White paper
Cisco public

Wi-Fi 6 and Private LTE/5G Technology and Business Models in Industrial IoT

Wireless trends and the different phases of technology adoption

With the recent availability of Wi-Fi 6 solutions, the launch of 5G pilot projects tied to the ongoing 5G worldwide spectrum allocation, and new shared license spectrum policies (i.e., Germany-BNetzA, Sweden PTS, and U.S. CBRS), many decision makers, systems integrators, and industry partners are wondering what the most appropriate wireless strategy will be for the Industrial Internet of Things (IIoT).

The answer? There is no one-size-fits-all solution. IIoT will require multiple technologies to meet the fluid demands of the varied industries with complex infrastructures.

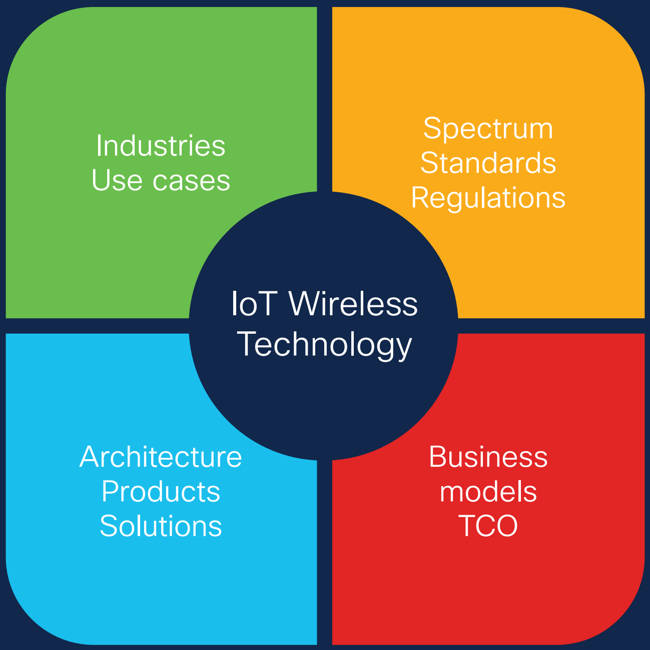


Figure 1: Aspects of IIoT wireless technology adoption

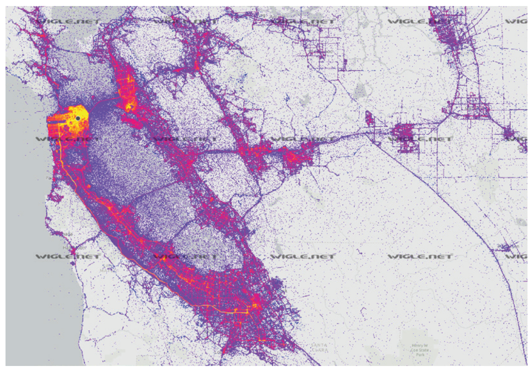
This paper reviews the latest wireless trends and discusses the different phases associated with technology adoption, including licensed, shared license, and unlicensed spectrum; standards and regulations; architecture and equipment; and operational requirements. It also describes business models that may be adopted when deciding to integrate these new wireless trends.

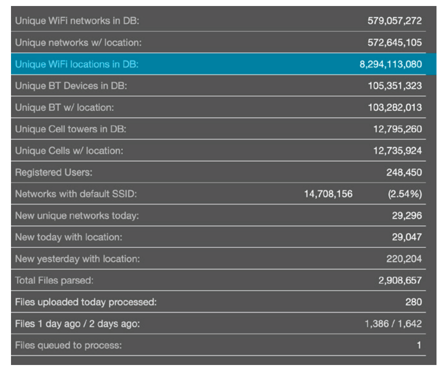
Network history

Networking history has demonstrated that the network access layer consists of multiple technologies while all data is exchanged over the Internet Protocol (IP).

The case for private cellular

Wi-Fi networks are everywhere, enabling connections within IIoT transportation verticals (bus stations, railways, planes and cars), smart cities, health, utilities, oil, and mining to consumer homes, small businesses, and global enterprises. As illustrated in Figure 2, there are now more than 8 billion unique locations worldwide.





Unique WiFi networks in DB:		579,057,272
Unique networks w/ location:		572,645,105
Unique WiFi locations in DB:		8,294,113,080
Unique BT Devices in DB:		105,351,323
Unique BT w/ location:		103,282,013
Unique Cell towers in DB:		12,795,260
Unique Cells w/ location:		12,735,924
Registered Users:		248,450
Networks with default SSID:	14,708,156	(2.54%)
New unique networks today:		29,296
New today with location:		29,047
New yesterday with location:		220,204
Total Files parsed:		2,908,657
Files uploaded today processed:		280
Files 1 day ago / 2 days ago:		1,386 / 1,642
Files queued to process:		1

Figure 2: Wi-Fi statistics (source: https://wigle.net and https://wigle.net/stats#)

Mobile service providers deploy cellular infrastructures, mainly targeting mobile phone users as well as IIoT machine-to-machine (M2M), remote, or mobile Internet access from small businesses to global enterprises. Figure 3 shows a visualization of one of these cellular databases.

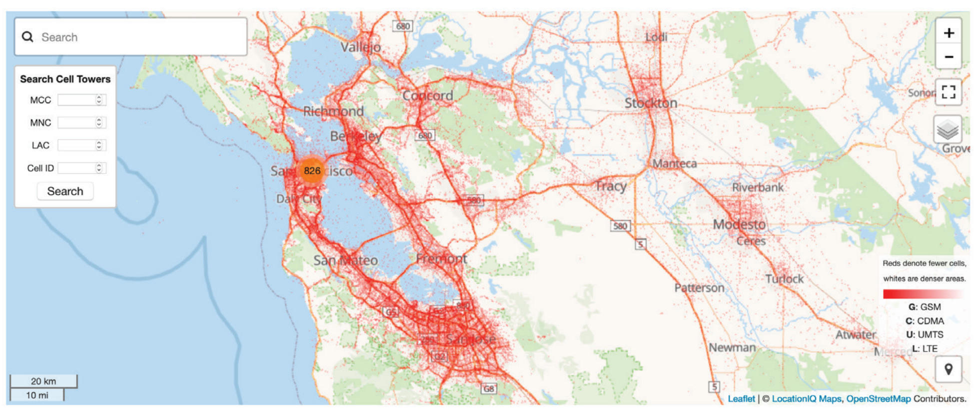


Figure 3: Cellular infrastructure (source: https://opencellid.org)

However, vertical industries requiring IIoT solutions may not always get the appropriate coverage from public cellular services. Therefore, deployment of private cellular infrastructures is considered for use cases such as the following:

- Mining, ships, aircraft, oil fields, and other locations with no public cellular service coverage
- Underground tunnels, factory floors, ports, warehouses with heavy metallic environments, and other locations where signal propagation may require too many Wi-Fi access points to deliver proper services
- Nuclear plants, defense locations, and other areas with strong government policies and regulations on wireless access

IIoT wireless technologies trends in 2020

Licensed spectrum

5G
Spectrum: licensed or shared licensed or *unlicensed*, bands: Sub-GHz, 1 to 6 GHz, mmW (i.e. 24 to 28 GHz)
Infrastructure: public *& private (i.e. shared license model)*
Data rate: 4.9 Gbps to 10 Gbps (MIMO)
Distance: Long range and short (mmW)
Modulation: OFDMA
Channel: 5G NR maximum carrier bandwidth is up to 100 MHz in frequency range 1 (FR1: 450 MHz to 6 GHz), or up to 400 MHz in frequency range 2 (FR2: 24.25 GHz to 52.6 GHz) that can be aggregated with a maximum bandwidth of 800 MHz.
Network slicing services: 3GPP rel. 16
Ultra Reliable Low Latency Communications

4G/LTE
Spectrum: licensed or shared licensed (i.e. CBRS, B43), bands: Sub-GHz, 1 to 6 GHz
Infrastructure: public *& private, i.e. CBRS*)
Data rate: LTE category dependent: 100/50 Mbps (cat.3), 150/50 Mbps (cat.4), 300/50 Mbps (cat.6)
20/60 kbps (NB-IOT, half-duplex), 1200/150 (cat.18)
Distance: Long range
Channel: LTE carriers are narrow in bandwidth, up to 20 MHz maximum that can be aggregated together to create a channel bandwidth up to 100 MHz in LTE-Advance, or up to 640 MHz in LTE-Advanced Pro.

