MOVING
HOSPITALITY
FORWARD

INTERNET OF THINGS (IOT): PROTOCOLS WHITE PAPER

11 December 2020

Version 1

About HTNG

Hospitality Technology Next Generation (HTNG) is a non-profit association with 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 hotel community, articulating the technology requirements of hotel companies of all sizes to the vendor community. HTNG facilitate 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.

Manufacturers and software providers shall not claim compliance with portions of the requirements of any HTNG specification or standard, and shall not use the HTNG name or the name of the specification or standard in any statements about their respective product(s) unless the product(s) is (are) certified as compliant to the specification or standard.

Permission is granted for implementers to use the names, labels, etc. contained within the specification. The intent of publication of the specification is to encourage implementations of the specification.

This specification has not been verified for avoidance of possible third-party proprietary rights. In implementing this specification, usual procedures to ensure the respect of possible third-party intellectual property rights should be followed. Visit http://htng.org/ip-claims to view third-party claims that have been disclosed to HTNG. HTNG offers no opinion as to whether claims listed on this site may apply to portions of this specification.

The names Hospitality Technology Next Generation and HTNG, and logos depicting these names, are trademarks of Hospitality Technology Next Generation. Permission is granted for implementers to use the aforementioned names in technical documentation for the purpose of acknowledging the copyright and including the notice required above. All other use of the aforementioned names and logos requires the permission of Hospitality Technology Next Generation, either in written form or as explicitly permitted for the organization’s members through the current terms and conditions of membership.

TABLE OF CONTENTS

1 Executive Summary

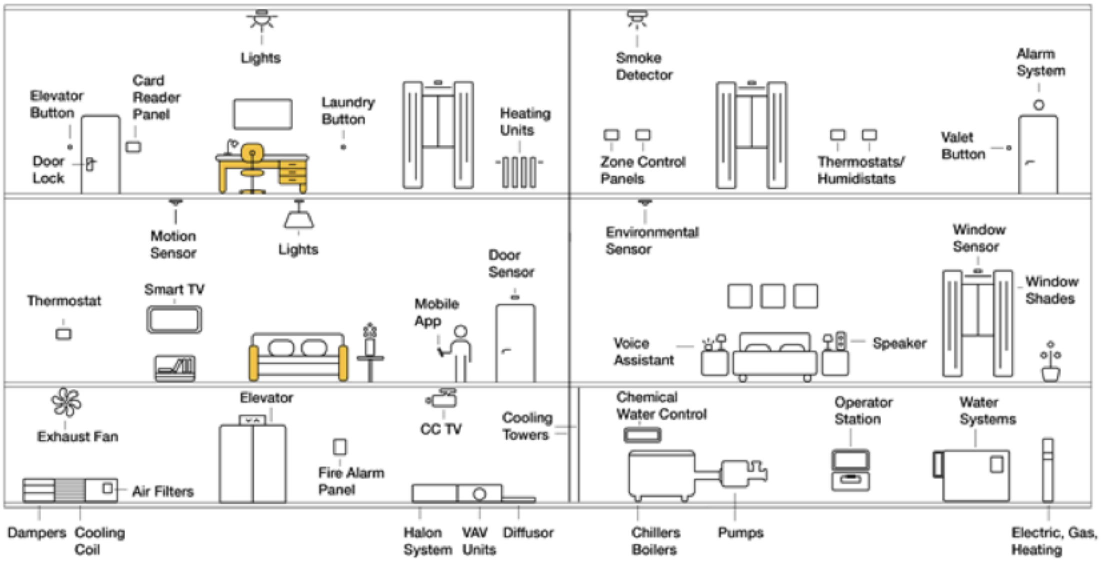
The Internet of Things (IoT) is the collection of electronic components and devices that can be connected via Internet protocols to create a holistic ecosystem. These IoT devices typically provide a combination of computing, sensing and controlling capabilities. Examples of IoT devices include “smart” light bulbs, thermostats, printers, TVs, door locks and cameras.

The many systems and sub-systems that operate within a hotel, and especially within the guest room, make the hospitality industry a prime candidate for IoT. Additionally, guest expectations around technology tend to match their experience at home (and to some extent, at work) – and IoT in the workplace and home is maturing at a rapid pace.

The Internet of Things encompasses a huge range of industries and use cases that scale from a single device to cross-platform deployments made up of hundreds of devices. This may include premise-based technologies and cloud systems connecting to each other in real-time.

Tying it all together are numerous legacy and emerging communication protocols that allow devices and servers to talk to each other in new, more interconnected ways.

As all of these factors have direct bearing on the application of IoT to a hotel environment, this paper will provide background information required by hotel decision makers to make selections around design, selection, implementation and operation of property-level IoT infrastructure and networks. This paper will outline the questions decision makers should be asking and some of the answers they should expect when seeking guidance from technical personnel. For readers seeking a baseline understanding of IoT principles, please consult HTNG’s IoT Workgroup’s “How Hospitality can win with IoT” resource.



2 IoT in the Hotel Environment

The most common usages for IoT in the hotel environment typically fall into three categories: facility management, security and Guest-facing. Typically, IoT used for facility management has the job of efficiently managing the resources required to operate a facility.

Examples of IoT used for facility management include:

- **Thermostats** - controls temperatures in guest rooms and public spaces
- **Environmental Controls (HVAC)** - manage temperature, humidity, air-quality and airflow through the facility
- **Presence Sensors** - monitors for human presence in rooms so lights and air conditioning can be adjusted for guest comfort and energy savings
- **Smart Lighting** - controls external lighting and lighting in guest rooms and public areas for mood, safety and energy savings

Guests interact directly with guest-facing IoT devices. These interactions allow the guest to adjust various settings to make their environment more comfortable. Some IoT devices provide entertainment or information access functions. Many guest facing functions are tied to guest occupancy, with the facility controlling the room when it is empty and the guest controlling the settings when the room is occupied.

There is significant potential for the application of IoT to the hotel environment with respect to guest-facing technologies. The guest as a “user” of the environment in a hotel room changes frequently, and each new user likely has some change in preference regarding the atmosphere, lighting or other controls. Some typical examples of guest-facing IoT devices include:

- **Voice Assistant** - used for general information access and entertainment as well as a means to communicate and make requests known to the hotel staff
- **Television Set Top Box (STB)** - used to control the in-room television and connect with guest devices
- **Thermostat** - gives the guest control of the room temperature settings while the room is occupied
- **Smart Lighting** - provides brightness and color control of the room lighting while the room is occupied
- **Blinds\Curtains** - provides automation for curtains and blinds while the room is occupied
- **Printers in the hotel's business center** - used by guests to print boarding passes, work documents and more

The modern guest is technologically savvy (perhaps even dependent) and expects the same interaction with and control of their environment as they have at home in their day-to-day lives.

Security and safety are another hotel concern that IoT helps to address. Some examples include:

- **IT Cameras** - on property security cameras are better than the older CATV cameras and the video can be controlled remotely and stored online
- **Staff Alert Devices** - allow staff to call out for help when in a dangerous situation
- **Door Locks** - used to monitor and control entry and exit from rooms and public areas such as pools and gyms by both guests and staff
- **Emergency Signs and Lighting** - can provide automated testing and more effective notifications during emergencies

Other devices that are important but have not previously been covered include:

- **Digital Signage** - used throughout the hotel to direct guests and inform them about activities

- **Network infrastructure** - used to provide network services to the hotel business and the guests

Nearly all modern technologies available today are IoT enabled. Every new build and upgrade should include consideration for fit into the property’s current and/or future IoT strategy.

The business challenge hoteliers face is knowing when and how to implement an IoT solution that meets or exceeds guest expectations and/or adds operational efficiency for the hotel.

3 OSI Model

The Internet of Things (IoT) is a collection of devices that connect and communicate through networks using the collection of protocols used by the Internet. The Open System Interconnection (OSI) Model is a conceptual model used to describe network communications abstractly without the need to describe the underlying technologies. The "Internet" is an interconnection of many networks that typically share a common set of protocols for layers 3-7 in the OSI Model; these protocols are collectively known as "Internet protocols." The seven-layer OSI model is represented in the table below with mappings to common Internet protocols.

OSI Layer	Description	Internet Examples
1: Physical	The hardware, wiring or medium that the signal carrying data travels through	Ethernet, Wi-Fi, Bluetooth
2: Datalink	The signals used to carry the data through the medium from point to point	
3: Network	Provides packet routing, fragmentation and reassembly	IPv4, IPv6, IPSec, ICMP
4: Transport	Provides quality, flow and error control, and establishes connections	TCP, UDP
5: Session	Establishes sessions to maintain connections for reliable communication between computers	TCP, Sockets, RTP
6: Presentation	Provides context to application layer and supports compression, encryption and transformation	MIME, TLS, MPEG, MIDI, GZIP
7: Application	Enables network services to allow interactions with applications	HTTP, FTP, SMTP, MQTT, XMPP

**NOTE: Some protocols span multiple OSI layers; Ethernet, Wi-Fi and Bluetooth protocols span both layers 1 and 2, and TCP spans both layers 4 and 5.*

The things that participate in the Internet of Things all communicate over a network. Specifically, by definition, IoT devices must be able to communicate using a specific set of protocols known collectively as the Internet Protocols with the base being provided by the "Internet Protocol," which is typically referred to as the IP.

The IP protocols IPv4 and IPv6 appear in layer 3; the network layer of the OSI model. IPv4 is the older version of the IP protocol, still widely supported but limited to 32 bits for addresses. The public IPv4 address space has been exhausted and the world has started to move to the newer IPv6 version of the protocol which provides 128 bits of address space. This is enough address space to support the expected needs of the Internet for thousands of years.

