The next wave of adoption of Wi-Fi will be Industrial Internet of Things and one such example is the heterogeneous environment found at airports that needs public Wi-Fi as well as wireless access for retailers, building, and engineering personnel, immigration, and passenger flow monitoring.

New Incremental Business Opportunities with Wi-Fi 6

May 2020

Written by: Bill Rojas, Shaily Ajay Shah, Hugh Ujhazy

Introduction

Wi-Fi 6 (IEEE 802.11ax) is the next generation of Wi-Fi connectivity technology that will deliver more capacity, and support more simultaneous users and devices than previous generations. Wi-Fi 6 will be incorporated in the latest generation of smartphones, laptops, access point, and wireless routers as well as an increasingly wide range of Internet of Things (IoT) devices for smart homes, smart buildings, smart cities, and smart industries. Operators/Owners of enclosed public spaces such as airports, stadiums, school and business campuses, and shopping malls will be able to deliver more bandwidth to more simultaneous users and IoT devices and this will be complemented with more network intelligence and cloud-enabled management. Manufacturers of complex system products including automobiles, buses, trucks, and construction machinery will be able to build Wi-Fi 6 modems into their products for diagnostic purposes while at the same time providing usage and status information to users.

In order to demonstrate the business impact and potential of Wi-Fi 6 in the enterprise space we have elected to look in more detail at the airport use case. Airports are an excellent proxy for a range of environments that have mixed high-density public access with private/enterprise communications and Industrial Internet of Things (IIoT) services. In that sense, an airport is a collection of several use cases under one umbrella. Other such public/private environments include transport hubs, stadiums, theme parks, public parks, enterprise and university campuses, and tourist spots. In this study we list the key sub-use cases that fall under airport operations and we provide a quantitative hypothetical business model in order to understand how the different use-cases can coexist but each with their own design and operational requirements.

AT A GLANCE

WHAT'S IMPORTANT

The ability to manage up to 8 simultaneous broadband users via MU-MIMO and allocate resources to maximum 9 simultaneous users in 20MHz via OFDMA means that Wi-Fi 6 can deliver excellent bandwidth even in highly congested environments.

KEY TAKEAWAYS

Wi-Fi 6 has the bandwidth and performance operating across two bands, 2.4GHz and 5GHz, to support heterogenous environments of public internet access and Industrial Internet of Things devices.

In a conservative hypothetical model where we assume 0.2% of passengers use premium Wi-Fi in Year 1, increasing to 1.1% in Year 10, purchasing two-month access for US$5 an airport can monetize the enhanced user experience that Wi-Fi 6 brings to the table, leading to a 10-year ROI of 21% and cash flow positive by Year 6.

Wi-Fi Use Cases

Wi-Fi has become an integral part of home, office, and business life as more and more devices including automobiles, smart TVs, broadband modems, smart home devices, laptops, tablets, and smartphones are shipped with the latest Wi-Fi standards. As fiber-to-the-home (FTTH) penetration continues to increase, mobile devices, smart home devices, and laptops need to support the latest Wi-Fi standards that enable multi-hundred Mbps speeds. As the performance increased with each generation of Wi-Fi, more and more use cases emerged, as shown in Table 1. Each use case has a different motivation and requirements – most will be a pure cost center but the quality of the service will have direct (manufacturing, mining, cruise ships) and indirect impact (e.g., shopping malls) on the business efficiency, brand and customer experience.

Table 1: ***Wi-Fi Use Cases and Key Deployment Considerations***

Use Case	Motivation	Benefits
Airports	Airports are heterogenous environments with a requirement for wireless infrastructure for public and private Wi-Fi access as well as a number of IIoT use cases for luggage location, facilities management, and immigration control. Airports also house many retail stores and restaurants.	Utilizing the same wireless infrastructure for both retailing, public Wi-Fi access, and IIoT enables a more efficient use of the unlicensed spectrum. Wi-Fi quality directly impacts customer experience and provides revenue opportunities for wholesale access to tenants.
CSP cellular offload	Wi-Fi hotspots built and owned by communications service providers (CSPs) can also be used to offload 3G/4G cellular traffic in congested areas.	Dual use provides additional operational expenditure (opex) and capital expenditure (capex) savings to the CSP, and improved customer experience (CX).
Public hotspots	Usually owned by municipal governments to provide service to tourists and local citizens. Oftentimes these are outsourced to local CSPs, ISPs, or IT services companies. Government-owned hotspots can be found in parks and recreational areas along tourist spots.	This is treated as a public service, with additional benefits for the tourist industry.
Home	Internet access including video streaming; smart-home-connected devices such as thermostats, smart speakers. More and more users want full coverage in their homes. Some operators include home Wi-Fi routers as part of the monthly service plan, but they might charge extra for high-performance 802.11ac and 802.11ax routers. The COVID-19 global pandemic has forced large swaths of the working population to work from home and for students to participate in online education. This has generated a significant spike in home broadband traffic. While in the short term there will be a spike in video, content, collaboration tools, and data heavy traffic, even in the long-term homes, schools, and workplaces may look at infrastructure upgrades to support these new ways of working.	By having all the smart home devices on the home WLAN it is easier to introduce gateway products and analytics. Wi-Fi is the key enabler of additional smart home services; such-as entertainment and security. Wi-Fi can provide the added bandwidth needed for all users at home for simultaneous sessions (parents on work-related video conference calls, students doing online homework and online classes, online gaming, and streaming video content).
Hotels and hospitality	Excellent room coverage as well as coverage across all hotel restaurants, fitness center, lobbies, and swimming pool areas; considered critical to guest satisfaction; treated as a cost center.	The key benefit is protection of the brand. Some hotels still charge for Wi-Fi access but more and more, the trend is for it to be included with the room.