Unlicensed spectrum

Wi-Fi 6 (IEEE 802.11ax)
Spectrum: Unlicensed, bands: 2.4 GHz, 5 GHz, *6 GHz*
Infrastructure: Public & private
Data rate: Wi-Fi 5 (.ac) 1.3 Gbps (W1) to 6.9 Gbps (.ac W2, 4x4 MU-MIMO)
Wi-Fi 6 3.5 Gbps (160 Mhz channel, single stream) - 4x4 MIMO 14 Gbps
or 800 Mbps @ 40 GHz channel – 3.2 Gbps 4x4 MIMO
Distance: Medium range
Modulation: OFDMA (Wi-Fi 6), Channel: 20, 40, 80 & 160 MHz

Wi-SUN (IEEE 802.15.4g)
Spectrum: Unlicensed, bands: 902 to 928 MHz
Infrastructure: Private
Data rate: 50 kbps/150 kbps (2FSK) to 1.2 Mbps OFDM
Distance: Medium range, Mesh

LoRaWan
Infrastructure: Public & Private
Data rate: 250 bps to 5.4 kbps (EU868), 980 bps to 21.4 kbps (US915)
Distance: Long range – LoRa modulation
Channel: 125 kHz & 500 kHz (US915), 125kHz (EU868)

Figure 4: IIoT wireless technologies trends in 2020

New multi-gigabit wireless technologies

In Industrial IoT, the emergence of new multi-gigabit wireless technologies for access and backhaul–ranging from low data rate (bps to kbps), i.e., LoRaWAN or NB-IoT (narrowband IoT), to medium (kbps to Mbps), i.e., Wi-SUN, Wi-Fi (802.11a/b/g), and 2G/3G to high, i.e., Wi-Fi (802.11n/ac) and 4G/LTE–means that a new generation of wireless standards is now emerging, enabling multigigabit data rate: IEEE 802.11ax or Wi-Fi 6 and LTE Cat.18 (gigabit LTE) and 5G. See Figure 4.

Spectrum drives access technology

Whatever the technology or business model used, decision makers, systems integrators, and business partners must address the availability of spectrum; standards and regulations; architecture and equipment; and automation and security tools to ensure successful wireless services deployments. This will be discussed in the following sections.

Regulatory environment and spectrum

Spectrum is *the* critical resource for wireless infrastructures and is categorized in three main buckets: unlicensed, licensed, and shared license. Strongly controlled and regulated around the world, the allocation of frequency bands attempts to keep aligned with market developments.

A country's regulations are key elements of wireless operations. For example, local regulations for Wi-Fi apply to access points (APs), mandating that a product's references to identify the country or the world region where it can be deployed and the parameters of its radio coverage.

Local regulations for 5G and 4G may vary between mobile operators and fully private deployment. Regulators are actively working to allocate and, in some cases, reallocate spectrum for the 5G transition across licensed, unlicensed, and shared spectrum to support the anticipated demands. Regulators are focused on balancing spectrum allocation to support the needs and growth in the expanding multiaccess environment. This balance includes spectrum allocations between licensed, unlicensed, and shared as discussed in more detail later in the paper.

Spectrum categories

Spectrum is often referred to in the following three categories: low-band (600 to 900 MHz), midband (1 to 6 GHz), and millimeter wave (mmW) (> 24 GHz). One evolution with the development of 5G technology is the opening of mmW frequencies (above 24 GHz). Examples of current 5G frequency allocations in some countries can be found in Figure 5 below.

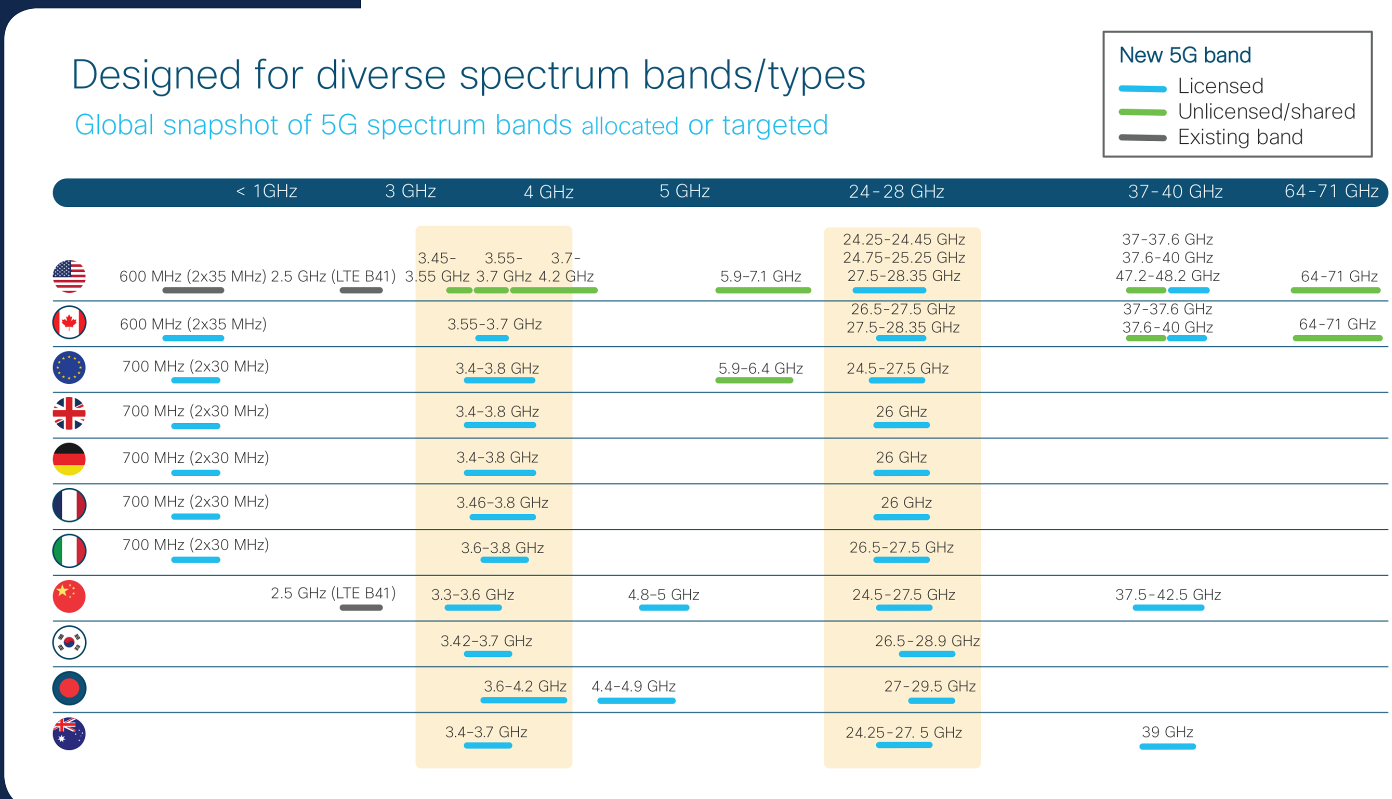


Figure 5: 5G spectrum allocation sample as of today

Regulations and spectrum "harmonization" avoid issues related to the interference in spectrum usage. Many users are very sensitive, and side-band interference can create negative impacts to other services.

Spectrum types

Unlicensed spectrum

Unlicensed bands, such as 863 MHz, 915 MHz, 2.4 GHz, and 5 GHz, are available internationally under the industrial, scientific and medical (ISM) umbrella as defined by the International Telecommunication Union (ITU). They are generally free of charge, regulated locally, and at the heart of many industrial wireless networking protocols, such as Wi-Fi, Wi-SUN, Wireless Hart, ISA100, and Bluetooth.

