ENTERPRISE CBRS AND PRIVATE LTE/5G THE CONVERGENCE OF PRIVATE CELLULAR AND WI-FI

A Disruptive Analysis thought-leadership paper

This is an independent research and analysis report. It has been commissioned by and for Juniper Networks, but represents authentic third-party views, opinions, and recommendations held by consulting and advisory firm Disruptive Analysis Ltd. It does not represent endorsements of any specific companies or products.

TABLE OF CONTENTS

Overview

Introduction

There is currently a tremendous amount of interest in enterprises using cellular technologies—4G/LTE and 5G mobile—for private or localized site-specific wireless use cases and applications. This goes beyond the public service-type models offered by carriers/mobile network operators (MNOs), overlapping with the ownership and operation models more common with Wi-Fi and IT. In industrial settings, cellular technology coexists alongside other specialized wireless technologies and operational technology (OT) systems.

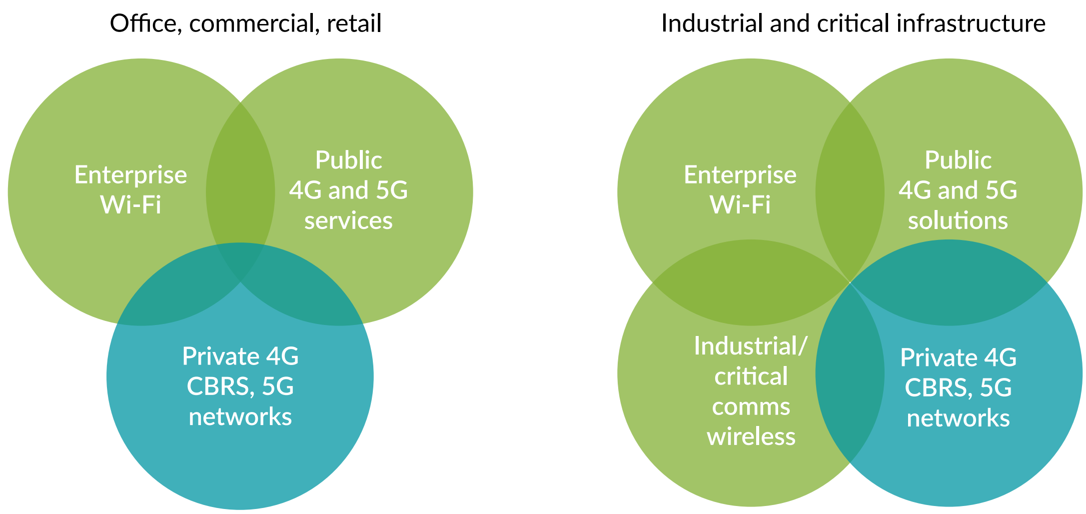

Figure 1. Private cellular bridges the worlds of Wi-Fi and public mobile

This theme is quite complex since, as with Wi-Fi, there are multiple options for infrastructure delivery and operation. Further complicating matters is the growing breadth of end-user device[1] (client) support and the myriad options for integrating private cellular with enterprise IT and operational systems. Cellular technology also overlaps with the heavily regulated world of public mobile networks and the radio spectrum.

In the U.S., the term Citizen's Broadband Radio Service (CBRS) refers to both a specific spectrum band as well as a well-defined architecture and ecosystem for delivering private wireless networks. In countries such as Germany, Japan, and the U.K., similar moves are underway, although each has important differences in regulation and applicability.

Demand and supply

Private cellular applications are exceptionally broad. Examples include:

- Onsite employee communications at an airport, both inside the terminal and on the ramp
- Campus- or district-wide online learning networks for students on laptops and phones
- Improved indoor and outdoor wireless coverage for both visitors and staff at retail malls
- Low-latency connections for robots and machine-vision cameras in factories
- IoT sensors and safety systems on an offshore wind farm

This reveals the huge range of *demand* for private cellular networks, ranging from familiar IT connectivity applications to more complex OT (such as industrial systems) and critical communications (such as two-way private mobile radios) use cases. There are often other options or legacy systems in place, but these may be limited or costly—especially in the face of industry transformation and growing expectations of "connected" customers or workers.

[1] Confusingly, CBRS small cells are called CBSDs, with the D standing for "device." In this paper, "device" is used to describe a user's terminal/client such as a smartphone, laptop, or IoT product.

While the supply-side catalysts for private LTE/5G are also diverse, they are not purely technical. New shared and local spectrum options, plus small cells, cloud/edge computing, and enhanced security/operational tools are critical enablers.

But there is also a commercial perspective: MNOs that are seeing consumer revenues flatlining are looking at enterprise networks as a possible new source of growth. This telco-led interest has matured from merely selling add-ons to national "macro" networks to one that embraces the more granular on-premises needs of specific industries and site types, including IT integration. Other value-chain participants, from systems integrators (SIs) to tower companies, are also viewing the sector with great interest, along with some investment firms.

Finally, there is also considerable regulatory and policymaker interest in private 5G (P5G) as part of national "Industry 4.0" plans, particularly linked to rapid economic recovery from the pandemic. This is helping to accelerate the shift on spectrum availability, as well as fitting the growing geopolitical dimension of wireless networks. Numerous other government initiatives are also fueling the private cellular market with extra funding, from the U.S. CARES act for education access to the U.K.'s vertical-focused Testbeds & Trials program.

Focus and purpose of this paper

We are still in the foothills of the new private cellular terrain. There is a lot of development and evolution to go, both technically and commercially. We can see mountains in the distance, but they are indistinct, and the path to them remains uncertain.

We need to be aware of hype, identifying near-term opportunities while remaining wary of risks and simplistic exaggerations. Private 4G/5G (P4G/P5G) will absolutely not replace Wi-Fi in the enterprise for most use cases, but the arguments for it will become more nuanced and multidimensional by raising the profile of better platforms for optimization and control. Some deployments may even be slower if specific projects need to assess which (or if both) options are best suited to the applications at hand.

This white paper is intended to help readers understand the wireless technologies available to enterprise networking and IT decision makers, systems integration executives and architects, vertical-focused solution providers, and telecoms operator teams focused on B2B services. It may also be of interest to some technology vendors, infrastructure investors, and government representatives.

This white paper does not cover all aspects of CBRS and private cellular networks, which span a large and diverse number of use cases, delivery models, and sub-elements. It focuses on:

- Where private LTE (PLTE) or private 5G displaces, works alongside, or integrates with Wi-Fi
- Integration of PLTE/P5G with enterprise IT, LAN, and Wi-Fi estates
- Multi-network scenarios, such as PLTE/P5G roaming with Wi-Fi or public cellular
- Operational management, security, service assurance, automation, and user experience

This white paper has been written as an independent report by Disruptive Analysis. While it has been commissioned by Juniper Networks and is aimed at its clients, partners, and internal teams, it is not intended as an endorsement of any vendor products or strategies.

Other research from Disruptive Analysis has covered aspects such as industrial wireless network use cases and opportunities, the relevance of P5G to regulators and policymakers, and opportunities for telcos and other service providers. Please contact information@disruptive-analysis.com for more details.

CBRS and PLTE/P5G—how did we get here?

Private cellular and defining the relevant market

Historically, enterprises have used three basic types of wireless connectivity on their premises:

- **Private Wi-Fi**, using IEEE 802.11 technologies in unlicensed spectrum, usually linked to the company's wired networks and IT estate. This method dominates indoor "IT-centric" wireless connectivity. In some cases such as hotels or airports, for instance, a third-party managed service provider (MSP) runs the network. Various generations of Wi-Fi have enhanced speeds and performance, up to the current iteration of Wi-Fi 6 (and 6E in the new 6 GHz band), based on the 802.11ax standard.
- **Public cellular 4G and 5G**, delivered by public operators (MNOs or "carriers") on licensed spectrum bands using Third-Generation Partnership Project (3GPP) standards. This method is the mainstay of wide-area smartphone and outdoor/vehicular connections. For larger buildings, a dedicated indoor system may boost outdoor signals or provide dedicated coverage for MNOs' signals, although this is rarely used for IT-type or industrial/IoT functions.
- **Specialized wireless systems** such as industrial mesh, point-to-point links, broadcast solutions, satellite connections, and two-way radios. These specialized systems often use licensed bands, obtained on a localized basis and operated either privately by the enterprise or by an industry-specific MSP.

Today, however, a new cross-over concept is emerging: **Private Cellular**, or **PLTE/P5G**. The basic idea behind PLTE/P5G is to deploy a customized, company-specific cellular access network built with 3GPP radios and a variety of spectrum options, notably CBRS in the U.S. In some scenarios, this may bridge the gap between the indoor Wi-Fi world and outdoor/cellular services.

There are multiple ways to define and deliver private cellular. The two most important are:

- **A dedicated local 4G/5G radio network** for the enterprise site, either owned and operated by the company itself or provided by a third party as a managed service. Typically this approach will use local or shared spectrum bands (see Figure 2). Some software elements (such as the core) may be hosted onsite, near site at an edge data center, or in the cloud. This type of deployment is gaining significant traction and is the main emphasis of this paper.
- **An extension or slice of a public (MNO) network**, where a telecom service provider enables enterprise connectivity using its own spectrum bands with improved onsite radio coverage, perhaps with a virtual segment called a "network slice" delivering customized functions or application isolation. Some software elements may be hosted on premises and perhaps controlled by the enterprise itself. Some telcos use terms like "campus network" or "non-public network" to describe their private network services.

