



Private Cellular Networks: Revolutionizing the Wireless LAN Across Large Spaces

How organizations use Private LTE and Private 5G instead of Wi-Fi to cost-effectively control network performance and security

Overview

Our world is now dominated by IoT devices — and by the data-rich, highly actionable business insights they enable. Even the largest and most remote locations need the flexibility of wireless connectivity for both wide-area networks (WAN) and local-area networks (LAN) so they can connect those devices. But existing LAN technologies, including Wi-Fi, aren't sufficient to address this challenge:

- The sheer size and scope of many deployments demands long-range coverage, and the number of Wi-Fi access points needed to cover that range isn't feasible.
- Highly sensitive information calls for layers of security unavailable with in Wi-Fi.
- Stringent budgetary limitations, particularly in the public sector, make it important to minimize infrastructure expenditures as much as possible.
- Applications like live streaming of HD footage require low latency.
- The broad scope of what organizations connect puts a premium on the ability to monitor, control, and automate network traffic flow and Quality-of-Service (QoS).

Think about all of the Internet-connected staff, devices, vehicles, and applications spread across shipping ports, campuses, manufacturing plants, warehouses, and many other expansive areas. And with the boundless potential of 5G expanding companies' long-term ideas and vision, the complexity of these scenarios is sure to grow.

In sprawling areas where a Wireless LAN is critical, Private Cellular Networks (PCN) have emerged as an excellent option. PCNs, which include both Private LTE and Private 5G deployments, are helping organizations with locations that require wireless connectivity but are not well supported by Wi-Fi and may not even be ideal for public LTE usage.

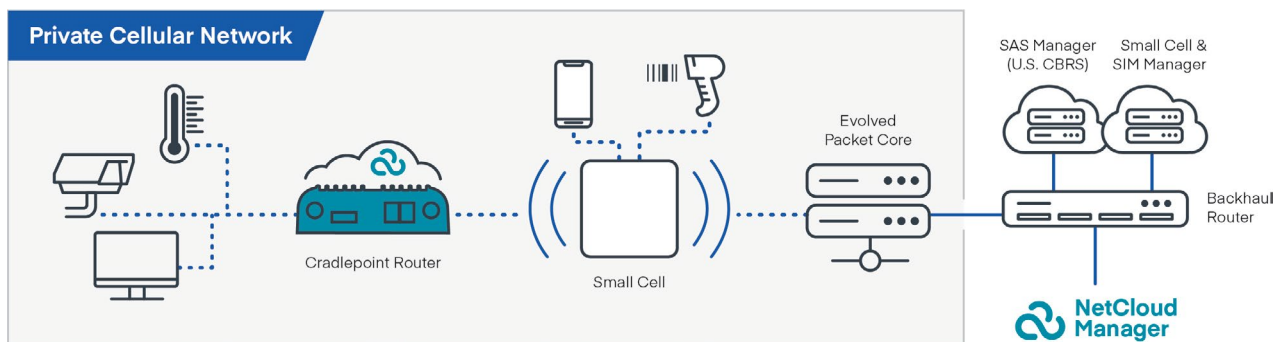
Private networks are beginning to play a unique role in the world of Wireless LAN, providing benefits that range from reduced congestion and enhanced traffic flow to better information security and dramatic cost savings.

How Private Cellular Networks work

Most businesses and agencies today are at least somewhat familiar with the process of using cellular-based broadband for WAN — whether for primary links, failover, or augmentation. But turning LTE or 5G into Wireless LAN? For most organizations, that’s new territory.

Placing micro towers and small cells — similar to Wi-Fi access points — on-site allows companies to mimic a standard public cellular network. This creates a Wireless LAN that is more reliable, high-performing, secure, and cost-effective than Wi-Fi.

PCN architecture usually user equipment, or routers; small cells, or radios; a management system; the evolved packet core; and a spectrum allocation server. That said, private networks can be delivered various ways: by either a third-party network provider, a traditional cellular operator, or the enterprise customer itself. The decision of which operator or infrastructure provider to use mostly hinges on the spectrum of choice, and the level of private management the enterprise is willing to take on.



