi, Bluetooth, and other systems that operate on the 2.4 GHz band. The lower layers MAC

and PHY, are described by ITU-TG.9959 and are fully backward compatible. Silicon Labs supply the Z-Wave transceiver chips.

8.2.3.1 Current Standards and Roadmap

The Z-Wave protocol was developed by Zensys, a Danish company based in Copenhagen, in 1999. That year, Zensys introduced a consumer light-control system, which evolved into Z-Wave as a proprietary system on a chip (SoC) home automation protocol on an unlicensed frequency ban in the 900 MHz range. Its 100 series chipset was released in 2003, and its 200 series was released in May 2005, with the ZW0201 chip offering high performance at low cost. Its 500 series chip, also known as Z-Wave Plus, was released in March 2013 with four times the memory, improved wireless range, and improved battery life. Five companies formed the Z-Wave Alliance, whose objective was to promote the use of Z-Wave technology, with all products by companies in the group being interoperable.

Sigma Designs acquired Z-Wave in December 2008. Following the acquisition, Z-Wave's U.S. headquarters in Fremont, California merged with Sigma's headquarters in Milpitas, California. The Z-Wave technology and business asses were once again sold in April 2018 to Silicon Labs.

The Z-Wave Alliance was established in 2005 as a consortium of companies that manufacture products using Z-Ware wireless mesh networking technology. The Alliance is a formal association focused on expanding Z-Wave and the continued interoperability of any device that utilizes Z-Wave.

In October 2013, a new protocol and interoperability certification program called Z-Wave Plus was announced based upon new features and higher interoperability standards bundled together and required for the 500 series system on a chip (SoC) and included some new features that had been available since 2012 for the 300/400 series SoCs. In February 2014, the first product was certified by Z-Ware Plus.

In 2016, the Alliance launched a Z-Wave Certified Installer Training program to giver installers, integrators, and dealers the tools to deploy Z-Wave networks and devices in their residential and commercial jobs. That year, the Alliance announced the Z-Wave Certified Installer Toolkit (Z-CIT), a diagnostic and troubleshooting device used during network and device setup. It can also function as a remote diagnostics too.

Z-Wave Alliance maintains the Z-Wave certification program Z-Wave certification has two components: 1) technical certification, managed through Silicon Labs, and 2) market certification, managed through the Z-Wave Alliance.

8.2.3.2 Current Adoption in Hospitality

Due to several factors, Z-Wave has yet to achieve much success within the hospitality industry.

While Z-Wave has a lower cost basis than Wi-Fi and Zigbee, it also does not have the same ROI when reviewing the communication speed and data rates versus the cost of Zigbee or Wi-Fi. Due to this, a limited number of products are manufactured by a limited number of companies that incorporate Z-Wave as the transport technology.

In addition, because of its proprietary nature and use of unlicensed spectrum, Z-Wave presents several inherent flaws that do not exist with other, more prolific, IoT technologies.

8.2.3.3 Key Considerations for Hoteliers

One of the most significant considerations for potential users is that since Z-Wave operates in an unlicensed spectrum, deployments will compete with other technology in the space, such as garage door openers and wireless telephone systems, which makes troubleshooting problematic and scaling network deployments uncertain. A second key consideration since the chip is proprietary and the technology is licensed by Silicon Labs, all manufacturing and availability components are entirely dependent on Silicon

Lab's business.

In addition to these key questions, there are a few factors to consider when choosing whether to deploy a Z-Wave network as either part of, or the entire architecture for, technology solutions in hospitality. To properly consider all applicable variables, the following questions should be answered by prospective users:

- Which technology products will be implemented now or in the future as part of the technology/automation deployment?
- Are those products available with Bluetooth connectivity built-in?
- How does the pricing of these Bluetooth products compare to those with other built-in networking capabilities?
- Which existing networking infrastructures are already available with with property?
- What speed is required for communication?
- What is the proximity of the individual devices?
- What is the breadth of choices among products necessary to meet each of the required abilities?

8.2.4 Mobile Networks

Mobile networks, now based on a global standard established by the Third Generation Project Partnership (3GPP), can provide an excellent connectivity method for IoT devices. While previous generations of standards (2G and 3G) supported IoT device connectivity, the current 4G standard has specific narrow-band protocols to address the data-only latency-flexible needs of IoT addressed in this section.

Mobile networks, due to their licensed frequency band operation, have inherent security and Quality of Service (QOS) benefits. The 4G LTE standard and the Subscriber Identity Module (SIM) provide additional QOS, policy, rules control, and mobility from location to location – all benefits compared with other connectivity solutions.

The 3GPP has developed, and mobile network providers are rolling out the next-generation mobile network standard – 5G. As with 4G, the new network standard will take time to deploy with a 4G interoperable transition period. In fact, the narrow band 4G LTE protocols will continue to be supported for some time.

It is important to note the 5G standard has attributes developed to directly enhance IoT device connectivity which will become available as the network matures. The 5G standard accommodates thousands of more devices per square kilometer and interoperability with other non-3GPP protocols. It also provides virtual slices of the network ('Network Slicing') to streamline and provide automatic flexibility directly supporting IoT devices and other requirements.

Please refer to Section 2.4 to find the link for HTNG's 5G for Hospitality technology documents.

8.2.4.1 Current Standards and Adoption

Mobile networks are not typically used for most hotel IoT applications other than POS in remote (non-Wi-Fi/Ethernet) areas. Some panic button solutions do have a mobile network backup.

8.2.4.2 Key Considerations for Hoteliers

While networks largely exist, the mobile network signal level must be available for the IoT device to connect, which the narrow-band protocols greatly enhance. Given the network is owned and operated by others, where connectivity is available, the control plane information is not available, and there is a recurring cost for the service to the network provider to be considered as an operating expense. For more details on how to enhance mobile networks inside hotels, see Section 9: Indoor Cellular and 2-Way Wireless Solutions in this document.

8.2.5 Sigfox

Sigfox is a global network dedicated to IoT based on low power, long-range (up to 25 miles), and small data. Sigfox offers an end-to-end connectivity service communicating over unlicensed frequencies. Sigfox has a simple technology stack, low module cost, and long battery life. Sigfox has designed its technology and network to meet the requirements of mass IoT applications, including long device battery life, low device cost, low connectivity fee, high network capacity, and long range. With 100 bits/sec – 600 bits/sec (depending on the region), the bandwidth is by design kept very low to be conservative with power consumption to achieve a long battery life. Unlike cellular protocols, a Sigfox device is not connected to a specific base station. Instead, any base station in range can receive the broadcast message. Sigfox operates on a public network model, where all devices connecting to the Sigfox network require a subscription to Sigfox.

8.2.5.1 Current Standards and Roadmap

Sigfox was founded in France in 2010 to build LPWAN based on its proprietary technology on an unlicensed spectrum. Sigfox completed nationwide coverage in France in 2012 and launched its network in the United States in 2015. The public Sigfox network is now available in over 70 countries. As of April 2020, 849 certified Sigfox devices *have been* developed by 732 IoT companies.

8.2.5.2 Current Adoption in Hospitality

Sigfox has a simple technology stack, low module cost, and long battery life, making it a popular choice for IoT deployments with low bandwidth, long distance, and small packets of data (12 bytes max payload). A challenge with Sigfox is that there is a long delay, so this is not a suitable technology for real-time response. Sigfox has a presence in multiple industries, including supply chain and logistics, manufacturing, smart cities, utilities and energy, smart buildings, retail, agriculture, insurance, hospitality, and the home.

Examples include asset tracking, soil moisture monitoring, leak detection, connected smoke detectors, smart ordering buttons, and environmental sensors (including temperature, humidity, and air quality). In the hospitality industry, applications include minibar sensors, asset tracking (e.g. room tray monitoring), utility monitoring, and panic buttons.

8.2.5.3 Key Considerations for Hoteliers

Before considering deploying applications or devices that utilize Sigfox, the hotelier should review the following:

- The type of data I wish to transfer - for example, do I have something I want to monitor that does not require real-time data?
- My existing infrastructure - for example, are there other technologies that would work better using existing infrastructure, such as Wi-Fi?
- My building material - for example, what transport will best propagate in my hotel?
- How extensive of a network would I need to deploy - for example, would one base station be enough, or do I need a network of base stations?

8.2.6 LoRaWAN

LoRa is a wireless modulation technique derived from Chirp Spread Spectrum (CSS) technology. It encodes information on radio waves using chirp pulses. LoRa-modulated transmission is robust against disturbances and can be received across great distances. End devices are mostly battery-powered with a low cost of around 20 USD. With 250bit/sec – 11kbit/sec, the bandwidth by design is kept very low to be conservative with power consumption to archive a long battery lifetime of up to 10 years.

LoRa is ideal for applications that transmit small chunks of data with low bit rates. Data can be transmitted at significantly longer ranges compared to technologies like Wi-Fi, Bluetooth, or ZigBee. LoRaWAN is suitable for transmitting small-size payloads (like sensor data) over long distances. Figure

32 shows some access technologies that can be used for wireless data transmission and their expected transmission ranges versus bandwidth.