Table 1 (Cont.): *Wi-Fi Use Cases and Key Deployment Considerations*

Office Wi-Fi	Most enterprises provide Wi-Fi service at the office for their employees. Organizations do need to implement a security policy. Most large organizations have deployed enterprise WPA2 security (802.1x and AES-CCMP) and corporate AAA (Authentication, Authorization, and Accounting) servers.	Mobility and collaboration are the main benefits of implementing office Wi-Fi. The deployment of more Wi-Fi means less cables and the associated maintenance, plus encourages new smart office work practices like hot desks and wireless collaboration.
Shopping malls	Shopping malls typically will have Wi-Fi access points installed in a flush against the ceilings so as to be aesthetically pleasing.	Excellent Wi-Fi coverage can help to generate more customer foot traffic in the mall. This presents opportunity for the mall owner to monetize footfall analytics and wholesale access to tenants.
Stadiums	Generally treated as a cost center but may outsource management and maintenance of the service to CSPs and systems integrators.	Main benefit is brand and customer experience. Can offer new functionality such as POV cameras; strengthen the branding of the stadium and the teams/athletes and for events.
Private Industrial Networks	This would include mining camps, manufacturing floors with high levels of automation, shipbuilding yards, shipping ports, cruise ships, offshore oil rigs and cargo ships. Remote locations need bandwidth for both crew welfare and for automated operations. There could be a large number of Wi-Fi-enabled machines and robotics in the modern factory.	Along with flexibility, analytics, and supervisory control the additional benefits are precision in workflow and reduced manual errors and cost due to automation.
Transportation hubs	Wi-Fi is well suited for both outdoor platforms as well as indoor train and subway platforms. Oftentimes, it can be found adjacent to 4G small indoor cells.	CSPs oftentimes provide the Wi-Fi in transportation hubs and can be used for cellular offload as well.
University campuses	Both outdoor and indoor coverage is required with high levels of bandwidth. Large campuses can be found with as many as 10-17K access points.	Wi-Fi coverage has become almost a de-facto service expected by modern students.

Source: IDC, 2020

Wi-Fi 6 Technical Features

In September 2019, the Wi-Fi Alliance released its certification program for Wi-Fi 6 which is based on the IEEE 802.11ax standard. The new generation of Wi-Fi provides more bandwidth simultaneously to many devices, including IoT devices, across two frequency bands – 2.4GHz and 5GHz. Prior to Wi-Fi 6, engineers tended to focus on the theoretical peak speed of the Wi-Fi access point, but with Wi-Fi 6 the focus has turned to overall capacity that can be delivered to each device on the network. In the United States the FCC circulated draft rules permitting unlicensed devices to operate in the 6GHz band making the entire band available for unlicensed access. On April 23, 2020 the FCC voted to approve the full 1200MHz band in the 6GHz band for unlicensed use and will become available in 2H20. IDC expects that other markets will follow the FCC's lead. Wi-Fi 6E standard will extend Wi-Fi 6 to the 6GHz band and is currently being finalized. The total available unlicensed frequency across the three Wi-Fi bands depends on the geography. For example, in the United States there is 72MHz available from 2,401–2,473MHz, 700MHz from 5,150–5,850MHz, and 1,200MHz from 5,925–7,125MHz (expected). In the 5GHz band, wider channels are aggregated or bonded from the basic 20MHz channels to form 40MHz (note that 802.11n first introduced the 40MHz bonded channel), 80MHz, and 160MHz channels (see Table 2). The superwide 160MHz channels are ideally suited for augmented reality/virtual reality (AR/VR) and wearable devices.

Table 2: *Comparison of Wi-Fi Standards*

Parameter		Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E
Frequency		5GHz	2.4GHz, 5GHz[2]	6GHz[3]
Number of channels[1]	20MHz	25	28	59
	40MHz	12	13	29
	80MHz	6	6	14
	160MHz	2	2	7
	320MHz	0	0	0
Access technology		OFDM	OFDMA	OFDMA
Antennas (and spatial streams)		MIMO (4x4)	MU-MIMO (8x8)	MU-MIMO (8x8)
Modulation		256 QAM	1,024 QAM	1,024 QAM
Maximum data rate		3.5Gbps	9.6Gbps	9.6Gbps

Note 1: Non-overlapping channels; the number of channels depends on the regulatory environment

Note 2: 5GHz Band is 5.150–5.850GHz and the USA and some of the channels are required to use Dynamic Frequency Selection and Transmit Power Control (TPC) to prevent interference with weather-radar and military systems.

Note 3: Channelization has not been finalized.

Source: Skyworks, 2019

The key technical features that differentiate Wi-Fi 6 from previous generations are given below. It should be noted that performances listed are theoretical and actual performance will vary depending on the number of multiple-input and multiple-output (MIMO) antennas in the client device and geography (i.e., regulatory); most Wi-Fi 5 client devices have 2x2 MIMO.

Increase in Spectral Efficiency through advanced modulation and more spatial streams. 256 Quadrature Amplitude Modulation (QAM) enabled Wi-Fi 5 to achieve roughly 5.4 bits per second per Hertz spectral efficiency and for comparison purposes, LTE achieves 4bps/Hz with 256 QAM. By upgrading to 1024 QAM, Wi-Fi 6 is able to achieve roughly 7.5bps/Hz for a single spatial link on a 20MHz channel. Wi-Fi 6 can deliver up to 8 spatial streams in the 5GHz band, which means that Wi-Fi 6 infrastructure can deliver double the capacity of Wi-Fi 5. Thus for a 160MHz channel (this is the maximum channel size in the 5GHz band) and 8x8 MIMO, Wi-Fi 6 can produce a throughput of 20 MHz x 7.5 bps/Hz x 8 spatial streams x eight (number of 20 MHz channels) = 9.6 Gbps.

