

Executive Summary

Private 5G networks are emerging as a transformative solution for enterprises seeking greater control, security, and performance in their wireless infrastructure.

While Wi-Fi remains a cost-effective and widely adopted option, its limitations become evident in certain demanding scenarios. This whitepaper outlines three strategic use cases where deploying a private 5G network can deliver substantial operational advantages. This whitepaper outlines three practical and strategic scenarios in which deploying a private 5G network may offer significant advantages.

A graphic showing a city skyline at night with a large, glowing blue "5G" logo in the center, surrounded by circular and arrow-like patterns, suggesting connectivity and technology.

3 Strategic Use Cases to Deploy a Private 5G Network Today

Use Case 1: Uplink-Heavy Traffic Requirements

Private 5G networks are an ideal solution in environments where large volumes of uplink data need to be transmitted reliably and continuously. This is especially true when aggregate uplink traffic — often in the range of 100 Mbps or more — is sustained across multiple devices, such as video cameras or sensors. In many environments, the presence of just 10 or more concurrently uploading devices can cause Wi-Fi uplink performance to degrade drastically due to channel contention and increased interference, often reducing aggregate uplink throughput drastically and introducing high latency and jitter. Under such loads, Wi-Fi performance commonly degrades due to contention, interference, and uplink inefficiency.

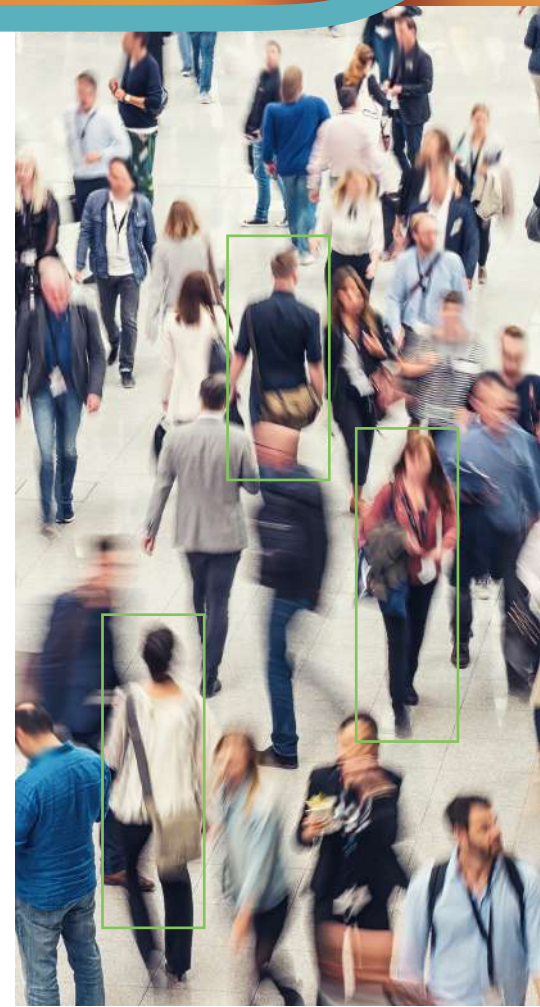
Traditional Wi-Fi struggles under such conditions due to its contention-based access mechanism (CSMA/CA), which leads to collisions, retransmissions, and increased latency. Furthermore, when many devices attempt to upload simultaneously, the overall noise floor rises, degrading signal quality and reducing effective throughput.

Private 5G addresses these limitations by offering:

- Configurable uplink and downlink resource allocation, including the ability to adjust timeslot configurations (e.g., DSUU or DSUUU) to optimize uplink-heavy applications
- Scheduled uplink access for consistent performance
- Better interference and noise management
- Higher uplink capacity with scalable device support

Typical applications include:

- Real-time video streaming for AI-based surveillance and analytics
- Continuous telemetry from autonomous systems and robotics
- University campuses, multi-level car parks, parks with numerous surveillance cameras deployed to monitor activity, detect suspicious behavior, and predict accidents or emergency events in real time



Use Case 2: Reliable Outdoor Coverage

Outdoor wireless connectivity poses unique challenges for Wi-Fi, which is constrained by low transmission power and vulnerability to interference. Wi-Fi access points typically provide effective outdoor coverage of only 20 to 50 meters under real-world conditions. This limitation stems from regulatory power constraints and environmental factors such as buildings, foliage, and interference, which all reduce signal reliability and contribute to interference from nearby devices or networks.

Private 5G, in contrast, offers:

- Higher transmission power (e.g., 1–5W) with extended range
- Outdoor coverage of 500 meters to 1 kilometer per cell
- Coordinated or licensed spectrum use for minimal interference

Ideal use cases include:

- Broadcast or event companies requiring reliable outdoor connectivity for live coverage streaming
- Military or first responder deployments requiring on-the-fly communication networks
- Connectivity for camping sites or temporary pop-up events requiring reliable POS systems
- Manufacturers/Warehouses that require large uninterrupted wireless coverage
- Large campuses and industrial estates
- Ports, transportation hubs, and logistics yards
- Mining sites and utilities needing wide-area infrastructure monitoring for pipelines, grids, or substations

Private 5G delivers the performance and reliability needed for demanding outdoor environments where Wi-Fi cannot scale effectively.



Use Case 3: Offloading or Isolating Critical Services from Wi-Fi



As enterprise Wi-Fi networks become increasingly saturated with devices and applications, performance and security concerns often arise. A private 5G network can serve as a dedicated overlay to isolate mission-critical services or offload high-priority traffic, thereby enhancing overall network efficiency.

This approach is particularly beneficial when:

- The existing Wi-Fi network suffers from congestion and interference
- Critical services require dedicated resources and better QoS
- Security policies demand traffic isolation or enhanced authentication

Private 5G enables:

- Deployment of parallel networks for segmented traffic
- SIM-based authentication and end-to-end encryption
- Traffic prioritization and application-level QoS

Relevant scenarios include:

- Manufacturing environments where Wi-Fi performance is degraded due to interference from unlicensed band technologies (including Bluetooth, Zigbee, or proprietary industrial protocols), or where OT and IT traffic must be segmented for security compliance
- Supporting uninterrupted and reliable AR/VR applications
- Providing secure and stable links for surveillance and control systems
- Airports using private 5G for critical operations such as ground staff coordination, security systems, and real-time baggage tracking, while reserving Wi-Fi for passenger connectivity
- Stadiums deploying private 5G for point-of-sale systems, live broadcasting equipment, and emergency communication, avoiding interference from public Wi-Fi networks heavily used by spectators

By integrating private 5G as a strategic overlay, enterprises can optimize both performance and security without overhauling their existing Wi-Fi infrastructure.

Conclusion

Private 5G networks are not a replacement for Wi-Fi, but a powerful complement in environments where reliability, performance, and control are paramount. Organizations should consider private 5G when facing uplink-heavy traffic, outdoor coverage challenges, or the need to isolate and protect critical network services. By deploying private 5G in these targeted scenarios, enterprises can future-proof their connectivity infrastructure and unlock new levels of operational efficiency.





Communication for the future



About Askey

Askey Computer Corporation is headquartered in Taipei, Taiwan with offices across the globe and within North America. Founded in 1989, Askey Computer Corporation is a member of AsusTEK (Asus) Computer Inc., and leveraging 35 years of telecommunication development has created an industry leading portfolio of global 5G and private 5G end-to-end network solutions for modern business environments to enhance their digital transformations. As a manufacturer of rugged mobile computing solutions since 2001, Askey has produced over 20M mobile devices to date and has helped shape Enterprise mobile computing.