Example for U.S. FCC

In the U.S., CBRS is a shared licensed spectrum access with three licensing options.

In terms of CBRS spectrum, two categories of base stations (CBSD) are defined.

Category A is permitted to a maximum Equivalent Isotropically Radiated Power (EIRP) of 30 dBm or 1 watt; if installed outdoors, the antenna must not exceed 6 meters or nearly 20 feet in height. CBSD Category B allows a maximum EIRP of 47 dBm or 50 watts for outdoor antennas only, with a height expected to be greater than 6 meters. CBRS client devices are permitted to transmit at maximum power 23 dBm or 200 mW. Category A CBRS users, whether GAA or PAL, are required to transmit their FCC ID number, authorization status, call sign, contact information, manufacturer's serial number, air interface capability, and sensing capability that they support.

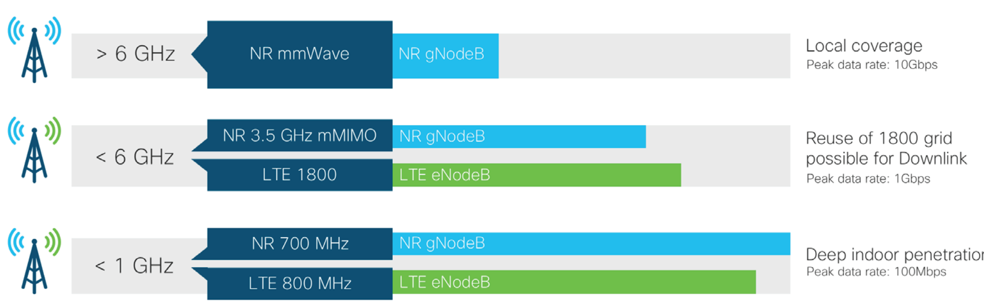
Category B CBRS users must support all of the previous stated requirements plus azimuth, beam-width, antenna gain, down-tilt angle, and antenna height (above ground).

These frequencies are fundamental to the digital economy. With potentially new allocation, i.e., 6 GHz in the United States, several attempts have been made to add unlicensed support to Long Term Evolution (LTE), such as multeFire, and 5G services (3GPP release 16 5G New Radio (NR) unlicensed spectrum definitions). Wi-Fi 6 is ready for the new 6-GHz adoption, and work is done in the 60-GHz band (IEEE 802.11ad).

Licensed spectrum

Mainly available for service providers offering 4G/LTE and soon 5G services, licensed bands are allocated to operators at a negotiated cost (through auctions) in each respective country. In addition, there is a potential for public safety or industries to get some reserved licensed bands.

There are significant differences from low-band to mmW related to coverage and throughput capabilities. Low-band supports longer distances; however, it has lower data rates compared to mmW. As the spectrum map moves up to mmW, there are much higher data rates, but the distances are very short and can require more than 100 times the number of antennas/NRs compared to 4G/low-band spectrum deployments. FCC Commissioner Brendan Carr noted earlier this year that: *"There are roughly 300,000 cell sites across the country today, but 5G is going to require a 10- to 100-fold increase in cell sites."* This is known as the "5G densification" challenge for mmW build-outs. Figure 6 [from GSMA] provides a good visual representation of the differences from low-band to mmW characteristics. It is important to note that while mmW propagation is not as good, it has the potential for high-spectrum reuse due to its short reach.



Notes:

- LTE not suited for mmW deployment
- Higher propagation loss at 3.5 GHz compensated by
  - Massive MIMO (mMIMO)
  - Beamforming
- Limited availability of spectrum below 1 GHz limits performance

Figure 6: 4G/LTE and 5G coverage comparison

Antenna elements

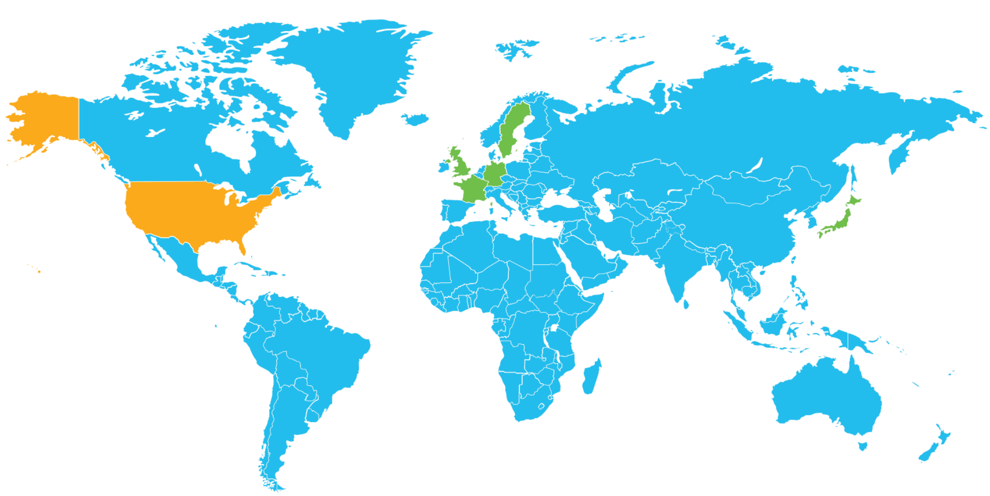
5G R&D studies, such as FP4-ICT-671650-mmMAGIC/D1.1, assessed the suitability of mm-wave spectrum on key KPIs related to mobile communications, i.e. coverage, capacity, mobility and device complexity.

Results validate the need for the "**5G densification**," estimating the need to increase the number of antennas, in order to compensate the path loss, roughly at the rate of square of the frequency increment, as shown in the table to the right.

Carrier frq (GHz)	10	28	38	73
Numbers of antenna elements	4	32	64	256
BW (MHz)	500	500	500	600
Cell radius (m)	250	250	250	100
Coverage – No. of cells (Rref/R)	1	1	1	6.25
Suitability value	10	10	10	1.6

Shared license spectrum

A number of countries currently provide shared license spectrum usage. Many are studying the need and value for shared spectrum as well as dedicated spectrum. The United States has Citizen Broadband Radio Service (CBRS) –150 MHz of 3.5 GHz (band 48) – and Europe is looking at the 2.3 to 2.4 GHZ band for shared licensed spectrum [ETSI LSA]. Figure 7 provides a global view of both shared and dedicated spectrum allocations to date.



* China, US, Japan, Germany, Sweden, South Korea, UK, France, Italy, Netherland

Figure 7: Dedicated/shared spectrum around the world

Shared license spectrum

In the U.S., CBRS is a shared spectrum access with three licensing options:

Incumbent Access (IA)

Priority Access Licenses (PAL)

General Authorized Access (GAA)

Access to the shared license spectrum requires a management system, such as the U.S. CBRS Spectrum Access System (SAS), to avoid interference between incumbents and users sharing the spectrum. The U.S. CBRS model has three levels of access as shown in Figure 8:

- Incumbent Access (IA): Access that has absolute priority over any other user(s), i.e., U.S. Navy or fixed satellite services.
- Priority Access License (PAL): A PAL will be granted to users, such as government agencies, utilities, or network operators, through competitive bidding within the 3550 to 3650 MHz frequency. Licenses (FCC rulemakings 12-354 and 17-258) are obtained for up to 10 years for a well-defined geographical area and are renewable. PALs provide authorization to use a 10 MHz channel in a small geographical area. A total of seven PALs may be assigned in any given county in the United States;; a maximum of four PALs can go to a single applicant/user.
- General Authorized Access (GAA): This tier is referred to as the rule-to-permit open flexible access to any portion of the 3350 to 3650 MHz spectrum band not assigned to any higher tier applicants or users. GAA also allows for operation in unused PAL channels. The goal of GAA is to open up spectrum for a wide variety of potential users and use cases.

