ericsson.com/airports

A buyers' guide to private cellular networks for airport operators and airlines

The essentials of building a private 5G or LTE network

How airports and airline hubs leverage private cellular networks to improve connectivity, operational efficiency and security

Contents

Reimagining digital infrastructure at the airport

In today's demanding airport environment, seamless coordination between ground crews, airline staff and passengers is crucial to ensuring the safety and security of all involved. Real-time data, reliable communications and continuous connectivity are essential to making this coordination possible.

Private LTE and 5G networks are gaining traction in sectors like airports, where vast areas with numerous devices and critical applications need seamless, secure connectivity. These networks enable continuous data sharing between devices and servers, overcoming challenges when Wi-Fi or public cellular solutions fall short.

Private cellular networks offer greater coverage, capacity and flexibility, outperforming Wi-Fi in large, complex environments.

What is a private cellular network?

A private cellular network comprises of cellular access points (often small cell radios) and a dedicated cellular network core that manages network traffic going through them. It provides wireless connectivity coverage across an airport or other campus site, over LTE and 5G spectrum network operates similarly to a public cellular network, but offers an airport on-site, secure cellular infrastructure that enables the full coverage, control and customizable traffic prioritization that is not available on a public network's general shared infrastructure. With private 5G networks, airports benefit from a purpose-built wireless network, designed for assured performance, security and cost-effective scalability. Thus, private 5G networks are uniquely equipped to handle the connectivity needs for critical applications, moving equipment, and autonomous operations where 'mostly good' connectivity, such as that which Wi-Fi or public cellular offers, is not good enough.

Components of a private 5G cellular network

Cellular access points: Small cell radios, part of the Ericsson's industry leading 5G Radio Access Network (RAN) portfolio, are installed at strategic locations on-site to ensure seamless indoor and outdoor coverage.

Cellular core: An on-site 5G cellular core (a converged LTE/5G core smaller than the size of a full server rack) serves as the brain of the private cellular network. It defines security, access, and network policies and manages traffic flow across the network.

Private SIMs/eSIMs and endpoints: These enable access for connecting to the private LTE/5G network. They are provisioned to authenticate and connect devices to the private network, ensuring that airport equipment like push-to-talk devices, cameras, IoT sensors and autonomous vehicles can be securely connected and operated.

Network management tools: A consolidated dashboard (through Netcloud Manager) provides a "single pane of glass" dashboard that offers real-time visibility and tools to control and manage the entire network, for simplified operations.