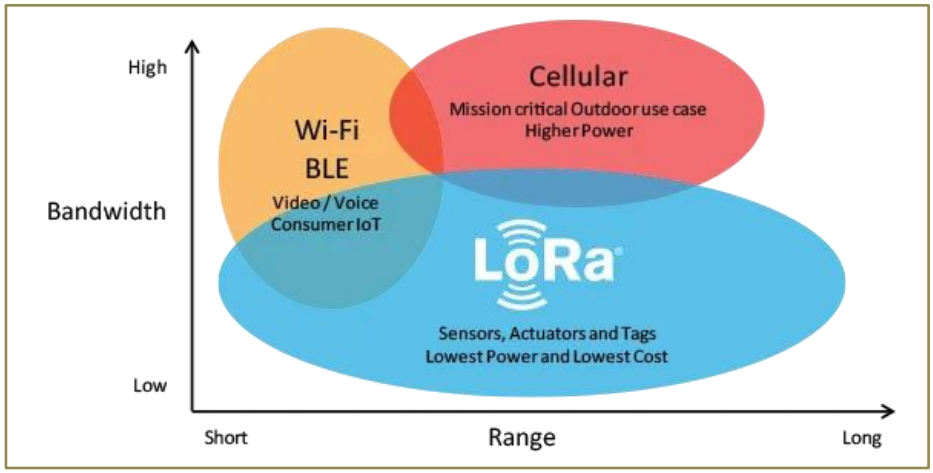


Figure 32

LoRa can be operated on license-free sub-gigahertz bands. In North America, the frequency assigned to LoRaWAN transmissions is 915 MHz. It can also be operated on 2.4 GHz to achieve higher data rates than sub-gigahertz bands at the cost of range; however, previously this application was limited due to concerns of strict cycle duty limitations. These concerns have been elevated with the transition to >5.2 GHz frequencies with the adoption of Wi-Fi 6.

8.2.6.1 Current Standards and Roadmap

LoRaWAN standards are driven by the LoRaWAN Alliance, an open, nonprofit association with over 500 members.

8.2.6.2 Current Adoption in Hospitality

Applications for LoRaWAN include anything that requires low bandwidth, long distance, and no requirement for real-time. Some examples include smart metering for electricity or water, cattle GPS tracking (or animal tracking in general), smart parking, outdoor text-based bus, tram, or train terminal displays, and environmental sensors (including temperature, humidity, and air quality sensors). In the hospitality industry, current applications include minibar sensors and window sensors. Another common application is door usage in a public space, for example, a restroom or elevator. This data enables predictive monitoring and cleaning schedules to be adjusted depending on usage.

LoRaWAN is not the right technology to control lights, door locks, or anything requiring real-time or close-to-real-time communication.

8.2.6.3 Key Considerations for Hoteliers

Here are several considerations key for hoteliers:

- The type of data I wish to transfer - for example, do I have something I want to monitor that does not require real-time data?
- My existing infrastructure - for example, are there other technologies that would work better using existing infrastructure, such as Wi-Fi?
- My building material – for example, what transport will best propagate in my hotel?
- How extensive of a network would I need to deploy – for example, would one gateway be enough, or do I need a network of gateways?
- Cost considerations of different transport mechanisms

8.2.7 BACnet

BACnet is a communication protocol for building automation and control (BAC) networks that use the ASHRAE, ANSI, and ISO 16484-5 standards protocol.

BACnet was designed to allow communication of building automation and control systems for applications such as heating, ventilating, and air-conditioning control (HVAC), lighting control, access control, and fire detection systems and their associated equipment. The BACnet protocol provides mechanisms for computerized building automation devices to exchange information, regardless of the building service they perform.

8.2.7.1 Current Adoption in Hospitality

BACnet continues to be supported by many of the current HVAC manufacturers, however, the HVAC systems are typically not interfaced with a BACnet network due to the lack of required network infrastructure. Therefore, the hotels lose the ability to monitor the HVAC systems.

The BACnet protocol currently provides support for over 60 standard object types.

8.2.7.2 Current Standards and Roadmap

BACnet has been under development since June 1987, when Standard Project Committee 135P (SPC 135P) first met at the ASHRAE Annual Meeting. In 1995, the first official BACnet standard was published. Consolidated versions of both BACnet standards, including all errata and addenda, have been published every year since the standards were first published. Finally, BACnet is currently used in hundreds of thousands of installations worldwide.

8.2.7.3 Guest Adoption in Hospitality

As noted above, many of the current HVAC manufacturers presently support BACnet. However, because the property's infrastructure is not designed to support a converged environment or the HVAC vendor cannot provide the required gateway or monitoring software, the property does not take advantage of the features the BACnet functionality provides. Finally, it should be noted that the property may not calculate the ROI of installing the required BACnet radios and gateway and may not realize the financial benefit of deploying the required infrastructure.

8.2.8 Thread

Thread is an IPv6-based, low-power mesh networking technology for IoT products. Thread is dependable, secure, and it delivers fast response times, extended coverage, and years of battery life to elevate smart home and building experiences. The Thread protocol specification is available at no cost, however, this requires agreement and continued adherence to an End-User License Agreement (EULA). This agreement states that "Membership in Thread Group is necessary to implement practice, and ship Thread technology and Thread Group specifications."

Thread uses 6LoWPAN, which, in turn, uses the IEEE 802.15.4 wireless protocol with mesh communication, as does Zigbee and other systems. However, Thread is IP-addressable, with cloud access and AES encryption. A BSD-licensed open-source implementation of Thread called "OpenThread," is available from and managed by Google.

8.2.8.1 Current Adoption in Hospitality

The Thread protocol is a new protocol that is just now being adopted by vendors. Therefore, the technology can co-exist with other IoT protocols, but as more vendors adopt the technology, more products will become available for deployment in hospitality.

8.2.8.2 Current Standards and Roadmap

In July 2014, the Thread Group alliance was formed as an industry group to develop, maintain, and drive the adoption of Thread as an industry networking standard for IoT applications. Thread Group certifies components and products to ensure adherence to the specification. Initial members were ARM Holdings, Big Ass Solutions, NXP Semiconductors/Freescale, Google-subsidiary Nest Labs, OSRAM, Samsung, Silicon Labs, Tyco International, Qualcomm, and the Yale Lock Company. In August 2018, Apple Inc. joined the group and released its first Thread product, the HomePod Mini, in late 2020.

8.2.8.3 Guest Adoption in Hospitality

With Thread being a new protocol, there are currently few IoT products that have deployed this technology. However, since Thread is a low-power and low-latency wireless mesh networking protocol built using open and proven technology, it will eventually become embedded in many of the IoT products currently on the market today. Once that migration happens, many guests will expect to have this protocol supported in hotels.

9. INDOOR CELLULAR AND 2-WAY WIRELESS SOLUTIONS

As mobile wireless devices have become nearly ubiquitous across all generations who are living and working in all parts of the country, indoor wireless service is no longer a luxury but a requirement. Commonly known as the "4th utility," indoor cellular service is a must-have for guests, employees, security personnel, and first responders.

Due to the incredible proliferation of mobile phones over the last decade, businesses and homeowners alike are choosing to eliminate expensive landline phone systems. Approximately 97% of Americans own a cellphone, and 80-90% of all cellular calls are made indoors. Even more critically, about 80% of all 911 emergency calls are made from cell phones.

Business calls, mobile data connections, social media, video conferences, and emergency service requests must be seamless, whether outside or indoors. As business travel is ramping up, there has been a massive boost in the requirement for mobile connectivity for remote work using cloud-based applications and messaging apps for communication. This dramatically increases hotel guests' demand for a more robust and stable connection. Whether guests are traveling for business, leisure, or both, wireless service is critical.

Hotel guests have become far more sensitive to connectivity, especially following the recent skyrocket of daily video calls. Guest comments and reviews about poor cellular coverage are becoming very common on travel review websites. Due to competition in the marketplace, hotel owners will need to adapt to meet guests' wireless connectivity requirements. In addition, many jurisdictions around the country are now incorporating new regulations that require a set minimum level of indoor coverage for first responders. In some areas, these requirements must already be met for the property owner to obtain or maintain a Certificate of Occupancy.

Wireless solutions also add incredible value to real estate by making guests and employees feel happier and safer while also allowing property owners and managers to justify increases in room rates or additional facility fees.

It is essential for a hotel to choose an experienced partner to perform the design, installation, and operation of a high-quality, cost-effective indoor wireless solution. This Third-Party Operator or "3PO" should assess current and future needs and design a solution that fits the property's requirements and budget.

Using a wide selection of equipment options, a solution can be tailored to meet each venue's and its occupants' specific criteria and needs. Many indoor voice and data solutions are available in today's expanding wireless industry including:

1. Cellular DAS – active or passive, coverage and capacity including 5G
    a. Voice calls
    b. Internet connectivity
        i. Video calls – Zoom, WebEx, GoToMeeting, FaceTime
        ii. Messaging
        iii. Business applications
        iv. Cloud services
        v. Email
        vi. Social media
2. Private LTE Networks/CBRS
    a. Security
    b. Privacy
3. Public Safety
    a. Currently required by law for new building construction in most cities and for existing

buildings in many jurisdictions (NFPA 72 & IFC requirements)

4. 2-Way Radios
    a. Fast and easy communications between employees and security throughout a property

9.1 CELLULAR DISTRIBUTED ANTENNA SYSTEM (DAS)

Mobile phone and tablet users inside buildings often experience inferior voice call quality, slow Internet connections, or the inability to make and receive phone calls or even access the Internet at all. These problems tend to result from a lack of "coverage" or "capacity."

Wireless radio signals have an extremely difficult time passing from an outdoor cellular tower through a structure's exterior walls and reflective low-E windows, resulting in inferior coverage inside the venue. Alternatively, a building may have good indoor coverage but could be located in a "high traffic" area with many users on the cellular network, both inside and outside of the building. In this case, the issue is one of network capacity. The average user cannot typically tell one issue from another, but both problems can be easily solved with a cellular distributed antenna system (DAS).