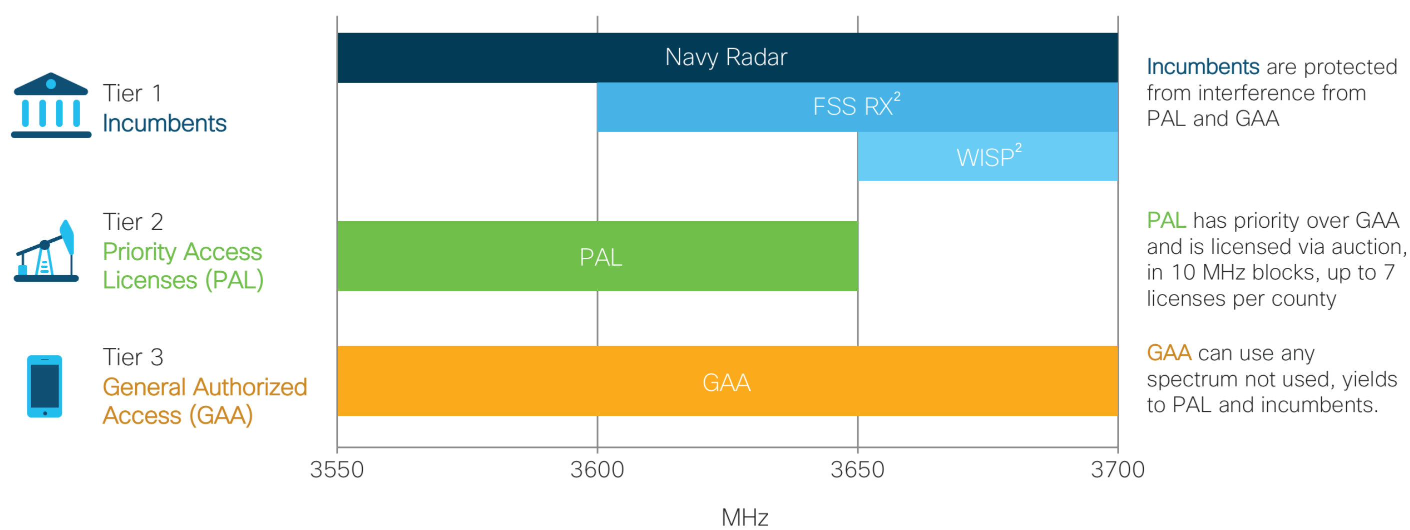


Figure 8: U.S. CBRS overview

Standards development organizations, alliances, and nonprofit organizations

IEEE

Wi-Fi Alliance

3GPP

ITU

CBRS

While the shared license spectrum is an opportunity for private LTE or 5G deployments, the allocation process, cost, and duration must be well understood for the selected locations. In suitable use cases, CBRS or shared licensed spectrum will complement Wi-Fi with wider coverage.

A subset of the shared spectrum is known as dedicated spectrum. Several countries are providing a dedicated spectrum that is nonpublic/incumbent spectrum that could be used for specific uses outside of the service provider model. Germany, Sweden, the U.K., and France are all active in creating dedicated spectrum. Again, Figure 7 shows a summary of various countries' activities. One of the key areas of focus is IIoT for the manufacturing vertical. Dedicated spectrum will require a country-specific license and a purpose-built network that would be used to provide services run by an IT department or a third-party contracted company.

Standards

During the past 30 years, standardization has become one of the fundamentals of the networking industry, enabling interoperability, easing regional and industrial certifications and compliances, and simplifying architecture and design of solutions.

IEEE and Wi-Fi Alliance

The Institute of Electrical and Electronics Engineers (IEEE) is the main standards development organization (SDO) for LAN/MAN Layer 1 and Layer 2 specifications as well as for their manageability and enhanced functions sitting between the ISO model Layer 2 and Layer 3. With more than 20 years of development, the IEEE 802.11 working group has defined multiple generations of wireless LAN standards (IEEE 802.11a/b/g/n/ac), referred to as Wi-Fi. The latest generation—IEEE 802.11ax, also referred to as Wi-Fi 6 discussed in Cisco Wi-Fi 6—was initially defined with the objectives of IEEE 802.11ax:

- Improving spectrum efficiency and area throughput
- Improving real-world performance in indoor and outdoor deployments
  - In the presence of interfering sources, dense heterogeneous networks, and
  - In moderate- to heavy-user loaded APs

Standard status is that the 802.11ax Task Group called for an initial sponsor ballot in July 2019, with planning for final approval by January 2020.

The Wi-Fi Alliance leads the promotion, certification, and interoperability of the technology. To increase the public recognition of the latest enhancements, the Wi-Fi Alliance decided to brand each Wi-Fi generation, e.g., Wi-Fi 6 for IEEE 802.11ax and Wi-Fi 5 for IEEE 802.11ac.

3GPP 5G use cases classification

Enhanced Mobile Broadband (eMBB)

Massive IoT (mIoT)

Ultra-Reliable Low-Latency Communication (uRLLC)

Speed increases with each generation. With Wi-Fi 6, speeds reach over 1 Gbps while offering a symmetrical data rate of the bandwidth. And while Wi-Fi clients are universal, individual countries have local regulations defined for the AP characteristics that mandate compliance with specific transmit power and channels.

One of the benefits of Wi-Fi 6, in addition to its enhanced performances characteristics, is its backward compatibility with other Wi-Fi generations. Wi-Fi 6 APs can connect previous generations of devices, while Wi-Fi 6 client devices can connect to older generations of APs.

Also well known for the Ethernet standard suite (IEEE 802.3), one IEEE Task Group of particular interest is the Time Sensitive Networking (TSN) Task Group. It develops a set of specifications to provide deterministic services over Layer 1 and Layer 2. While today it is implemented only on Ethernet switches, i.e., the Cisco® Industrial Ethernet 4000 Series, to cover manufacturing process or transportation use cases, there is a trend to expand TSN to the new emerging wireless access technologies.

3GPP (4G/LTE and 5G)

The 3rd Generation Partnership Project (3GPP) leads the cellular telecommunications network technologies' architecture and specifications (radio access, core transport network, and service capabilities) through subsequent releases. Developed for mobile operators over multiple generations (2G GSM/GPRS/Edge, 3G UMTS), the predominant technology deployments around the world are known as 4G or LTE. 5G is the next generation developed with the objectives of:

- Enhanced Mobile Broadband (eMBB)—Higher data rate (+ Gbps), area capacity, and traffic/users
- Massive IoT (mIoT)—Large number of devices per square km
- Ultra-Reliable Low-Latency Communication (uRLLC)

Other alliances and organizations

Several alliances work on products' certification and promotion of private cellular use, including the CBRS Alliance and the MulteFire Alliance (LTE over unlicensed). Speed increases were done for LTE, with the various LTE categories' definitions introduced over 3GPP releases. It increases the data rate of the asymmetric cellular radio up to gigabit speed, while new radio 5G promises to reach multigigabit speed. As technology evolves, new devices with 5G radio won't be able to connect to or with previous generations of LTE services unless their radio also complies with 4G (backward compatibility), as seen with previous GPRS and 3G/UMTS generations. In private 5G use cases, it will call for both 4G and 5G support – radio and enhanced packet core – if backward compatibility is a requirement. The new fifth generation, or 5G, is a multiyear project of 3GPP with multiple releases. Figure 9 below provides an overview of the overall schedule for 3GPP and ITU as well as commercial adoption.

