A Private Cellular Buyers' Guide: How to Build a Private 5G or LTE Network

How organizations use private cellular networks to control performance and security across wireless LAN

Overview

Our world is dominated by connected devices and 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) to connect those devices. But in some cases, existing LAN technologies, including Wi-Fi solutions, aren't optimized to address this challenge because:

- The sheer size and scope of many deployments demand long-range coverage, and the number of Wi-Fi access points needed to cover that range isn't feasible.
- Business critical devices and highly sensitive information calls for layers of security unavailable within Wi-Fi networks alone.
- Strict budgetary limitations — particularly in the public sector — make it important to minimize infrastructure expenditures as much as possible while still accommodating for scale.
- Applications such as live streaming of HD video footage require dedicated bandwidth and 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).

Consider all the Internet-connected people, places, and things. From devices to vehicles and campuses to warehouses and more, the boundless potential of 5G adds complexity and opportunity to the long-term vision of enterprise businesses as they continue to grow.

In sprawling areas where a Wireless LAN is critical, private cellular networks have emerged as an excellent option. Private cellular networks, which include both private LTE and private 5G deployments, are helping organizations with locations that require wireless connectivity but are not well supported by current wireless infrastructure.

Private networks play a unique role in the world of Wireless LAN, providing benefits that range from increased coverage, capacity, and mobility, to enhanced security and reliability.

Addressing the challenges of secure network coverage in large areas

Across cities and campuses and throughout logistics facilities, venues, and more, 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 alone can be challenging, if not untenable. Private cellular networks can help companies address the problems associated with using Wi-Fi or public cellular 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 millions of dollars for the fiber alone.

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

Keeping high-bandwidth content on-site with a private cellular network and local servers reduces costs in situations when that content doesn't need to leave the area. Even in scenarios where managed service providers (MSPs) are used for private cellular, flatrate plans likely will drive down costs.

Performance and reliability

5G and LTE have proven to be an excellent WAN option in both backup and primary roles, depending on the use case. However, in certain scenarios, public cellular doesn't provide the cost-efficient, unwavering high performance needed to keep business-critical 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 increases network latency and drives up data costs when carried via a public LTE or 5G network with pay-per-bit pricing.

Organizations that rely on Wi-Fi for connectivity may still encounter performance limitations when supporting the types of high-bandwidth applications that are becoming standardized in most business operational situations, especially across vast areas. Examples include automated guided vehicles (AGV) and real-time video surveillance streaming.

One significant cause of Wi-Fi deficiency is when portable user equipment such as a phone, tablet, or IoT device clings to a Wi-Fi connection even when it has no actual coverage — an event known as "client stickiness." Through the prioritization and preemption orchestration capabilities of a private cellular network, the organization controls the connections between access points (APs) and the user equipment, resulting in better coverage flexibility and overall QoS.

Security

In many cases, the security of Wi-Fi 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. This has gotten better with Wi-Fi 6, but when various types of sensitive data and IoT devices are at stake, additional layers of security are necessary.

5G and LTE deployments include SIM-based authentication and edge networking devices, providing additional layers of security through encryption 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. Additionally, network architecture with private 5G or 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 cellular inherent security advantages over other wireless infrastructure and help protect an organization's most critical information from malicious attacks.

How private cellular networks work

Most businesses and agencies today are at least somewhat familiar with the process of using cellular-based connectivity 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 cellular access points on-site allows companies to mimic a standard public cellular network while having the visibility and control of Wi-Fi. This creates a purpose-built Wireless LAN that is more reliable, high-performing, secure, and cost-effective than Wi-Fi or public cellular, making it the ideal solution to support business critical applications.

Private networks can be installed 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 network management the enterprise is willing to take on.

Spectrum used for private cellular networks

Licensed

Enables carriers to operate private cellular networks for enterprises as a managed service. Alternatively, enterprises can deploy their own private cellular network using spectrum licensed by carriers.

Shared

Enterprises can operate private cellular networks in spectrum owned by others. For example, enterprises in the U.S. can use CBRS, which leverages up to 150 MHz of interference-free spectrum.

Unlicensed

Enterprises or carriers can operate LTE or 5G networks in unlicensed spectrum — such as MulteFire in 5.4 GHz — and use carrier aggregation to augment capacity for their networks.