Numerous steps are involved in creating an indoor DAS:

- Complete detailed on-site survey and analysis – layout, structural, and radio frequency (RF) benchmarking
- Evaluation of specific requirements and expectations, both existing and long-term
- Creation or modification of venue floorplan in an electronic format
- Detailed iBwave RF design creation with coverage “heat maps” based on the site survey
- Full construction drawings of the equipment room and distributed wireless system throughout the venue
- Leasing and permitting
- Negotiations with wireless carriers
- Acquisition and installation of all wireless radio equipment, including headend, cabling, fiber optics, antennas, power systems, fire suppression, alarms, and monitoring systems
- System monitoring/NOC services
- Ongoing system maintenance

9.1.1 What is a DAS?

A distributed antenna system (DAS) is a network of antennas, cables, and radio equipment installed inside (and sometimes outside) a venue that significantly improves the quality of the wireless cellular services. In its basic form, a DAS has two primary components:

1. Signal Source – because a DAS does not generate a cellular signal, it must be fed a signal from the wireless carrier, typically an on-site BTS (Base Transceiver Station) or a Small Cell (miniature cell site).
2. Distribution System – the cellular signal from the signal source is amplified, distributed, and rebroadcasted throughout the venue using fiber optic cables, Ethernet cables, Coaxial cables, or a combination of these, finally reaching numerous antennas spread throughout the venue.

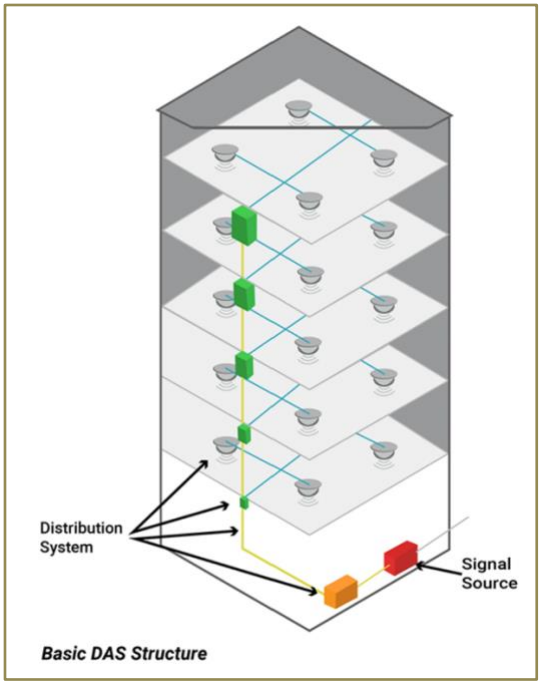


Figure 33

9.2 SIGNAL SOURCES

The Base Transceiver Station (BTS, or sometimes referred to as an eNodeB) is the fundamental radio equipment commonly used at outdoor cell phone towers to generate the cellular signal. The BTS is connected to a wireless service provider's primary or "core" network by fiber optic cables. A very large venue may have multiple BTSs feeding a DAS. This type of signal source is more robust than small cells, providing more power and capacity. Also, each wireless carrier (e.g. AT&T, Verizon, T-Mobile) will have a separate BTS feeding the DAS. A purpose-built wireless system designed to work with all current and future wireless carriers is commonly called a "Neutral Host" system.

Small cells (sometimes called femtocells, picocells, nanocells, or metrocells) connect to the carrier's core network over a standard, yet robust Internet connection. Small cells provide a high-quality wireless signal and are typically only used in smaller venues due to their somewhat limited power and capacity and are not easily scalable.

9.3 DISTRIBUTION SYSTEMS

There are Passive, Active, and Hybrid DAS topologies.

9.3.1 Passive DAS

In this scenario, the signal source is amplified at the DAS headend – the primary equipment at the “head end” or beginning point of the DAS – and then distributed throughout the venue through a series of splitters, couplers, and Coaxial cables to the individual antennas.This scenario is more affordable as it leaves the radio frequency (RF) signal in its original analog form but can only cover a limited area due to the natural attenuation or losses of the RF signal in the Coaxial cables.

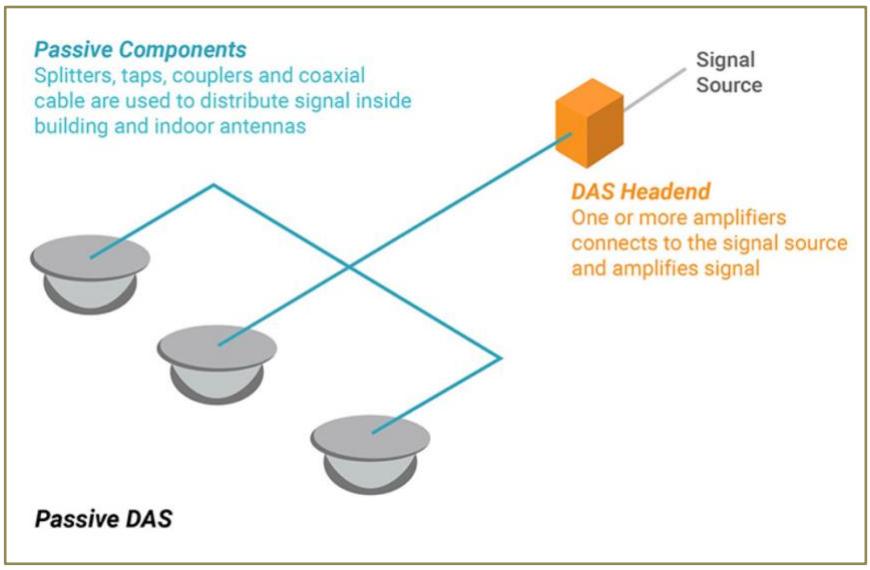


Figure 34

9.3.2 Active DAS

In an active DAS, the headend may combine multiple signal sources (usually from multiple carriers), convert them into digital signals, and then distribute those signals throughout the venue via Ethernet or fiber optic cables. These cables terminate at remote radio units (RRUs) or "nodes," which convert the digital signal back into analog RF signals. Depending on the manufacturer of the DAS equipment of the DAS equipment, the RF signals are then transmitted through the antennas attached directly to the RRUs (often referred to as "fiber-to-the-node") or may be distributed through short runs of Coax from the RRUs to the antennas.

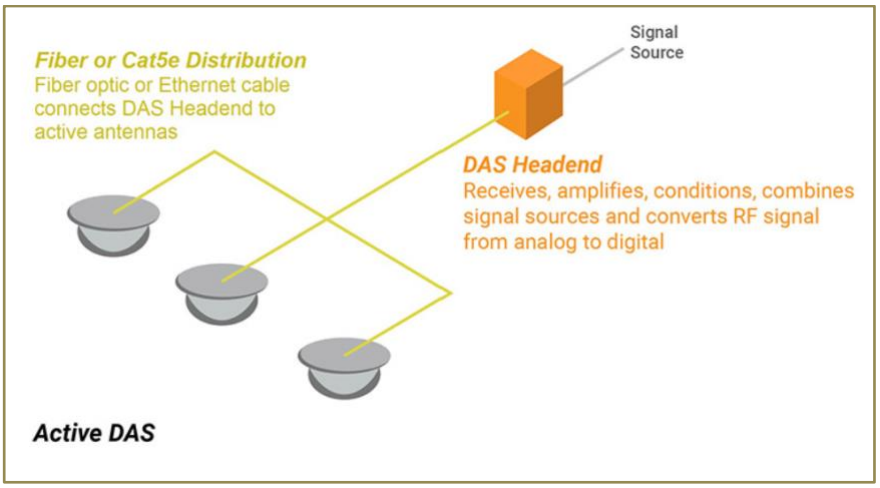


Figure 35

9.3.3 Hybrid DAS

This configuration combines elements of both the passive and the active DAS. By using a network of both fiber optic cables and Coaxial cables, the RRUs are separated from the antennas, and the number of remote units is reduced, which reduces the overall cost of the system. A hybrid DAS is far more robust than a passive DAS but less expensive than an active DAS. Simultaneously, this setup allows the DAS to cover large venues and it is easily scalable. Additional portions of the venue can even be added on future dates.

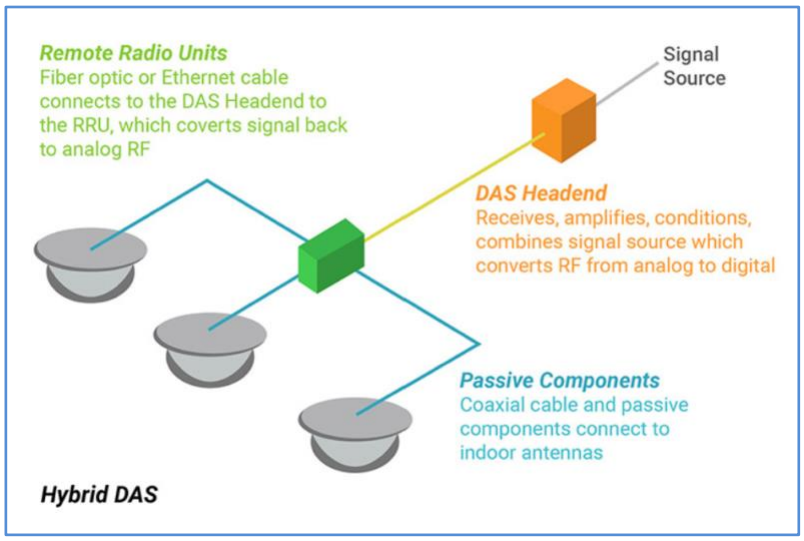


Figure 36

In a hybrid DAS, the headend combines multiple signal sources, converts them into digital signals, and distributes those signals throughout the venue by fiber optic cables to the RRUs, which in this case, are spread much further apart than in an active DAS. The RRUs convert the digital signal back into analog RF signals, which are then distributed in a particular defined portion of the venue through a series of splitters, couplers, combiners, and Coaxial cables to the individual antennas. One RRU may feed the antennas for one or two floors of a building, or some other defined area of a venue.