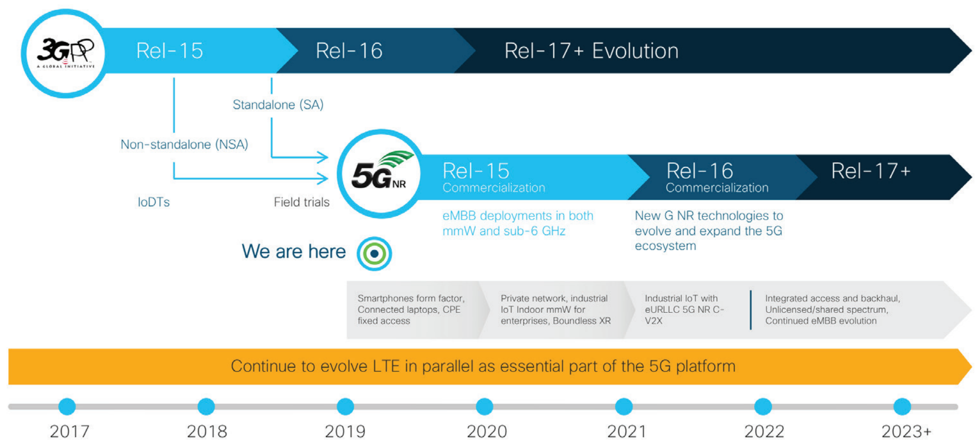


Figure 9: 3GPP release overview

ITU

The ITU is focused on global harmonization between spectrum regulations and standards. There is a deep collaboration related to 5G. 3GPP will present its recommendations for 5G uses which ITU will include in the International Mobile Telecommunications-2020 (IMT2020) procedures. ITU embodies principles of public-private partnership, with its current membership of 193 countries and more than 800 private-sector entities and academic institutions.

Relative to 5G, the ITU coordinates the global usage scenarios of the radio spectrum as shown below.

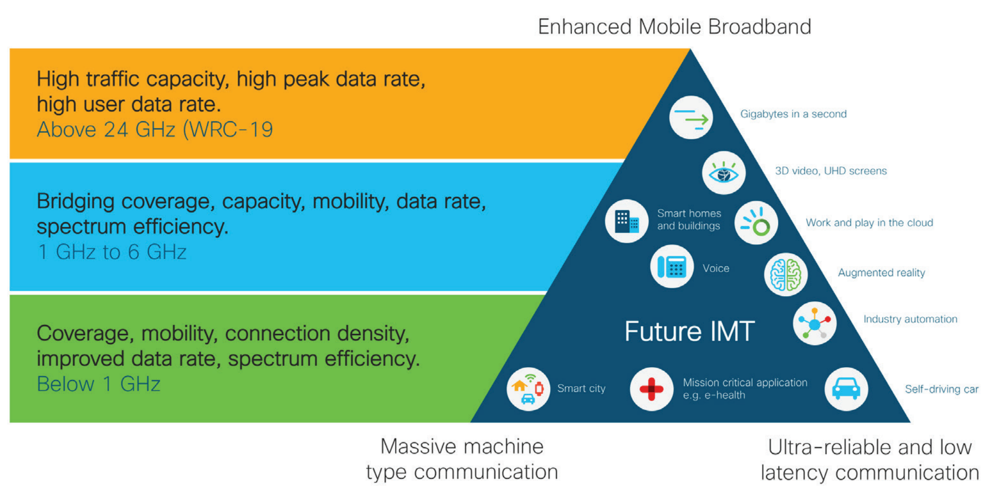


Figure 10: Usage scenarios of IMT for 2020 and beyond

IIoT Use Case and Requirements

Low latency

In Industrial IoT networking, latency and bandwidth requirements are largely dependent on the use cases as shown in Figure 11.

Industries	Use cases	Latency	Throughput
Manufacturing	Robot control, packing machine, printing machine	<1 ms	Kbps
Manufacturing, Warehouse, Distribution Center	Automated guided vehicle – AGV Autonomous mobile robots – AMR	<10 ms	Kbps
Manufacturing	Robot health predictive maintenance	<10 ms	Kbps
Mining	Production monitoring and data telemetry, fleet tracking, dispatch, PTT, video, voice, and messaging, machine health, personal safety	<10 ms	Mbps
Oil & Gas	Offshore/remote site production control and data telemetry, mobile workforce tracking, data and voice, security and video surveillance	+10 ms	Mbps
Utility	Power plant production monitoring, data telemetry, safety, DA	+1 s	Mbps

Figure 11: Industrial IoT use cases latency and throughput

Today, low latency in control loop use cases is handled through wired technology, i.e., Ethernet Time-Sensitive Networking (TSN) standards [Cisco TSN] or local computing. For example, an autonomous guided vehicle (AGV) or autonomous mobile robot (AMR) must stop if it detects a human and is not dependent on communication media to prevent accidents. Therefore local computation generally handles the physical security tasks.

Existing Wi-Fi deployments, i.e., railways, subway controls, or entertainment park attractions, have demonstrated latency as low as 5 msec for a 40-Mbps stream of PLC traffic using IEEE 802.11ac solutions with product optimizations. It is expected that Wi-Fi 6 with new features such as Orthogonal Frequency-Division Multiple Access (OFDMA) can achieve better results.

On 5G, 3GPP release 16 defines Ultra-Reliable Low-Latency Communications (URLLC) with requirements of <5 msec (1 msec stretch goal)/1 Mbps stream. In private 5G industrial deployments, this is expected to lead industrial innovations in process control and automation. 3GPP and 5G-ACIA are now evaluating how TSN could help on such wireless technologies and use cases. Release 16 defines more specific features and capabilities for URLLC. Also, it is expected that 3GPP release 17 will provide detailed coverage of the use cases and further refinement of the standards related to URLLC.

Essential architecture and equipment

Architecture and equipment - what it means to deploy

Developing new wireless technologies is similar to building a house. You need to have a master plan or blueprint before you can start building—whether it's a simple cottage or a mansion. Similarly, a business interested in deploying wireless technologies must have a "blueprint" that addresses standards, regulations, and spectrum to ensure a "solid foundation." The next step (for our house and wireless deployment) is to build the structure—put up the walls and add the roof (architecture and equipment). And don't forget the final touches—automation and security—before moving in (deployment). Continuing the analogy, we all know it's easier to deal with one contractor as a single point of contact—whether it's building a house or installing wireless networks. Cisco is the one provider committed to delivering multiaccess solutions, services, and support.

Both Wi-Fi 6 and 5G are Layer 1 and 2 technologies that must integrate the overall data communications infrastructures. These are mostly based on IP as deployed by enterprises and service providers. In addition, backward compatibility must be ensured to keep running all existing devices and services. As it is rare to see the full deployment of new technologies overnight, automation, security tools, and solutions must be able to adapt to these newer devices (Wi-Fi 6 and 5G), while preserving the older one's functions. Let's review the components required for such deployment.

- Client devices or UE (user elements) – A device with Wi-Fi 6 interface (backward compatibility is part of Wi-Fi 6) or 5G interface(s) (4G backward compatibility requiring 4G modem capabilities) and associated software support. While mobile phones are generally available with both technologies, in IIoT, machines, PLCs, tablets, and PCs require extra support to add a cellular interface. On IoT gateways, connecting machines' new interfaces are required to connect through either Wi-Fi 6 infrastructure or 5G infrastructure or both.
- Access point (AP) or base station (BS) – Infrastructure devices provide the connectivity between clients and the overall network. Indoor or outdoor Wi-Fi 6 APs can connect all generations of Wi-Fi clients at different data rates. On private 5G, base stations – also referred to as gNodeB – enable connectivity for 5G NR for one or more of the different frequency bands (sub-GHz, 1 to 6 GHz or mmW). If 4G/LTE backward compatibility is required, the base stations must support both radio types.
- Centralized controller – Managing ten or more APs or BSs in an enterprise has driven the need for centralized management. The Cisco wireless LAN controller portfolio is an example of the topology's flexibility and ease of operations, regardless of the Wi-Fi protocol version. On cellular infrastructure, Evolved Packet Core (EPC) is at the center of the communications. With the evolution of 5G packet core, functions

Phases of deployment

Spectrum, radio planning, design

Network planning

Security planning

Installation

Operations

Troubleshooting

can be virtualized, enabling user plane functions (UPF) in private 5G to be distributed closer to the user's applications, while control plane functions (CPF) stay a key central element. If private 4G and 5G must be considered, EPC must be able to support both, as discussed later.