It is common practice to use IPv4 inside a local area network (LAN), but use IPv6 when traversing the Internet using some form of network address translator. Limitations in many IoT devices may require a translator if they are incapable of being configured to use IPv6.

3.1 Network Infrastructure Components

A number of devices are used to provide the infrastructure required to create a network and make it accessible and securable. In this section we describe the most common components of a network and how they might typically be used in an IoT environment.

Access Point

An access point provides a wireless endpoint allowing devices to connect to one or more devices on the wireless network. Typically, the access point will provide access to a router or gateway allowing the device to access resources available on the wider network. A wireless network can also be used for connections between devices.

Bridge

A bridge is typically used to connect two networks that are logically or physically separate from each other. Bridges send network packets between the bridged networks to combine two networks and allow them to act as one. Most current bridging technologies work at layer 2, the datalink layer of the OSI model.

Firewall

A firewall is a network control system that determines what network traffic is allowed to cross the firewall based on a set of rules. Packet filtering firewalls may work on OSI Layer 3: Network or Level 4: Transport Layer. Application layer firewalls work on specific application layer (OSI Layer 7) protocols. Most modern Linux and Windows systems have a firewall built into the operating system. Most home and SOHO routers include a firewall as an integral part of their gateway function.

Gateway

A network gateway provides interoperability between a network and other networks behind the gateway. Unlike a bridge which simply connects the two networks, a gateway may also provide services such as protocol translation, firewall and connections between different physical layers. An IoT gateway provides the bridging between an IoT device network and cloud or Internet networks. Gateways may operate at any of the OSI layers.

Hub

A network hub connects multiple Ethernet network segments together to form a single network. Most hubs work at the physical layer, layer 1 of the OSI model. The hub repeats data received on any port to all other ports on the hub. Most hubs have become obsolete and replaced by network switches.

Repeater

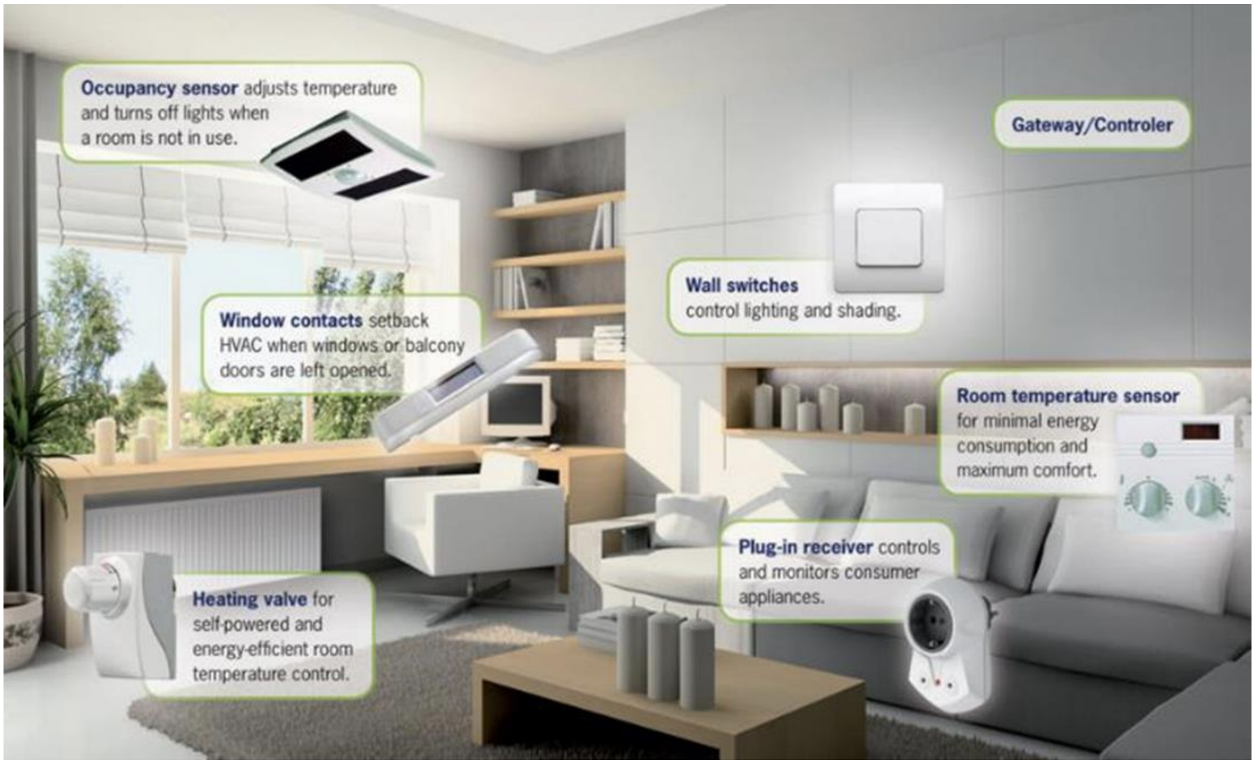
A repeater simply repeats any incoming signal as an outgoing signal for the purpose of increasing the distance a signal can propagate. As a signal travels through a medium-like wire, optical fiber or over the air, the signal weakens the further it travels. The repeater relays incoming signal boosting it so the signal can travel a longer distance. This extends the distance that a signal can be carried over the air, wire or fiber. Repeaters typically are physical layer (OSI layer 1 devices).

Router

Routers are the network devices that forward data packets through the networks and Internet. When a packet is sent by an IoT device or a computer, the packet is typically sent to a gateway router. Each router has a routing table maintained internally that tells the router where to send the packet so it will eventually reach its intended destination. Most routers intended for home and small office networks also provide gateway and firewall services as well.

Switch

A switch is a packet switching device that forwards data to the appropriate destination based on the MAC addresses (Media Access Control addresses). Switches are typically Ethernet devices that work at OSI layer 2: Datalink, however, some switches are designed with lightweight routing features allowing them to work in layer 3, the Network layer, of the OSI model. In some networks layer 3 switches may be useful to provide better network isolation through VLANs, in turn allowing the IoT devices to be segmented apart from the rest of the network.


Occupancy sensor adjusts temperature and turns off lights when a room is not in use.
Gateway/Controler
Wall switches control lighting and shading.
Window contacts setback HVAC when windows or balcony doors are left opened.
Room temperature sensor for minimal energy consumption and maximum comfort.
Plug-in receiver controls and monitors consumer appliances.
Heating valve for self-powered and energy-efficient room temperature control.

4 Physical and Data Link Layer Protocols

The criteria for selection and deployment of IoT devices and networks varies widely between consumer and commercial markets. Commercial environments require far greater planning and coordination of product selection and deployment. But in some ways, application of IoT in guest rooms is akin to an orchestrated, massive consumer level implementation, replicated many tens, hundreds or thousands of times in one installation (each guest room). Hoteliers must consider both consumer (guest expectation level) and commercial (overall system, infrastructure, network and compatibility) factors into their IoT implementation strategy and decisions.

Key to these decisions are the following factors:

- Business problem to be addressed
- Compatibility of devices with the overall design and supporting network
- Security, both the physical IoT devices and the underlying network
- Scalability of the supporting network
- Communication standards
- Integration capabilities
- Quantity and cost of devices
- Ease and cost of implementation

Consumers typically purchase individual products, each designed to perform a singular action. Whether lights, door locks, thermostats, video screens, voice speakers or other devices, consumers aren't concerned about the underlying protocol(s) used for communication whether the device relies on Wi-Fi, Zigbee, Z-Wave, Bluetooth, or any other emerging standard. This limited scale of deployment removes a large number of complexities that are central to commercial deployments.

The need to physically secure devices is unique to commercial environments and must be considered when designing the network to ensure optimal performance of the devices. Legal ramifications of an inadequately secured solution at the commercial level are vast in comparison to a consumer's responsibility for securing – or not securing – their home IoT system. For more information, reference HTNG's IoT Security White Paper.

Lastly, commercial environments require protocol standardization to limit the number of integration hubs required on the network, which in turn can simplify the network's design and therefore help control cost. This integration and cross-device compatibility requirement explains why the majority of IoT technology providers have standardized the same communication technology within the hospitality environment in order to ease integration and reduce the need for redundant network infrastructure updates.

Protocols in play for hospitality, including a brief description of their specific technology as well as their ease of use, compatibility with the network, interoperability, cost and overall fit are listed in the next section.

5 Wireless Protocols

Wireless protocols work in the physical layer, layer 1, of the OSI model. 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 to the other devices on the wireless network. Most wireless connections and all of the protocols covered here use radio waves as the medium that carries the signal. Some devices may use light, such as laser or infrared, 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 NFC (Near Field Communications) is technically a wireless protocol, it is not an Internet protocol and its range is too short to be useful in an IoT world - except when paired with another device - so it is not covered in this document.

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

5.1 Spectrum Planning

Wireless spectrum management and planning has become increasingly important due to the rapid growing number of spectrum uses. Physical layer protocols such as Wi-Fi, Bluetooth and Zigbee can compete for the same frequencies, along with non-network wireless devices such as microwave ovens, cordless phones and mobile radios. The following best practices will help ensure wireless IoT deployments co-exhibit harmoniously with other wireless devices:

1. Conduct wireless site surveys before deploying new network infrastructure to verify current spectrum use and identify potential sources of interference.
2. Avoid deploying multiple networks using the same frequency spectrum in the same physical spaces.
3. Design shared-use wireless networks to support anticipated aggregate throughput requirements.
4. Tune wireless networks to utilize the least congested frequency bands.
5. Conduct post-deployment wireless site surveys to validate networks are performing as expected.