9.4 CELLULAR DAS VS. REPEATER

Alternative systems exist, often referred to as repeaters, boosters, bi-directional amplifiers (BDAs), or "off-air" DAS. These systems simply take the cellular signal from a nearby outdoor tower or small cell and retransmit that signal inside the venue. These systems are less expensive than a DAS; but still, they are typically only a temporary band-aid for cellular issues and often create other detrimental problems, such as signal interference. These solutions also cannot do anything to resolve capacity issues, a challenge when a system needs to provide a signal to many guests. Wireless carriers must approve the use of these systems through a re-transmission agreement (RTA), and often do not give such approval due to the possible interference issues and the capacity overloading of a nearby cell site.

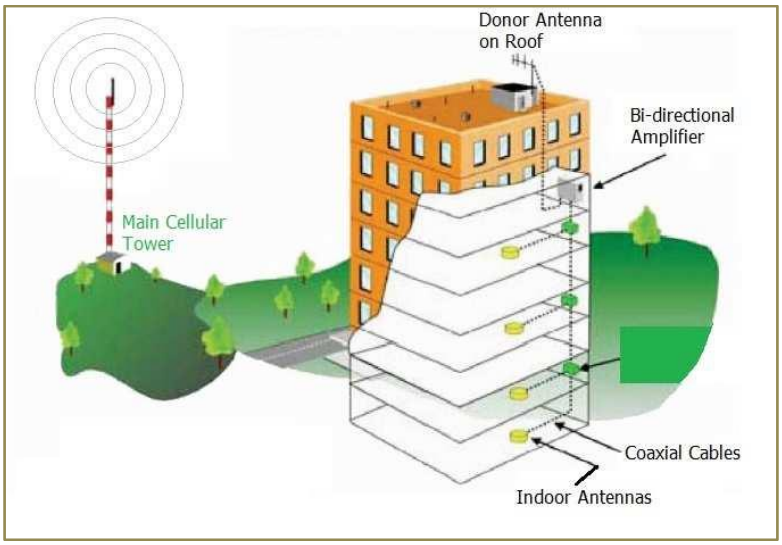


Figure 37

9.5 CELLULAR DAS VS. Wi-Fi

Many venue operators question why a DAS is needed if their property already has Wi-Fi. Ideally, Wi-Fi and cellular DAS are used together and complement each other. Wi-Fi is a relatively low-cost network; nearly all laptops and mobile phones can connect to a Wi-Fi network and take advantage of that Internet connectivity. However, for cellular subscribers, the first obvious advantage of the cellular network is that it is automatic and universal. The user never needs to open their Wi-Fi settings, search for the correct SSID, acquire and enter a password, or approve the connection, its legal fine print, and go through any other setup steps.

The seamless "invisible" access of cellular makes it the best choice for voice calls because users can call and be called no matter where they are. Wi-Fi can also be used for voice, often requiring shared applications such as Zoom, Teams, or a particular device platform. Wi-Fi calling also exists but frequently provides poor voice quality with choppy audio and periods of silence.

Next, cellular carriers operate on a licensed spectrum with exclusive rights to that spectrum, but Wi-Fi operates on an unlicensed spectrum available for anyone to use, which opens it up to potential interference. And while the latest Wi-Fi technology (Wi-Fi 6) can provide comparable data speeds and performance in normal situations, Wi-Fi systems can also suffer from congestion due to a lack of adequate bandwidth to serve the system's users, leading to low speeds and high latency. Cellular technology also has a greater range to cover larger spaces, operating primarily at frequencies much lower than Wi-Fi, which effectively travels further due to lower propagation losses.

Mobility is another feature that makes cellular especially well-suited to voice calling. Users' sessions are maintained as they move between areas ("handoff"), inside or outside a venue. Voice calls, streaming video, and streaming audio user experiences can be disrupted or entirely lost by Wi-Fi session interruptions.

Lastly, because of its longer range, mobility, and universal access, cellular is also the technology on which many first responders and all emergency services organizations (fire, police, ambulances) have transitioned their communications. Cellular DAS systems can provide this mandated connectivity via the FirstNet 700 MHz operated.

With the combination of cellular and Wi-Fi technologies, applications have more use at the edge, driving an edge computing strategy. This multi-RAN strategy allows software applications to integrate with devices and services across all wireless technologies to integrate into a single compute strategy.

9.6 PRIVATE LTE/5G NETWORKS / CBRS

As one of the most recent developments in wireless communications, Private LTE networks are privately owned and operated cellular networks, and properties worldwide are deploying them. A business typically uses them throughout its property to provide voice and data connectivity in conjunction with a Wi-Fi network. Wi-Fi provides sufficient wireless connectivity for small or medium-sized venues where users are primarily stationary, whereas Private LTE provides robust, high-capacity, highly secure, interference-free connectivity for larger venues and properties, with seamless handoff as users move from one area to another.

As a private network, only authorized users can access the network. While some venues limit access to only employees, others allow guests to access the network and provide seamless high-bandwidth wireless connectivity as they move throughout the property. Access to the network is only granted to a device by a physical or digitally assigned SIM rather than a password. The venue/network owner can also prioritize specific groups of devices (e.g., guests vs. employees) and even define which applications are provided a particular throughput, latency, and service level agreement (SLA). Private LTE networks are also less costly than traditional cellular DAS networks and can be deployed as a neutral host system, where users of multiple carriers can access the network.

Private LTE networks in the United States operate in the BCRS (Citizens Broadband Radio Service) 3.5 GHz band, also known as LTE band 48, and function nearly the same as cellular networks. Deployment can occur in two different ways:

1. Priority Access Licenses (PAL): licensed users who acquire spectrum licenses through an FCC auction or sublease.
2. General Authorized Access (GAA): a shared, no-cost, unlicensed spectrum where 80 MHz is always available. Any spectrum not used by PAL holders, or the protected incumbents can be used by GAA users.

Access to the channels is dynamic and controlled by dedicated spectrum-management services known as Spectrum Access Systems (SAS). All Private LTE systems must register with an FCC-certified SAS and obtain a channel grant or permission from the SAS before beginning transmission in the CBRS band. The SAS allocates spectrum to individual systems to prevent interference with incumbent systems and PAL license holders.

9.7 PUBLIC SAFETY

Indoor Public Safety coverage is quickly becoming legally mandated in countless areas nationwide. In some cities, an indoor public safety system is required to obtain a Certificate of Occupancy (CO) for newly constructed buildings or maintain the CO for buildings' requiring renewal. At a high level, the networks operate similarly to cellular networks.

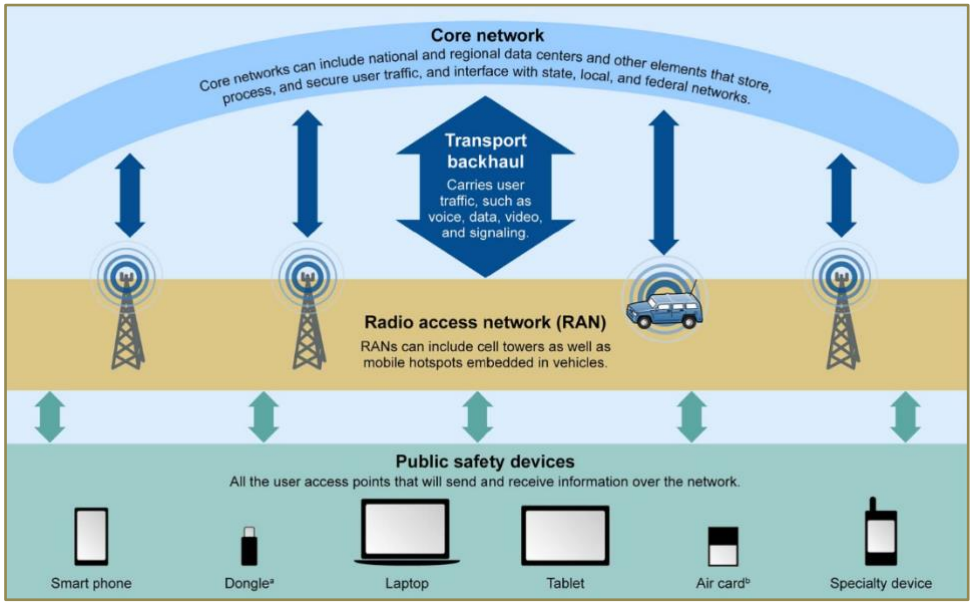


Figure 38

Two primary Public Safety systems exist:

1. Traditional Public Safety Communications – used by nearly all first responders such as fire, police, ambulatory services, homeland security, and disaster response. These are older technologies, and the spectrum is fragmented across a wide frequency band. Spectrum usage occurred as the FCC continued allocating new bands to meet growing demands since the 1930s.

Band	Frequency (MHz)	Mode(s)	Remarks
HF	25-30	TIA-603	
VHF	30-50	TIA-603	
	138-174	TIA-603, P25	
	220-222	Voice/Data (not TIA-603)	5 kHz
UHF	406-512	TIA-603, P25	
700 MHz	764-776	TIA-603, TIA-902, P25, 802.16(e)	RL
	794-806	TIA-603, TIA-902, P25, 802.16(e)	FL
800 MHz	806-817	TIA-603, P25	RL
	824-849	Cellular (many modes)	RL
	851-862	TIA-603, P25	FL
	869-894	Cellular (many modes)	FL
PCS	1850-1990	PCS (many modes)	
ISM	2400-2483	IEEE 802.11	
4.9 GHz	4940-4990	IEEE 802.11, VoIP, UMTS/ TDD	

Frequency bands and modes for public safety mobile radio communications. RL= Reverse link (mobile to base), FL= Forward link (base to mobile).

Figure 39

2. FirstNet 700 MHz system – created in a federal partnership between the FirstNet Authority and AT&T on what is known as Band-14. This system uses spectrum that is already deployed by AT&T for public cellular communications. When access is needed for first responders, the spectrum is automatically allocated only and specifically for use of first responder devices. This provides instant coverage and capacity for emergency responses, including both voice and data.