Initially, the traditional mobile industry expected the second type (extension or slice of a public network) to drive demand—and generate revenue—for public 5G networks and services, especially for IoT. Yet many enterprises, while interested in 4G/5G applications and capabilities, are not convinced that MNOs are the best providers, at least not on the terms and timelines they are prepared to accept. There are differences of opinion over control, cost, coverage, and fine-grained functionality.

There is instead a growing emphasis on the dedicated network option, along with numerous hybrids—such as MNOs' enterprise units offering to deploy private dedicated networks rather than re-using their main public (macro) networks.

A variety of specialist service providers also bridge the divide. Tower companies and fiber operators offer private 4G/5G networks, with vertical-specific or regional carriers focusing on enterprise solutions. Wholesale network providers are becoming "neutral hosts."

Other enterprise mobile solutions can use direct-routed IP links to the cloud or corporate data centers via a private interface (APN) bypassing the public Internet. Some (very large) enterprises have negotiated with MNOs to host their own internal wholesale mobile virtual network operators (MVNOs) for staff or assets. Some public safety/first responder mobile broadband networks run as secure MVNOs on public networks. These are outside the scope of this paper.

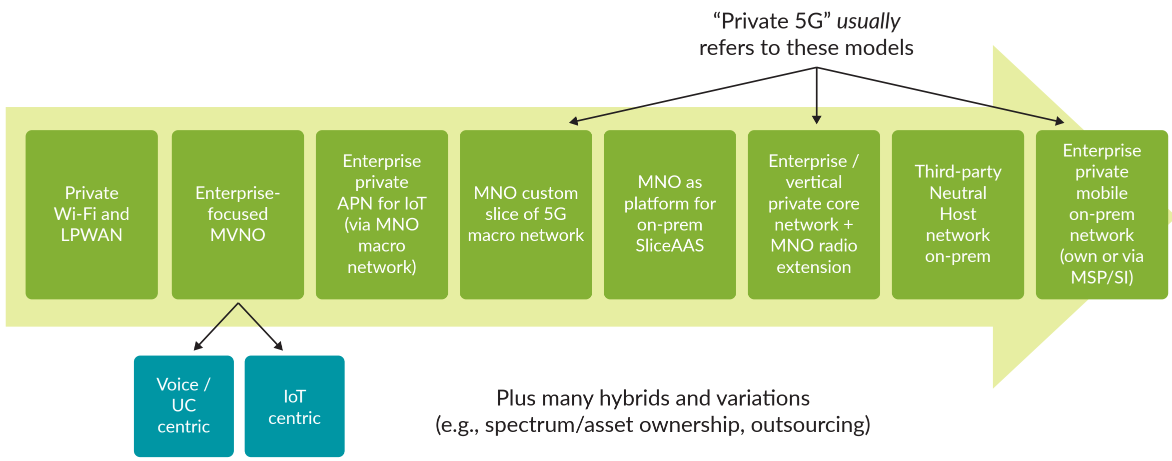

Figure 2. Slicing private networks and other models on a continuum

The history of private cellular and the role of CBRS

Private cellular networks are not entirely new. Private 2G and 3G networks have existed since the late 1990s and early 2000s and are used at places like mining sites, oil and gas extraction facilities, utility grids, military bases—locations where public cellular carrier coverage is absent or unsuitable. Railways have their own special standard, GSM-R, which is widely deployed. Most are used for critical communications or OT/IoT use cases.

Private cellular networks, however, remain quite rare. Maybe 1000[2] exist worldwide, most designed and deployed at considerable cost by specialist providers and managed by expert staff. Until recently, suitable spectrum has often been obtained through complex one-off leasing or sub-licensing arrangements with regulators.

In most of those cases, the alternatives to PLTE/P5G are fiber or dedicated wireless systems such as P25, TETRA, and industrial mesh. While this is a hugely exciting area for the mobile industry, it is relatively distinct from the traditional enterprise IT and LAN/Wi-Fi networking arena.

This situation is changing rapidly. Tens of thousands of private cellular networks will be deployed over the next few years. We are seeing "democratization" of private LTE and 5G, enabled by local spectrum allocations, cloud-based core networks, and a rapidly-growing ecosystem of vendors and integrators. This is bringing cellular technology into the domain of normal enterprise networks, such as offices, retail, commercial property, and so on.

In monetary terms, various analysts have created forecasts for private 4G/5G networks, although it is unclear how they account for software/cloud elements, systems integration, and Spectrum Access System (SAS) access services, or whether they are counting parts of MNOs' and other SPs' infrastructure spends as "private." A recent report from analyst firm IDC predicts the private 4G/5G market will grow to $5.7 billion in 2024[3]; other firms have suggested more modest growth in the $2 billion range. Disruptive Analysis believes these forecasts may prove quite conservative—as a comparison, the distributed antenna systems (DAS) market for indoor/campus cellular coverage systems is now worth around $10 billion.

Central to the recent explosion of PLTE/P5G has been the growing availability of suitable spectrum bands that enterprises can use directly *on a local basis*—and for which there is an ample supply of both infrastructure (small cells) and end-user devices, which requires support from chipset suppliers.

Given that enterprises cannot compete with MNOs in national spectrum auctions, a pivotal trend has been towards smaller quanta of license coverage size and granularity, ideally down to the level of local regions or even individual buildings. Such allocations can be shared (using either manual or automated/dynamic systems) or exclusively awarded to specific site owners or tenants.

[2] There may be several thousand more ultra-small private networks, mostly using individual 2G or 3G cells, on ships, executive jets, military vehicles, or for "cordless" local indoor phone use in countries like the U.K., Netherlands, and Japan with small slices of suitable spectrum.
[3] https://www.mobileeurope.co.uk/press-wire/15431-idc-predicts-private-lte-5g-market-will-reach-5-7-bn-in-2024

The most important regulatory innovations for enterprise-suitable spectrum include:

- **CBRS/OnGo networks**: The U.S. CBRS spectrum band 48, which runs between 3.55 and 3.7 GHz, uses a three-tier licensing model to share access between incumbents (mainly the U.S. Navy). It employs protected priority licenses in county-sized areas and a more open “general access” tier roughly equivalent to Wi-Fi and unlicensed spectrum. A set of databases called the Spectrum Access System[4] provides each access point (called a CBSD) with dynamic permissions to use parts of the band on a localized basis. There is a rapidly growing diversity of devices, infrastructure vendors, and integrators for CBRS systems.
- **Germany** has allocated 100 MHz between 3.7 and 3.8 GHz for industrial/local use at a site/building level. This is within the 3.4-3.8 GHz band identified by the EU as a core frequency range for 5G, with an ample supply of devices. More than 100 applications have been made for this resource. This model is being considered by other countries (e.g., Sweden), and Germany is offering a tranche of mmWave spectrum as well for private use.
- **The U.K**. now has local 4G/5G-suitable licenses available in various bands such as 1.8 GHz, 2.3 GHz, 3.8-4.2 GHz, and 26 GHz. It also has a separate arrangement where enterprises or alternative SPs can apply for secondary re-use of MNO bands in select areas. Enterprise-grade device and equipment supplies for these bands are less mature today, but they are improving, with the 400 MHz of 5G-suitable midband a particularly attractive long-term allocation for private networks.
- **France** has made spectrum available in the 2.6 GHz band for certain industries and enterprises to deploy private networks, but primarily for “critical infrastructure” such as airports, power stations, and railways. Its recent 5G spectrum auctions for MNOs also have a provision for local leasing or indoor coverage arrangements for broader enterprise use.
- **Japan** has a range of bands suitable for private 4G/5G cellular use, including a legacy 1.9 GHz range for low power, and more recent 2.6 GHz, 4.7 GHz, and 28 GHz options.
- **Other countries** have released various bands for local/enterprise use as well, often in the 2.3 GHz band. One of the European regulatory bodies (RSPG) recently indicated support for the 3.8-4.2 GHz range for local licensing, which may point towards a more harmonized approach in future. A number of markets such as Malaysia and Hong Kong have enabled enterprises to use 26-28 GHz mmWave, although that range remains largely restricted to indoor and specialized use cases.
- **Globally**, the unlicensed 5 GHz band (commonly used for Wi-Fi) can also support forms of private 4G/5G networking, modified for use on a listen-before-talk basis. The newly-available 6 GHz unlicensed bands are likely to be used for private 5G NR-U (the unlicensed-spectrum version of 5G New Radio) in the future, as well as Wi-Fi 6E.

There are three key takeaways from this:

- In the last two to three years, there has been a surge in the number of countries offering local/shared spectrum for enterprise use. This trend is likely to continue, with many other regulators now examining available options.
- There is little international harmonization on the available bands or the rules for their use. This fragmentation adds to the complexity of private cellular for multinational companies, especially compared to Wi-Fi’s harmonized 2.4 GHz, 5 GHz, and (increasingly) 6 GHz bands.
- Some countries such as India, China, Spain, Canada, and Italy remain largely absent from the local spectrum trend, favoring enterprise 4G/5G solutions from national MNOs rather than independent ownership.