5.2 Overview

Amongst the most well-known wireless technology in the world, Wi-Fi’s first version was released in 1997 providing 2 Mbps speed, and development has continued ever since.

Wi-Fi is meant for local area network usage (LAN) inside buildings or on-campus. The original design of the standard was optimized for transmitting data while in today's involved standards, real-time application such as voice or video calls are also supported.

It is fair to say that any smart device, laptop and even most IoT devices are equipped with Wi-Fi technology.

The original naming of the standard wasn't very human friendly with its IEEE 802.11 numbering. The decision was made to start using easier naming. For example, 802.11ax became Wi-Fi 6 and the next version of the standard will become Wi-Fi 7.

5.2.1 Current Adoption (in the Hospitality Industry)

Wi-Fi has become critical to the hospitality industry. Without reliable Wi-Fi, hotels risk disappointing a guest and losing guest loyalty. Signal quality and throughput must be good enough for a home-like or office-like experience. Business travelers rely on quality Wi-Fi to be able to do work while traveling. Children, family members and recreational travelers use Wi-Fi for gaming, social media and to stay in touch with loved ones while away. High performing, well-functioning Wi-Fi is an assumed and expected amenity in all hotels.

5.2.2 Current Standards and Roadmap

As of 2020, Wi-Fi uses two main radio frequency spectrums: 2.4 GHz and 5 GHz. It is sometimes confused, but 5 GHz Wi-Fi is not related to 5G, which is the latest standard for cellular communication. 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

5 GHz gained traction with 802.11n when the need for higher bandwidth and low latency became prevalent for video streaming and communication use cases. 5 GHz also serves a greater density or number of devices because there are more channels available.

2.4 GHz is a crowded spectrum with fewer channels and competition from other protocols (Bluetooth and Zigbee) that overlap with some of those channels. 2.4 GHz does have advantages in that it can travel greater distance and penetrate walls and solid services better than 5 GHz. 2.4 GHz radio chipsets are also less expensive.

Due to the low cost and longer range, 2.4 GHz radios are almost ubiquitous in IoT devices. With the growing number of IoT devices leveraging 2.4 GHz, the spectrum is getting more crowded.

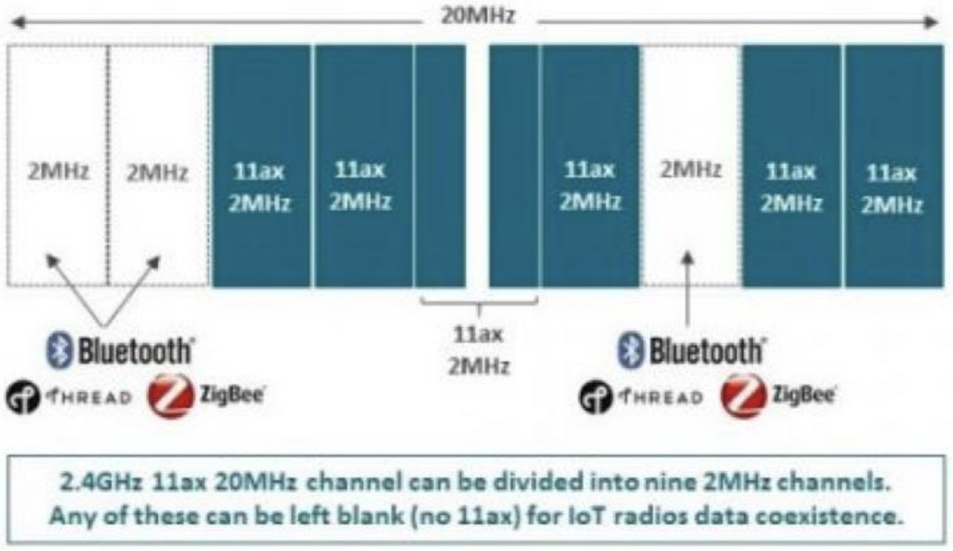
Higher throughput is as equally important as supporting the high density of devices. Technologies such as Multi-User Mimo (MU-MIMO) were introduced in 802.11ac (Wi-Fi 5), and will play an important role moving forward to help with competing Wi-Fi devices in the same proximity.

HaLow, also known as IEEE 802.11ah was adopted in 2017 as a long-range, low-power addition to the Wi-Fi standards. HaLow uses the 900 MHz unlicensed band to provide improved range, power consumption and battery life for IoT devices. MAC layer changes were made to specifically work with lower data rate devices that only send data occasionally. Enhancements in wake-up times, sleep modes and network association help keep standby power low. A simple "single hop" mesh-like functionality was implemented for range and network robustness. Finally, a concept called sectorization allows for more devices to share the same spectrum. To date, commercial acceptance has been very limited.

Additionally, 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:

1. Improved battery performance: Battery life of IoT devices is increased with Target Wake Time (TWT) mode. This enables IoT devices with low transmission requirements to remain in sleep mode for extended periods of time.

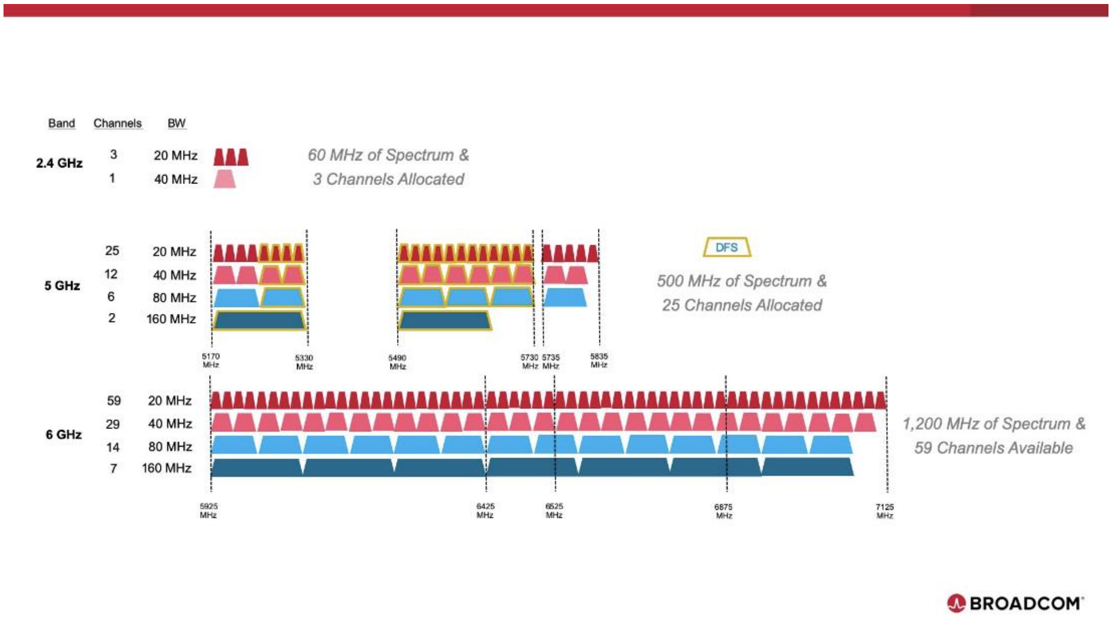
2. Airtime optimization: Small packets of IoT device data can be aggregated with OFDMA (Orthogonal Frequency-Division Multiple Access). This enables increasing numbers of IoT device connections, with minimal bandwidth impact, providing more bandwidth to more data-intensive applications.
3. Improved coexistence with other IoT Technologies: Utilization of the 2 MHz channels allows for an improved coexistence with other 2.4 GHz technologies.
4. 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.
5. 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.


20MHz
2MHz
2MHz
11ax 2MHz
11ax 2MHz
11ax 2MHz
2MHz
11ax 2MHz
11ax 2MHz
11ax 2MHz
Bluetooth
THREAD
ZigBee
Bluetooth
THREAD
ZigBee
2.4GHz 11ax 20MHz channel can be divided into nine 2MHz channels.
Any of these can be left blank (no 11ax) for IoT radios data coexistence.

Source: https://www.quantenna.com/wp-content/uploads/2018/02/coexistance-e1517608190794.jpg

In April of 2020, the FCC approved the unlicensed public use of a new spectrum for Wi-Fi. “Wi-Fi 6E” will be enhanced by 1200 MHz of additional spectrum in the 6 GHz range. This third frequency spectrum provides nearly five times the bandwidth available in 2020 (see the following chart). Simple IoT sensor devices found in hospitality are unlikely to need this new spectrum when it becomes available, but in the coming years use cases will be developed.

For more information see Section 11.1 on Wi-Fi 6e.



Source: https://www.extremetech.com/wp-content/uploads/2020/04/wi-fi-6-frequency-bands.jpg

5.2.3 Key Considerations for Hoteliers

- Is your Wi-Fi signal coverage good enough to satisfy your guest? What about its throughput in busy evening hours?
- Am I having the right technology in place to support large conferences with a high number of Wi-Fi users and devices within a small footprint?
- Does my Internet connection have the capacity to support multiple guests' needs?
- Is my cable infrastructure ready for the future? Cat-6? AP per room?
- Are my network devices supporting at least 1G throughput?

5.3 Bluetooth

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

5.3.1 Current Adoption (in the Hospitality Industry)

While currently seeing significant growth, Bluetooth technologies have not historically carried a substantial audience in the hospitality space. A listing of some of the most popular historical and future uses is provided below.