- **Edge computing** – A key component of IIoT network design, edge computing was made available across the Cisco industrial IoT portfolio, including IoT gateways, switches, and industrial wireless APs. Therefore, it is an expected feature on Cisco Wi-Fi 6 APs and IoT gateways within private LTE/5G deployment. 3GPP 5G architecture defines Multi-Access Edge Computing (MEC) as one of the key pillars for low latency. Coupled with the policy control function that will locally route the traffic through the User Plane Forwarding (UPF) function, it is expected to play an important role in private 5G deployment, as discussed in a later section.
- **Automation and management** – Scalable deployment and operations in IIoT require software solutions that ease a deployment to lower the overall TCO. The overall integration of either Wi-Fi 6 or private 4G/5G elements in operations must consider how functions, such as SD-WAN, Zero Touch Deployment (ZTD), device provisioning and authentication (i.e., SIM, SSID, WPA keys) should evolve. The emergence of high data rate technologies (Wi-Fi 6, 5G) cannot be treated differently, as industrial operations are consolidated over IP. Integration of new clients' devices and AP/BS must be supported by tools, solutions, and proper processes and training to go through the steps of operations:

- **5G backward compatibility and deployment options** – 5G is being deployed in two models, standalone (SA) and non-standalone (NSA). Most global deployments will be NSA, which allows for 5G NR to connect to the 4G packet core. Over time, the 4G packet core will be upgraded to a 5G next-gen packet core. 3GPP is still working on the 5G evolution paths. Figure-12 shows how 3GPP defined a set of four deployment strategies in release 15.

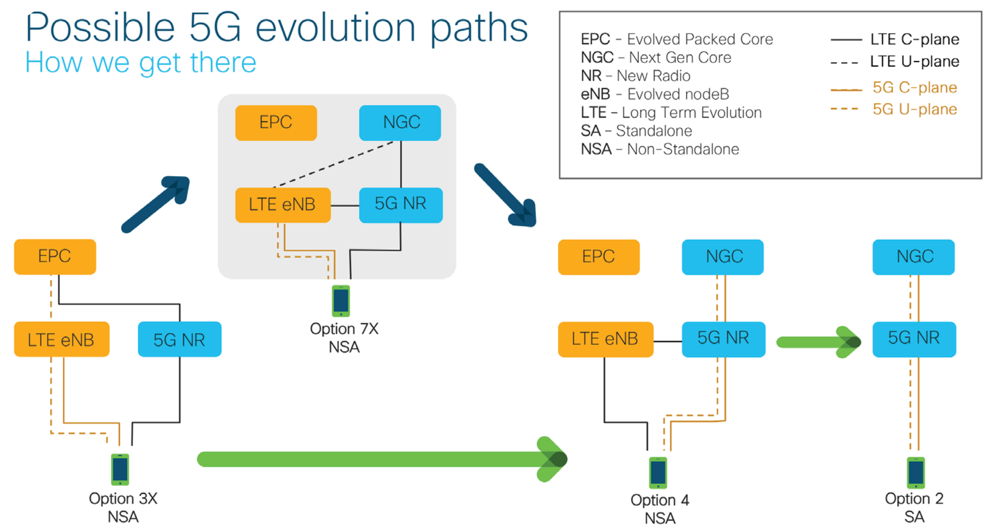


Figure 12: Possible 5G evolution paths

Security – As discussed in the Cisco security blog, security is a multilayered and multidimensional concept. Adoption of new access technologies must cope with the threats specific to those and provide specifications, processes, best practices, and tools that address the potential risks. Wi-Fi 6 emerging solutions are tied to the WPA3 protocol, while 3GPP 5G security threats were discussed in the following paper [The Evolution of Security in 5G – A “Slice” of Mobile Threats, July 2019], focusing on the Americas regions.

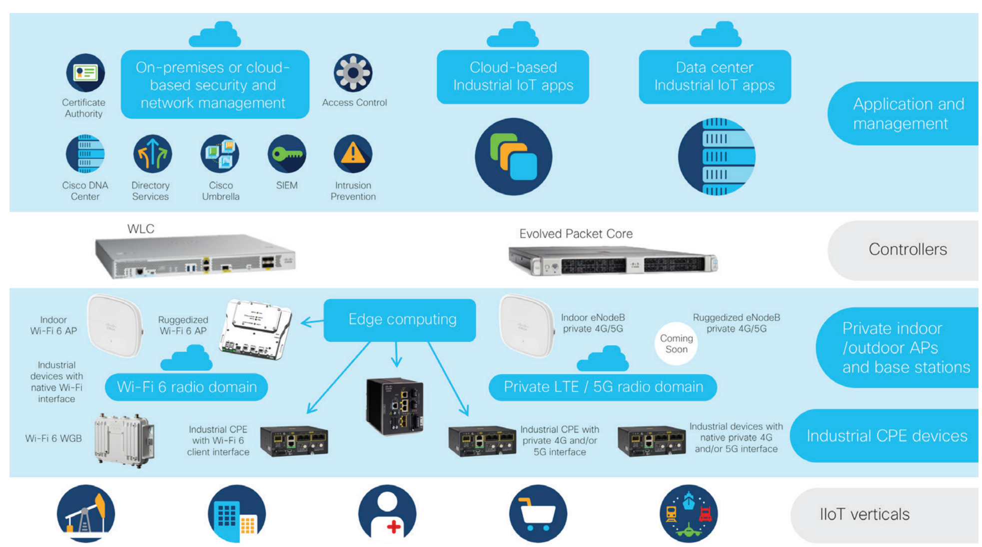


Figure 13: Architecture and equipment overview

Before discussing the different business models tied to the adoption of the new wireless technologies, we should make clear that all component layers represented in Figure 12 will have to be considered for the selection of a model, enabling enhancements and optimizations of the Industrial IoT operations.

Impacts of multiaccess edge computing (MEC)

Cisco is a leader in edge computing, locating general-purpose compute, storage, switching, control functions, and application support close to a user or IoT endpoint. One of the key advantages of edge computing is the benefit to application performance and QoE/efficiency, and therefore the economics based on the use case. Clearly, edge computing improves network latency due to transit to a data center or cloud. Reduced latency provides significant improvements in performance and reliability as well as data control (depending on the use case and deployment model).

There are also regulations that may drive the deployment and use of edge computing. Edge computing in the 5G realm is referred to as multiaccess edge computing (MEC). Today the mobile network has core data centers at regional and local levels as well as public and private clouds in support of SP services. As 5G is deployed to support many of the high-bandwidth and low-latency services, there will be an investment in edge computing at various levels: local, cell towers and on-premises. This will be necessary to achieve the 1- to 5-msec latency needed for various verticals, including IIoT. It may call for vast compute and storage capabilities to meet the stringent application demands. These platforms will support hardware acceleration, such as GPUs, processor arrays, and dedicated ASICs.

MEC is expected to evolve from fully owned SP or private-edge clouds to network operators, webscale cloud operators, and third-party services owners, including enterprises and related companies. A key technology driver for MEC is network functions virtualization (NFV). NFV allows for flexibility of network implementation, and cloud levels of flexibility and dynamics related to network implementation. 5G has a significant architectural evolution compared to previous versions of LTE: control and user plane separation (CUPS). This allows for multiple levels of user-plane gateways that correspond to multiple levels of edge cloud application placement and distribution. In addition, there are enablement functions that support application placement across distributed edge clouds. These features allow application hosting and APIs for instantiation of network intelligence to individual applications – providing the ability to transfer state to another application instance in another serving edge cloud or MEC environment.

MEC use cases include autonomous vehicles, industrial automation, augmented reality/virtual reality, retail, connected homes, video processing, and predictive maintenance.

Private 5G

Potentially preceded by private LTE/CBRS, private 5G is more disruptive in terms of Industrial IoT operations and expertise. Its business models are largely dependent on countries and their respective regulations as well as operational use cases and constraints. Traffic flow and applications have to evolve, leveraging new capabilities such as MEC and UPF. This calls for additional expertise among the operations and development teams. (Note: If the deployment of a private 5G mmW infrastructure in manufacturing automation or other indoor use cases should be compared with Wi-Fi 6, the number of antennas may become a capital expenditure data point to evaluate.)