Shared spectrum using the Citizens Broadband Radio Service (CBRS)

CBRS is a 150 MHz band of shared spectrum operating between 3.5-3.7 GHz available only in the United States. Access to this spectrum band — also known as LTE Band 48 — is divided into three tiers, each occupied by users with different types of access.

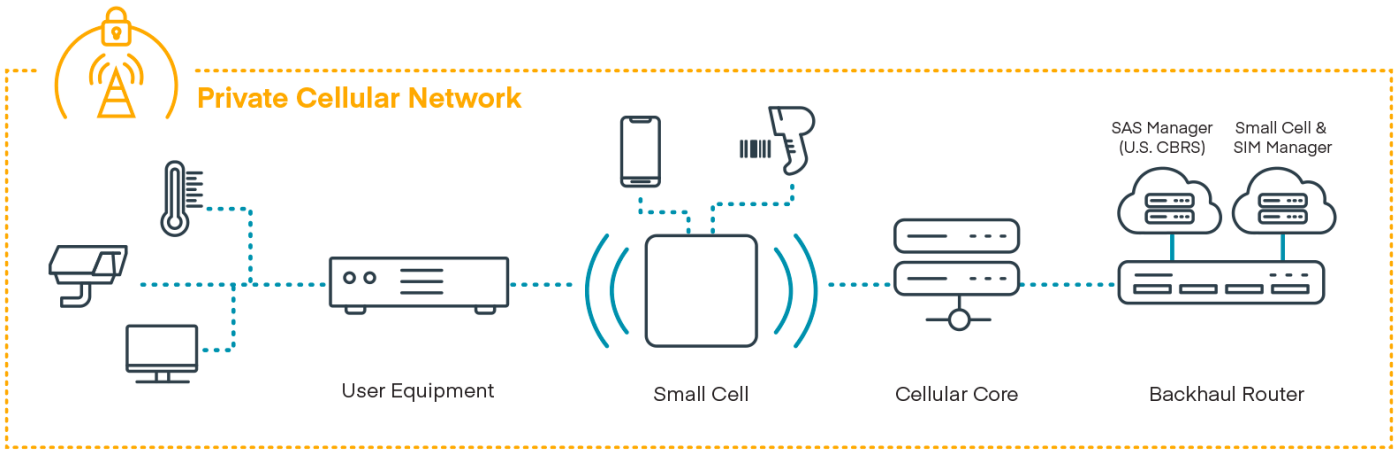
- **Incumbent Access Tier:** Used solely by the U.S. Navy and commercial fixed satellite stations, whose access is grandfathered and prioritized to protect them from interference.
- **Priority Access Tier:** Includes Priority Access License (PAL) holders, such as internet service providers and enterprises users, who have purchased spectrum licenses from the FCC during auctions and can use their personal stake in the CBRS spectrum to build their private 5G networks.
- **General Authorized Access (GAA) tier:** Composed of users who can access the CBRS spectrum for free using phones, laptops, home routers, etc., but are not given priority over incumbents or PAL users.

What do enterprises need to build a private cellular network?

To implement a high-performance, high-capacity private cellular network throughout an enterprise, IT teams must be familiar with the components that bring the network to life. On top of that, it's important to recognize that when each component is developed and deployed by a single vendor, the resulting unified solution gives users the ability to orchestrate their network within a single cloud-based management platform.

Parts of a private cellular network

- **Cellular core:** The cellular core — also known as the evolved or converged packet core — is the brain of the private 5G or LTE network. This is where policies are set to determine which devices can access the network and how traffic can move throughout the network.
- **Cellular access points:** The cellular access point (CAP) — also known as the RAN or small cell — is used to provide access to the network for SIM-enabled edge devices such as laptops, IoT sensors, surveillance cameras, tablets, and more, the same way a Wi-Fi access point is used to connect TVs, printers, and smartphones to an in-home network.
- **Endpoints and private SIMs:** A SIM card — whether physical or embedded — is required to gain access to the network and for authentication to the private 5G or LTE cellular core before connected devices such as cameras, IoT sensors, and more can join the network.
- **Network management tools:** A cloud-based network management portal provides real-time visibility and control through a single pane of glass. This is crucial for configuring, monitoring, and troubleshooting the network from anywhere, gaining access to key insights, and reducing costly truck rolls.



When and how organizations use private cellular

The benefits of private LTE and private 5G are piquing interest in virtually every industry where organizations have large areas filled with lots of devices and applications that must be connected at all times without exception — and where sensitive data must be gathered and then shared between devices and servers. When Wi-Fi or public cellular aren't ideal or even possible, a private cellular network can fill 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, private cellular networks help prevent congestion and are much less expensive to provision and maintain vs. Wi-Fi.