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

5.3.2 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 development of the specification, manages the qualification program and protects the trademarks. A manufacturer must meet Bluetooth SIG standards to market as a Bluetooth device.

A full table of protocols and their different versions can be found in Section 8.

5.3.3 Key Considerations for Hoteliers

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

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

5.4 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, as well as device discovery and security.

ZigBee devices may be configured and controlled remotely through the use of 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.

5.4.1 Current Adoption (in the Hospitality Industry)

When considering automation and sensing technology, Zigbee has historically enjoyed the most prolific coverage across products and technology. Ranging from sensing, building control and product integrations to breadth of products available, existing product and platform integrations and proven deployments, ZigBee’s longevity in hospitality is unmatched. A listing of some of the most popular historical and future uses is provided below.

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

5.4.2 Current Standards and Roadmap

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 availability of Specification 1.0 on June 13, 2005, known as the ‘Zigbee 2004 Specification.’

Established in 2002, the Zigbee Alliance is a group of companies that maintain and publish the Zigbee standard. The term **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 similar to that between IEEE 802.11 and the Wi-Fi Alliance.

In September 2006, the ‘Zigbee 2006 Specification’ was announced, obsoleting the 2004 stack. The 2006 specification replaces the Message/Key Value Pair structure used in the 2004 stack with a ‘cluster library’. The library is a set of standardized commands organized under groups known as clusters with names such as ‘Smart Energy,’ ‘Home Automation’ and ‘Zigbee Light Link’.

In January 2017, Zigbee Alliance renamed the library to ‘Dotdot’ and announced it as a new protocol to be represented by an emoticon (||:). They also announced it will now additionally run over other network types using Internet protocol and will interconnect with other standards such as ‘Thread.’ Since its unveiling, Dotdot has functioned as the default application layer for almost all Zigbee devices.

Zigbee PRO was finalized in 2007. A Zigbee PRO device may join and operate on a legacy Zigbee network and vice versa. Due to differences in routing options, Zigbee PRO devices must become non-routing Zigbee end devices (ZEDs) on a legacy Zigbee network, and legacy Zigbee devices must become ZEDs on a Zigbee PRO network.

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.

5.4.3 Key Considerations for Hoteliers

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

1. Which technology products will be implemented now, or in the future, as part of the technology/automation deployment?
2. Are those products available with Zigbee connectivity built-in?
3. How does the pricing of these Zigbee products compare to those with other built-in networking capabilities?

4. Which existing network infrastructures are already available within the property?
5. What speed is required of the communications?
6. What is the proximity of the individual devices?
7. What is the breadth of choices among products necessary to meet each of the required abilities?

5.5 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 through the use of 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 products.

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

Z-Wave's interoperability at the application layer ensures that devices can share information and it allows 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 of both in order 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. Communication distance between two nodes is about 30 meters (40 meters with 500 series chip), and provides the message ability 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, at 908.42 MHz in the North America and other frequencies in other countries depending on their regulations.

This band competes with some cordless telephones and other consumer electronic devices, but avoids interference 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 backwards compatible. The Z-Wave transceiver chips are supplied by Silicon Labs.

5.5.1 Current Adoption (in the Hospitality Industry)

Due to a number of factors, Z-Wave has not achieved 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, there have been a limited number of products manufactured by a limited number of companies which incorporate Z-Wave as the transport technology.

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

5.5.2 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 band in the 900 MHz range. Its 100 series chip set was released in 2003, and its 200 series was released in May 2005, with the ZW0201 chip offering a high performance at a 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 alliance being interoperable.

Z-Wave was acquired by Sigma Designs in December 2008. Following the acquisition, Z-Wave's US headquarters in Fremont, California were merged with Sigma's headquarters in Milpitas, California. The Z-Wave technology and business assets were once again sold on April 18, 2018 to Silicon Labs.

The Z-Wave Alliance was established in 2005 as a consortium of companies that manufacture products using Z-Wave wireless mesh networking technology. The alliance is a formal association focused on both the expansion of 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 including some features that had been available since 2012 for the 300/400 series SoCs. In February 2014, the first product was certified by Z-Wave Plus.

In 2016, the alliance launched a Z-Wave Certified Installer Training program to give 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 that can be used during network and device setup and can also function as a remote diagnostics tool.

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

5.5.3 Key Considerations for Hoteliers

One of the largest considerations for potential users is that since Z-Wave operates in 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 is that since the chip is proprietary and technology is licensed by Silicon Labs, all manufacturing and availability is entirely dependent on Silicon Lab's business.

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

1. Which technology products will be implemented now, or in the future, as part of the technology/automation deployment?
2. Are those products available with Z-Wave connectivity built-in?
3. How does the pricing of these Z-Wave products compare to those with other networking capabilities built in?
4. Which existing networking infrastructures are already available within the property?
5. What speed is required of the communications?

6. What is the proximity of the individual devices?
7. What is the breadth of choices among products necessary to meet each of the required abilities?

5.6 Mobile Networks

Mobile networks, now based on a global standard established by the Third Generation Project Partnership (3GPP), can provide an excellent method of connectivity 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 and 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 along with the Subscriber Identity Module (SIM) provide additional QOS, policy and rules control as well as mobility from location to location – all benefits when compared with other connectivity solutions.

The 3GPP has developed and mobile network providers are presently rolling out the next generation mobile network standard – 5G. As with 4G before, 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 going forward.

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

The HTNG 5G for Hospitality Workgroup has developed a White Paper and use case documents which can be found here.

5.6.1 Current Adoption (in the Hospitality Industry)

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 have a mobile network backup.

5.6.2 Current Standards and Roadmap

LPWA (Low Power Wide Area) refers to specific technologies used within the mobile network industry to support IoT connectivity. The benefits of LPWA over other means of IoT connectivity typically center around high penetration capabilities within buildings and underground facilities, very low power requirements resulting in battery life of over 10 years in some instances, low cost of both hardware and connectivity as well as inheriting the security benefits of the mobile network. LPWA is inclusive, not exclusive, of other IoT technologies and can complement other smartphone-related technologies such as Bluetooth and LTE Direct. IoT Mobile connectivity is typically reserved for data only (no voice), requiring a short burst of data to and from the devices. When voice and video requirements are needed, other elements of the LTE and 5G deployments may be utilized. Worldwide, there are two types of LPWA that a user will typically encounter:

1. **CAT-M** (Category M) or **LTE-M** (Long Term Evolution for Machines) is an IoT-friendly version of the tried and true LTE (4G) technology. There are two versions: LTE Cat M1 with 1 Mbps up/downlink and LTE Cat M2 with 7/4 Mbps up/downlink capacity. This technology is perfect for connectivity where mobility requirements are a must (think asset tracking on and off property, fleet tracking for shuttles, etc.).
2. **NB-IoT** (Narrow Band-Internet of Things) is another standards-based Low Power Wide Area (LWPA) technology primarily designed for non-mobile device connectivity where long range, deeper penetration of signal, lower power consumption and the security of the mobile network is

required. There are two variants: LTE Cat NB1 with 66/26 kbps up/downlink and LTE Cat NB2 with 159/127 kbps up/downlink capacity. NB-IoT is more commonly used for use cases such as HVAC monitoring where the connectivity requirements will not change over time.

5.6.3 Key Considerations for Hoteliers

While the 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.

5.7 LoRaWAN (Long Range Wide Area Networks)

LoRa (LongRange) is a technology design for wireless long distance (up to 30 miles) communication over unlicensed frequencies. End devices are mostly battery-powered with a battery lifetime of up to 10 years and low cost for around 20 USD. With 250bit/sec – 11kbit/sec the bandwidth is by design kept very low to be conservative with power consumption to archive a long battery lifetime. LoRaWAN is not an open standard, and there are reoccurring costs associate with. its use. LoRaWAN is already heavily adopted worldwide in the IoT space.

The main application of LoRaWAN is outdoor communication, but it can be used indoors as well. For example, one gateway can be enough to connect all end points in a hotel.

5.7.1 Current Adoption (in the Hospitality Industry)

Applications for LoRaWAN are anything that requires low bandwidth, long distance and no requirement for real-time. Good 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, environmental sensors (including temperature, humidity and air quality sensors). In the hospitality industry, applications include minibar sensors to assess consumption and window sensors. Another common application is door usage in a public space, for example, a restroom. This data would enable predictive usage monitoring and cleaning schedules could be adjusted to account for heavy or light usage.

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

5.7.2 Current Standards and Roadmap

LoRaWAN Standards are driven by the LoRaWAN Alliance, which is an open, nonprofit association with over 500 members. The current standard is 1.1.

5.7.3 Key Considerations 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 already 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

5.8 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, the broadcast message can be received by any base station in range. Sigfox operates on a public network model, where all devices connecting to the Sigfox network require a subscription with Sigfox.

5.8.1 Current Adoption (in the Hospitality Industry)

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 & Logistics, Manufacturing, Smart Cities, Utilities & Energy, Smart Buildings, Retail, Agriculture, Insurance, Hospitality and the home. Good examples include asset tracking, soil moisture monitoring, leak detection, connected smoke detectors and smart ordering buttons and environmental sensors (including temperature, humidity and air quality sensors). In the hospitality industry, applications include minibar sensors, asset tracking (e.g. room tray monitoring), utility monitoring and panic buttons.