Connecting more client devices (including Voice-Over-IP devices) with OFDMA. Orthogonal Frequency Division Multiple Access (OFDMA) is a critical ingredient in the success of 4G Long Term Evolution (LTE) because it allows both narrowband and wideband devices to use the same frequency bands, but with different channel sizes and dynamic scheduling. This capability has finally been included in Wi-Fi with Wi-Fi 6 being the first Wi-Fi standard to utilize OFDMA. OFDMA is critical for mixed use case environments such as airports that have multiple IIoT use cases and may require hundreds of IoT and consumer devices to connect simultaneously to a single access point.

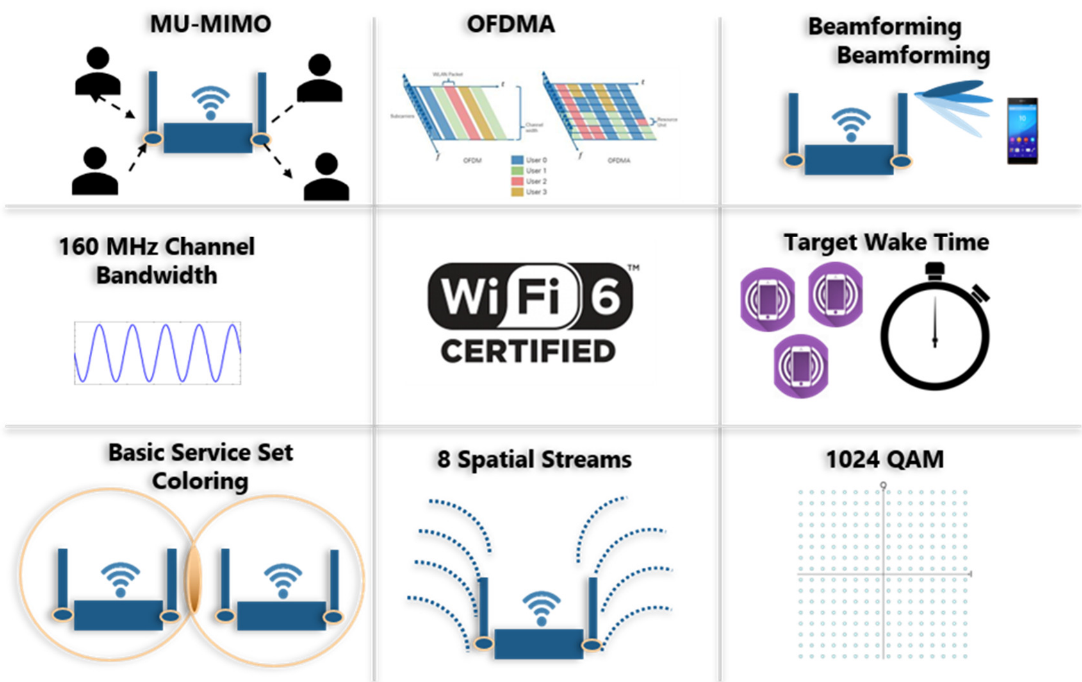
Improved throughput with MU-MIMO, OFDMA, and Beamforming. Wi-Fi 6 utilizes two technologies that were not available as a pair in previous Wi-Fi systems: multiuser multiple-input multiple-output (MU-MIMO) and OFDMA MU-MIMO expands on MU-MIMO in 802.11ac (Wi-Fi 5) by enabling up to 12 spatial streams in both uplink and downlink as compared with four spatial streams in 802.11ac and only in the downlink. In Wi-Fi 5, if an older device is connected to the access point it becomes the speed limiting device to the entire access point, but in Wi-Fi 6 the use of MU-MIMO with up to 12 spatial channels means that the access point can allocate a channel to support the older devices without slowing down other devices. Beamforming improves data rates by directing signals toward specific devices instead of omnidirectional transmission. Beamforming assists MU-MIMO when devices are physically moving.

Better spectral efficiency in the 2.4GHz band. Wi-Fi 6 supports both the popular 2.4GHz band and the high-frequency 5GHz bands but one of the new and important features of Wi-Fi 6 is its ability to provide MU-MIMO in both the 2.4GHz and 5GHz bands with the latest contention techniques, whereas Wi-Fi 5 could only support the 5GHz band.

Reduction in IIoT device traffic congestion. Target Wake Time (TWT) is a technique used in Wi-Fi 6, which reduces power consumption and traffic congestion by scheduling when an IIoT device (such as a beacon) will transmit data. In order to keep the costs of IIoT modems down, it is preferred that the 2.4GHz band is used for IIoT devices and fortunately Wi-Fi 6 supports devices that use 802.11n in the 2.4GHz band.

Basic Service Set (BSS) Coloring. This is a technique that is used to prioritize traffic and effectively shut out traffic that is on the same channel but not communicating on the network. BSS Coloring is very useful in very dense environments.

Figure 1: *Wi-Fi 6 Technology Building Blocks*



Source: Qualcomm, 2020

Wi-Fi 6 Versus 5G Comparison

Cellular (3G, 4G, and now 5G) is a wide area access technology that users connect to in order to get internet connectivity and this will be typically outside of the home and outside of the office including commuting routes, public places such as shopping malls, buses, subways, and train stations. Wi-Fi has become the secondary access method in which mobile users connect to the internet, especially in enclosed areas where the cellular signal might not be available such as train stations and subway interchanges. From 2020 onward, most medium/premium smartphones will ship with Wi-Fi 6 similar to the way that smartphones were shipped with Wi-Fi 5.