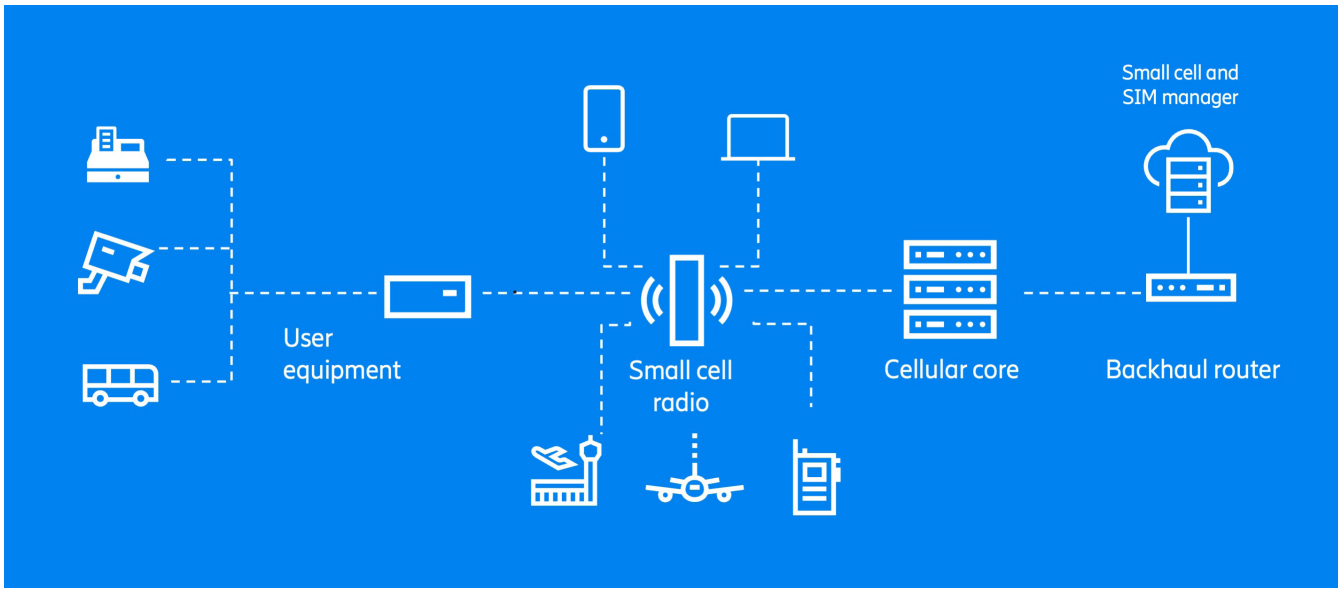

Fig 1: Overview of a private cellular 5G network at an airport

Deploying a private cellular network: Key considerations

Addressing the spectrum requirement

Private LTE/5G networks require the use of certain spectrum bands, which are designated ranges of frequencies that 4G and 5G cellular traffic utilize. Decisions around spectrum choices, methods of accessing them, and preferred deployment models should be aligned with existing IT resources as well as operational and geographical requirements since spectrum allotments vary across countries.

Implementing a private cellular network should involve strategic planning and consideration in selecting right partners as well as and the right technology mix. Airports have a couple ways to manage private network implementation, each offering distinct advantages based on their specific needs and resources.

Spectrum options for private cellular networks

Licensed: Enterprises can deploy private cellular networks using spectrum licensed by carriers or opt for a managed service from mobile operators. In some countries, like Germany, dedicated industry spectrum provides an additional licensed option.

Shared: Businesses can operate private networks on spectrum allocated for shared use. For example, in the US, Citizens Broadband Radio Service (CBRS) offers up to 150 MHz of interference-free spectrum for enterprise applications.

Unlicensed: Both enterprises and carriers can leverage unlicensed spectrum to deploy LTE or 5G networks, often using carrier aggregation to enhance capacity and performance.

The private 5G advantage

Airports function like self-contained cities, each with its own set of challenges. Their infrastructure supports thousands of connected devices, serving diverse users—from passengers to personnel. Increasingly, airports are integrating advanced technologies into airside and terminal operations, including autonomous vehicles, robotics and Augmented reality (AR) solutions. While existing wireless and wireline networks address basic connectivity needs, they often fail to provide the coverage, capacity, latency, reliability and security needed for next-generation applications.

Private cellular networks offer greater coverage, capacity and flexibility, outperforming Wi-Fi in large, complex environments.

Stay connected everywhere

A common issue with Wi-Fi is that portable devices like phones, tablets and IoT often "stick," trying to stay connected to one Wi-Fi network even when they're beyond the network's coverage, making for problematic handoffs Private cellular networks address this challenge by using prioritization and preemption orchestration, giving organizations control over the connections between access points (APs) and devices. This results in enhanced coverage flexibility and improved overall reliability.

Cost efficiency

Expansive sites like airports are taking advantage of Internet of Things (IoT) sensors and machine-to-machine (M2M) communication to enhance operational visibility and efficiency. However, installing in-ground fiber for Wi-Fi access points can be prohibitively expensive, often costing millions.

Private cellular networks offer a cost-effective alternative for reliable, airport-wide connectivity. Instead of deploying dozens of Wi-Fi access points with extensive wiring, a cellular-based wireless local area network (LAN) requires only a handful of private cellular radios.

Additionally, keeping high-bandwidth traffic on-site with a private cellular network and local servers enhances data security and can reduce recurring costs by eliminating the need to pay the data usage fees charged per device by public cellular service providers. Private network owners retain the ability to maintain full control their network traffic, data and cybersecurity.