Local/shared spectrum is not just suitable for enterprise private cellular use. Depending on the specific rules in each country, it is also open for public network operators, government bodies, and others. It is usually “technology neutral”; although 3GPP-based 4G and 5G radios are the most likely to be deployed, other options are also available—for instance, for fixed-wireless access[5].

[4] There are several SAS providers. The market leaders are currently Google and Federated Wireless.
[5] For instance, Cambium has both LTE and proprietary non-3GPP FWA product lines that can use CBRS spectrum.

In the U.S., CBRS spectrum is also being used beyond the enterprise sector by MNOs adding capacity in urban hotspots, fixed-wireless access ISPs, and cable companies building out mobile infrastructure. Of the 100,000 or more CBSDs (access points) deployed so far, maybe half have been installed by MNOs for public network coverage enhancement, while a quarter have been earmarked for Fixed Wireless Access (FWA).

While most CBRS deployments today are based on 4G LTE, 5G versions are also on the way. The CBRS Alliance, recently rebranded as OnGo specifically for 4G/5G networks, is attempting to push the brand to be used for private cellular internationally.

Key drivers for private/enterprise cellular

Some businesses want to commission (and directly own) their own 4G/5G networks, in roughly the same way they own Wi-Fi today. Others want customized and/or optimized solutions from MNOs, or various new classes of specialized service providers targeting this market. There is a diverse set of rationales, use cases, verticals, applications, and user groups driving this demand:

- **Coverage** is the easiest requirement to understand. MNO public networks—especially at frequencies suitable for high-performance 4G and 5G—often have poor or no reach to areas used by mining, agriculture, utilities, and transport. Indoor and industrial campus coverage is patchy at best. MNOs have limited capacity (and budget) for "special projects" like 4G/5G.
- **Control** of wireless networks is also important for many enterprises. They may want to own the security, identity, administration, user experience, and other aspects of their 4G/5G connectivity. They may require sovereignty over sensitive data, so they ensure it never leaves their premises over public infrastructure by locating the core elements physically on site. For more demanding use cases, they may configure the wireless network to meet specific requirements (such as aerial coverage for drones, or different uplink/downlink balances for cameras and IoT data capture vs. large video displays).
- **Cloud and IoT** alignment is an important driver of private cellular, along with broader transformation projects. Many organizations are increasing their use of automation systems, robotics, cameras/surveillance, and sensors—often using cloud-based management, analytics, and data storage functions. Private 5G (and/or Wi-Fi 6 and fiber) is an integral element. There is also a strong link with public cloud providers as enablers of private 5G.
- **Wi-Fi alternatives**. The ability of private 4G/5G to replace Wi-Fi is relevant but often overhyped. The relationship of private cellular and Wi-Fi is discussed in the following section.
- **Alternatives for other connectivity**. Although there is often a focus on Wi-Fi vs. private 5G, in many cases the immediate comparison is with fiber, industrial Ethernet, proprietary wireless, Digital Enhanced Cordless Teleco (DECT), or private two-way radio systems like TETRA or P25. Cellular can bring down costs and make it easier to use multifunctional smartphones or tablets.
- **Commercialization**. Some enterprises are becoming micro MNOs in their own right, providing paid connectivity to local tenants or visitors. Property companies can offer private 5G connections to condominium residents, retail stores in malls, or office tenants in a business park. Some sites may be able to derive tenancy or roaming fees from national MNOs through neutral host propositions that are similar in concept to Wi-Fi offload.

Coverage	Control	Cloud	Cost	Compensation
In-Building	Security	Edge computing	Replace legacy LMR	Productivity
Rural	Sovereignty	Lowest latency	Factory 4.0	Private SIMs
Industrial	Customized	IT / 5G integration	Fiber replace	Roaming
Offices	Beyond Wi-Fi	Cloud marketplace	Avoid carrier per-GB fees	Local MVNO
Road / Rail	Deployment	5G in IoT platform	TCO for IoT connectivity	Govt funding
Utility	Lifecycle	Digital Twins		Local FWA
Metro areas	Mobility			MNO offload
Military / Govt	Private QoS			

Figure 3. The 5 Cs of private cellular

Private cellular use cases

There are three ways to divide up the specific use cases for PLTE/P5G:

- Functional purpose
- Industry sector/vertical
- Type of location, or specific areas within a larger site

The main *functions* and use cases serviced by private cellular include:

- A similar usage model to Wi-Fi, but with more mobility support, better coverage, and less congestion, albeit with greater complexity and new skills requirements. This is mostly aimed at smartphones and laptops for accessing the public Internet or enterprise cloud/IT resources.
- Efficient medium-area backhaul for Wi-Fi or other local-area connections, especially outdoors.
- Replacing some fixed/fiber connections or niche/legacy wireless technologies, either indoors or outdoors.
- Mid-/wide-area critical communications outside of traditional carriers' geographical reach or technical competence (such as utilities and rail).
- New connectivity applications, especially linked to IoT and industrial automation.
- Alternative mechanisms for a third party to deliver indoor/on-premises cellular signals, where normal public network coverage is constrained.
- Backups for outdoor/wider area fiber/wired connections—for instance, in oilfields or for utility grid assets.

From an *industry vertical* perspective, PLTE/P5G is first appearing in the following domains:

- Critical communications for utilities, rail, oil and gas, and mining. These were the mainstays of the early private wireless market, and they continue to grow in importance.
- Transport hubs such as ports and airports, used especially for push-to-talk, video surveillance cameras, IoT, and onsite vehicles. In some cases, coverage is expanding to passenger terminals, staff offices, and retail areas.
- Logistics and warehousing, especially in modern sites with high degrees of automation and robotic systems like automated guided vehicles (AGVs).
- Manufacturing and process plants. A significant amount of effort on later versions of 5G, including ultra-reliable low-latency capabilities (URLLC) and high-precision location, is aimed at factories and automation systems. In the long term, this will likely be a huge market for private cellular, but prototypes and trials will take considerable time to move to full production.

- Healthcare settings, especially hospitals, are looking to private 4G/5G for both in-building uses such as medical image transfer and robotics, as well as outdoor/area coverage for large campuses and wireless connections to new structures such as COVID tents. Some health authorities are also using P4G/P5G networks for connections to smaller primary-care facilities, mobile units such as vaccination trucks, and broader local community coverage.
- Business parks, convention centers, shared offices, and other property developments (such as retirement villages) are considering adopting PLTE/P5G for both onsite mobile access for vehicles and tenants as well as for FWA connections to individual buildings from a hub site.
- Retail chains are looking to private cellular for outdoor wide-area coverage, either directly to customers' phones or as backhaul for Wi-Fi access. Some are also considering indoor cellular at larger stores, either for staff/IoT dedicated access (such as for handhelds) or, in future, as an option for neutral-host models providing indoor cellular coverage for visitors.
- Schools, universities, and education authorities are considering a variety of use cases for PLTE/P5G, both for student connectivity from phones and laptops as well as for staff, onsite vehicles, and camera/smart infrastructure services. During the pandemic, some in the U.S. have also used CBRS for FWA services to homes lacking wired broadband, or for backhaul of Wi-Fi access points set up in car parks and other areas.
- Public safety and military organizations are using private cellular systems for both major sites (such as bases) and field units (such as fire and rescue command, special forces overseas).
- Sports and entertainment venues are looking at private cellular networks for staff terminals (such as payment handhelds), audio-visual and broadcast systems, and potentially future neutral-host platforms for visitors' phones to roam to—although that requires widespread support for the relevant bands. At present, the newer high-end smartphones support CBRS 3.5 GHz for LTE, but many legacy devices do not. It will take some time for penetration to increase, and even then, foreign roaming visitors and others may not be able to access the private cellular network if a country has a unique band choice.
- Other sectors such as finance (both retail branches and major offices), government buildings, hotels/hospitality, and others are also investigating PLTE/P5G for a variety of employee, visitor, and IoT scenarios.

Many of these sectors occupy large sites which are complex mixes of environments and applications/users. Airports have very different network needs for passengers and staff in terminals vs. operations staff and vehicles in the ramp area, or in maintenance hangars and cargo terminals. Multi-building office complexes, business parks, and mixed retail/apartment developments may have different zones with unique requirements.