High-bandwidth traffic within budgetary limitations

Organizations looking to connect many video surveillance cameras could use public LTE or 5G, but data usage would likely be cost prohibitive. Fixed-rate private cellular is a much more cost-effective option.

Remote locations lacking wireless infrastructure

In places where carriers have not set up wireless infrastructure, organizations easily can set up a private cellular network to use as their Wireless LAN.

Constant connectivity for applications on the go

Mobile use cases such as connected workers, AGV, asset monitoring, and more require a connection that can move with them. Private cellular networks give users control over connectivity and QoS, virtually eliminating client stickiness that can cause downtime.

High-risk information

In some scenarios, transmitting and storing highly sensitive information is unavoidable, creating alluring targets for hackers. Organizations such as hospitals can keep business-critical information on-site via a private cellular network, enabling additional layers of security that are unavailable through Wi-Fi alone.

Given the ubiquity of IoT and connectivity-dependent technologies, private LTE and private 5G are relevant solutions in most industries. The ability to set up a Wireless LAN that is much more high-performing, reliable, flexible, cost-effective, and secure than Wi-Fi or public cellular meets the specific needs found in many use cases.

Real-world uses for private cellular networks

Warehouse and logistics

Data storage and transmission
High-definition surveillance cameras
Predictive maintenance
Inventory lifecycle management

Smart city

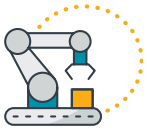
Crime and environmental monitoring
Intelligent traffic control
Smart lighting and parking
Video surveillance

Venues and hospitality

Kiosks and digital signage
Retail stores and restaurants
Security and surveillance
Vehicles (service, bus)

Healthcare

Ambulance connectivity
Telehealth
Medical equipment
Asset management



Manufacturing

Predictive maintenance
Automated manufacturing
Quality control
Factory floor mobility

Education

Campus Wi-Fi and security
Special events and arenas
Temporary and remote classrooms
Distance education

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 is often the hardest part. Here are some best practices on where to begin:

1. **Clearly identify the problems to solve.** Do you need more flexibility on the manufacturing floor? Are areas of your business lacking reliable connectivity? Do infrastructure limitations impede connectivity for IoT devices? Understanding operational barriers is key when developing a successful private cellular network deployment.

2. **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 including coverage needs as well as technical requirements for devices and applications based upon the business hurdles you're trying to solve for.

3. **Establish key performance indicators (KPIs).** KPIs may include processing and production rates, network uptime, man-hours, data expenditures, and more. These KPIs should be revisited and adjusted as needed after the private network is deployed. Clear, achievable KPIs will set the foundation that justifies future investments in the growth of a private cellular network.

4. **Investigate infrastructure providers.** When building a private cellular network, you can avoid frustration and failure by choosing infrastructure components designed to fit your unique use case. Cradlepoint makes this easy by providing a complete, end-to-end private cellular network solution.

5. **Design a proof of concept.** Combine your infrastructure solutions and anchor business case to design a proof of concept that is scalable, future-proof, and able to produce results that align with your KPIs.

6. **Conduct a site survey.** Using a radio frequency (RF) planning tool to determine the placement of cellular access points, map out your private cellular network architecture, accommodating for the location of walls and windows, signal obstructions, and environmental challenges.

7. **Get ready to grow.** After building the private network, conduct a post-deployment verification to test its performance and ensure the network performance is on track to achieve your KPIs. If so, begin to plan for commercial deployment and expansion.

Explore private cellular network solutions at **cradlepoint.com/private-cellular.**

About Cradlepoint

Cradlepoint enables the freedom to connect people, places, and things that drive more experiences, more ways to work, and better business results — anywhere. The company is a pioneer in Wireless WAN, offering advanced 4G and 5G routers and adapters — controlled through Cradlepoint NetCloud™. Enterprises rely on Cradlepoint and its Cellular Intelligence to build a reliable, secure network for fixed and temporary sites, vehicles, IoT devices, and remote employees. Headquartered in Boise, Idaho, Cradlepoint is a subsidiary of Ericsson's Business Area Technologies and New Businesses division. It has international offices in Asia Pacific, Canada, Europe, India, and Latin America. www.cradlepoint.com