Operator data from around the globe suggests that about 1/3 of cellular traffic actually occurs near or at the office and during commutes. Moreover, 25% of cell sites typically handle 75% of the traffic. In cities like Tokyo, commuters might spend an average of 90 minutes one-way on the train and they are discouraged from talking on the phone. 5G and Wi-Fi 6 will utilize mid-band frequencies in a complementary fashion, with higher frequency bands providing shorter coverage ranges but more bandwidth due to larger channel widths.

Table 3 provides a generalized comparison of 5G and Wi-Fi 6.

Table 3: ***Comparison of 5G NR and Wi-Fi 6***

	Pros	Cons
5G NR	• 5G network slicing will enable communications service providers an expanded toolset to address the specific connectivity needs of industry verticals. • 5G is designed as a multiaccess platform, which could include unlicensed solutions. • SIM-based security has a strong reputation.	• Cellular network builds, whether public or private, can be cost prohibitive in comparison with Wi-Fi. • The CBRS ecosystem (LTE and 5G) will require time to grow; CBRS is currently available in the United States only. • Building private 5G networks may require enterprises to invest in new skill sets, driving up costs.
Wi-Fi 6	• Ubiquitous existing Wi-Fi deployments, devices, and enterprise investments make for a simple upgrade path. • It can be integrated with enterprise management tools, especially for security, visibility, and analytics. • 802.11ax brings faster speeds and more deterministic RF management. • Wi-Fi 6 capable IoT devices will proliferate before 5G IoT because of cost and availability.	• Compared with cellular, it is not as ideal for large outdoor, long-range use cases. • It involves radio frequency (RF) contention between Wi-Fi, BLE, Zigbee, and Thread protocols, particularly in 2.4GHz band. • It is primarily an access technology that requires fiber backhaul on the order of 100Mbps – 1Gbps depending on the use case. 5G will also have this requirement.

Source: IDC, June 2019, IDC #US45266619

Generally speaking, IDC's view is that these technologies are very complementary and can provide backup for each other depending on the use case.

Best Practices for Designing and Building Wi-Fi 6 in Airports

Airports present an exciting umbrella of use cases comprising consumer public and retail internet as well as enterprise and Industrial Internet of Things (IIoT). Airports have a number of use cases that can benefit from wireless connectivity including smart building management, luggage tracking, surveillance, passenger movement monitoring, passenger body temperature monitoring, airport hangers, aircraft telemetric data downloading, and engineer/technician information support system. Airport ICT planners often struggled with public Wi-Fi 802.11n installations as they were prone to interference and capacity issues. Of course, best practices such as managing a single wireless infrastructure with multiple service set identifiers (SSIDs) can mitigate many of the interference issues but it did not solve the capacity or lack of scalability. The emergence of 5G and Wi-Fi 6 presents airport planners with the opportunity to improve reliability and performance of public Wi-Fi while at the same time provide connectivity for a wide range of IIoT applications. The airport Wi-Fi infrastructure thus must also support both IT operations and engineering and facilities management.

Airport network planners thus have multiple access technologies to work with including Bluetooth, Low-Power WAN (LPWAN), 4G cellular, 5G cellular, and Wi-Fi 6. In some cases, Wi-Fi 6 will suffice and in other cases cellular will in combination act as either a primary or secondary access technology to improve reliability and availability. Network designers need to design for interference mitigation, traffic congestion, and prioritization of services. As a result, the public Wi-Fi internet access will typically be assigned a different SSID network while operations and other critical airport services will not be accessible to the general public.

Evolving Ecosystem

Airports are like mini indoor cities that have a host of stakeholders such as the retail mall/restaurant services, immigration or government agencies, service providers, tech teams, and third-party partners (see Figure 2). All partners need a robust and secure IoT-enabled Wi-Fi network that delivers efficient airport operations and contributes to a delightful passenger experience. Wi-Fi 6 has a strong use case for high-density environment such as airports where a sudden influx of users can overwhelm a conventional network. The evolving ecosystem can be grouped under five main entities:

Solutions providers: These companies provide the core wireless infrastructure comprising access points, switches and routers, controllers, and analytical engines that are encrypted and secure so as to not compromise a sensitive airport environment.