Table 1: P5G users and applications cross indoor/outdoor boundaries

Campus type	Indoor areas	Outdoor areas
Airports	Terminals Hangars and maintenance Rail stations Hotels and offices Parking structures	Aircraft apron Arrival/departure zones Maintenance, fuel, cargo areas Outdoor parking Runways and taxiways
Ports	Warehouses Passenger terminals Office areas Inspection and customs	Dockside Container terminal and storage Open water Roads/rail lines
Logistics	Warehouses Office areas	Air cargo terminal Roads/rail lines
Mixed-use property developments	Apartment buildings Office/hotel towers Retail and malls Entertainment venues	Public outdoor spaces Parking Public transport

Campus type	Indoor areas	Outdoor areas
Hotels and resorts	Hotel towers Convention/meeting areas Condominiums	Pools, courtyards, and gardens Golf courses Beachfront
Sporting/entertainment venues	Retail and hotels Media center Theme park, golf course, racetrack	Outdoor seating Parking Walkways
Business parks and office campuses	Office building Light industrial units	Parking/private roads Parks and landscaping
Industrial and manufacturing plants	Factory buildings Process and machine plants Offices Warehouse storage	Roads and passages Outdoor storage/dumps Open areas
Universities	College and faculty buildings Accommodation blocks Sport and entertainment facilities	Central campus zones, quads, parks Parking/transport areas
Oil, gas, and mining sites	Industrial process plants Site offices Underground facilities/tunnels	Pit/drill sites Logistics and transport facilities
Military bases	Barracks/accommodations Offices Engineering, hangars, warehouses, etc.	Training grounds Runways, docks, etc. Vehicle storage and movement
Large construction sites	Site offices Partially completed buildings	Ground-works Access roads Airspace (drones)
Scientific research sites	Laboratories Underground facilities/tunnels	Parking facilities Logistics areas
Retail parks	Malls and individual stores Covered/uncovered car parks	Parking lots Logistics bays Advertising and direction boards

Source: Disruptive Analysis

Deployment and delivery models: MNOs, SIs, and MSPs

Most early discussion of enterprise 4G and 5G has hinged on "classic" MNOs and converged carriers—AT&T, Verizon, BT, Vodafone, DT, Orange, Telefonica, NTT DoCoMo, and so on. Typically, the underlying narrative describes two choices:

- Enterprises can obtain private/on-premises cellular networks as a service from telcos, perhaps with dedicated coverage plus a "slice" of the main macro network and core functions. Some MNOs now treat private cellular networks as more of a custom systems integration opportunity.
- Enterprises can build their own cellular networks the same way they build Wi-Fi or wired Ethernet LANs today.

These choices, however, present a false binary. In reality, a number of service providers are chasing the private LTE/5G opportunity. These include:

- Fixed and cable operators, especially those with a traditionally large enterprise customer base. One such example is Colt in the U.K.
- TowerCos moving up the value chain into private or neutral networks (for instance Cellnex, which acquired industrial specialist provider Edzcom, and Digital Colony's ExteNet and Freshwave units).
- IT services firms affiliated with specific enterprises (for example, HubOne, the IT subsidiary of the company running Paris' airports, is deploying P4G/P5G).

- Industrial automation suppliers such as Siemens or Kuka acting as "industrial mobile operators" on behalf of their customers (such as a robot or crane supplier that runs/owns a local 5G network for a manufacturer or port).
- Utility companies that can run their own private 4G/5G network and provide critical communications to other companies (for instance, Southern Linc in the U.S.). Numerous utilities have acquired CBRS PAL licenses in 2020[6].
- Dedicated MNOs for particular industries, such as oil and gas, often in specific regions such as TampNet and RigNet.
- Regional operators such as CityMesh in Belgium, which also covers offshore wind farms.
- Municipalities and local authorities that deploy networks for internal use, citizen services, or as public neutral-host networks for MNOs.
- FWA/wireless Internet service provider (WISP) networks that are shifting to 4G/5G and targeting enterprises (for instance, for agricultural IoT).
- Overseas telcos without a national spectrum that want to service multinational local sites and offices for their enterprise clients. This may align more closely with the fixed/enterprise/WAN business unit. Verizon Business is publicly pursuing private cellular in the U.K., Germany, and elsewhere, for example.
- Major cloud providers that may create or enable 4G/5G networks for a variety of use cases and enterprise groups. Amazon and Google are both involved (albeit opaquely, beyond Google's SAS business).

(For more information, read this article[7] aboutMNOs vs. private 5G networks on LinkedIn.)

In the near future, we will also increasingly see broadcasters, event management, and content production companies deploying private 4G/5G networks on behalf of sports and entertainment venues—for instance at festivals or convention centers.

In essence, there is a growing attitude among enterprises that "if we have to pay for indoor/onsite coverage, we might as well own the network ourselves."

That said, MNOs (and many other vendors) have some difficult internal politics to manage. Many want to obtain as much spectrum as possible for national 5G networks, on more favorable terms. This causes some to vociferously oppose spectrum "set-asides" for enterprises to use directly. At the same time, however, their enterprise customers clearly want dedicated PLTE/P5G, so they are essentially competing for regulators' attention.

The telcos' enterprise business units are increasingly pivoting to enable such fully private networks in local dedicated spectrum and on-premises infrastructure if that's what businesses will pay for today. They recognize that they can still monetize various pragmatic service offers such as installation, maintenance, backhaul, voice connectivity, Subscriber Identity Module (SIM) management, and more in the near term—and perhaps link private networks to their public 5G services in future as a follow-on.

National differences

Initial deployments of enterprise PLTE/P5G differ by country, reflecting local spectrum frequency bands and rules, as well as the prevalence of particular industries, end-user device availability, investment/funding models, and local technology ecosystems.

The U.S. is seeing more IT usage of CBRS for purposes such as backhauling from Wi-Fi access points, or for smartphone/laptop usage across large campus sites. Health and education use has also been stimulated by various government programs. A number of utilities acquired PAL licenses for critical communications. There is also widespread use of the band by various service providers, either MNOs adding extra capacity or FWA and cable players for broadband connectivity. There is also significant interest in neutral-host and public/private cellular roaming models, although this is still early.

[6] https://www.fiercewireless.com/private-wireless/why-did-utilities-pay-so-much-for-cbrs-licenses
[7] https://www.linkedin.com/pulse/mnos-vs-private-5g-networks-false-binary-dean-bubley/

German PLTE/P5G uptake has been heavily driven by manufacturing automation (especially automotive) as well as some transport hubs and universities.

The **U.K.** has a broad mix of applications reflecting multiple available bands. Ports, airports, manufacturing, local communities and smart cities, warehousing, offshore wind, and broadcast are some examples. There is also considerable innovation around neutral host scenarios.

France has focused mainly on the use of PLTE for critical communications, replacing TETRA two-way radios for sectors like rail, airports, energy, and utilities.

Private cellular networks in the **Nordic region and Belgium/Netherlands** have been heavily driven by ports, offshore activities such as wind farms and oil/gas, and other industrial sectors like forestry and mining.

Japan has seen local 5G networks driven by a mix of manufacturing, heavy industry, and smart cities, including university campuses.

There are also widely varying engagements by traditional MNOs in private cellular. Some are acting primarily as systems integrators for dedicated PLTE/P5G networks. Others are more focused on linking enterprise networks to their wider public/macro 5G infrastructure and capabilities such as network slicing and edge computing.

Over time, the various P5G markets will likely converge and cover all verticals, especially as more (ideally harmonized) spectrum becomes available. There are early signs that more countries in Europe may adopt the same 3.8-4.2 GHz band already available in the U.K., for instance. That said, many markets may still be reluctant to pivot away from MNO-centric approaches, pushing macro network extensions and slicing rather than true private cellular.

When and where is Wi-Fi challenged by private cellular?

We are starting to see more interest in use cases where private cellular and CBRS are used alongside Wi-Fi or, in rare cases, replacing it. Various enterprises have indicated their intentions to either cap existing Wi-Fi installations and upgrades (for instance in warehouse settings) or to migrate specific applications and systems to mobile-based networks. While many such cases are still in the exploratory and trial stages, others are now deploying or running production networks.

There are two separate issues to consider here:

- Which applications and locations might *realistically* see Wi-Fi replaced by private 4G/5G? Is this a significant risk for the Wi-Fi industry, and can it regain its current position in the future? This is considered below.
- Where both private cellular and Wi-Fi coexist in a given location, will they be integrated/converged in some fashion, or will they be deployed and operated as distinct and separate infrastructures? This is considered in the following section.

In general, the most difficult Wi-Fi vs. private cellular debate pivots on *non-industrial* settings. (Most *industrial* uses for PLTE/P5G involve replacing other technologies such as fiber or private radios.)

The real battleground areas for Wi-Fi vs. PLTE/P5G are not the typical carpeted office environments. Instead, they are focused on sectors such as retail, hospitality, education, healthcare, and other “people-centric” locations where the main considerations are centered on smartphone and handheld device usage rather than laptops or IoT. They typically blend indoor and outdoor areas, across a campus or mixed-use development area.

Device-centric decisions

A key determinant of whether to use Wi-Fi and/or cellular is the type(s) of devices being used and the level of ownership or control over them exerted by the site/business owner.

- Smartphones all have both 4G/5G and Wi-Fi. However, this support varies widely when examined more closely. Some may be unsuitable for private cellular, either because they do not support the right frequencies (such as CBRS band) or because they are "SIM-locked" by the user's carrier and do not support roaming to local networks. Phones issued by a company to its own employees will have greater success than visitor or staff personally owned devices. iOS devices have some features that need specific profiles from Apple to work properly—profiles that enterprises may not have access to. That said, Wi-Fi connectivity and authentication may create friction as well.
- Laptops and Chromebooks are available with cellular radios, but only a small number (<10%) are sold with these today, and their support for different bands vary widely. The vast bulk of usage is via Wi-Fi. As a result, venues with large numbers of laptop users will not switch to private 4G/5G, except when corporate-issued or mandated for visitors—perhaps on military sites or schools buying fleets of devices for students.
- Most (noncritical) business devices such as cameras, barcode scanners, tills, etc. can be specified with Wi-Fi and/or cellular modules, although many do not have both. And they may not be easily upgradeable during their working lives.
- Vehicles and other moving devices (robots, drones, and so on) are increasingly equipped with cellular radios, especially if they operate on public roads as well as on site. While they may use Wi-Fi as well (especially indoors), they are important use cases for the future of CBRS and PLTE/P5G. That said, older vehicles may not support the right frequency bands or SIM/roaming capability. Automated systems bought by the enterprise can be specified up front to support the local network.
- Many audio-visual systems such as CCTV cameras, digital display boards, and kiosks (for ticketing, information, and the like) have multiple connection options, supporting plug-in modules or USB dongles. PLTE/P5G products are increasingly available for these devices.