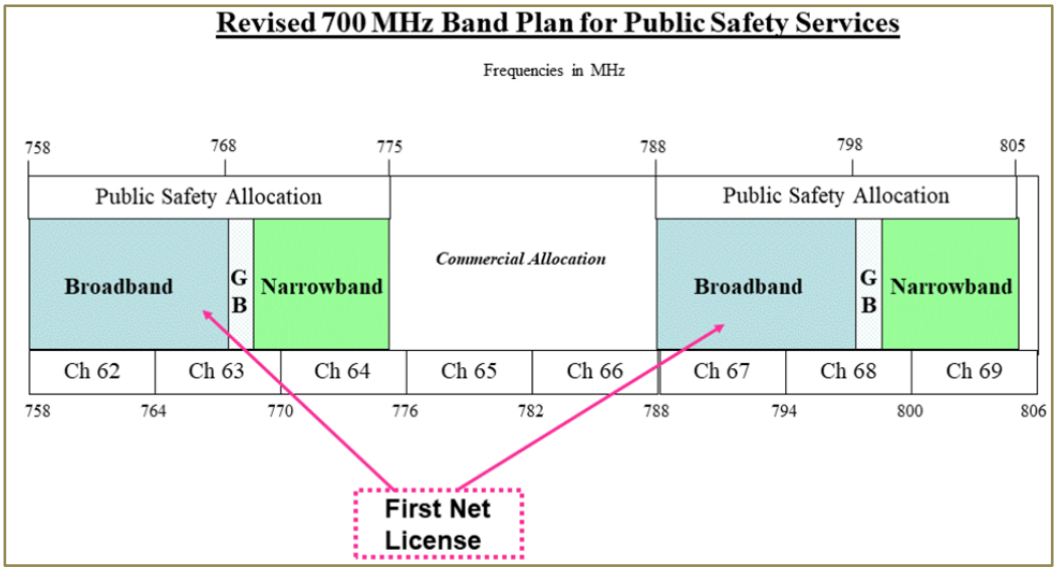


Figure 40

9.7.1 2-Way Radios

Hotels and other venues have used two-way radios for fast, simple communications throughout properties for many years. These systems quickly connect guest services, housekeeping, maintenance, security, valet, bell staff, and management at the click of a button. While there are several manufacturers, Motorola has historically led this space with their 400 MHz hand radios. These systems do not require towers, DAS, or other infrastructure to provide communication. They can even continue operating when there is a power outage as they are battery-powered and directly communicate device-to-device.

The most used two-way radios include:

- VHF (Very High Frequency) 136-174 MHz
  - Best suited for outdoor applications where maximum range is required with little to no obstructions and typically used for rural two-way radio systems
  - Typical industries include rural fire departments, agriculture, long-haul trucking, and field operations for energy companies
- UHF (Ultra High Frequency) 403-470 MHz
  - Best suited for indoor applications or environments with obstructions and typically used for city two-way radio systems
  - Typical industries include hotels, resorts, warehousing, manufacturing plants, and educational facilities
  - Note: UHF is the default indoor and outdoor frequency, and its versatility makes it the most common frequency band in use with approximately 80% of business radios.
- 900 MHz On-site
  - Best suited for organizations that need excellent in-building coverage
  - Typical industries include K-12 education, hotels, retail, and light manufacturing

9.7.2 Reference Documentation

Please refer to Section 2.4 for all reference documentation.

10. RECOMMENDED NETWORK INFRASTRUCTURE AND POTENTIAL LIMITATIONS

Every successful renovation or new build hotel, resort, casino, or support building project consists of the same basic approach – clearly defining a basis of design for the network infrastructure that meets the developer's financial goals and the operations team's technology applications. As mentioned earlier in this document, Property Type is a significant consideration when determining the optimal network infrastructure and supported technology solutions. Once the owner and project teams have clearly defined the work scope, they must ensure the infrastructure design meets both the present and future requirements that will arise over the typical twenty-year product life cycle of the physical network infrastructure.

New builds, major renovations, and technology refreshes all require specific attention to network design details. It is worth noting, however, that easily achievable goals for a new build "Greenfield" project may be challenging for a proposed renovation or "Brownfield" scope of work.

10.1 NEW BUILD, "GREENFIELD" PROJECTS

Planning for new build hotels or "Greenfield" projects must include a clear design for the following.

- Technology rooms (MDF/IDF), size, locations, and quantities
- Power requirements per technology room
- Space available for wall-mounted or rack-mounted solutions
- Pathways and infrastructure

Regardless of the type of converged network solution selected, it is important to understand next how the physical network will use the existing pathways and building infrastructure and any modifications required to support your project. This includes:

- Internet Service Provider (ISP) and Main Point of Entry (MPOE) room
- In Building pathways and infrastructure
  - Quantity, size, and type of conduits required between technology rooms
  - Core drill size or sleeves required between floors for new vertical cabling pathways
  - Horizontal cable trays out of technology rooms
  - Horizontal cable pathways down hallways or floors and associated support
- Outside Plant (OSP) pathways and infrastructure requirements
- Applications and port requirements per room type
- Applications and port requirements for BOH, hallway, and admin areas
- Applications and port requirements for all public guest areas, including meeting, conference, and fitness areas
- POE requirements per application and per room type to ensure the correct infrastructure and supporting technology rooms are sized appropriately
- CCTV, security systems, and associated cabling
- AV systems and associated low-voltage cabling

Typically, the architect and technology consultant will define all items above based on the geographic location, program space requirements, building levels, brand standards, and network applications supported. Your consultant must coordinate these items with the project architect in the early design stages to ensure the project covers all identified infrastructure requirements. Maximizing the network infrastructure will allow for the optimization of the planned spaces to support the technology systems with the least budgetary impacts to the owner.

10.2 RENOVATION, "BROWNFIELD" PROJECTS

The design team should leverage the "as built" diagrams, if existing, to accurately depict infrastructure design supporting the renovation scope of work, including the existing conditions that may need attention and the extent of the planned project. Like Greenfield projects, the pathway and infrastructure requirements must be determined to support the project. The property owner will have an existing Internet Service Provider (ISP) but will need to define the "In Building" and "Outside Plant" pathways and infrastructure based on the same requirements defined for a Greenfield project. Therefore, the project team needs to evaluate the existing infrastructure for re-use during the project carefully.

The converged Ethernet network can be achieved by upgrading the active gear at each end of the existing infrastructure. A typical example may include providing an Ethernet over Coax solution (such as DOCSIS, G.hn, or MoCA, described previously) over existing coaxial cable. The project team can utilize this solution to reach an area of the project with minimal construction effort and disruption.

Alternatively, the owner may decide to pull new cabling to the rooms, such as Traditional Converged Network or Fiber to the Room infrastructure. We recommend that a technology consultant provides any additional programming and planning to define the exact area that will receive the new network infrastructure cabling.

10.3 INFRASTRUCTURE CHOICES

Whether you have a new build "Greenfield," renovation "Brownfield," larger sprawling resort, high rise, midsize, limited service, or small boutique hotel, there are really three choices for converged network infrastructure covered in this document: Traditional Converged Network (usually a mix of category wiring and fiber), a Fiber to the Room, and the re-use of existing cabling (like coaxial cable) in a Brownfield scenario.

No matter which technology is selected, converged networks combine support for multimedia, telephony, and high-speed data on a single network. This type of network primarily serves large, complex organizations. The local IT resource may set up a Local Area Network (LAN) connection for the BOH application that is managed behind the same firewalls or sign-on credentials and isolated from any guest traffic. Registered users access Internet, Ethernet, Wi-Fi, and mobile connections through a dedicated network that supports email, VoIP, web browsing, text messaging, and more. Network convergence also allows large IT departments to apply firewall rules, automated anti-virus and malware scanning, and other security measures universally across all data connections.

10.3.1 Traditional Converged Network Infrastructure

The basis of design for a traditional network utilizes fiber backbone cables from the MDF/Server Room to the Technology Room (TR)/IDF, then provides horizontal category, copper cabling from the TR/IDF to the guest suites. A traditional configuration allows multiple network applications to be supported through core servers and distributed switches located in the MDF and IDF locations.

For example, a large, 350-unit, garden-style property could utilize this traditional network type. The design would show fiber running from a system of IT spaces, typically two IDFs per floor, with a copper infrastructure providing connections in each of the media panels in the suites. This infrastructure design can support enhanced amenities on the property, including a speak-easy bar, conference spaces, a club room, a social lounge, a two-story fitness center, and an outdoor pool. Copper cabling on the guest floors is an efficient solution to meet the bandwidth requirements for applications over a compact footprint.

10.3.2 Fiber to the Room (FTTR) Utilizing PON Technology

The second solution provides a Fiber to the Room design utilizing Passive Optical Networking (PON) technology, including a single mode fiber backbone cable from the MDF to Technology Room (TR) closets, then extends the fiber directly to Optical Network Transmitters (ONT) located near the Telecommunications Outlet device(s) in the guest suite. Typically, the fiber optical cable utilized in a PON solution does not have the same distance limitations as copper category cable. This advantage can

translate into a design with fewer TRs and smaller cable bundles if space is at a premium. In addition, single-mode fiber can handle 1Gb or 10Gb network connections utilized in today's networks but can scale up to 40Gb-100Gb in the future if ever needed.

A PON system consists of an Optical Line Terminal (OLT) typically installed in the MDF that connects several Optical Network Terminals (ONTs) using a passive Optical Distribution Network (ODN) located at the IDF/TR. PON is a point-to-multipoint access network. The main characteristic of PON is that it uses passive splitters in the fiber ODN. This allows a single feeding fiber from a PON port on the OLT to an optical splitter. Splitter size/split ratio can vary based on property type and design requirements. PON LAN offers significant capital and operational benefits. Utilizing a PON solution can extend the reach of the network beyond the usual 300 ft limitations of Ethernet over category wiring and deliver data/power (with the use of hybrid fiber cable and remote distributed DC power supplies) over 2,000 ft to enable hard-to-reach devices with limited local power and data drops.