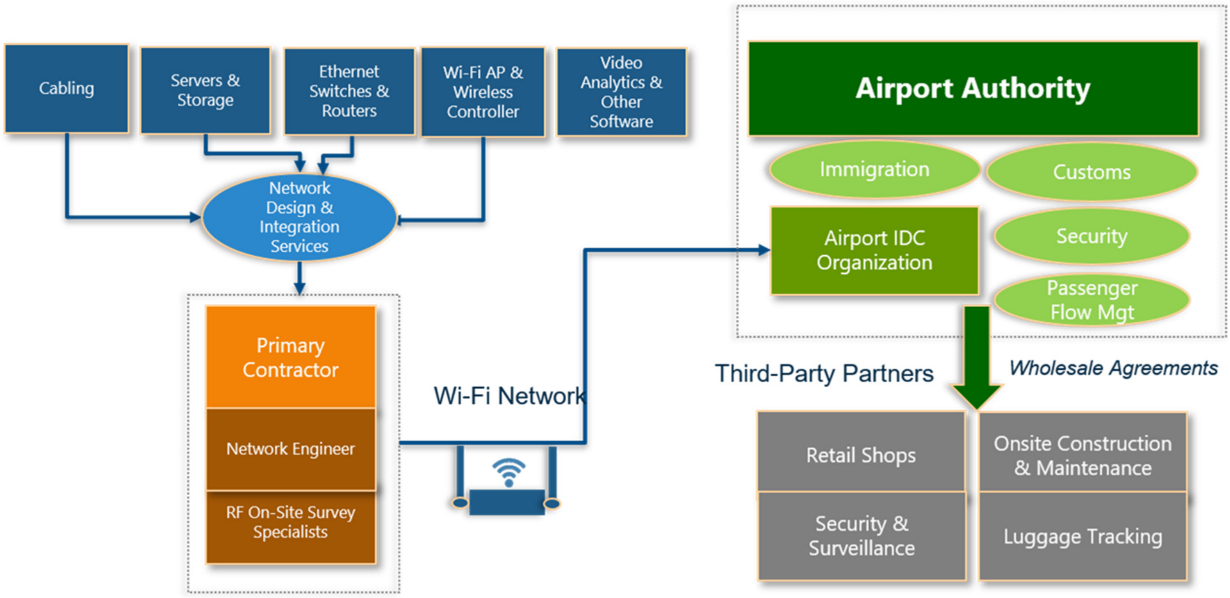
Systems integration providers: These companies provide design, planning, connectivity, and tech support, and also help gauge the bandwidth requirements of different types of travelers and enable seamless traffic handoff between cellular and Wi-Fi networks.

ICT airport team: Once the Wi-Fi network is operational the Airport ICT team will need to manage network operations including monitoring performance and congestion and carrying out periodic capacity expansion (e.g., adding more access points). It can be beneficial to have a single systems integration partner to work through since there can be multiple suppliers involved.

Third-party partners and/or users: These will include malls, airport lounges, restaurants, and other retail outlets that are present at the airport. Airport lounges typically also provide Wi-Fi connectivity to their members.

Government agencies: These will include the airport security, immigration, and custom officers who also interact with airport systems.

Figure 2: ***Ecosystem of Partners for Airport Wi-Fi Communications***



Source: IDC, 2020

Selecting the Cabling and Power Delivery System

As shown in Figure 3, the airport public Wi-Fi network is a 3-Tier network. Wi-Fi 6 access points (APs) should be spaced at no more than 20–25 meters apart in order to provide full coverage with excellent bandwidth in the terminal halls and corridors. Terminal halls usually have high ceilings that might be 15–25m in height, which makes ceiling mounting impractical. APs are typically placed no higher than 10 feet with an average distance of 20–25 meters. Moreover, APs are connected to an aggregation Ethernet switch and powered by a Power Over Ethernet (POE) cabling system, which precludes the need for electric power sockets. Two choices have to be made in selecting the APs and cabling: (1) the power level, and (2) the speed of transmission. The first generation of POE is known as IEEE 802.3af and supports speeds up to 1Gbps (1000BASE-T) and can deliver a total of 15.4 Watts of power to devices. POE was originally developed to deliver power to desk phones and wireless APs. The next generation of higher transmission speeds is known as IEEE 802.3bz and supports 2.5Gbps (over Cat 5e) and 5.0Gbps (over Cat 6). The newest standard for POE is IEEE 802.3bt, which was defined by the IEEE in September 2018.

POE+, known as IEEE 802.3at-2009 and published as 802.3-2012, is considered the current standard of power over Ethernet and delivers up to 30W over Cat5e cables with 25.5W available to devices. POE+ costs more than POE but the additional power means that it can be used to deliver power to a range of devices including Pan/Tilt/Zoom IP Cameras, video IP phones, and alarm systems. IDC believes that POE+ with 2.5Gbps multi-gigabit Ethernet cabling system would be the logical choice for airport terminals being upgraded or newly built in the 2020–2021 timeframe.

Onsite Radio Frequency Survey, AP Mounting, and Antenna Selection

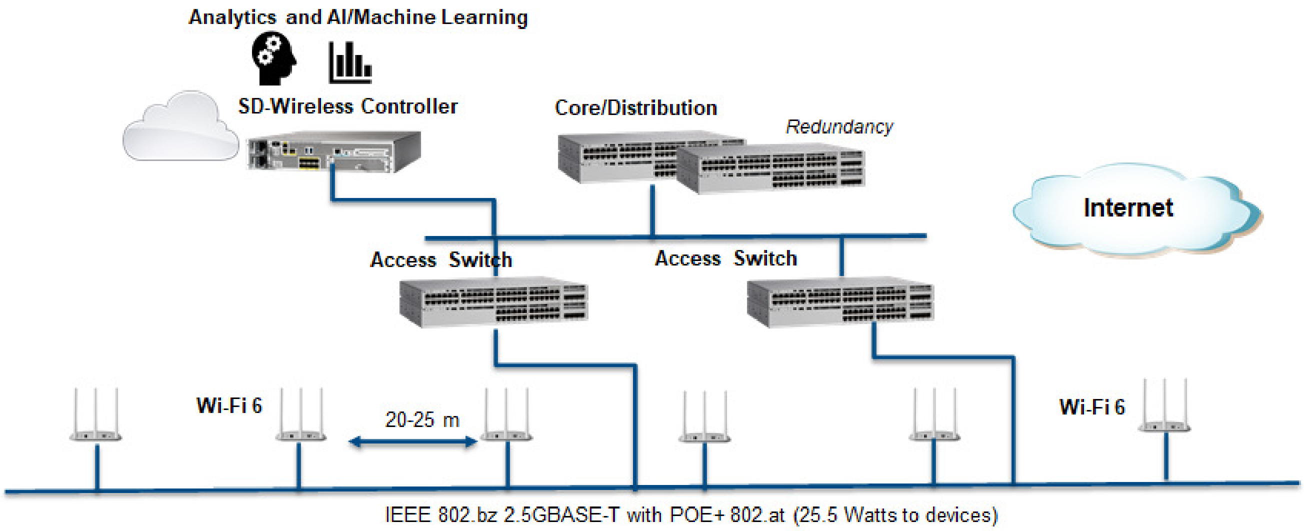
It is important for a major upgrade of the Wi-Fi system that an onsite survey be carried out to understand the radio frequency (RF) characteristics of the geometry and materials of the terminal hall and any corridors that it encompasses as well as escalators and multiple floor areas. Thus Wi-Fi 6 for airports will necessarily have to be an active network of APs connected by a multi-gigabit Ethernet cabling system with POE+.