5.8.2 Current Standards and Roadmap

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

5.8.3 Key Considerations 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 already 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?
- Cost considerations of different transport mechanisms

6 Wire Protocols

Wire protocols are carried over a physical medium such as a wire or fiber cable. Wire protocols typically begin at OSI layer 1 defining the physical characteristics of the medium or wire that will carry the signal. Additional components are typically added at layer 2 to define the characteristics of the signal, essentially how data is represented on the wire. Finally, additional OSI components at layers 2 and 3 define how data is routed, blocked and deblocked, and made compatible with the IP sets of protocols.

6.1 Ethernet

Ethernet is probably the protocol most familiar to people today. Introduced in 1980 and standardized by the IEEE in 1983, IEEE 802.3 today's Ethernet is still generally compatible with the standards established in the 1980's. The protocol has been modified over the years to support different physical media, higher speeds, longer distances and more nodes. The elements of the Ethernet protocols are used in other protocols such as Wi-Fi and Bluetooth. The ubiquitous MAC (media access control) address was originally defined by Ethernet and is now used for Bluetooth, Wi-Fi and many other protocols to identify Network Interface Controllers (NIC) on a network. The IP series of protocols run over Ethernet so Ethernet is often considered a core technology for the Internet.

6.1.1 Current Adoption

Ethernet replaced earlier networking protocols like token ring, FDDI, and Novell IPX/SPX protocols. The current standards are worked on by the IEEE 802.3 working group. Current projects include higher bandwidth and longer distance transmission over optical networks and higher performance for networks embedded in automobiles. The Ethernet protocols are currently alive and actively being worked on.

6.1.2 Roadmap

Most of the new features of Ethernet are designed to extend the protocols to new physical mediums, improve network speeds, bandwidth and distance, and improve features such as Power over Ethernet (POE).

6.1.3 Key Considerations for Hoteliers

Today Ethernet, whether carried over shielded twisted pair or fiber, typically forms the backbone of a hotel's network infrastructure. It feeds the access points for Wi-Fi and drives the internal connections to the Internet. It forms the core underlying technology for most Local Area Networks. The choice of a physical medium then becomes an important consideration. Current best practice here is CAT 7 shielded twisted pair or fiber when building for the future and planning to support for 10 Gigabit speeds.

6.2 Fiber Protocols

Fiber is a popular physical layer for the Internet and therefore IoT. The two most common protocols over fiber that directly relate to IoT are GPON (Gigabit-capable Passive Optical Network) and EPON (Ethernet Passive Optical Network). EPON standards are set by the IEEE 802.3 working group and GPON standards are set by the ITU-T. GPON uses IP protocols over ATM (another protocol). When a GPON line is terminated, the ONT converts the signal into an Ethernet signal that travels over a typical Ethernet LAN.

6.2.1 Current Adoption

GPON has been more widely adopted for fiber installations because of the ability to carry separate data, video and voice channels (triple play). EPON proves a data network and carries video and voice over the data.

6.2.2 Roadmap

Both the EPON and the GPON standards are being actively worked on by their respective standards bodies.

6.2.3 Key Considerations for Hoteliers

Once the fiber network has been terminated at an ONT, the network connection is Ethernet.

6.3 Broadband DOCIS Protocol

Data over Cable Interface Specification or DOCIS is the standard for sending data over a cable TV system. Coaxial cable used in cable TV systems can carry a large number of signals at different frequencies. The cable tuner can select a range of frequencies associated with a channel and extract a TV signal for the channel. DOCIS allows channels to be defined to carry IP-based data instead of the TV signal. A modern DOCIS modem can combine multiple channels to deliver both upstream and downstream channels providing higher bandwidth for the consumer. Currently DOCIS modems can provide download speeds of over a gigabit per second of data. Unfortunately, upload speeds are often a small fraction of download speeds.

6.3.1 Current Adoption

DOCIS specifications are maintained in the US by CableLabs and in the EU by Excentis. The two stands vary due to the different bandwidth specifications between the regions. The ITU-T has approved the specifications as ‘International Standards.’ These standards have been widely adopted by the cable industry and set-top box manufacturers. DOCIS is rarely used by IoT devices except internally in set top boxes. Normally, a modem is used to convert the DOCIS signals to Ethernet or USB signals that can be used by a computer or network device.

6.3.2 Roadmap

The DOCIS 4 standard was released in 2017 allowing up to 6 GPS download speeds and improvement in upload speeds.

6.3.3 Key Considerations for Hoteliers

DOCIS is rarely used by IoT devices except internally in set top boxes. Most modern set top boxes have an IP address and an Internet connection and some of these boxes are able to make the Internet connection available to other systems.

6.4 Point-to-Point Protocol (PPP)

Point-to-point protocol (PP) is a layer 3 protocol designed to connect two points on a network with nothing in between them. It is often considered a serial line protocol and can be used over serial cables, phone lines and radio links for example. PPP is an IETF standard first specified in RFC-1661).

The current IoT adoption has only been used in isolated low-bandwidth situations. PPP standards are maintained by the IETF and were last updated in 1997. Use the PPP protocol when nothing else fits the need.

7 Considerations for Proprietary Protocols

The building automation industry has historically favored the creation and implementation of proprietary solutions. Initially, this was by necessity, as open protocols with the proper characteristics weren’t widely adopted when early building automation platforms were designed. However, major building automation vendors have been slow to adopt open protocols. As a result, gateways and separate cabling and/or wireless network infrastructure are still frequently required to integrate proprietary building automation systems with other IoT systems and IP-based networks. As a result, integrating systems utilizing proprietary protocols with other systems can prove costly and/or provide limited functionality.

Other IoT system manufacturers tend to leverage open protocols, or those readily available through a license fee. Open protocols typically reduce network complexity, and permit the use of shared network infrastructure which reduces costs and increases flexibility.

Current IoT best practices would be to utilize open protocols whenever feasible, to simplify networks, improve system integration, reduce infrastructure costs and increase future flexibility. However, it may not be feasible to completely avoid proprietary protocols – especially for retrofits of existing properties.

Another emerging area of concern for interoperability in hospitality is the rapid expansion of consumer-focused IoT solutions, such as Apple HomeKit, Google Home and Amazon Alexa. Hospitality guests increasingly expect the same capabilities and level of convenience they find within their own homes. While these consumer-focused platforms typically utilize open protocols at the physical layers, they often include proprietary software protocols to provide functionality not yet supported by open protocols. As a result, deploying consumer-based IoT solutions in a commercial environment requires careful consideration, and may require special accommodations.

8 Table of Protocol Versions

			Approximate Range			
Standards	**Year Released**	**Frequencies**	**Indoor**	**Outdoor (line of sight)**	**Data Rates**	**Typical Battery Life (for edge IoT devices)**
Wi-Fi						
Wi-Fi 6 (IEEE 802.11ax)	2019 2020 (6GHz)	2.4 GHz, 5 GHz, 6 GHz Indoor: 5.925-7.125 GHz Outdoor (AFC): 5.925-6.425 & 6.525-6.875 GHz	30m (98ft)	120m (390ft) > 5km (@6 GHz)	600-9608 Mbps > 1 Gbps (6 GHz)	
HaLow (IEEE 802.11 ah)	2017	900 MHz (unlicensed band)	Up to 500m (1,640ft)	>1KM (3,281ft)	150 kbits to 200 Mbits	3-7 years
Wi-Fi 5 (IEEE 802.11ac)	2014	5 GHz	35m (225ft)	120m (390ft)	433–699 Mbps	
Wi-Fi 4 (IEEE 802.11n)	2009	2.4 GHz 5 GHz	70m (230ft)	250m (820ft)	72–600 Mbps	
Wi-Fi 3 (IEEE 802.11g)	2003	2.4 GHz	38m (125ft)	140m (460ft)	3–54 Mbps	Up to 5 years depending on battery type and frequency of heartbeat
Wi-Fi 2 (IEEE 802.11a)	1999	5 GHz	35m (115ft)	120m (390ft)	1.5–54 Mbps	
Wi-Fi 1 (IEEE 802.11b)	1999	2.4 GHz	35m (115ft)	140m (460ft)	1–11 Mbps	Up to 5 years, depending on battery type and frequency of heartbeat
ZigBee						
ZigBee 3.0 (ZigBee Pro-2015, IEEE 802.15.4) ZigBee 2.0 (ZigBee Pro, ZigBee-2017, IEEE 802.15.4)	2015	868/915MHz & 2.4GHz	30m (98ft)	200m (656ft)	20 Kbps–250 Kbps	2-7 years, depending on battery type and frequency of heartbeat

ZigBee 2.0 (ZigBee Pro, ZigBee-2007, IEEE 802.15.4)	2006 – 2012					
ZigBee 1.0 (ZigBee-2004, IEEE 802.15.4)	2004					
Bluetooth						
IEEE 802.15.1	1999	2.4 GHz	9m (30ft)	100m (328ft)	1 Mbps (Smart/BLE) 250 Kpbs–3 Mbps	Up to 5 years, depending on battery type and frequency of heartbeat (Smart/BLE)
Cellular						
GSM/GPRS/EDGE (2G), UMTS/HSPA (3G), LTE (4G)	1981 – 2020	600, 700, 900, 1800, 1900, 2100, 2500 & 3500 MHz 5G to add mmWave in the 24, 28 and 38 GHz bands		35km (GSM); 200km (HSPA)	35–170 kps (GPRS), 120–384 Kbps (EDGE), 384 Kbps–10. Mbps (HSPA), 3–10 Mbps (LTE), 600 Mbps–20 Gbps	
5G (through Release 16)				~1km (mm Wave 5G)		
Cellular Narrowband LTE						
LTE Cat-M1	2016	Same as cellular		>35km	1 Mbps (up/downlink)	
LTE Cat-M2	2018	Same as cellular		>35km	~7/1 Mbps (up/downlink)	
LTE Cat NB1	2016	Same as cellular		>35km	66/26 Kbps (up/downlink)	
LTE Cat NB2	2018	Same as cellular		>35km	159/127 Kbps (up/downlink)	
LoRaWAN						
LoRaWAN	~2012	433, 868 & 915 MHz		2-5km (urban area), 15km (suburban area)	0.3–50 Kbps	Up to 10 years
Z-Wave						
802.15.4	1999	800–900MHz	30m (98ft)	200m (656ft)	100 Kbps	2-7 years, depending on battery type and frequency of heartbeat

9 Application Layer Protocols for IoT

Application layer protocols specify communication standards on networks and rely on the underlying transport layer protocols to establish host-to-host data transfer channels and manage data exchange. This section reviews application layer protocols commonly utilized for IoT deployments.