It is important to note that many Wi-Fi-only devices can benefit from private cellular by using a local gateway/hotspot that connects to 4G/5G across a medium-scale distance, with a secondary Wi-Fi connection for nearby devices. For instance, a passenger bus at an airport or a security gate house at an office complex could have a CBRS gateway that allows phones or laptops to connect onward via Wi-Fi and then private cellular. Another important example is remote learning, where students connect laptops or tablets via Wi-Fi to CBRS- or P5G-backhauled access points or fixed wireless services.

One other important difference compared to Wi-Fi is the lack of backward compatibility. Many private cellular small cells/CBSDs support just a specific G, and often just a specific frequency band. It may be difficult or expensive to support 4G and 5G devices on the same network, especially if it requires both 4G evolved packet core (EPC) and 5G standalone core functions as well. This is different from Wi-Fi, where almost all Wi-Fi 6 access points will also support Wi-Fi 4 *and* 5, although this may change with 6E and the use of 6 GHz band.

Location-specific decisions

Certain physical environments are better suited to PLTE/P5G than Wi-Fi, reflecting the typical greater coverage area of small cells and other performance characteristics. CBRS or other private cellular deployments can often expect to need 3-4x fewer cellular radios than Wi-Fi access points indoors, or up to 8x fewer outdoors, although this varies according to local shared spectrum rules, Wi-Fi generation, and physical construction and obstacles. In theory, Wi-Fi (especially 6E in new spectrum) can offer higher theoretical speeds for individual users, but cellular tends to offer greater consistency and predictability as the core network allows more control over user access, congestion, and quality of service (QoS).

Typical situations where private cellular can often outperform Wi-Fi (or cost less) include:

- End-user devices ("clients" in Wi-Fi terminology) that are controlled by the enterprise itself, which issues SIMs and determines configuration and permissions
- Outdoor areas such as parking lots or university campuses
- Midsize areas with a mix of fixed wireless and outdoor mobile needs, such as business parks, RV parks, and retirement villages
- Large indoor spaces such as convention center halls (which have high ceilings, regularly changing internal structures, and temporary clusters of high-density usage)
- Warehouses and large retail stores, especially those with poorly performing (often older) Wi-Fi
- Visitor-led venues, where business-critical systems must be isolated from congestion/interference (such as payment terminals at a sports stadium)
- Manufacturing or industrial environments such as factories, chemical plants, or open mines with wide/outdoor areas, fast mobility, and significant RF interference

In some cases, the focus is on either replacing existing Wi-Fi systems or delaying upgrades/extensions in favor of a private cellular overlay. In other instances, enterprises will decide to invest in PLTE/P5G upfront, where they may compare/contrast the options and decide against Wi-Fi. Examples include:

- Greenfield properties such as new warehouses built to align with growth in e-commerce and delivery services
- Major refurbishments, such as when a new retailer moves into a building as a tenant, with many fittings and systems being replaced
- Specific process-transformation initiatives, such as a shift from fixed payment terminals and ticket booths in a transport hub to roving staff with handhelds or automated gate lines
- Additional space coverage needs, such as a "click-and-connect" car park zone, a rooftop bar, a hospital COVID tent, or remote education needs across a midsize area

	Public 4G / 5G	Private 4G/5G/CBRS	Wi-Fi 6, 6E, 7	Other technologies
Employee and tenant/ contractor smartphones	May need extra indoor coverage system	Core opportunity for private cellular	Widely used and will continue	
Visitor smartphones	May need extra indoor coverage system	Onboarding complex (e.g., private SIM) or roaming	OK unless clunky portal. PassPoint/OpenRoaming	
Two-way radios/walkie-talkie	Hard to implement	Core opportunity for private cellular	OK but limits on coverage and mobility, especially outdoors	Existing DECT, TETRA, P25 common and robust
Handhelds (e.g., barcode scanner, payment terminal)	OK but costly and coverage dependent	Core opportunity for private cellular	OK but limits on coverage and mobility, especially outdoors	Some proprietary solutions
Laptops and tablets	Very few cellular laptops	Enterprise could specify	Ubiquitous use	Some wired Ethernet
Cameras and video displays	Expensive option	Potential opportunity	Good but limited outdoors	Fibre/wired is common
Industrial automation IoT (e.g., robots, conveyors)	Theoretical use for future network-slicing. Unproven	Potential killer app, especially URLLC/TSN	Good but risks of interference in unlicensed	Fibre/wired is common
Sensors (temp, motion, proximity, location etc.)	Ongoing OpEx costs/ lock-in risk	Ideally needs low-power option (maybe NBIoT)	Good indoors, less good for campus/outdoor	BLE, ZigBee, LoRA are low-power and cheap
Vehicles (cars, trucks etc.)	Wide-area/roaming	Larger campus e.g., mine	Limited coverage	Satellite an option

Key: Ideal | Good | Limited | Unsuitable

Figure 4. Future options for device connectivity on enterprise sites

What should the Wi-Fi industry do to respond?

How should the Wi-Fi industry respond to the changing landscape? An important consideration is the number of grey areas in this analysis—for instance, logistics and warehousing, which has historically been a major domain for Wi-Fi but where older versions and suboptimal installations have struggled to keep pace with the rapid growth of automation and robotics.

- Many of the historic problems with Wi-Fi can be addressed by Wi-Fi 6 or, soon, 6E (in 6 GHz), both of which are capable of higher throughputs, greater transmission efficiency, better latencies, and support for higher device densities and forms of QoS. More effort is needed to communicate the differences to dissatisfied users as well as to industry commentators and government policymakers who often underplay Wi-Fi's potential and development trajectory.
- Backward compatibility is a double-edged sword. For public venues, the ability to support older Wi-Fi 4 and Wi-Fi 5 clients will be useful for some time—something which may prove difficult for CBRS and P5G installations when confronted with legacy devices. Conversely, the main benefits of Wi-Fi 6E in 6 GHz, beyond the additional spectrum, only really appear because legacy clients are not supported in the band.
- Work on future iterations—Wi-Fi 7 and eventually Wi-Fi 8—need to address the specific capabilities being promised for private 4G/5G. In particular, work needs to be done to improve support for mobility, user device densities, low latency, and high reliability functions. It may also be important to create versions of Wi-Fi that can work in locally licensed spectrum bands to allow better isolation and interference protection. This could also allow the use of higher powered access points that improve coverage areas. (In theory, Wi-Fi 6E could use CBRS spectrum or other current P5G bands, although 10 MHz channel widths may be problematic, as well as the lack of current radios and chipsets.)
- The Wi-Fi industry needs to improve its targeting of specific vertical markets. There is far less specialization by vendors, industry bodies, conferences, and others on "Wi-Fi in Sector X" products and marketing than is seen with the cellular industry (public or private 4G/5G).
- The industry must continue to push for reducing friction related to onboarding users and devices, whether for the public (visitors to a venue) or for enterprises managing their own user bases and device fleets. Outbound roaming (onto cellular networks) must be considered, as well as inbound offload. Initiatives such as OpenRoaming and PassPoint should be accelerated and optimized for different device/venue/industry scenarios.

PLTE/P5G and Wi-Fi "better together"? Sometimes, but not always.

From the previous discussion, it is clear that almost all business sites will continue to operate (and upgrade) both Wi-Fi and cellular systems. Even locations which do not need *private* cellular or CBRS installations will still rely on *public* cellular services, including indoor coverage systems like DAS.

What is less clear is the extent to which Wi-Fi and private cellular should be integrated, either in terms of physical infrastructure, control/security platforms, or operational and investment models.

Numerous organizations (including the sponsor of this white paper) have solutions that can be used to integrate and manage hybrid Wi-Fi/cellular installations, also known as converged wireless or HetNet systems. In general, convergence makes more sense when devices are likely to move between networks, although there will always be a debate about network-side coordination vs. device/client-side choice.

Table 2: Wi-Fi and cellular better together or separate

Wi-Fi and cellular better together	Wi-Fi and cellular better separate
Corporate-controlled devices roam across network domains (e.g., indoor vs. outdoor).	Private cellular used to isolate specific devices/applications from Wi-Fi.
Active load-balancing, backups, or bonding across Wi-Fi and cellular networks.	Different ownership/MSPs (or enterprise itself) running cellular and Wi-Fi networks.
Private cellular used as backhaul for Wi-Fi APs (e.g., in car parking areas).	Separate monetization models (e.g., free Wi-Fi vs. neutral-host wholesale mobile).
Requirement for "single pane of glass" for Wi-Fi and cellular radios across a site.	More emphasis on Wi-Fi multisite federation vs. Wi-Fi + cellular hybrid.
Hybrid AIOps for IT service and experience management for wireless client devices.	Wi-Fi fits with IT estate/ops, while cellular controlled by MNO or integrated into OT.
Single identity/security model for all wireless connectivity and devices.	Regulatory gaps between technologies (e.g., because of spectrum rules).
Same physical infrastructure (e.g., hybrid access points/cabling/switches).	Private cellular directly integrated into a specific industry system (e.g., automation).
Long (or partial) migration of existing Wi-Fi devices to support private cellular.	Indoor cellular coverage primarily provided via a DAS or repeater model.
Use of 3GPP core networks supporting non-3GPP access technologies.	Separate operational teams, budgets, or legacy systems for Wi-Fi vs. cellular.
Desire to integrate private cellular into the broader IT/LAN environment.	Desire to integrate private cellular with OT systems and industrial IoT.
MNO/carrier-driven deployments of both cellular and Wi-Fi for the venue.	Greater urgency to combine public and private cellular on single system rather than add Wi-Fi.