For example, a 165-room luxury boutique hotel decided to utilize a PON solution to connect all their technology through a single platform. All the amenity spaces, guest rooms, restaurants, and entertainment spaces from the first floor to the top floor were connected. The designers built a fiber network to support innovative technology throughout the guest suites and amenity areas, including a wine room, market, on-site restaurant, members bar and club, pool, private dining areas, spa, luxury retail shopping, banquet halls, and fitness area with a new-age treatment center. Further, the hotel lobby is set up as a mixed-use space to accommodate arriving guests or attendees for a special event party.

The owner envisioned a "rock concert" level audio and video experience in the lobby, bar, and club areas. Guest suites are tech-heavy, with multiple displays and room devices, including the Presidential Suite with a built-in display in the bathroom. As you can see, a Fiber to the Edge infrastructure utilizing PON technology was the correct design for this luxury hotel to support the most demanding applications throughout the property.

Furthermore, it is common for projects to utilize a shared PON and traditional converged network. A hotel owner may provide a PON solution to the guestroom areas and a traditional converged network in the podium FOH/BOH spaces. The consultant will need to design special hubs, routers, and switches to connect wired, wireless, and other server-based networks. These flexible solutions are highly scalable and make adding new hardware and endpoints simple without interrupting the network and services. The downside is the complexity of managing a hybrid network and the need for IT professionals with knowledge of both sides.

10.3.3 Ethernet Over Coax in Existing Brownfield / Renovations

Utilizing an Ethernet over coax solution in an existing property to reduce the costs of pulling the latest category cables or single-mode fiber to each room may be the best solution. Pathways can be limited or non-existent and using cabling that is in place is the least invasive option to deliver a 1Gb – 10Gb network.

Like PON, Ethernet over Coax uses passive splitters (or low-attenuation taps) to bring a converged network infrastructure to each guest room cost-effectively. Another unique benefit of Ethernet over Coax solutions is that it can share the coax infrastructure with legacy (QAM) "free to guest" TV services and let the property determine when it needs to migrate to an IPTV service without any additional changes to the coaxial feed in the back of each TV inside the guest rooms.

For instance, a 500-room hotel was using an older DOCSIS 3.0 solution and was experiencing stability and performance issues. Faced with budget constraints, the property decided to leverage the G.hn technology to eliminate the existing CATV/DOCSIS amplifiers that were causing support concerns and deliver Gigabit speeds to each guest room along with a revamped IPTV service with casting and in-room Wi-Fi. In another similar instance, a brand selected a smart concierge application that had stability and reliability issues when using the existing corridor Wi-Fi coverage. It achieved nearly 100% uptime when it transitioned to an EoC wired connection in the back of the TV set.

10.3.4 Summary Technology Comparison

For a comparison of Traditional Category Cabling (Ethernet), FTTR (PON), and Ethernet over Coax (MOCA, DOCSIS, G.hn) capabilities, see Figure 41.

Network Infrastructure	Traditional	Fiber	Coax
Supports 1-10Gbps[1]	YES	YES	YES
Supports Long distance	Up to 100M	Up to 20km	800m
Cable Pathways and support	More cables	Less Cables	Typically reused in Brownfield (no change)
Reduces TR (IDF) space	NO	YES	No Change
In room POE output up to 71W	YES	YES	YES
IPTV / VOIP / HSIA Plus other IP based Technologies	YES	YES	YES
Broadband – Coaxial based TV (RF/QAM) ports	NO	YES	YES
Analog Phone	YES	YES	YES
Potential EMI (Electrical Magnetic Interference)	YES	NO	NO
Backhaul for Cellular DAS or Small Cell[2]	YES	YES	YES
Recommended Property Types	Limited Service, Midsize Hotels	Full-Service Convention / Resort Hotels	Brownfield properties

Figure 41

1 – Active Hardware per technology may be specific to 10Gb capabilities. Ensure that the infrastructure utilized can support 10Gb at all distances installed.

2 – Manufacturers of Cellular DAS or Small Cell solutions may have specific backhaul infrastructure requirements.

In summary, the infrastructure, whether traditional, Fiber to the Room (FTTR), or Ethernet over Coax, must support your network and dictate the effectiveness of your physical and network infrastructure.

It is this converged Ethernet network that supports the advancing technological needs of your business. A well-designed network optimizes your infrastructure and helps companies accommodate new hardware and increase data usage. It is important for businesses such as hotels to keep up with the rapidly growing bandwidth demand with more data applications being placed on their networks. The equipment supporting the hotel network must be dependable, easily adaptable to changes and network additions, and more.

11. APPLICATION NETWORK MAPPING

As noted throughout this document, the successful operation of a hotel requires many third-party-developed applications to be deployed in a hotel. The number of applications deployed will depend upon the size, location, and category of the hotel. For example, a limited-service hotel with 150 rooms would require fewer applications to be deployed than a conference or resort hotel. In addition, many applications in a hotel may not require access to the hotel's back-office network. For these applications, the security requirements of the specific brand will determine the networking requirements.

To satisfy many brand security requirements, past deployments of applications require dedicated networks for each application. That was proven costly, and with the deployment of a converged network using either VLANs or policy-based routing, most of the applications can co-exist in the deployment of a converged network.

11.1 APPLICATION CATEGORY DESCRIPTION

To better understand how various applications must be mapped to a hotel converged network, the table in Figure 42 below lists the application categories and the required mapping that must be implemented to satisfy most hotel security requirements.

Application Category	Example Applications	Cloud Outbound Connectivity	Back-Office Connectivity	Dedicated IP Segment Connection	Remote Management Connectivity
Networking (Outsourced)	Network Swtich, PON, Firewall	Y/N (Outsourced provider may or may not have cloud management of the devices, as a minimum, may require a VPN to the property	Y/N (Y, if outsourced provider is managing these devices, N, otherwise)	Y (in the case of a converged network, each of these devices will be required to be managed on a dedicated IP segment)	Y (Outsourced provider will require access to manage these devices)
Networking (Internal)	SD-Wan, Network Switch, PON, Firewall	Y/N (Cloud access will depend upon the application on and how it needs to be managed)	Y	Y	Y/N (Remote management may be required if the brand is managing the property centrally or with a local associate)

Telecommunications	PBX, Volcemail, Call Accounting	Y/N (Cloud access will depend upon the application and how it needs to be managed)	Y/N (Back-office connectivity may be required if the phone system is IP based. If not, then no back-office connectivity is required)	Y/N (The need for a dedicated IP segment will depend upon the application)	Y/N (The need for remote management will depend upon the application)
Facilities-Building	Door Lock System, Access Control, Elevators, Energy Management	Y/N (Cloud access will depend upon the application and how it needs to be managed)	N	Y	Y/N (Remote management will depend upon the application and how it needs to be managed)
Facilities-Guestroom (Outsourced)	Room Thermostats, Safes, IPTV, Mini bar	Y/N (Cloud access will depend upon the application and how it needs to be managed)	N	Y	Y/N (Remote management will depend upon the application and how it needs to be managed)
Facilities-Guestroom (Internal)	Room Thermostats, Safes, IPTV, Mini bar	Y/N (Cloud access will depend upon the application and how it needs to be managed)	Y/N (The need for back-office connectivity will depend on the requirement for an application to access PMS)	Y	N
Facilities-Back Office	Surveillance, Fire and Safety, Access Control	Y/N (Cloud access will depend upon the application and how it needs to be managed)	Y	Y	N

Operations (Outsourced)	PMS, POS, SPA, Golf	Y/N (Cloud access will depend upon the application and how it needs to be managed it)	Y/N (The need for back-office connectivity will depend on the requirement for an application to access PMS)	Y	Y/N (Remote management will depend upon the application and how it needs to be managed)
Operations (Internal)	PMS, POS, Reservations, File/Print Servers, PC and Mobile Device management	Y/N (Cloud access will depend upon the application and how it needs to be managed)	Y	Y/N (The need for a dedicated IP segment will depend upon the application)	Y/N (Remote management will depend upon the application and how it needs to be managed)

Figure 42: Application Network Mapping Requirements

Therefore, in reviewing the contents of Figure 42, the mapping of a specific application to a converged network will depend upon the operating characteristics of the application.

In summary, before implementation, each application will require a review of the following items:

- Connectivity requirements (what other applications or network segments does this application need to access)
- IP Subnet size
- VPN or cloud access requirements
- Specific security requirements that need to be satisfied (e.g. PCI, PII)
- Access to the Internet and bandwidth requirements

The actual mapping process for each deployed application will be performed by either a third-party MSP or a technical associate from the property or brand corporate associate.

12. IMPLEMENTATION REQUIREMENTS AND CONSIDERATIONS

While installing a new infrastructure to support wired or wireless networks or when upgrading/expanding an existing system, several considerations and recommendations may result in cost savings and prevent readjustments later on.