Types of Private Cellular Network spectrum

Shared Spectrum

In the U.S., CBRS is a lightly licensed spectrum within the 3.5 GHz band. The U.S. FCC will auction off this spectrum, but the auction winner will only receive priority access, not exclusivity. In many cases, enterprises will operate their own Private LTE networks by using the CBRS spectrum. In the rest of the world, many countries are exploring similar spectrum sharing for industrial IoT.

Licensed Spectrum

Network operators can install their own equipment using the same spectrum they use in the macro network. The operator would most likely deliver this private network as a managed service with flat-rate pricing.

Unlicensed Spectrum

Both enterprises and operators can operate Private LTE networks in unlicensed spectrum such as the 5 GHz band that is used for Wi-Fi; well-known examples include MulteFire and LTE-U. Operators can aggregate unlicensed bands with their own spectrum to expand their bandwidth for Private LTE scenarios.

Addressing the challenges of Wi-Fi in large areas

In an office, store, or vehicle, Wi-Fi enabled by access points and other network hardware is an excellent tool for connecting a multitude of devices. However, for organizations that oversee operations across vast, sprawling areas and/or rapidly changing spaces, Wi-Fi is challenging, if not untenable. PCNs can help companies address the problems associated with using Wi-Fi as Wireless LAN.

Costs

Many large facilities, campuses, downtown areas, and other spaces now are equipped with an array of IoT devices — all of which require connectivity. Unfortunately, laying fiber in the ground and installing a huge quantity of Wi-Fi access points is exceptionally expensive. Outfitting just one large site could cost many millions of dollars for the fiber alone.

The infrastructure needed for PCN is far less expensive than a widespread Wi-Fi deployment, which requires extensive wired line installation. Also, whereas dozens of Wi-Fi access points would be required in a big area, a LAN based on cellular broadband would call for just a few PCN radios.



Performance and reliability

Even if an organization can afford to bear the cost of widespread Wi-Fi throughout a large area, limitations regarding performance and reliability likely will derail success. Wi-Fi isn't sufficiently stable or robust — without significant cost — to support the types of high-bandwidth applications that are becoming more standard in most business operations situations, especially across vast areas. Examples include wireless robotic devices and real-time video surveillance streaming.

One of the reasons for Wi-Fi's deficiency is that the client — such as an IoT device, computer, or phone — decides when to roam from one AP to another (sometimes with the help of the AP), but with virtually no ability to improve performance when it lags. With PCN, the organization itself controls its connections. Through priority and preemption, the network equipment can provide better Quality-of-Service (QoS) to designated SIMs and devices.

Security

Wi-Fi security is limited to a username and password, which may be acceptable for logging in at a coffee shop but is concerning within the framework of a large organization's corporate network. When various types of sensitive data and IoT devices are at stake, additional layers of security are necessary.

LTE deployments include SIM cards and edge networking devices, providing additional layers of security that aren't possible with Wi-Fi. A PIN can also be required to unlock a SIM inside a router. This is a form of two-factor security for the edge device.

Network architecture with Private LTE usually includes on-site servers, enabling organizations to keep traffic between IoT devices and corporate servers on the Wireless LAN instead of the public Internet.

Altogether, these factors give Private LTE inherent security advantages over Wi-Fi and help protect an organization's most critical information from malicious attacks.

When public LTE isn't the best available option

Wireless broadband has proven itself to be an excellent WAN option in both backup and primary roles, depending on the use case. However, in certain scenarios, public LTE doesn't provide the cost-efficient, unwavering high performance needed to keep high-bandwidth applications running smoothly 24x7.

For instance, many enterprises operate sites that gather and pass huge amounts of data, including a lot of information that is pushed to the corporate data center. This traffic drives up latency and costs when carried via a public cellular network with pay-per-bit pricing.

Also, sometimes these sites are located in remote areas where sufficient public LTE infrastructure isn't readily available. However, even when infrastructure is in place, if high-traffic neighborhoods or business parks are located nearby, network traffic fluctuations at certain times of day could make high-bandwidth applications — such as robotics in a manufacturing plant — unreliable.