9.1 HTTP/HTTPS

HyperText Transfer Protocol (HTTP) is the application layer protocol used for delivering web pages and content through the World Wide Web (WWW), and is the primary communications protocol used between most web servers and web browsers. HTTP is a synchronous protocol where the user-agent sends a request and waits for a response from the web or application server.

HTTPS is the secure version of the HTTP protocol providing a secure handshake between the web server and the user-agent/browser and transport layer security (TLS) once a channel has been established. These protocols are standardized by the IETF (Internet Engineering Task Force).

9.1.1 Current Adoption

The HTTP and HTTPS protocols are standardized by the IETF and are widely adopted globally. HTTP Version 1.1 is universally supported. The IETF published the HTTP/2 standard in 2015. This new standard has been adopted by 42% of the servers on the WWW as of January 2020.

9.1.2 Roadmap

Both the EPON and the GPON standards are being actively worked on by their respective standards bodies.

9.1.3 Key Considerations for Hoteliers

A draft of a new HTTP/3 standard exists and a handful of implementations can be found on the web.

9.2 XMPP

The Extensible Message Presence Protocol (XMPP) is a communication protocol for message oriented middle-ware allowing exchange of structured data between multiple network devices in real-time. The protocol was originally created as the Jabber protocol by the open source community to support Instant Messaging (IM) applications. In 2002, the IETF formed an XMPP working group and formalized the core protocols as an a set of open technologies for instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication, and generalized routing of XML data.. The XMPP Standards Foundation https://xmpp.org (XSF) defines extensions to the IETF Core XMPP protocols. The XSF has a group that looks specifically at IoT extensions to XMPP which can be found at https://www.xmpp-iot.org.

The XMPP protocol runs on the TCP protocol but has implementations that can also run on the HTTP/HTTPS protocols allowing XMPP to work with most firewalls.

9.2.1 Current Adoption

XMPP has existed as Jabber since 1999 and formally as XMPP since 2004. The latest IETF standards are RFC-6120 and RFC-6121 adopted in 2011, and RFC-7622 adopted in 2015. XMPP has been widely used by companies including Google, HipChat, WhatsApp and Cisco with many open and commercial implementations. Google and Cisco have also used XMPP as an alternative to the SIP protocol for web phone calls and video chat applications. There are a large number of XMPP standard extensions in both final and various stages of development that can be found at: https://xmpp.org/extensions/.

9.2.2 Roadmap

The XMPP community is very active and currently has a significant number of proposed and recently adopted extensions to address use for IoT and other applications. More information on this standard extensions community can be found at: https://xmpp.org/

9.2.3 Key Considerations for Hoteliers

XMPP is a mature and open protocol designed for supporting real-time communication with extensions that support both audio and video communications in addition to the more traditional text messages.

9.3 AMQP

The Advanced Message Queuing Protocol (AMQP) is an open standard for an asynchronous message-oriented middleware protocol standardized by OASIS and ISO/IEC 19464. AMQP provides message queuing and brokering services with interoperable messages and it supports message authentication and encryption. AMQP has become popular for higher-end IoT devices like and to create distributed IoT control and monitoring infrastructures.

9.3.1 Current Adoption

AMQP is supported by a number of different vendors and products including several open source solutions. Some recognizable solutions include:

- RabbitMQ
- Apache ActiveMQ
- Azure Service (Bus, Event Hub and IoT Hub)
- Red Hat A-MQ
- IBM MQ Light

9.3.2 Roadmap

AMQP appears to be very stable at the current 1.0 version adopted in 2014 and outside of new implementations, there appears to be little effort enhancing the standard at this time.

9.3.3 Key Considerations for Hoteliers

AMQP was originally created to meet the needs of the financial industry and while it has become useful for managing large IoT networks, it is not the typical protocol to collect information from devices used, for example, for facility control. It may, however, be a good solution to provide the messaging infrastructure to monitor all of the facilities within a region.

9.4 MQTT

Message Queuing Telemetry Transport (MQTT) is a publish-subscribe-based messaging protocol. It is lightweight, designed to be implemented with a small code footprint and supports running in low bandwidth environments. MQTT is standardized by the ISO (ISO/IEC PRF 20922) and by the OASIS (Organization for the Advancement of Structured Information Standards).

Some believe MQTT is not secure, however, MQTT is designed to use the transport layer security implemented in the lower level protocols to protect credentials and message content. An alternative is to use message-level encryption to protect message content.

More information about MQTT can be found at https://mqtt.org.

9.4.1 Current Adoption

MQTT is currently supported by a number of organizations and their projects. Some recognizable ones include:

- Amazon IoT
- Microsoft Azure IoT Hub for telemetry
- Adafruit IO

The current OASIS recognized MQTT version 5.0 standard was approved in 2019. The new features include:

- Reason codes: return codes, can provide a reason for a failure
- Shared subscriptions: allows load balancing across clients, reducing the risk of load problems
- Message expiry: messages can include an expiration date and will be deleted if not delivered before the expiration
- Topic alias: topic names can be replaced with a number

9.4.2 Roadmap

MQTT is actively maintained by OASIS. MQTT 5.0. was approved by OASIS in March 2019. Highlights of the recently adopted version of MQTT 5.0 include:

- Better error reporting
- Shared subscriptions
- Message properties – metadata in the header of a message
- Message expiry – optionally discard messages if they cannot be delivered within a time limit
- Session expiry – optionally discard subscriptions and messages if a client does not connect within a specified time limit

Source: http://mqtt.org/news, heading: MQTT v5.0 now an official OASIS standard

An OASIS Committee is also working on MQTT-SN (sensor networks), which is an extension designed for low power uses over the UDP connectionless protocols, and a separate committee is working on enhancements to MQTT Security.

The detailed complete list of new features to the 5.0 standard can be found at: https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.html#_Toc3901293

Most of the changes were designed to provide more robust services for IoT applications.

9.4.3 Key Considerations for Hoteliers

Typically, MQTT is implemented as a light-weight middleware that other applications and APIs are built on. If MQTT is being used, it is important to make certain that MQTT has been implemented with the use security protocols built-in by default. MQTT is typically used to collect or gather regular event information from a number of IoT devices and to send control messages to the same devices. MQTT is most often implemented in a hub and spoke model with devices reporting to a central hub.

9.5 DDS

Data Distribution Service (DDS) is a message-oriented middleware, publish-subscribe model designed for high performance, real-time data exchanges and is standardized by the Object Management Group

(OMG). The DDS protocol provides reliability, multi-casting (the ability to send messages to multiple receivers) and quality of service control.

9.5.1 Current Adoption

The current standard (version 2.3) was adopted and published by the OMG in May of 2019. DDS is found in the following industry verticals:

- Healthcare patient monitoring
- Autonomous cars
- Mass-transit systems
- Power-plant energy generation
- Robotics
- Smart-grid power distribution

9.5.2 Roadmap

The DDS standards are actively maintained by the OMG.

9.5.3 Key Considerations for Hoteliers

The DDS protocols are designed for high-speed real-time monitoring and control applications. These are not typical of facility management needs and most hoteliers are unlikely to see the benefit in the use of DDS in their typical environments.

9.6 CoAP

Constrained Application Protocols (CoAP) is designed for devices with limited capabilities like 8bit CPU, low RAM and other memory constraints. This IETF standards (rfc7252) protocol uses the UDP protocol (from the TCP/IP family of protocols) and supports request-response messages and service discovery among its features. CoAP can use DTLS (Datagram Transport Level Security) which is the UDP datagram equivalent of TLS used in application protocols such as HTTPS.

The CoAP protocol includes a limited subset of the HTTP protocol including the methods GET, POST, PUT and DELETE. The semantics are similar to the HTTP protocol with a similar set of response codes. This eases transformation of CoAP requests and responses into standard HTTP requests and responses.

CoAP supports resources represented in JSON, XML or Binary formats. Extensions to the standard provide point-to-point security and integrity of messages, as well as the ability to send blocks of data by using multiple packets to overcome some of the limits of the UDP protocol.

9.6.1 Current Adoption

The current base standard was adopted by the IETF in 2014. This standard was adopted specifically to address the need to support devices with limited capabilities such as sensors and switches. CoAP has been finding use in very low bandwidth, stateless applications over ZigBee, Bluetooth, and LoRa. In particular, it seems to be serving as a universal language for bridging pre-IoT protocols to the IoT world.

9.6.2 Roadmap

Various groups within the IETF are regularly creating and publishing extensions to the core CoAP standards with an extension being published as recently as July 2019.