12.1 GENERAL CONSIDERATIONS

- Pull more fiber optic cabling than needed because materials are relatively inexpensive, while installation labor is quite expensive. The ultimate ownership of excess “dark” fiber (fiber that is installed between two different points but not connected or “lit” and therefore “dark”) should be clearly defined. After reserving enough fiber for future network upgrades or expansions, additional dark fiber could be designated for use by the hotel for unforeseen future systems and technologies.
  - A minimum of 25% more strands for future capacity between closets is typical.
  - Terminate and test all fibers between buildings or closets to ensure space is allocated and fiber is ready for the future.
- If remote powering with hybrid fiber is utilized, consider the gauge of the conductors from the power supply location (IDF) to the room. Identify what the total POE budget in the room is today and have some room to add more power in the future.
- Consider installing non-metallic electrical tubing (i.g. Smurg Tube) from the hallway to each of the guest rooms to allow easier access during future upgrades.
- Ensure that the correct cable type and associated jacket meet code requirements as referenced below in the Code Requirements section. For example, cables traversing through plenum space should be plenum-rated. Cables that are traversing through outdoor spaces or buried in conduit should be indoor-/outdoor- related per installation requirements, including temperature ratings based on location.
- Any outdoor cabling shall have adequate lightning/surge protection as required.
- If there are any planned venue remodels, expansion, or other construction projects, take these into consideration in the design of the network to allow for reconfigurations more easily as needed.

12.2 CONSIDERATIONS FOR MOBILE NETWORKS

- Allow network operators/installers to take advantage of existing cable trays, sleeves, conduits, and J-hooks where space is available. Adding additional cable passes in the future can be very costly, lengthen the installation timeline, and may cause more noise and interference with hotel operations.
- If cost-feasible, have DAS or Private LTE/5G provider design a higher node/antenna density to allow for future technologies at higher frequencies rather than adding additional nodes later, which requires another round of installation.
- Consider providing DAS and Private LTE/5G coverage in the overlooked areas for first responders and staff in emergency situations, such as a fire, flood, earthquake, or active shooter. These areas of concern may include elevators, back hallways, storage areas, loading docks, etc.
- Take advantage of existing venue generator backup power if available. Communication is generally considered critical, especially for first responders. If generator backup power is unavailable, install UPS units (uninterruptable power supplies/batteries) for all DAS and Private LTE/5G radios.
- The venue/Third Party Operator (3PO) DAS lease should clarify items such as DAS monitoring, maintenance, upgrades, and expansions. The 3PO typically retains ownership of the active equipment (radios, power supplies, etc.) at the end of the lease, while the venue generally takes ownership of all fiber and cabling.
- Where permitted and aesthetically acceptable, install permanent access panels/hatches to allow for future repairs and modifications. This will also prevent the need for future cutting and patching of drywall or other surfaces.
- While typically more costly, aesthetics can often be addressed with various methods such as the creative location of antennas, lower profile antennas, painting antennas to match surfaces (RF transparent paint required), and placing antennas behind RF transparent surfaces such as approved fiberglass shields.

12.3 DOCUMENTATION

Equally as important as installing the proper cable-infrastructure is the requirement to have the certified Structured Cable System (SCS) integrator provide the “Pre-Construction” and Post-Construction” Documentation for the project.

Pre-Construction documentation prepared by the awarded contractor should include:

- Shop drawings defining the intention of the infrastructure design
- Pull schedules detailing each fiber/copper cable’s origin, destination, and cable type with a unique numbering sequence with detailed information noting the building, technology room, rack/cabinet, patch panel, and port
- The proposed cable certification/testing procedures that are acceptable to the active system vendors/operators that will uphold a standard 20/25 product performance warranty after installation

Post-Construction documentation often referred to as “Close-Out” documents, typically include:

- Drawings that detail any adds, moves, or deleted infrastructure cable runs also noting the unique labeling identifications at all termination points
- Final pull schedules revised to show any adds/moves/deleted cable infrastructure
- Completed test results of all point-to-point infrastructure cables (bulk feed and horizontal cables)
- Project warranty/certification documents from the cable manufacturer(s)
- Relevant active product operation and equipment (O&E) manuals
- Any or all proposed maintenance and service agreements

All Pre-Construction project documentation should be provided by the Structured Cable Integrator through electronic media (i.e. Excel, CAD, PDF formats) to the owner/operator/consultant for review before installing the Structured Cable System. All Post-Construction project documentation should be provided by the Structured Cable Integrator through electronic media (i.e., Excel, CAD, PDF formats) to the owner/operator/consultant for review before the final acceptance and payment to the infrastructure contractor.

12.4 LABELING

All project labeling is to include a unique identification system provided to each fiber/copper infrastructure cable, Technology Room (TR), Rack/Cabinet, Patch Panel, Port, and Telecommunication Outlet (TO) for the installation, maintenance, and serviceability of all Structured Cable Systems (SCS). All infrastructure cables and passive SCS hardware labeling should be comprised of computer-generated media. Proper-sized "wrap around" cable labels will be provided at each end point of all copper and fiber cables. The unique label identification information provided on the wrap-around label should include the origin and destination of that cable. This information must also match the "Pull Schedule" and "As Built" drawing identification information so that the owner/operator/active system vendor can easily locate all cables at the appropriate TR closet and TO. In addition, all TRs, Racks/Cabinets, Patch Panels, Ports, and TOs should also include computer-generated labels that will permanently adhere to the face of each device. This information should clearly be visible and match the information provided in the "Pull Schedule" and "As Built" drawing documentation for easy cross-referencing by the owner, operator, and active system vendor(s).

12.5 CODE REQUIREMENTS

Before beginning the installation of any network infrastructure for your property, businesses must ensure that they are aware of governing code requirements and standards. BICSI standards specify best practices for structured cabling by providing guidance on installing telecommunications and information communication technology (ICT). BICSI standards give businesses guidance on installation practices that meet the National Electrical Code requirements (NEC) and the National Fire Protection Association code requirements (NFPA). A knowledgeable, experienced architect can consult the AHJ (Authority

Having Jurisdiction) to determine which code requirements apply to your property.

A knowledgeable installer will know the proper steps your business must take to ensure that the structured cabling installation meets all requirements. The owner must ensure that they choose a vendor to oversee the installation from day one properly. The vendor will understand building standards and best practices for your property type and location.

12.6 BRAND STANDARDS

Owners, operators, property managers, and vendors in the hospitality market must find a way to satisfy the ever-increasing demand for dependable, high-quality services. Guests at hotels and resort properties have high expectations for fast, secure, and reliable access to wired and wireless communication services. Robust and usually dedicated networks are also at the heart of hospitality operations, supporting critical resort and hotel management systems. Brand standards are a quick reference guide, providing direction and guidance to ensure your technology is consistent across the properties under the same flag. Setting standards on manufacturers for audiovisual, security, digital signage, telephony, Wi-Fi, high-speed data, and hospitality software services will help you determine the needs of your network for your technology and IoT services and guide your path to decide what is right for your business and your team. These requirements on your converged network form the basis of the blueprint for putting the pieces together in determining the proper physical and network infrastructure. A major brand will usually specify standards for the systems listed below:

- Horizontal and Backbone Copper Cabling – Category 6, 6A, 6E Cable
- Fiber Cabling – Bulk Feed Fiber Optic Cable, Fiber-to-the-Room
- Re-use of the Coaxial Cabling to the Guest Room
- Audio Visual Technology – TV Displays, Video Walls, Background Music, Teleconferencing Equipment
- Security – CCTV Cameras, Card Readers, Wireless Door Locks, Intercom, Vehicle Gates, Emergency Stations
- Distributed Antenna Systems – Emergency Responder Radio Communication System, Cellular DAS, Cellular Booster System
- IoT Technology – Smart Room (including Lighting, Thermostat, Window Shades, and In-Room Entertainment)

13. ONGOING SUPPORT CONSIDERATIONS

To provide ongoing support in a next-generation network, many of the same requirements remain from legacy deployments in terms of documentation, spares, and troubleshooting. The major differences are the consolidation of documentation, the ease of updating the information, and the simplification of Move/Add/Change and Onboarding/Offboarding of devices and users. These improvements not only make for less confusion and easier manageability but also increase efficiency and lower resource requirements to manage and maintain, allowing IT to focus on more important tasks than just the network. The following section will highlight the most important requirements to ensure that the next-generation network can be easily managed, monitored, supported, and utilized.

13.1 SOLUTION DOCUMENTATION REQUIREMENTS

Upon completion of a next-generation infrastructure deployment or any network deployment, it is best practice for the network integrator to provide complete documentation to the owner and/or network management company detailing the specifics of the network at that specific property. Hotel management teams and IT staff should implement change management processes to keep the documentation current and readily available for support and troubleshooting. The following items are suggested.

13.1.1 Project Design / As-Builts

Naming conventions, port assignments, and dial plan information may vary based on the type of infrastructure and applications leveraged by the network. What is important is that the nomenclature is consistent and identifiable and, in many instances, is site or brand-specific. This is a definable structure whose enforcement needs to be conveyed to and followed by the installing party.

- Naming convention/list of rooms/floors/IDF
- Port assignments/VLAN information/policy assignments
- Analog phone port assignments and room extension list
- Dial plan information

13.1.2 Project Design / Topology

Design and topology documentation requirements do change when deploying a next-generation infrastructure. It is best to ensure that all devices are shown on the topology diagram explaining physical connection points such as uplinks, cable type(s), key equipment, and logical and configuration information such as VLANs or policy assignments. This will allow quicker and more efficient troubleshooting and change management. This process should be automated using modern network software tools and kept current over time. Special detailed attention should be given to documenting critical equipment related to regulatory compliance, such as PCI/credit card security.

13.1.3 Project BOM / Material List

A project Bill Of Materials (BOM) lists all network components required for the project. BOMs should include the manufacture, model, and quantities of all equipment in use.

13.1.3.1 Spares List

Having spare equipment on-site is common between Active Ethernet, G.hn, and PON systems to limit downtime of critical services. As the size, complexity, and level of business risk increases for any hotel, so does the need for on-site spare equipment to minimize downtime and financial impact. In most cases, a site should have at least one spare of the most capable critical device. For example, if a site has 24 and 48-port switches and a mix of POE and NON-POE, it should have a 48-port POE switch on hand as a spare, as it can replace any other model. This same logic applies to APs, OLTs, OLT Cards, ONTs, G.hn endpoints, and required power supplies. A site should also have a mix of the required connectivity

components, such as SFPs, taps, splitters, patch cables, and jumpers.