This can enable better oversight by enterprise management of their whole wireless estate, and especially fits with scenarios where the IT function is in control of the private cellular network, either directly or via an MSP.

There are numerous converged scenarios:

- Wi-Fi for indoor areas, plus CBRS/private cellular outdoors—for instance, around a shopping mall or logistics/warehouse site
- CBRS backhaul for remote Wi-Fi access points (e.g., in a parking area, or in the outdoor areas of a university campus)
- Devices able to use Wi-Fi or cellular in different parts of the site, or simultaneously—perhaps sending different data streams or applications over each path
- IT systems capable of assigning different users/devices to either Wi-Fi or cellular networks, depending on levels of network congestion, temporary workgroups, need for backup connections, and so on

In reality, there will be complex trade-offs, depending on the timing of investments, existing legacy systems, skill sets, and relationships with service providers and other system vendors. Spectrum availability may vary between location—for instance whether local incumbent users impact access to a band.

It is helpful to consider two example scenarios:

- **Converged scenario**: A major retail chain wants good wireless coverage for customers, staff, IoT systems, and vehicles, both indoors and outdoors across its 300 sites. It has both existing use cases (customer "click-and-collect" and wireless EPOS tills) and expects new applications in the next few years (auto checkout cameras, EV charging points, and robotic shelf-stackers). It is considering a neutral-host model when it upgrades indoor coverage to high-performance 5G in the future. The pattern of usage is different during shopping hours and overnight. It has a major integrator overseeing its general transformation project. In this case, a combined infrastructure and "single pane of glass" management platform for private cellular and Wi-Fi makes a great deal of sense.

- **Diverged scenario**: A railway network is midway through a deployment of passenger Wi-Fi in its major stations using a dedicated installation company and a cloud-based provider of authentication and portal software. In the future, it hopes to federate Wi-Fi access with on-train systems and local smart-city organizations. It is also examining possible IoT and footfall-counting systems, which might use Wi-Fi, Bluetooth, and cameras. At the same time, it wants to provide excellent indoor cellular coverage across all public MNOs and intends to pilot a private 4G/5G network at one site, although that is a very long-term project. It is working with an indoor cellular specialist that offers a managed neutral-host infrastructure with no additional CapEx for the railway company—good news given low post-pandemic fare revenue. Here, there may be some convergence on physical infrastructure such as power and fiber, but the cellular and Wi-Fi networks will likely remain otherwise separate.

As this suggests, the question of whether Wi-Fi and private cellular are better together is likely to be very situation-specific. It will also likely change over time as use cases evolve and both P5G and Wi-Fi 6E/7E generations mature at different speeds.

One important area to consider with Wi-Fi + private cellular solutions is how authentication and handover are managed. While there has long been a focus on 3GPP-based solutions such as Extensible Authentication Protocol (EAP)-SIM authentication for public cellular, combined with Wi-Fi integration for offload, these have been strongly oriented towards the MNO operating model and core network/subscriber management platforms.

For *private cellular* + Wi-Fi, we are likely to see additional options emerge that align more with enterprise IT and security—and perhaps with less dependency on the SIM management and core network functions. (It should also be noted that SIMs are optional for certain devices connected to PLTE/P5G.)

There is ongoing development in this arena around PassPoint, which can link Wi-Fi to either SIM credentials or downloaded profiles, as well as more sophisticated approaches such as the Wireless Broadband Alliance (WBA)'s federation model called OpenRoaming. This can already link Wi-Fi access rights at different venues and user groups and across identity providers—and is being extended to support CBRS networks at present.

There are lots of other variables here as well. IT operations will sometimes need to map SIM identity to Wi-Fi media access control (MAC) addresses, which is becoming harder with revolving/randomized MACs. Some devices support eSIM and/or dual SIMs, which could allow phones to simultaneously have both public and private 4G/5G identities, each of which may have separate interactions with Wi-Fi. There may also be dependencies on iOS and Android features, especially if Apple or Google need to give specific permissions around eSIM or other capabilities—which may be easier for service providers to obtain than individual enterprises.

All of this likely means that some "better together" scenarios for PLTE/P5G+Wi-Fi will be highly effective, while others may face some practical obstacles in the near term.

Neutral host and hybrid public/private cellular models

Overview

The previous section examined scenarios where it makes sense to combine private cellular/CBRS systems with Wi-Fi for converged enterprise wireless.

Another set of scenarios relates to the blending of *public* and *private*/local cellular connectivity on the same infrastructure and platform, perhaps with Wi-Fi as well. This reveals an important difference between the technologies:

- Anyone can access a Wi-Fi network, at least in theory, as long as they have the right security and authentication credentials.
- *Dedicated* private cellular networks are limited to a specific subset of users and devices—those who have been given a suitable identity and authentication mechanism by the enterprise or an MSP. For example, they may issue special SIM cards for employees' handheld devices, or security cameras and IoT units.

- *Public* cellular networks are only accessible to subscribers of a given MNO, or those who have roaming privileges such as international travellers. For large venues, this means that visitors must be able to access *all* the various public MNO networks, as the enterprise or location-owner likely will not want to confine mobile accessibility to just a fixed percentage of customers.

The old DAS model needs to evolve

A full discussion of indoor/on-premises multi-operator cellular coverage is outside the scope of this paper, but historically has mostly involved DAS or repeaters, predominantly in large venues and public buildings.

These create extra coverage for the outdoor mobile carrier networks inside a building, each installing extra radio sources (cellular base stations) on site. They can be expensive and time consuming to deploy, and do not give the building owner any direct control or ownership of the wireless networks, even though they may be paying for the installation.

Sometimes a third-party provider manages the DAS while, in other cases, one MNO acts as a lead and then onboards its peers. In either case, they act as the indoor coverage equivalent of TowerCos. This does not involve a separate core network or subscriber management; it just supports radios that broadcast on the outdoor carriers' own spectrum.

Often, DAS systems do not support *all* operators—indeed, an average of just 1.7 MNO tenants per system has been suggested, reflecting different design or contractual requirements. They also do not scale down to midsize buildings or many enterprise sites.

Various new models are now blending the idea of public (multi-operator) LTE/5G network coverage in-building with private network ownership of the assets, as well as (sometimes) parallel private cellular connectivity.

Introducing neutral host networks (NHNs)

A neutral host network (NHN) is a wholesale-based mobile infrastructure provider that offers mobile coverage or capacity enhancements as-a-service, typically to multiple retail MNOs as tenants. NHNs can also support private networks as additional tenants on the same infrastructure. They represent a growing subset of the wider arena of network sharing and wholesale tower/infrastructure services.

The growing importance of 4G and now 5G mobile for visitors and employees, together with extra coverage challenges at higher frequencies, means that NHNs will be a larger part of the future telecom landscape, including for many small and midsize premises such as retail stores and university buildings.

Localized 4G/5G spectrum licenses such as the U.S. CBRS band may fit here as well, although full integration between private and NHN sectors is not always needed. Some of the new approaches to NHNs focus on multitenancy of the radio infrastructure, which is mostly transparent to the underlying traffic.

Others essentially create a new tier of wholesale MNOs using shared (that is, third-party CBRS) or pooled (operator's existing bands) spectrum. These may have their own full or partial core network facilities as an intermediate layer before using a variety of interconnect/roaming mechanisms with their tenant MNOs' cores. There are various models emerging, such as the multi-operator core network (MOCN) as well as another option, the gateway core network (GWCN).

The exact architectures will depend on the willingness of carriers to establish roaming or core interconnections with NHNs, based on both security and commercial concerns. There may also be regulatory constraints on domestic roaming, while other technical considerations such as how to deal with 5G carrier aggregation may also emerge.

Third-party NHNs will expect to connect to multiple physical sites owned by numerous enterprise/venue clients. Given the willingness issue, there may be an advantage for existing wholesale mobile carriers, which already have established roaming and interconnect relationships with MNOs. Geoverse is an example of this category, along with Mobilitie and Boingo (recently acquired by Digital Colony). We may see more acquisitions or partnerships between indoor/private radio specialists and roaming hubs/wholesale operators.

Use cases for NHNs

Most NHNs operate in locations where economic or practical constraints prevent MNOs from running their own infrastructure directly, either individually or in consortia.