Private cellular eliminates these potential obstacles of public cellular across broad areas, providing several key benefits:

- **Infrastructure:** Private LTE and 5G can be deployed rather easily in locations where public LTE isn't available.
- **Costs:** Keeping high-bandwidth content on-site with PCN and local servers reduces costs in situations when that content doesn't need to leave the area. Also, using CBRS eliminates the need for recurring fixed-rate cellular data costs. Even in scenarios where MSPs are used for private cellular, flat-rate plans likely will drive down costs.
- **Latency:** The ability to avoid sending high-bandwidth information off-site minimizes latency.
- **Security:** Whenever possible, most enterprises prefer the extra level of security afforded by keeping data local instead of sending it elsewhere.
- **Congestion:** Putting an organization's network on a different frequency alleviates the need to compete for coverage against nearby users. Additionally, priority and pre-emption can be activated for control over how traffic is prioritized — a level of QoS that isn't possible through public cellular networks.

When and how organizations use Private Cellular

The benefits of Private LTE are piquing interest in virtually every industry where organizations have large areas filled with lots of devices and applications that absolutely must be connected at all times — and where sensitive data must be gathered and then shared between devices and servers. When Wi-Fi and even public LTE aren't possible or even ideal, PCN fills needs in several key use cases:

Vast areas with complex networking needs

In large spaces with extensive network requirements and hundreds of users and devices, PCN helps prevent the congestion likely with Wi-Fi and public cellular and is much less expensive to provision and maintain.

High-risk information

In some scenarios, highly sensitive information that is very valuable to hackers is unavoidable. Organizations such as hospitals can keep important information on-site via Private LTE, enabling additional layers of security unavailable through Wi-Fi.

High-bandwidth traffic within budgetary limitations

Organizations looking to connect many video surveillance cameras could use public LTE, but data usage likely would be cost-prohibitive. Fixed-rate private cellular is a much more cost-effective option.

Remote locations lacking wireless infrastructure

In the middle of nowhere — in places where carriers have not set up wireless infrastructure — organizations can relatively easily set up a Wireless LAN via private cellular.

Given the ubiquity of IoT and connectivity-dependent technologies, Private LTE is becoming very applicable in most industries. The ability to set up a Wireless LAN that is much more high-performing, reliable, flexible, cost-effective, and secure than a Wi-Fi network meets the specific needs found in many use cases.

Real-world uses for Private Cellular Networks



Education

K-12 Distance Learning
University Campuses
Administrative



Smart Cities

Convention Centers
Large Public Areas
Buildings



Transportation

Shipping Ports
Rail Hubs
Airports



Manufacturing

Factory
Warehouse
Distribution



Natural Resource

Oil & Gas
Mining
Energy Generation

Getting started with Private Cellular Networking

Interest in Private LTE and 5G is growing at a rapid rate, as more and more organizations in most industries envision its potential to evolve the Wireless LAN. But getting started often is the hardest part. Here are some best-practice steps for getting started:

- 1. Gather information about your environment.** To accurately determine whether Private LTE or 5G is a good fit for your organization, you must first understand as much as possible about the location(s) in question and factors in play.
- 2. Clearly state the problems to solve.** Is latency your project's main inhibitor? How about security or infrastructure expenditures? Knowing the main barriers to address is the best path toward a successful PCN deployment.
- 3. Investigate infrastructure providers.** Cradlepoint can help you engage with a private cellular infrastructure provider.
- 4. Select an edge routing solution that supports private cellular.** Cradlepoint provides several cloud-managed edge routers that support CBRS and other spectrum bands that can be leveraged for Private LTE and 5G..

[Explore Private LTE solutions at cradlepoint.com/pltenow.](https://www.cradlepoint.com/pltenow)

About Cradlepoint

Cradlepoint is a global leader in cloud-delivered 4G and 5G wireless network edge solutions. Cradlepoint's NetCloud™ platform and cellular routers deliver a pervasive, secure, and software-defined Wireless WAN edge to connect people, places, and things — anywhere. More than 25,000 businesses and government agencies around the world, including many Global 2000 organizations and top public sector agencies, rely on Cradlepoint to keep mission-critical sites, points of commerce, field forces, vehicles, and IoT devices always connected. Cradlepoint was founded in 2006, acquired by Ericsson in 2020, and operates today as a standalone subsidiary within Ericsson's Business Area Technologies and New Businesses. Cradlepoint is headquartered in Boise, Idaho, with development centers in Silicon Valley and India and international offices in the UK and Australia. www.cradlepoint.com