The height and direction of the mounting of the APs is important and as a general rule of thumb should be at a height below 3–4 meters. This requirement might limit the available mount locations so careful consideration needs to be given to the direction of the AP and the selection of the antennas which will be screwed and twisted onto the AP chassis. It goes without saying that the choice of the antenna is also important. Most OEMs provide the ability to connect different antennas using a standard low-loss connector. One of the competitive differentiators between Wi-Fi 6 vendors is the antenna combiner technology as there is no open standard for this.

Capex versus Leasing Business Model

Another important trend with Wi-Fi in commercial and industrial use cases such as hotels, shopping malls, and public transportation is that the leasing model is gaining more and more favor in certain geographies so understanding the total cost of ownership (TCO) is important not just for the end customer (e.g., the airport authority) but also the providers of leased wireless services.

Figure 3: ***Airport Public Wi-Fi 6 Network Architecture***



Source: IDC

Airport Wi-Fi 6 Use Cases

While leisure travelers rely on wireless connections to check social media; stream sports, TV and music apps; business travelers use it to read emails, download large files and to use video/audio collaboration tools. Going forward, airports are likely to turn to their wireless networks to integrate m-commerce strategies that tap into mobile to recoup some of the cost of providing seamless connectivity. Table 4 outlines some of the use case possibilities.

The growing trend is to offer passengers more choice and control and move away from Wi-Fi networks that are a one size fits all approach. Networks should be flexible to meet each passenger's individual needs. Hybrid Wi-Fi networks can enable an experience that is fast, multiplatform, analytics-driven, responsive, and tiered. Airports can secure these benefits by upgrading networks with Wi-Fi Protected Access (WPA2) security encryption; tiered services with varying speed and bandwidth levels; actionable insights such as queue management, pathing and wayfinding; content management system (CMS) tools; and device flexibility across smartphones, tablets, and laptops.

For seamless connectivity airports are adopting passpoints — so the user does not have to sign in or provide authentication each time he/she uses Wi-Fi. Hotspot 2.0 Passpoint networks provide a WPA2 encrypted connection automatically, ensuring enterprise-level security, with no additional software or Virtual Private Network (or VPNs) needed. Passpoint networks require hardware supporting the Hotspot 2.0 technical specification created by the Wi-Fi Alliance, to make ubiquitous hand-off between networks possible. While most networks provide free Wi-Fi for the first half hour or hour, heavy users needing secure uninterrupted connectivity may be willing to pay a small premium — that is, monetizing passpoint can help visualize new business models.

Normally airports have bandwidth issues due to the high rush of incoming and outgoing travelers especially during peak flight times. This can lead to a lot of interference, especially for business travelers who will want uninterrupted connectivity to send bulky files or participate in important work calls. Critical airport activities also need a low-latency network that has capability of handling hundreds of simultaneous connections at once — both these are features of Wi-Fi 6 network. Wi-Fi at airports could be paid or free. Within the free Wi-Fi service, there can be a captive promotions model where on-premises data can be collected and contextualized offers and discounts can be sent out based on customer preferences, travelling patterns, demographics, and others. The other free Wi-Fi model is where promotions are sought from third parties who or which pay for ad space and push out proximity promotions. In the case of a paid Wi-Fi model, there are a few different options. While the pay for use model is fairly conventional and not very widely used currently, the one that is most popular is a freemium model where guest information is collected to give free Wi-Fi for a certain duration. In case of business travelers and heavy data users, there is a Wi-Fi upgrade model where if higher speeds are needed, a certain fee needs to be paid.

Table 4: *Examples of Airport Use Cases*

Airport Use Case	Description
Flight operations (departures and arrivals)	There are a number of databases that either airport personnel need access to such as arrival and departure time and gate information, airplane parts service, emergency personal contacts, weather checking, and online flight planning.
Passenger movement tracking	When passengers disembark from a flight there is usually a fairly large crowd that makes its way to immigration counters and kiosks. If we consider multiple airplane arriving at around the same time, we can be looking at hundreds, if not thousands, of passengers disembarking and walking toward immigration.
Smart luggage tracking	IoT-enabled bags have fingerprint locking, GPS tracking, weight notifications, and proximity sensors all of which ride on the back of a strong Wi-Fi network. Also, connected beacons are used for baggage handling that transmit information at bag drop and claim about proximity of luggage.
Check-in kiosks	Wireless networks are used for instant flight updates, mobile ticketing, automated check-in processes without manual intervention (e.g., Changi Airport Terminal 4).
Immigration arrivals checkpoints	Wi-Fi has become an important component of automated kiosks where when passengers have a problem at the automated kiosk, such as difficulty in the machine recognizing the fingerprint, an automatic alarm is sent to an immigration officer standing nearby to come to the assistance of the passenger.
Smart buildings and facilities management	As a consequence, architects, engineers, and construction crews need access to detailed blueprint files with cloud-based support including analytical and costing tools. These can be provided via tablets but become much more effective if high-bandwidth is always available (20–30+Mbps] to replace the large scrolls that they often have to carry to the place of repair or new construction work.
Airplane telemetric download	Provided by Wi-Fi 6 and/or 4G/5G after the aircraft has arrived at the gate.
Airplane video upload	For onboard entertainment video content
Hangars	Owned by the Engineering Airline/Engineering company