9.6.3 Key Considerations for Hoteliers

CoAP currently seems to be a widely used, but behind-the-scenes protocol. Its power lies in the implicit lightweight implementation of the Restful model that the web is built upon. CoAP provides an application layer protocol that can be implemented by devices with limited capabilities, but can also be easily bridged to the heavier protocols such as HTTP.

10 Other Considerations

10.1 Power Consumption

Without exception, electrical power drives IoT devices. When upgrading existing non-connected electronic devices toward a next generation of connected IoT devices, for example a light dimmer, the increase in power consumption to facilitate the connectivity is typically rather small and can sometimes even be negative due to overall improvements in energy efficiency over time. Power consumption, however, needs to be looked at if simple electro-mechanical devices are upgraded to an IoT variant, or if IoT devices are added that previously did not exist in the building.

The power consumption of IoT devices falls into the three categories of line powered, battery powered or self-powered.

There are also other ways to power hybrids that are battery and line powered in special cases. Line powered devices are typically devices that are continuously in an active state and can be accessed in real-time while battery- and self-powered devices spend most of their time in a sleep mode, and are only periodically activated to communicate with the rest of the system. The cost of line power and batteries needs to also be taken into account.

We also need to consider the energy consumption of support functions to keep an IoT system operating. This includes the power consumption for gateways, network routers and the allocated costs of the cloud services.

The average yearly operating cost per IoT device is often in the magnitude of $10 USD.

10.2 Shared Networks

Today’s typical hotel has three to five times more Ethernet connections for hotel guests than associate back office connections. In addition, the need to deploy new IoT devices that support new business requirements as well as guest demands is on the increase. In order to provide the hotel with a common framework for network management as well as provide the ability to easily satisfy these new requirements, it is desirable to deploy a single converged network architecture.

At the highest level, the converged architecture which allows sharing of various devices and applications consists of the following:

- One set of network components that comprise the converged architecture;
- Software applications for network and security management that use industry standards protocols;
- Virtual LAN (VLAN) separation (or equivalent technology) for proper network security;
- And; access management software applications that allow for deployment, configuration and management of all of the applications and devices that are connections to the converged network architecture.

If 5G is being used to provide WAN connectivity to the IoT devices, the use of 5G network slicing could also be utilized to better control the traffic targeted for the various IoT devices in the hotel. However, in this case, the Ethernet network would need to be reconfigured to segment the various 5G slices (via VLANs) to take advantage of the 5G slicing.

10.3 Interoperability

For IoT sensors to enact certain functions, they must interoperate with the rest of the network. Every IoT implementation plan must consider not only how a contained IoT solution will operate on a common network infrastructure, but it must also be able to interoperate with other solutions to maximize the ROI.

For example, take into account an infrared or CO2 sensor installed to detect room occupancy for the purpose of triggering HVAC controls. The sensor may leverage some IoT protocols such as Zigbee or Z-Wave to communicate directly with the HVAC thermostat, but if it does so in a siloed network, it is not an IoT solution. The “I” in IoT is for Internet, not Intranet. Sensors and the networks they leverage for communication must use standard transport and messaging protocols so upstream components can consume the data and act on it.

There are many available communication standards or protocols (as referenced in sections 6 and 8) and some proprietary methods available in the countless “IoT” solutions, but interoperability cannot be assumed. Many of these protocols: Wi-Fi, Zigbee and Bluetooth, leverage the unlicensed radio frequency spectrum of 2.4 GHz, but the shared use of this spectrum necessitates more planning because each communication protocol leverages this spectrum very differently. For example, a solution that leverages Zigbee may have different implementations including 15 years-worth of standard versions and unique messages.

For these solutions to provide long-term value to the growing IoT landscape, they must leverage IoT bridges and gateways (covered in section 4.1) to translate messages to the “Internet” so they can be directed to other “things” including actuators, data collectors, dashboards and other components that are currently part of, or may someday be included in, the Internet of Things.

11 Appendices

11.1 Glossary

3GPP

Third Generation Project Partnership

6LoWPAN

6LoWPAN uses a lightweight IP-based communication to travel over lower data rate networks. It is an open IoT network protocol similar to ZigBee, and it is primarily used for home and building automation.

802.15.4

IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks (LR-WPANs) and is maintained by the IEEE 802.15 working group. It is the basis for the ZigBee,ISA100.11a, WirelessHART, and MiWi specifications, each of which further extend the standard by developing the upper layers which are not defined in IEEE 802.15.4. Alternatively, it can be used with 6LoWPAN and standard Internet protocols to build a wireless embedded Internet.

Access Point

An access point provides a wireless endpoint to allow devices to connect to one or more devices on the wireless network. Typically, the Access Point will provide access to a router or gateway allowing the device to access resources available on the wider network. A wireless network can also be used for peer-to-peer connections between devices.

Adafruit.IO

Adafruit.io is a managed cloud platform primarily used for storing and retrieving information. Adafruit.io provides many sensors, displays and robotics.

Ad Hoc Digital Radio Networks

An ad hoc wireless network is made up of multiple wireless end points connected by wireless protocols. Connections are created by considering the transmitter power, computing power and memory of an end point along with signal reliability.

AMQP

The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for message-oriented middleware. The defining features of AMQP are message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security.

BPSK Modulation

Binary Phase Shift Keying (BPSK) is a two-phase modulation scheme, where the 0's and 1's in a binary message are represented by two different phase states in the carrier signal: for binary 1 and for binary 0. In digital modulation techniques, a set of basic functions are chosen for a particular modulation scheme.

Bridge

A bridge is typically used to connect two networks that are logically or physically separate from each other. Bridges send network packets between the bridged networks to combine two networks and allow them to act as one. Most current bridging technologies work at layer 2, the datalink layer of the OSI model.

Cat-6

A standardized twisted pair cable for Ethernet and other network physical layers that is backward compatible with the Category 5/5e and Category 3 cable standards.

Cat 6 meets more stringent specifications for crosstalk and system noise than Cat 5 and Cat 5e. The cable standard specifies performance of up to 250 MHz, compared to 100 MHz for Cat 5 and Cat 5e.

Whereas Category 6 cable has a reduced maximum length of 55 meters (180 ft) when used for 10GBASE-T, Category 6A cable is characterized to 500 MHz and has improved alien crosstalk characteristics, allowing 10GBASE-T to be run for the same 100-metre (330 ft) maximum distance as previous Ethernet variants.

CATV

Cable TV (CATV) is delivered over a coaxial network to each television unit. There is typically a head-end onsite or remote. CATV is common in hospitality.

Firewall

A firewall is a network control system that determines what network traffic is allowed to cross the firewall based on a set of rules. Packet filtering firewalls may work on OSI Layer 3: Network or Level 4: Transport Layer. Application layer firewalls work on specific application layer (OSI Layer 7) protocols. Most modern Linux and Windows systems have a firewall built into their operating system. Most home and SOHO routers include a firewall as an integral part of their gateway function.

Gateway

A network gateway provides interoperability between a network and other networks behind the gateway. Unlike a bridge which simply connects two networks, a gateway may also provide services like; protocol translation, firewall and connection between different physical layers. An IoT gateway provides the bridging between an IoT device network and cloud and Internet networks. Gateways may operate at any of the OSI layers.

Hub

A network hub connects multiple Ethernet network segments together to form a single network. Most hubs work at the physical layer, layer 1 of the OSI model. The hub repeats data received on any port to all of the other ports on the hub. Most hubs have become obsolete and replaced by network switches.

Key Value Pair

A Key-Value Pair (KVP) is a set of linked keys which creates a unique identifier for some item of data. Key-value pairs are frequently used in lookup tables, hash tables and configuration files.

LoRa

LoRa (Long Range) is a spread spectrum modulation technique derived from chirp spread spectrum (CSS) technology and is the first low-cost implementation of chirp spread spectrum for commercial usage.

MAC Address

A media access control address (MAC address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. This use is common in most IEEE 802 networking technologies, including Ethernet, Wi-Fi, and Bluetooth. Within the Open Systems Interconnection (OSI) network model, MAC addresses are used in the medium access control protocol sublayer of the data link layer. As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator.

MAC addresses are primarily assigned by device manufacturers and are therefore often referred to as the burned-in address, or as an Ethernet hardware address, hardware address, or physical address. Each address can be stored in hardware, such as the card's read-only memory, or by a firmware mechanism. Many network interfaces, however, support changing their MAC address. The address typically includes a manufacturer's organizationally unique identifier (OUI).

Mesh Network

Mesh networks are solutions that leverage network nodes to connect physically or dynamically over wireless protocols. Bridges, switches and Access Points can connect to as many other nodes as possible and cooperate with one another to efficiently route data to or from clients.

MQTT

Message Queuing Telemetry Transport is an ISO standard (ISO/IEC PRF 20922)[3] publish-subscribe-based messaging protocol that works on top of the TCP/IP protocol suite. It is designed for connections with remote locations where a ‘small code footprint’ is required or the network bandwidth is limited.

MU-MIMO

Multi-User MIMO (multiple input, multiple output) allows compliant devices to communicate across multiple wireless streams simultaneously using multiple antennas. For example, a MU-MIMO access point can communicate with several devices at the same time.

Narrow Band Protocols

Narrowband IoT (NB-IoT) is a wireless standard for IoT. NB-IoT is classified in low-power wide-area networks (LP-WAN), providing a standard to connect devices that need tiny amounts of information, low bandwidth and extended battery life.