Security

Traditionally, Wi-Fi security measures are limited to a basic username and password protection, which is insufficient for business-critical airport data and IoT devices. While Wi-Fi 6 does improve security, private networks provide greater protection through built-in enterprise-grade encryption, SIM/eSIM authentication and on-site traffic management.

Private 5G and LTE networks further enhance security by integrating encrypted communication, localized traffic control, and a zero-trust approach. Their architecture typically includes on-premises servers, enabling airports to keep critical IoT and corporate data within their own network—eliminating exposure to public infrastructure vulnerabilities.

Performance and reliability in public vs private networks

Public cellular networks serve as effective wireless solutions for some airport operations. However, for mission-critical applications that demand uncompromising performance, security and cost efficiency, public networks by themselves cannot always deliver on key requirements.

For instance, many airports generate vast amounts of data, much of which is continuously pushed to a central data center. Using a public LTE or 5G network for this traffic can introduce higher latency, increased costs due to pay-per-bit pricing models and potential security risks from shared infrastructure.

Control over the airport's wireless infrastructure is another key consideration. Public 5G networks, managed by mobile service providers, limit an airport's ability to custom prioritize, secure and optimize its operational traffic separately from passenger data, typically involving internet browsing and usage. Private 5G networks address this challenge by enabling airports to isolate their operational data, keeping it secure and local through a locally hosted edge computing infrastructure.

With a private cellular network, airports can determine which data stays on-site and which can be securely shared externally, ensuring lower latency, greater reliability and full control over critical applications.

Maximizing ROI: Building the case for multiple use cases

Adopting private 5G technology provides multiple bottom-line benefits for airports through operational cost reductions, faster turnarounds, added commercial opportunity, and smart building efficiencies. To get the most out of a private 5G investment, working together with the right stakeholders across the airport to identify the right set of initial use cases to deploy over private 5G is key.

With the wide range use cases 5G can support and enable, leveraging one private 5G network to address multiple use cases, such as the ones below, unlocks more value and helps maximize the ROI of your airport's digital infrastructure.

Vast areas with complex networking needs

In large spaces with extensive network requirements and hundreds of users and devices, private cellular networks prevent congestion and provide a more cost-effective solution than Wi-Fi.

High-bandwidth traffic within budgetary limitations

For organizations that need to connect many video surveillance cameras, private cellular networks provide a more affordable alternative to public LTE or 5G, which can become prohibitively expensive due to data usage.

Remote locations lacking wireless infrastructure

Where carrier infrastructure is unavailable or unreliable, organizations can deploy a private cellular network to establish their own dedicated wireless local area network, ensuring consistent connectivity.

Constant connectivity for mobile applications

For use cases involving ground crew, automated guided vehicles (AGVs) and asset monitoring, private cellular networks provide uninterrupted, high-quality connectivity while avoiding issues like "sticky clients" that can cause downtime.

Critical information

Airport networks manage highly sensitive communications, making them prime targets for cyber threats. Private cellular networks keep business-critical data secure on-site, ensuring safety and compliance. Private 5G networks can segment data traffic to protect mission-critical applications from interference or vulnerabilities. For these reasons, private LTE and 5G solutions are becoming essential across industries, offering wireless connectivity that is more reliable, secure, cost-effective and flexible than traditional Wi-Fi or public cellular.

Common use cases for private cellular networks in airports

- Connected operations
- Connected workers
- Enhanced surveillance and security
- Autonomous vehicles
- Advanced analytics and biometrics
- Robotic applications

ericsson.com/airports

ericsson.com/en/private-networks

ABOUT ERICSSON:

Ericsson enables communications service providers and enterprises to capture the full value of connectivity. The company's portfolio spans Networks, Cloud Software and Services, Enterprise Wireless Solutions, Global Communications Platform, and Technologies and New Businesses and is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's investments in innovation have delivered the benefits of telephony and mobile broadband to billions of people around the world. Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.

www.ericsson.com

Ericsson
SE-164 80 Stockholm, Sweden
Telephone +46 10 719 0000
www.ericsson.com

The content of this document is subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document

© Ericsson 2025