13.1.3.1.1 Active Ethernet

AE Switching systems require power supplies, Optical Transceivers (SFP, SFP+, XFP, GBIC, etc. - both 1Gb and 10Gb), patch cords (fiber and category cable), PoE power injectors (in some cases), jack plates and the in-room AE switches. Replacement AE switches may have some configuration on them. Still, they will typically require additional configuration to be placed in service, which should be easily deployable via a template in the cloud.

13.1.3.1.2 PON

PON systems have the spares listed below, but a big difference is that replacing the parts requires little to no configuration and is capable of being done locally. The PON infrastructure standards define single-mode fiber with SC/APC connectors on the ONT and may vary between LC and SC connectors in the IDF/MDF locations. The OLT fiber connector is a single-mode fiber with SC/UPC connectors. This is much simpler than figuring out which fiber type was pulled to intermediate closets in the infrastructure and which type of SFPs were used as required in the active Ethernet environment.

13.1.3.1.3 G.hn

G.hn systems are very much like Active Ethernet Switches with the difference that they operate over existing coaxial cabling (Point-to-point and Point-to-multipoint) or telephone pairs (Point-to-point) to deliver Gigabit Ethernet speeds. A G.hn Access Multiplexer (GAM) plays the same role as an AE Switch and typically offers 1 or 2 SFP+ cages for uplink connectivity. These SFP+ ports usually support the same MSA-compliant SFP/SFP+ used to uplink AE Switches.

Like a PON system, a G.hn link terminates into a G.hn Endpoint (EP) device, usually located in a guest room. An EP will have one or more Gigabit Ethernet ports, some of which can offer a POE+ (30W) feed to power Wi-Fi APs, IP Phones, and similar devices.

13.1.4 SNMP MIBs

Manufacturer Installation Guides (MIBs) include manufacturer materials such as manufacturer SNMP MIB files and Installation Guides for monitoring.

All systems should follow the IETF standard interface and system MIBs, and there should be no additional proprietary MIBs to install unless the system provides non-standard information. As for all equipment types, there is typically an SNMP Trap MIB which may or may not be included for the systems in various SNMP manager software implementations. For each SNMP manager software implementation, the included MIBs, the method for loading MIBs, and the general requirements and operation of the system may differ. They will require expertise in applying to the correct parameters.

13.1.5 Manufacturer REST API Info

A REST API is simply a programmatic interface into a system. It supports common methods such as POST, GET, and DELETE but does not specify the underlying system names, classes, or functionality. REST APIs are a step in the SDN direction but are vendor-specific and do not guarantee easier operation within a network. For monitoring purposes, SNMP provides the same information. Either the vendor's controller or a customized controller is required for control.

13.1.6 Cable Testing Results

- All Ethernet and optical fiber runs should be tested and documented to establish baseline parameters for later use as a reference.
  - Utilize cable manufacturer guidelines for testing to help with warranty certifications

- All Coax or telephone pairs used for G.hn should be tested and documented to establish baseline parameters for later use as a reference
  - Use a DSL or CATV tester to test the existing wiring prior to the installation of the G.hn equipment
  - G.hn GAM devices usually have a built-in Spectrum Analyzer tool that can be used to collect noise and SNR info when the G.hn network is up and running

13.1.7 Warranty Documentation

Warranties for all equipment should be gathered and stored as part of the day two handoff deliverable. The purchase date and length of warranty should be included in this package.

13.1.8 Contact Information

Integrator and/or manufacturer contact information should be available for support and troubleshooting. Phone numbers, email addresses, and websites for the sales, engineering, and technical support teams should be included if possible. Any support escalation path documentation should also be made easily accessible.

13.2 TROUBLESHOOTING

With a next-generation infrastructure system, it is important to understand what type of technology is deployed. For example, does the property have an Active Ethernet, G.hn, or PON solution? In either case, specific high-level steps can be taken to identify the root cause. With either technology, it may be required to troubleshoot the physical network, which likely requires on-site discovery and remediation. Remote troubleshooting and correcting issues with the logical configuration of the network is likely to occur as changes are made to the applications and services are upgraded and changed over time. It is critical to define roles and implement a robust strategy for troubleshooting all the components of the network as well as a comprehensive delivery of on-site and remote troubleshooting scenarios. This is typically accomplished via service-level agreements with the network managed service provider (MSPs), corporate brand IT resources, local IT staff, or any combination. In addition to troubleshooting, change management should be defined similarly.

NOTE: we recommend using a central security setup such as RADIUS or TACACS+ authentication servers instead of locally administered accounts for network equipment. This suggests higher security and logging of all commands and actions applied to network devices.

13.3 MOVES / ADDITIONS / CHANGES (MAC) FOR POTENTIAL PERFORMANCE IMPACT

This section contains a high-level summary of possible moves, additions, or changes that may result in a connectivity outage if not performed correctly. Before making wholesale changes to the network, it may be best practice to set up a testbed to validate system updates before rolling out to the entire property. This could be done for one location or one room.

Although this list is not comprehensive, the following examples provide common suggestions for equipment modifications:

- The addition of new ports for new devices
  - To ensure security, the ports should be documented and updated on the As-Built and should be approved via a change management form
- The need for a new service with new drops
  - Depending on the amount of work, an installer may be subcontracted to do the job. If it is a hardware swap only, MSP may self-perform this
- Adding VLANs or new functionality
- A specific event or customer that requires new VLANs
  - New SSIDs (for example, customer ABC wants a new SSID called *ABC_CoWIFI*)

  - Local networking between rooms
  - Dynamic VLAN assignments through 802.1x (enabling this could vary based on manufacturer)
- Removal of ports or disconnecting services (for example, an office move)
- System software updates to layer two networks
- Application software updates connected to layer two networks

If a network is to be implemented using Zero Trust Network Architecture (ZTNA), there are additional considerations to be aware of. While ZTNA can offer a better security posture, planning and implementation requirements will likely be more robust. The minimum requirements for a ZTNA implementation are:

- Strong documentation on network topology
- Granular and descriptive roles for devices and users
- Proper documentation of roles and policies to ensure application and assist in troubleshooting
- A well-defined MAC management process and MAC request workflow to ensure proper policy assignment and approval
- A final process to document the addition after the MAC is completed and tested
- A monthly or quarterly policy and device and user audit to ensure compliance

In summary, although the above list of possible changes may result in an outage, there are other possible configuration changes that may also result in an outage. It is recommended that the hotel's support organization installs a test environment that allows moves, additions, and transformations to be tested before implementation into the operational environment.

For more specific details on Day 2 Support for converged networks, please reference the following document at this link: Fiber to the Room Day 2 Support.

14. APPENDIX

14.1 GLOSSARY

Please reference the HTNG Universal Glossary online.

14.2 REFERENCE DOCUMENTATION

MasterFormat®
2018 Edition
Master List of Numbers and Titles for the Construction Industry Contents reflect current MasterFormat titles and numbers as of May 2018. Consult masterformat.com for additional information about MasterFormat. © 2018 The Construction Specifications Institute, Inc. (CSI)
Reproduced by Construction Specifications Canada (CSC) under license from CSI.
CSI reserves all copyrights in this publication and all rights in the MASTERFORMAT trademark. You may not, without obtaining. CSI's prior written permission, copy, distribute, create derivative works from, or practice any of the copyrights in all or any part of this publication, or use the MASTERFORMAT trademark. If you want to use the MasterFormat® numbers and titles in commercial applications, educational programs, or publications, please contact CSI at csi@csinet.org to obtain a copyright license.

14.3 HOTEL SYSTEMS AND APPLICATIONS TABLE

System Type	Hardware/Application Type
Networking	Passive Optical Network (PON)
	G.HN (Coax)
	Firewall
	SD-WAN
	Network Switch
	HSIA Gateway
	Wireless Controller
	Wireless Access Points
Telecommunications	PBX Server
	VOIP Phone
	Voicemail
	Call Accounting
	Wireless VOIP Phone
	Voice Control
Facilities - Building	Door Lock System
	Access Control
	Building Management System
	Capacity Management
	Elevator/ Escalator
	Parking System

	Lighting Server
	Lighting
	Energy Management
	Digital Signage
	Digital Artwork
	Uniform Distribution
	CCTV Server
	CCTV Camera
	ATM
	Personal Safety/Employee Duress
	UPS
	Audio/Visual
	Fitness Equipment
Facilities - Guestroom	Room Thermostats
	Safes
	IPTV
	Video on Demand
	Casting
	Streaming Devices
	Tablet Compendiums
	Blinds/Shades Control
Operations	Server - PMS
	Server - Interface
	Server - POS
	Server - POS Payment Gateways
	Server - Reservations
	Server - Spa
	Server - Golf
	Server - Recreation
	Server - File / Print
	Server - Backup
	Server - 3rd Party Systems
	Workstation - Employee Signage
	Workstation - Employee Desktop
	Workstation - Employee Laptop
	Workstation - Guest Use/Business Center

	Mobile Device - Tablets
	Mobile Device - Handheld Devices
	Mobile Device - Communication/ Radio Replacements
	Self-Service Kiosk - Check-In/Out
	Self-Service Kiosk - Key Dispenser
	Self-Service Kiosk - Parking
	Printers
	Multifunction Printer
	Workstation - POS Terminal
	Workstation - Wireless POS Terminals
	Self-Service Kiosk - Ordering
	Self-Service Kiosk - Cashier
	Self-Service - Vending Machines
	Self-Service - Beverage Dispensing
	Printer - POS Printers
	Credit Card Terminals
	Timeclock
	KeyWatcher/Security
	Cashier/Change Machine