Source: IDC, 2020

Benefits of Wi-Fi 6 Airport Deployment

Most airports already have 802.11n networks and as they look to refresh and upgrade their networks (in a brownfield upgrade) in the next several years, Wi-Fi 6 offers a number of key advantages that they did not have with previous technology generations:

- The ability to scale by adding more capacity in an incremental fashion
- The ability to automate network operations via software-defined networking orchestration
- The ability to deliver much more bandwidth to IIoT use cases and connect more IIoT devices thereby achieving a dual role
- The ability to offer a much better customer experience for public Wi-Fi access
- The ability to integrate with analytics/AI tools and utilize high-resolution cameras and to realize location determination for passenger flows analysis

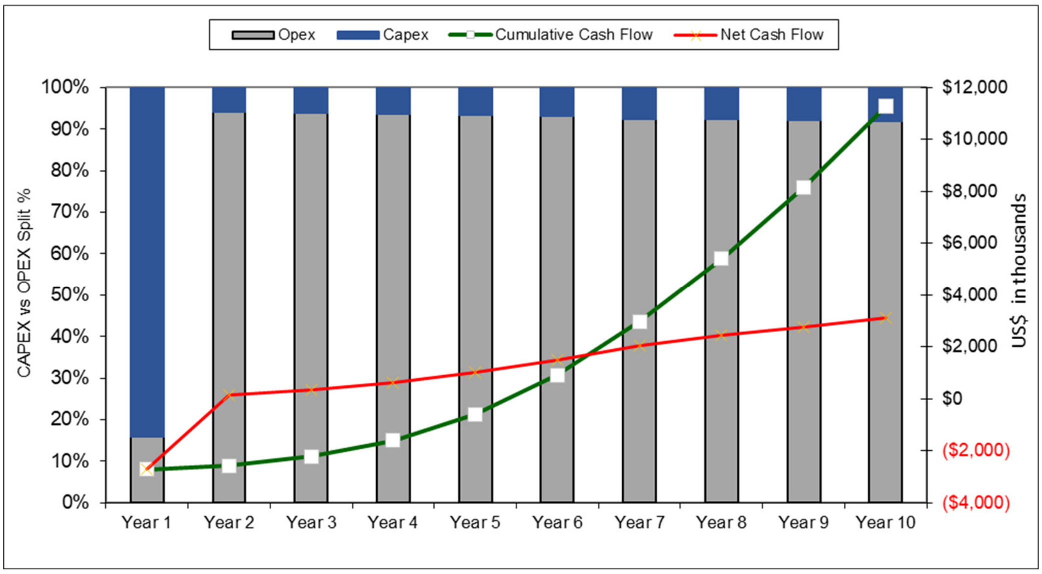
Passengers and advertisers will be more willing to pay for a Wi-Fi service that really delivers broadband all the time and everywhere inside the airport.

IDC has modeled a hypothetical greenfield airport with full public Wi-Fi 6 service in order to gain insights into the Wi-Fi 6 economics to better understand the potential to enhance operations and to create new opportunities. In our model, we have assumed a relatively large airport with terminal and entrance hall area totaling 350,000m^2 (see Figure 4) and we have made various assumptions about the spacing between Access Points, average bandwidths offered to end users, the number of minutes the average Wi-Fi user is connected, and the flow of passengers (47 million annually in our hypothetical case). As shown in Figure 4, the Project indicators are all positive and that is due to the fact that the airport Wi-Fi 6 installation does not need large capex injections once the whole network is built and opex can be contained over the project period from escalating. In our hypothetical model, the Internal Rate of Return (10 years) is 31%, the annualized ROI is 21%, and the 10-year NPV is US$6.6 million on a total capex investment of US$3.2 million. The key to making the airport as a successful business model is the ability to monetize the enhanced user experience Wi-Fi 6 brings to the table, either through premium access and/or advertising on an airport app/digital platform. Most airports already have Wi-Fi infrastructure in place so the capex needed for engineering and installation and routing will already be in place, which further improves the ROI model. The flow of passengers is a function of the overall layout of the airport, the number of airplanes arriving and departing as well as the average number of passengers onboard these flights. Modern large-scale airports track passenger crowd flows using CCTV or other means for the purposes of better managing queues at immigration counters and kiosks and for future terminal expansion. Some of the insights that we gained from the model are as follows:

1. **Possible revenue from advertising and premium Wi-Fi users**. Even with less than <1.5% of total passengers paying for premium Wi-Fi access, the wireless infrastructure can be transformed from what would normally be a cost-center model into cash positive by Year 6. Advertising revenue is another potential revenue stream. We believe this approach could work for major international and regional airport hubs. Premium Wi-Fi users could for example be given access for 1 month, 3 months, and 6 months.
2. **The use of Software-Defined Networking, video analytics and AI, and virtualized applications further strengthen the business model.** Software-defined network (SDN) and virtualization reduce the opex costs and enable for better ROI. We estimated that at least 700 APs would be needed and for larger airports the total number of APs could reach 1000–1500+. SDN orchestration is needed to implement efficient Wi-Fi operations by automating updates to the access points as well as collecting telemetric data from access points and Ethernet switches.