In summary, MEC is a key architecture building block related to IIoT use cases, 5G, and the next generation packet core. MEC has a number of benefits:

- Reduced need to backhaul traffic
- Reduced latency and increased QoE, ability to achieve 5G goals of <5-msec service (1-msec stretch goal)
- Overall reduced cost of ownership (TCO) through disaggregation of access functions
- Improved reliability
- Innovation for new third-party providers to build and host edge clouds

Business models

Since we've described the different implementations associated with the emergence of private 5G and Wi-Fi 6, let's now explore the impacts of business models, as TCO is key to Industrial IoT operations.

If we consider Wi-Fi 6 adoption, the business models are well-known, and no important change is expected in the way the technology can be consumed in an Industrial IoT environment. The technology is an evolution of previous Wi-Fi generations, adding more capabilities and higher throughput, while infrastructures and services can smoothly evolve as solutions become available.

Three different business models are reviewed below in the context of multiaccess technologies. The adoption of one business model over another will largely be dependent on considerations such as:

- TCO–Capital expenditure (CapEx) vs. operating expenditure (OpEx), cost of equipment/solution in an operational context
- Local expertise–Education, training, and profile required for operating the wireless infrastructure
- Security–Ensuring data privacy and cybersecurity that are crucial to Industrial IoT
  - Note that data sovereignty may also be a requirement
  - SLA/KPI/operations excellence–Guaranteeing that industrial product line gets the right SLA

CapEx model considerations: The enterprise fully owns and manages the network

Private 4G/5G

Wi-Fi 6

5G UPF and MEC

Roaming interactions

Management and automation solutions

SLAs and KPIs

Data privacy and cybersecurity policies

Overall wireless access technology managed by the enterprise

This is a CapEx business model, with associated OpEx, in which the enterprise fully owns and manages the networking infrastructure, tools, and operations. It is a business model that fits the needs in vertical use cases, such as mining, oil fields, ports, and ships. It requires a spectrum to be available, and potentially paid for, in the appropriate locations.

- Private 4G/5G infrastructure fully managed by the enterprise. CapEx should include the cost of securing the licensed spectrum, the 5G radios and antennas, the controllers associated with CPF, UPF, MEC, and the potential cost related to endpoint upgrades to support the private spectrum. OpEx includes the education and operations of IT/OT and engineers operating the private 5G infrastructure.
- Wi-Fi 6 is locally or cloud-managed (i.e., Cisco Meraki), including the solution to manage multiaccess technologies as a single infrastructure.
- 5G UPF, CPF, and MEC are deployed in the enterprise. These controller functions may be tailored to enterprise usage.
- Roaming interactions between private and public cellular services should be properly negotiated in light of CapEx/OpEx considerations.
- SLAs and KPIs must be locally defined and managed, either internally to the enterprise or with systems integrators and partners, to guarantee no interruption of the production chain.
- Data privacy and cybersecurity policies, processes, and KPI have to be reviewed in the context of the operations but should be an evolution of current rules.

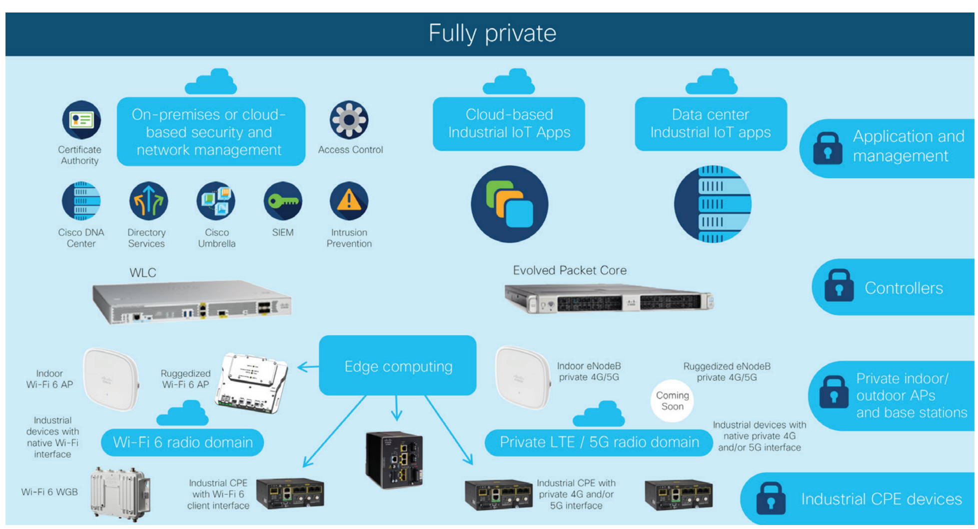


Figure 14: Managed by the enterprise

OpEx and CapEx mix model considerations

Private 4G/5G

Wi-Fi 6

5G UPF and MEC

Management and automation solutions

Roaming interactions

SLAs and KPIs

Data privacy and cybersecurity policies

Wireless access technology management split between enterprise and service provider, with some services managed by SP

This model is a mix of OpEx and CapEx where centralized management for private 4G/5G is performed by a service operator. It is expected to be the default model in countries where private spectrum is not available for enterprises.

- Private 4G/5G infrastructure is fully managed by service providers, mostly OpEx, while the cost of local 5G radios and antennas may still be CapEx, depending on the SP business model.
- Wi-Fi 6 is locally or cloud-managed (i.e., Cisco Meraki, Kinetic GMM) by the enterprise, representing CapEx and OpEx.
- 5G UPF and MEC are deployed in the enterprise by the service provider. The enterprise must consider the cost of an application's adaptations to MEC, if latency control is required.
- OpEx and CapEx associated with management and automation solutions allow the IT/OT managers to locally control some elements of the deployment. This is particularly important if multiaccess technologies should be managed as a single infrastructure.
- Roaming interactions between private and public cellular services are part of the managed SP services as OpEx.
- SLAs and KPIs must be defined to guarantee no interruption of the production chain. For the SP 4G/5G service, this must be negotiated and monitored to ensure that the appropriate QoS and reliability are delivered.
- Data privacy and cybersecurity policies, processes, and KPIs have to be reviewed in the context of the operations.

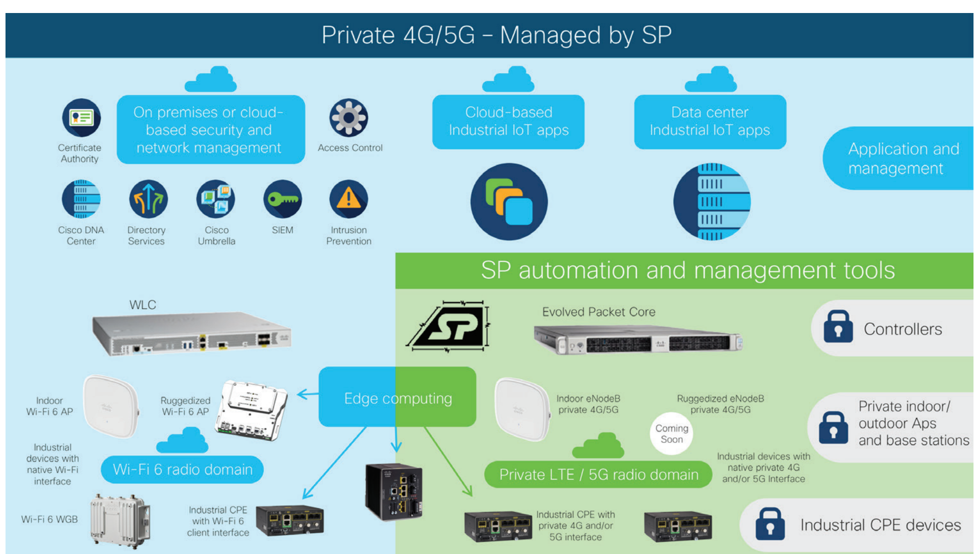


Figure 15: Private 4G/5G SP managed

OpEx model considerations

Private 4G/5G

Wi-Fi 6

5G UPF and MEC

Roaming interactions

Management and automation solutions

SLAs and KPIs

Data privacy and cybersecurity policies

Wireless access technology management by a service provider for the enterprise

This model is based mostly on OpEx, where the overall data communication's wireless infrastructure is outsourced and managed by a service provider.