The most oft-cited use cases for NHNs are to support:

- Multi-MNO in-building coverage, especially in sites where visitors or workers may be using public MNOs for their personal devices. Examples include retail stores, transport hubs, and shared office spaces such as WeWork facilities.
- Shared network infrastructure for rural "not spots," or mountainous/island areas where it may not be economical for public MNOs to build their own infrastructure. These sites might also have separate local spectrum licensing or local MNOs that act as roaming partners for the main national MNOs.
- Incremental "capacity as a service" in urban areas where MNOs are challenged to obtain or deploy extra sites. This could include shared small cells used as secondary nodes, providing localized in-fill or high-capacity hotspots alongside each MNO's owned primary infrastructure and sites in the city.

In addition to these applications, other potential NHN deployment scenarios include road/rail sites, inside industrial facilities, and fixed wireless access.

The direction of the neutral host market

The NHN market is still in its infancy, especially where it uses local spectrum on site, rather than an evolution of the historic DAS model with MNOs' spectrum. There is no "official" definition of NHN; there is no NHN Association or other trade body that represents the interests of the companies and business models described here. As such, the definition of an NHN is somewhat fluid and will likely evolve over time, with regional variations:

- **U.S.**: The ecosystem of CBRS spectrum and devices, together with existing in-building neutral DAS providers and (some) acceptance by carriers of domestic roaming models, is likely to catalyse NHN models. There will be a mix of CBRS-based local service providers with roaming or MOCN approaches—for instance, Geoverse, Digital Colony's ExteNet and Boingo units, BAI, Mobilitie, and others can be expected to take roles. Some will leverage existing roaming relationships or trust earned with carriers from installations on transit systems or elsewhere. We may first see CBRS-based NHNs in special cases such as indigenous/autonomous lands, with local MNOs and no existing coverage from national carriers.
- **U.K.**: The U.K. is likely to see a split between indoor and outdoor/rural NHN models. Indoor models will likely be based on MNOs' existing spectrum and cores, using advanced small-cell[8] and maybe Open RAN designs backhauled to secure NHN data centers, rather than CBRS-type full local operator models. The roaming/MOCN approaches may be adopted in other areas such as rural communities by companies such as Telet Research, or perhaps (eventually) by enterprise private networks adding NHN as a secondary capability. MNOs in the U.K. are generally reluctant to strike local roaming/spectrum-sharing deals, although Telefonica O2 seems slightly more enthusiastic.
- **Germany**: Although German regulators have allowed private 4G/5G networks in its 3.7 GHz band, it currently does not allow interconnection with public MNO services—for instance, for roaming or MOCN models. While this may change in future, it suggests that small-cell or DAS models for in-building coverage, using existing MNO spectrum and cores, will continue for some time.
- **Other Europe**: There are no harmonized local spectrum or policies for private LTE/5G across Europe. France, Belgium, The Netherlands, Denmark, Finland, and other markets all have some options for some locations, but the rules and bands differ widely. None are currently optimal for "thick" CBRS-style neutral host models. In Ireland, Belgium, and Portugal, some spectrum is held by wholesaler Dense Air, which is offering "small-cell-as-a-service" neutral host in New Zealand, although it does not yet have full multi-operator MOCN or roaming. Various European regulatory bodies have started discussing NHN in recent months, although timelines (or definitive architectures or rules) seem quite distant.

[8] The UK JOTS NHIB Joint Operator Technical Specification group's Neutral Host In-Building initiative is an important element, although not the only approach here.

- **China**: China is unusual in that the government has released a specific band in the 3.3 GHz range for in-building network sharing/neutral host between three of its four national operators. Most deployments use a proprietary small cell in-building solution such as Huawei's LampSite.

At the moment, it seems that the U.S. (via CBRS) will most likely be the first to evolve towards a blended private/NHN model, often with a third-party service provider involved—and typically for public venues such as retailers, hospitals, universities, and perhaps transport hubs. Industrial sites seem less likely to combine IoT-centric 4G/5G networks with coverage for public MNO services, on the grounds of complexity, cost, and skills.

NHNs will impose additional challenges in terms of network management and operations, especially if devices can connect to either public or private domains (for instance, if they are dual-SIM devices). It is also likely that roaming/MOCN partners will demand visibility into the services received by their subscribers while on the private CBRS infrastructure.

Security, automation, and AI-based operations in P4G/P5G

A recurring theme in this paper is the link between enterprise IT estates and PLTE/P5G cellular networks. Historically, cellular infrastructure and services (usually delivered by MNOs) have largely existed outside of corporate IT oversight, except for specific touchpoints such as mobile device management (MDM).

Conversely, Wi-Fi (and other corporate-run network components such as LAN switches) have been tightly coupled with the IT domain. Engineers and operations staff have been able to scrutinize overall applications end-to-end between servers/cloud, software platforms, network, and end users.

This has enabled root-cause analysis of faults, and at least in theory, a "single pane of glass" for monitoring performance and viewing usage statistics. In recent years, this has extended to a broader oversight of user experience—a shift from management of specific network elements to looking at a more end-to-end view of device connectivity and behavior.

For example, a retailer's stock control system might depend on a cloud-based supply chain application, connected via WAN and Wi-Fi to checkout tills in multiple stores as well as warehouse management systems and associated networks. A similar cross-domain management system could span an airline's reservation system through the wireless-connected check-in kiosks in an airport.

At a simpler level, a hospital's IT department may just need to ensure that nurses' tablets remain connected to the Wi-Fi network and to the patient care database as they move around the building and campus.

If private cellular networks, or an MNO's private network slice, are to be integrated into that type of environment, the enterprise IT function will need a similar level of visibility and control that is already present for the LAN and Wi-Fi. If passengers cannot check in for their flights, or if supermarket inventory cannot be analyzed in real time, then IT operations staff will need to be alerted and take appropriate action as quickly as possible, regardless of the underlying network.

The challenge is how to perform that type of analysis for a local cellular PLTE/P5G network, in the context of a wider IT system. There is a poor fit between traditional telecom network management tools and operational support systems (OSS) and enterprise IT, especially where those were originally designed for running nationwide carrier networks.

To address the issue, a paradigm shift is needed. In the carrier/telecoms world, the OSS (IT) runs the network, which is made up of complex and heterogeneous elements from the radio to the transport and core. But in an enterprise world, the reverse is true: the network is just part of the wider IT system. The same is largely true in the industrial OT operational technology world.

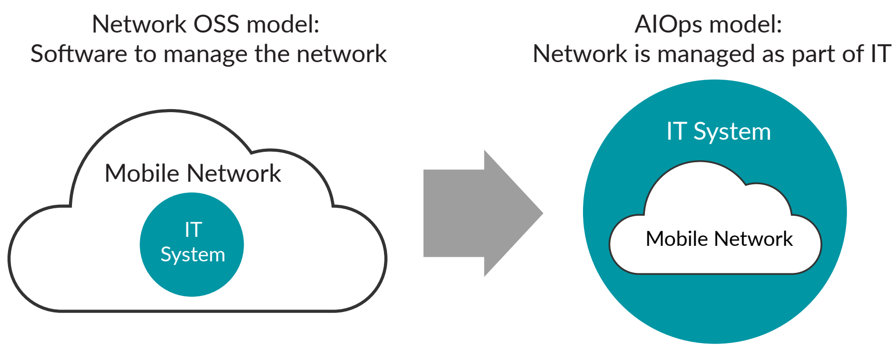

Figure 5. OSS model vs. AIOps model

In other words, in an ideal world, enterprise CBRS and P5G networks would dovetail with the IT management and operations world, which is itself evolving fast. In particular, private cellular used for IT use cases may need to be integrated with AIOps, especially in hybrid cellular/Wi-Fi deployments. (This is not applicable where CBRS is used as part of a public MNO network for extra capacity.)

AIOps, or Artificial Intelligence for IT operations, refers to technology platforms that automate and improve IT operations by using analytics and machine learning (ML). AIOps systems collect and exploit large volumes of data from various IT tools and devices, such as streaming telemetry and/or metadata, logs, and event records, to automatically detect and react to problems in real time.

AIOps essentially bridges:

- Service management
- Performance management (and thus implicitly user/device experience)
- Automation and intervention

In other words, the cellular components, from the radios and IP infrastructure such as switches and firewalls through to device/user identities, all need to be mapped onto the specific IT *applications* to provide a complete end-to-end view.

From a 3GPP/telecom perspective, AIOps is broadly similar to the trend sometimes called A3 (automation, AI, and analytics), which is often discussed[9] in the context of 5G, cloud-native core networks, orchestration, and network slicing. However, A3 comes more from the view of *customers* rather than *users* and also owes more to the internal complexities of the 3GPP architecture and legacy service provider OSS/BSS platforms.

More than likely, AIOps will be particularly important (and challenging) for the converged Wi-Fi + CBRS/P5G scenarios described above; for example, managing visibility of clients (devices) as they move around the network from one wireless network to the other.

For instance, in the healthcare example above, it will be important for hospital IT staff to be alerted to problems with client devices roaming from indoor Wi-Fi to outdoor CBRS as medical staff move between buildings, and get help resolving the issue. It is easy to see how a "single pane of glass" would be essential here.

At a simpler level, there will also be a need for oversight across the IP infrastructure underpinning an enterprise cellular-only network (i.e., without Wi-Fi). Switches, firewalls, WAN gateways, and other components will need to be managed holistically, and with as much automation as possible—either by the enterprise itself or by an MSP.