3. **Facilitate the creation of a Digital Platform.** The performance of Wi-Fi 6 makes it an ideal access medium to launch an airport Digital Platform. Airports can create a mobile app for passengers, airport personnel, ecommerce, and advertising. Passengers would be able via the mobile app to purchase Wi-Fi premium access vouchers and receive discount vouchers from retailers located inside and outside the airport. The Digital Platform also has the added benefit of enabling emergency management and alerts such as Digital Signage located through the airport and virtual Digital Signage that can sent to users' smartphone screens. Another example is in larger airports sometimes departing passengers find themselves far from their gate and a personalized message can be sent to the passenger notifying them that they need to walk now to the gate and to provide a map; the traditional way that location is monitored is via infrared sensors but Wi-Fi can also provide the necessary location accuracy.
4. **Improved connectivity and performance**. Wi-Fi 6 access points can handle >4X the number of real-time users (e.g., voice over Wi-Fi calling) as compared with previous generations, which means that busy airports with lots of passenger traffic (millions of passengers per year) would be able to offer a much better customer experience. By simply replacing the 802.11n infrastructure network capacity will increase by 30–40%.
5. **Wi-Fi 6 infrastructure complements cellular coverage.** The large amount of bandwidth and robust security (802.1x) which Wi-Fi 6 delivers for IIoT means that it can be used as a complement to cellular infrastructure throughout various parts of the airport for operations.
6. **Supports both public Wi-Fi and Industrial Internet of Things**. Securing airport wireless infrastructure is critical and Wi-Fi 6 can be partitioned logically to operate as shared resource with different levels of security for IIoT use cases. The airport wireless infrastructure comprising APs, multi-gigabit Ethernet cables, Ethernet switches, routers, and application servers can be used, with appropriate delineation of SSIDs and strict password control, for building facilities management, repairs and construction, and other purposes including surveillance and passenger flow monitoring.
7. **Potential revenue from the Digital Platform can subsidize IIoT infrastructure.** In order for passengers to experience the airport Digital Platform via the mobile app, the experience must be high-quality to build the airport's digital brand. This means that over time it would be possible to develop other revenue streams to offset operating costs.

Figure 4: ***Hypothetical Business Model for Airport Wi-Fi 6 Service***



Source: IDC, 2020

Conclusion

The wireless LAN infrastructure in airports is required to serve multiple purposes — passengers, airport and tenant enterprises, and IIoT for infrastructure. As a result, airports can design their wireless LAN network to provide comprehensive coverage across all floors, halls, and corridors. By deploying Wi-Fi 6 airports can offer much improved customer experience even in congested areas, while at the same time delivering more capacity for IIoT applications. Moreover, WLAN infrastructure must also complement the cellular infrastructure and in certain use cases within the airport can act as a secondary, backup network, or coexistence network for various use cases.

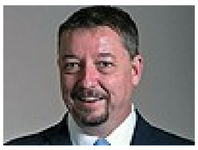
About the Analyst

Bill Rojas, *Research Director, IDC Asia/Pacific*

Bill Rojas is an Adjunct Research Director with IDC's Asia/Pacific Communications group. Based in Hong Kong, he is responsible for both telecom consulting projects and IDC's syndicated research products covering carrier infrastructure, M2M, and IoT. His research expertise includes mobile 3G/4Gcellular, wireless broadband, capital expenditure analysis of fixed and mobile carriers, and advanced fixed and wireless technologies and services.

Shaily Ajay Shah, *Research Manager*

Shaily Shah is a research manager for IDC's Asia/Pacific Internet of Things (IoT) practice. Based in Singapore, Shaily is responsible for driving the IoT program and delivering research and executing projects with respect to IoT in the Asia/Pacific region. In this role, she uses consultative-based approach to advise vendors and industry players on topics such as urban ecosystems, IoT readiness, smart cities, and wearables, among others.



Hugh Ujhazy, *Vice President, IoT and Telecommunications*

Hugh Ujhazy leads both the Internet of Things (IoT) and Telecommunications practices for IDC Asia/Pacific.

The Telecommunications research involves leading the analysis of fixed and mobile network services across APEJ. It also includes evaluation of service provider and equipment vendor strategies in meeting these user requirements in the increasingly competitive Asia/Pacific market, assessing the impact of market liberalization, and the evaluation of new services offerings.

MESSAGE FROM THE SPONSOR

With users expecting an immersive experience coupled with explosion of IoT and mobile devices, wireless networks need to be secure, fast, and reliable. Cisco has developed a wireless portfolio comprising access points and wireless controllers that support Wi-Fi 6 (802.11ax). From IoT to a growing inventory of applications, the **Cisco wireless network** provides an always-on, always-available solution that is founded on an intent-based architecture. Cisco provides comprehensive security with "Encrypted Traffic Analytics" (ETA) and Multilingual Access Points providing visibility and communications with Zigbee and BLE as well. Going beyond the Wi-Fi 6 standard, the Cisco Catalyst 9100 access points provide integrated security, resiliency, and operational flexibility, as well as increased network intelligence with custom RF ASIC. Cisco's RF ASIC provides flexible radio assignment, CleanAir, Wireless Intrusion Prevention System and DFS detection. **Cisco DNA Center** with the help of streaming telemetry and contextual data from every access point and controller, provides complete visibility and guided remediation that allows single-click resolution. It provides a 360-degree contextual view of user, network, and applications that allows it to isolate an issue and tell IT where to focus. **Cisco DNA Spaces** digitizes the physical space by synthesizing location data gathered from Cisco Wireless network to deliver location-based services at scale.

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com

IDC Custom Solutions