- Wi-Fi 6 and/or private 4G/5G infrastructure is fully managed by service providers, mostly seen as OpEx; but the connected devices and machines are still CapEx.
- 5G UPF and MEC are deployed in the enterprise by the service provider. The enterprise must consider the cost of an application's adaptations to MEC, if latency control is required
- Roaming interactions between private and public cellular services must be part of the managed SP services as OpEx.
- OpEx and CapEx associated with management and automation solutions allow the IT/OT managers to locally control some elements of the deployment. It may include options to switch ownership of operations to IT/OT over a period of time. It also includes the solution to manage the multiaccess technologies as a single infrastructure.
- SLAs and KPIs must be defined to guarantee no interruption of the production chain.
- Data privacy and cybersecurity policies, processes and KPIs have to be reviewed in the context of the operations.

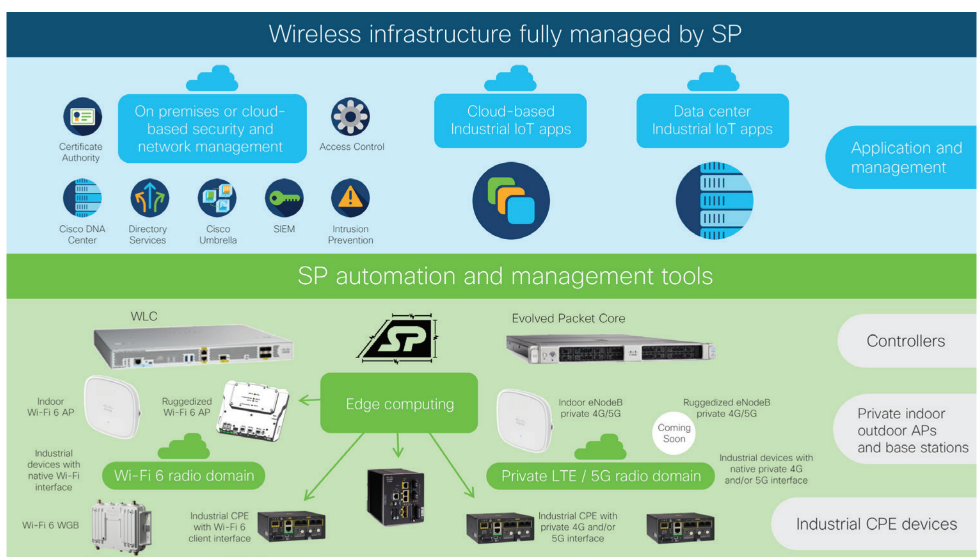


Figure 16: Wireless infrastructure managed by SP

Blueprint for IIoT wireless success

Industrial IoT operations expect faster, more secure, and easier-to-deploy access technologies. The demand is clear, and businesses that are unable to keep up with the latest wireless technologies will be left behind their competitors. This is especially true for enterprises with increasingly complex infrastructures.

As wireless technologies evolve to provide enhanced throughput, better latency, and scalability, Industrial IoT decision-makers have to learn how best to leverage and deploy the technologies in their infrastructures.

In this paper, we provided information on the latest wireless technologies—Wi-Fi 6, and private 4G and 5G—to help businesses navigate the different phases associated with technology adoption. These phases included licensed, shared license, and unlicensed spectrum; standards and regulations; architecture and equipment; and operational requirements. The paper also described business models that may be adopted when deciding to integrate these new wireless trends.

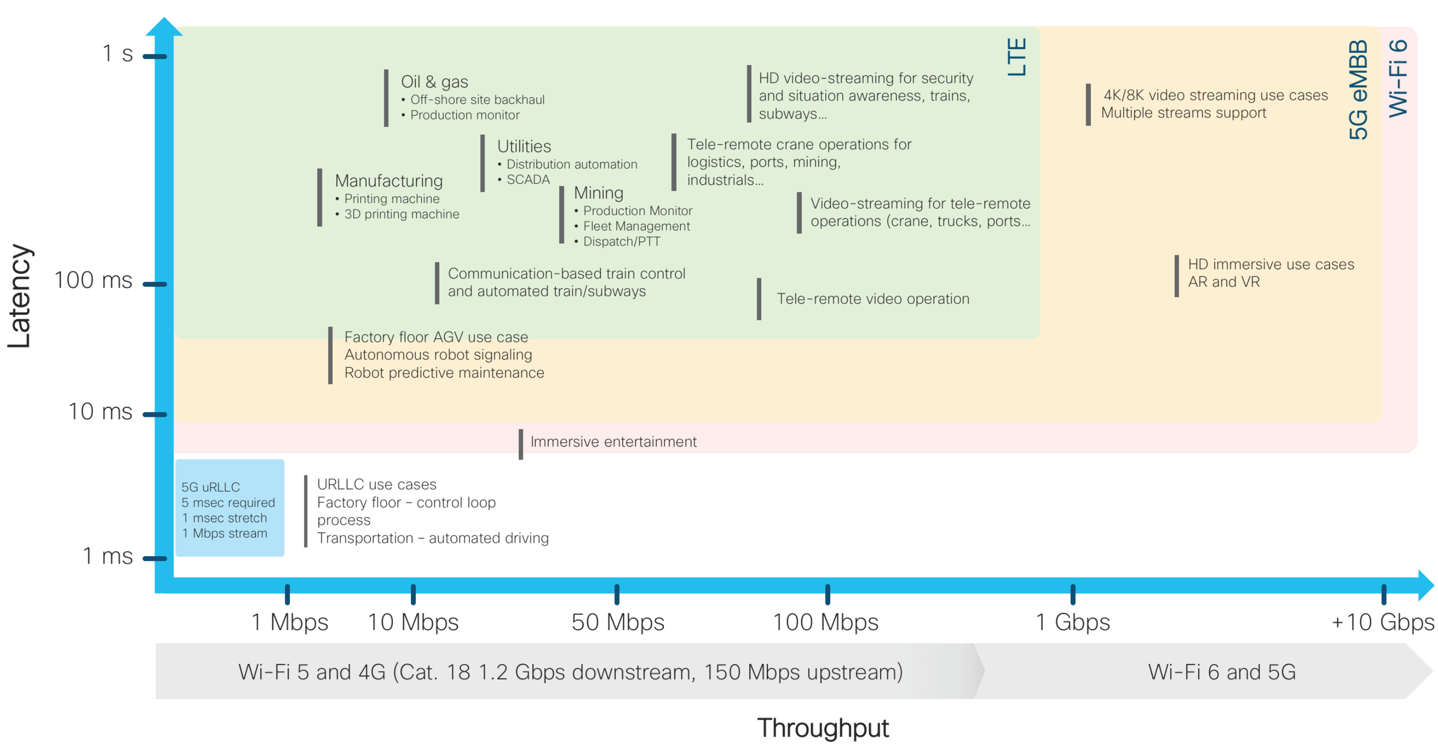


Figure 17: High data rate wireless technologies and use cases

Summary

Cisco is dedicated to delivering best-in-class access technologies in Industrial IoT – for Wi-Fi 6 and 5G solutions.

It's important to note that there is no one solution or strategy for IIoT. Real-world IIoT deployments are expected to have multiple solutions within enterprises that support the various use cases, KPIs, SLAs and reliability as well as economic needs and future evolutions.

This paper didn't try to fully detail the Wi-Fi 6 and private 4G/5G technologies but has provided enough information to Industrial IoT decision-makers when evaluating the impacts of new wireless technologies in their businesses. It considers that a choice of technologies should stay focused on supporting the business and operations, while also considering the total cost of ownership.

Cisco is dedicated to delivering best-in-class multiaccess technologies in Industrial IoT solutions, including Wi-Fi 6 and 5G solutions. By working closely with customers and partners, Cisco can deliver the most appropriate platform support using the Cisco Validated Design guide for various deployment options—ranging from fully private to an SP-managed environment.

Ready to take your enterprise to the next level in wireless solutions? Contact your local Cisco representative.

Cisco-IoT-5G-WP_V1-20191016