Network Slicing

Network Slicing is a network architecture that enables the multiplexing of independent logical and virtual networks on the same physical network infrastructure. Each network ‘slice’ is a virtual isolated end-to-end independent secure network configured for a specific application or service.

NFC

Near-field communication (NFC) is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm (1½ in) of each other.

OASIS

OASIS (Organization for the Advancement of Structured Information Standards) is a nonprofit consortium that works globally on the adoption of open standards for security. This includes the development of standards for the Internet of Things, energy, content technologies, emergency management and other areas.

OFDMA

Orthogonal Frequency Division Multiple Access

OMG

The Object Management Group (OMG), is an international, open membership, not-for-profit technology standards consortium founded in 1989. OMG standards include UML, CORBA and BPMN.

PHY

An abbreviation for "physical layer", is an electronic circuit, usually implemented as an integrated circuit, required to implement physical layer functions of the OSI model in a network interface controller. See section 3.

Piconet

A piconet is an ad hoc network that links a wireless user group of devices using Bluetooth technology protocols. A piconet consists of two or more devices occupying the same physical channel (synchronized to a common clock and hopping sequence). It allows one *master* device to interconnect with up to seven active *slave* devices. Up to 255 further slave devices can be inactive, or *parked*, which the master device can bring into active status at any time, but an active station must go into parked first.

Repeater

A repeater simply repeats any incoming signal as an outgoing signal for the purpose of increasing the distance a signal can propagate. As a signal travels through a medium like wire - optical fiber, or over the air - the signal weakens the further it travels. The repeater relays incoming signal boosting it so the signal can travel a longer distance. This extends the distance that a signal can be carried over the air, wire or fiber. Repeaters typically are physical layer (OSI layer 1) devices.

Router

Routers are the network devices that forward data packets through the networks and Internet. When a packet is sent by an IoT device or a computer, the packet is typically sent to a gateway router. Each router has a routing table maintained internally that tells the router where to send the packet so it will eventually reach its intended destination. Most routers intended for home and small office networks also provide gateway and firewall services as well.

Scatternet

A scatternet is a type of ad hoc computer network consisting of two or more piconets.

SigFox

Sigfox is a French global network operator founded in 2009 that builds wireless networks to connect low-power objects such as electricity meters and smartwatches, which need to be continuously on and emitting small amounts of data. Sigfox employs the differential binary phase-shift keying (DBPSK) and the Gaussian frequency shift keying (GFSK) that enables communication using the Industrial, Scientific and Medical (ISM) radio band which uses 868MHz in Europe and 902MHz in the US.

SOHO Router

A SOHO router is an Internet router designed for home offices and small offices. These are entry level networking devices with simple to configure settings.

Switch

A switch is a packet switching device that forwards data to the appropriate destination based on the MAC address (Media Access Control address). Switches are Ethernet devices that typically work at OSI layer 2: Datalink layer. However, some switches are designed with lightweight routing features allowing them to work in layer 3 the Network layer of the OSI model. In some networks, layer 3 switches may be useful to provide better network isolation through VLANs, in turn allowing the IoT devices to be segmented apart from the rest of the network.

Thread

Thread is an open standard, built on IPv6 and 6LoWPAN protocols. You could think of it as Google's version of ZigBee and can actually use some of the same chips for Thread and ZigBee because they're both based on 802.15.4.

TWT

Target Wake Time is a Wi-Fi 6 function that created the ability to configure an access point to allow individual devices to connect to a Wi-Fi network at a pre-defined time or set of times. This mechanism provides a way for devices to negotiate specific times to turn on and off, based on when they need to send and receive data. This functionality has a dramatic impact on device power consumption by allowing them to be switched off except when actively transferring data. Devices only turn on when they need to perform a task.

UHF

Ultra-High Frequency radio frequencies range from 300 MHz to 3 GHz. In the United States. also known as the decimeter band, as the wavelengths range from one meter to one tenth of a meter (one decimeter). UHF was also used in the past for analog television.

Weightless

Weightless is a set of LPWAN open wireless technology standards for exchanging data between a base station and thousands of machines around it. These technologies allow developers to build Low-Power Wide-Area Networks (LP-WAN). Currently used for mobile phone, digital television, GPS, Bluetooth, satellite communications and cordless phones among many other applications.

WirelessHart

WirelessHART is a wireless sensor networking technology based on the Highway Addressable Remote Transducer Protocol (HART Protocol). Developed as a multi-vendor, interoperable wireless standard, WirelessHART was defined for the requirements of process field device networks.

11.1.1 Wi-Fi 6e Report and Order ET Docket No. 18-295; GN Docket No. 17-183

This R&O is based on a previously released Notice of Proposed Rulemaking which solicited responses from the industry to allow unlicensed use of the 6GHz band (5.925-7.125GHz). The FCC has considered the responses and will be releasing current allocated spectrum (incumbent) to use by certain unlicensed devices and applications. These unlicensed devices and applications will be required to operate within a rules and coordination construct to protect the incumbent from interference.

A result of 1,200 MHz of additional spectrum is now for Wi-Fi use to add to the current 2.4 and 5 GHz bands.

Rule Change Highlights:

- Allows the unlicensed 'Wi-Fi operation of devices for indoor use in all 1,200 MHz of the 6 GHz band

- Low-power devices (access point or AP) only (+24 dBM, or ¼ Watt) to share with and protect the incumbent services
- No automatic frequency coordination (AFC) required
- Each AP utilizes the 1,200 MHz band on a contention basis (like Wi-Fi, listen before transmitting)
- No professional installation requirements
- Allows the unlicensed “Wi-Fi” like operation of devices for indoor and outdoor use under AFC control in 850 MHz of the band (5.925-6.424 & 6.525-6.875 GHz)
- Standard power APs only (+30dBm or 1 Watt)
- Under AFC control for channel and power allowances
- No professional installation requirements (AP geolocation required)
- Client devices can operate in the full 1,200 MHz of the 6 GHz band under the control of their indoor or outdoor access point (maximum 6 dB less than AP (1/4 of AP power)

Impact:

- Expands the application of the popular Wi-Fi standard bandwidths by almost five times the amount
- New Wi-Fi 6e indoor devices will be able to provide increased data rates to meet short-range consumer and enterprise demand
- New Wi-Fi 6e outdoor devices to provide broadband data to nomadic and fixed clients
- On 23 April 2020, official action at the April FCC meeting was taken to target a 31 December 2020 active date
- Generally available Wi-Fi 6e devices are thought to be available in 2022.

11.2 NFC

Near-Field Communications (NFC) is not generally considered an IoT Protocol, yet we are including it here given many NFC solutions connected on the backend to the Internet and the need to be bridged.

11.2.1 Overview (High Level Description & Market Position)

As the name suggests, Near-Field Communication is meant in applications within a proximity of one to two inches. Technology is based on RFID and employs electromagnetic induction between two loop antennas. Nearly any smartphone these days comes with NFC built in. One of the main applications is for identifying a smart device in a secure way. This can include contactless payment systems, electronic tickets, door entry systems or almost anything else that requires a secure authentication.

Another application is on social media when sharing contacts, photos or videos.

“Based on ISO/IEC 18092:2004, using a center frequency of 13.56 MHz. The data rate is 424 kbps and the range is a few meters short compared to the wireless sensor networks.”

11.2.2 Current Adoption (in the Hospitality Industry)

The only application seen in hospitality so far is for door look entry systems. However, more and more technologies are being replaced by BLE these days.

11.2.3 Current Standards and Roadmap

NFC is part of ISO/IEC 14443 with the current standard NFCIP-2.

11.2.4 Key Considerations for Hoteliers

There are a couple of questions to consider while evaluating NFC:

- Is it the right technology for a hotel?
- Which near-field authentication methods would be beneficial?

11.3 Useful Resources

Visit HTNG's Technical Specifications Page for previous IoT publications.

- **IoT Presentation, Original Workgroup 2017-05 v5 IoT in Hospitality**

https://www.htng.org/resource/collection/6753109B-63A9-4D2C-928C-70A90F56A578/HTNG-IoT-Presentation-template-(JTienor)-060917.pptx

- **IoT Definitions to Consider**

https://www.htng.org/resource/collection/6753109B-63A9-4D2C-928C-70A90F56A578/IoT_Definitions_(to_consider).docx

- **What does IoT mean to you and your company**

https://www.htng.org/resource/collection/6753109B-63A9-4D2C-928C-70A90F56A578/IoT_Breakout_Session_St_Johns_2016-08-24.docx

- **2017 Insight Summit Files**

https://www.htng.org/?page=ISNA17Files&hhSearchTerms=%22IoT%22&#rescol_4450444

- **2018 HTNG Asia-Pacific Conference Files**

https://www.htng.org/?page=APC2018_File&hhSearchTerms=%22IoT%22&#rescol_5560833

11.4 Referenced Documents

The following table shows the documents upon which this document depends:

Non-HTNG documents regarding specifications, particularly when quoted.

Document Title	Location/URL
Power saving methods for LTE-M and NB-IoT devices	https://htng.konverse.com/posts/13846822-IoT-LTEM-amp-NBIOT-Power-Saving
Original IoT Whitepaper	https://www.htng.org/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/IoT_Workgroup_-_Internet_of_Things_Fundamentals.pdf
IoT Presentation	https://cdn.ymaws.com/htng.site-ym.com/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/IoT_Workgroup_-_How_Hospitality_can_win_with_IoT.pdf
IoT Security White Paper	https://www.htng.org/resource/collection/CC1CE2B8-0377-457E-9AB0-27CFDD77E17B/HTNG_-_IOT_Security_for_Hospitality.pdf