In the future, this end-to-end management is likely to get significantly more complex if P5G networks start using sophisticated core network functions such as network slicing. Monitoring core network functions, device (UE) identity and state, radio access network (RAN), and Wi-Fi configurations and logs will need increasing AI sophistication to help IT operations teams.

[9] For more information, see the work on A3 done by STL Partners, an affiliate of Disruptive Analysis https://stlpartners.com/research/end-to-end-network-automation-why-and-how-to-do-it/

It is not yet clear whether E2E experience in PLTE/P5G networks will be more driven by an IT-centric AIOps model or a more 3GPP/telco-centric A3 approach anchored in network slicing and service assurance. Disruptive Analysis believes it may be easier for IT to add private cellular network intelligence if the complexity can be abstracted for administrators. Much will depend on the exact use case, trigger, and pathways for deployment—Wi-Fi + private cellular convergence may evolve differently to public + private cellular.

In either case, this is likely to be an area with differences in both technical architecture and language/terminology for years to come. Market participants should be aware of gaps in understanding and perspective.

Conclusion and recommendations

This paper has discussed a rapidly moving part of the wireless ecosystem, which has many moving parts:

- Local spectrum is becoming available in the U.S. (CBRS) and many other countries.
- There is a growing appetite for deploying private 4G or 5G networks among many enterprises, for a diverse array of use cases.
- Some of these deployments can be identified as IT-type implementations, which share similarities with traditional Wi-Fi and Ethernet applications. These will need to be integrated with the rest of the IT estate, as well as management/operation platforms and staff.
- Others are more linked to OT, critical communications, or fixed-wireless domains, especially in industrial sectors. They will have separate legacy and operational pathways.
- Another strand of local/private cellular is developing as an alternative to traditional mechanisms of indoor coverage for *public networks*, especially in visitor-led venues or where employees bring their own devices and need access to most/all MNOs. These neutral hosts may act as "micro MNOs," using roaming or other network-sharing architectures.
- Adoption of new private network bands, especially CBRS 3.5 GHz in the U.S. and 3.8-4.2 GHz in markets like the U.K., is still limited in consumer smartphones. This means that public facing use cases can only address a subset of a venue's visitors for some time.
- 5G makes all of this more complex in the future, given additional features such as network slicing, as well as its use of higher frequency bands and often worse indoor coverage.
- The extra investment needed may prompt many enterprises to reassess their indoor/on-premises wireless options, including comparing the roles of Wi-Fi and private cellular. Wi-Fi will remain critical and is evolving fast with 6/6E/7, but will face some challenges in areas such as outdoor coverage.
- Existing tools for managing MNO cellular networks, subscriber/user management, and experience/troubleshooting do not scale down well to private networks. They also cannot easily combine public/private or private/Wi-Fi hybrids. There will be a significant appetite for various enablers of convergence, with multiple paths to achieving it.

It is hard to know how far the private cellular model may go in future. It is possible to create long-term scenarios of millions of businesses running (or renting) private 5G networks, given enough automation and simplicity. With 5G in unlicensed spectrum and simplified radios and cores, we may even see "free 5G" emerge"[10] in a similar fashion to "free Wi-Fi." While MNOs may resist such moves, they could be embraced by other telcos such as cable and fiber operators without nationwide spectrum.

[10] www.linkedin.com/posts/deanbubley_5g-wifi-spectrum-activity-6725016179955535872-xBfG/

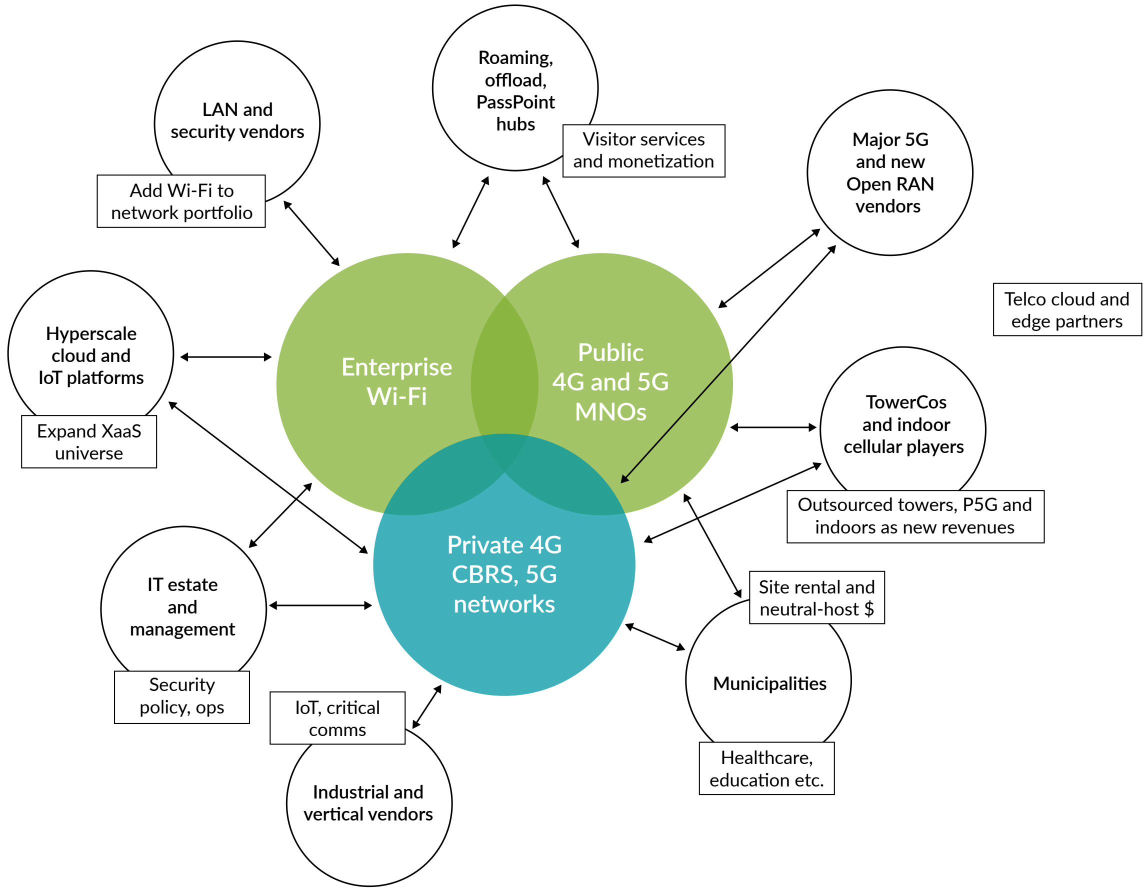

Figure 6. Private cellular scenarios

While the market for private 4G/5G networks is growing fast, it is not without significant challenges and uncertainties. Some of the tough questions include:

- Should private networks aim for 5G straight away, or should they deploy 4G with an upgrade path?
- How should international companies deal with the fragmented landscape of local spectrum suitable for private spectrum? Do they need separate network/partnership strategies for each country's facilities?
- What "soft" issues need to be addressed with private wireless? Are skills available? How will maintenance work? What training is needed or available?
- What are the roles for MNOs, systems integrators, tower/indoor wireless companies, and other classes of service providers? Who should enterprises be talking to?
- Will (or should) enterprise private 4G/5G networks also support neutral-host models for public cellular? Would this involve roaming, MOCN-type sharing, or something else?
- How will voice, video, and real-time communications evolve alongside private wireless? What are the use cases, challenges, and application-level issues?
- Can private wireless networks be used for visitors/guests? Or are they just for employees, machines, and partner organizations?
- How will private wireless networks overlap with edge computing? Will they be tightly coupled physically or virtually?
- What are the considerations for multi-site private wireless deployments (such as retail chains)? Will they intersect with SD-WAN and other wide-area options?

None of the answers are straightforward, but none of these uncertainties are show stoppers either. Disruptive Analysis believes that the broad area of private cellular is one of the most interesting developments in the wireless space in years. It aligns with many external trends—from industrial transformation to improved consumer experiences. There will likely be tens of thousands of CBRS and private 4G/5G networks built globally alongside Wi-Fi, satellite, and many other wireless technologies.

Overall, the next few years promise an era of network diversity for both public and private networks, securely connecting individuals' personal devices, buildings, vehicles, and IoT systems, both indoors and over campus-scale sites. Both demand and supply of radio technologies (and spectrum) is increasing rapidly, as are the number of stakeholders, vendors, network owners, and service providers. Some will be converged and others kept separate, optimized and single purpose.

The next evolution will come with the application of AI to manage multiple connections and devices, as well as to perform new tasks such as choosing the most secure, reliable, or even energy-efficient connection options.

There will be a strong requirement to manage performance and assurance at multiple levels of the network, from radio performance and interference to stability of network slices, WAN connections, IP network functions, and applications themselves. These tasks—and isolation/fixing problems—will become exponentially harder where devices cross between technology boundaries, or blend them as hybrids. Automation will take a growing role, especially given likely skills gaps in many enterprises.

Disruptive Analysis has covered the evolution of private cellular technology for more than 20 years, since the first LAN-attached small cells emerged. But it is only *now* that the real inflection-point has occurred, and it will bring huge opportunities in the coming years.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700

Driven by Experience™