Private 5G in airports: Ready for takeoff

SENZA FILI

Betacom

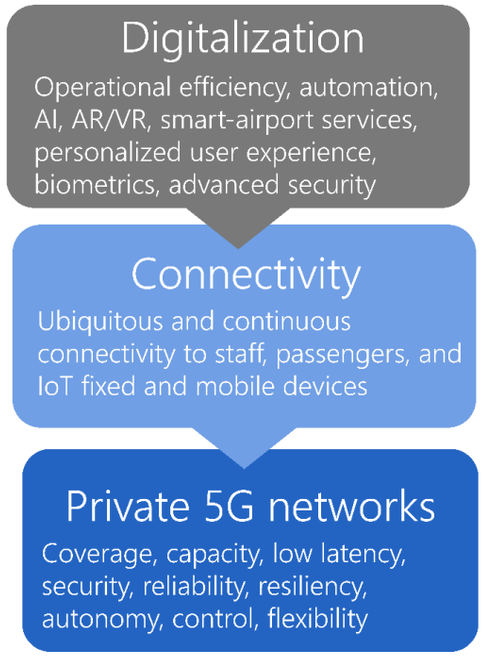
Digital transformation promises to fundamentally change the way airports operate and serve their stakeholders. Passengers will have a personalized experience and access to rich services. Airlines will boost their operations' efficiency and functionality, reduce costs and resources, and improve passenger satisfaction. Tenants and other airport partners will roll out new services to support their operations, their staff, and passengers more effectively. Security and safety partners will have more reliable tools to protect assets and people. Airports will overhaul their operations to manage assets, improve staff efficiency, and enable remote control for some applications. Innovation will impact the entire airport ecosystem dynamics: how partners collaborate, how they share information, and how they communicate with each other.

Realizing this vision is within reach. We have the technology, the devices and the business models to support it. A growing number of airports are actively engaged in developing a digitalization strategy and implementing it.

Connectivity is an essential enabler for the digital transformation in airports. Airports already have a mix of wireless and wireline networks, but in most cases, these networks do not provide the coverage, capacity, latency, reliability and security that new applications and services require. In many airports, legacy networks, proprietary solutions, and vendor lock-in prevent innovation or make it unaffordable. Airports need to overhaul their wireless infrastructure to get ubiquitous and continuous connectivity to assets, goods, staff and passengers across the entire airport footprint.

Private 5G networks address these requirements and give airports the performance and reliability they need to support their connectivity needs and those of their partners. In addition, and equally important, they give airports full visibility and control over their wireless infrastructure – from planning and deployment, to operations and upgrades.

Digitalization and connectivity needs drive adoption of private 5G networks



Read or watch the conversations with Betacom and Dallas Forth Worth International

Questions addressed in the report:

- Why do airports need to take control of wireless connectivity?
- How does the 5G ecosystem keep all connected?
- What are the top private 5G network use cases?
- Why do airports need to move beyond legacy networks?
- Why a private 5G network?
- Isn't Wi-Fi enough?
- Is CBRS a game-changer?
- Should airports choose traditional or Open RAN?
- How can airports manage the complexity of a private 5G network?
- Do airports need network slicing and edge computing?
- What are the benefits of accurate 5G positioning?
- Does 5G interfere with air traffic in airports?
- How can airports manage the complexity of a private 5G network?
- Do airports have to manage and operate private 5G networks?
- How does a NaaS model work?

Taking control of wireless connectivity

A successful digital transformation requires control over the wireless infrastructure. Airports have to be able to determine the coverage and performance of their wireless network to support the services that they want to deploy internally or that airlines and other tenants want to use. For security, safety and privacy reasons, they need to keep their traffic isolated from public traffic. To optimize efficiency, they need to decide what data and processing should remain within the premises, and what should be in the cloud. To extract the best value from the network resources available, they need to prioritize applications, services or traffic flows as they choose. And to make sure all this is happening as they expect, they need full visibility into the network.

As the criticality of the wireless infrastructure increases, having control over it becomes even more imperative for airports. Control has become the main driver in the shift from public to private networks in airports, as well as in other enterprises. A public 5G network owned and managed by a mobile operator would relieve the airport from having to pay, deploy and operate a demanding network, but it would not provide the level of control most airports require.

Control over the wireless infrastructure has become not just more valuable but also more affordable and feasible. 5G and new spectrum sharing frameworks such as CBRS make it possible to deploy a private network that the airport owns, deploys and operates on its own, or in partnership with a system integrator or NaaS service provider.

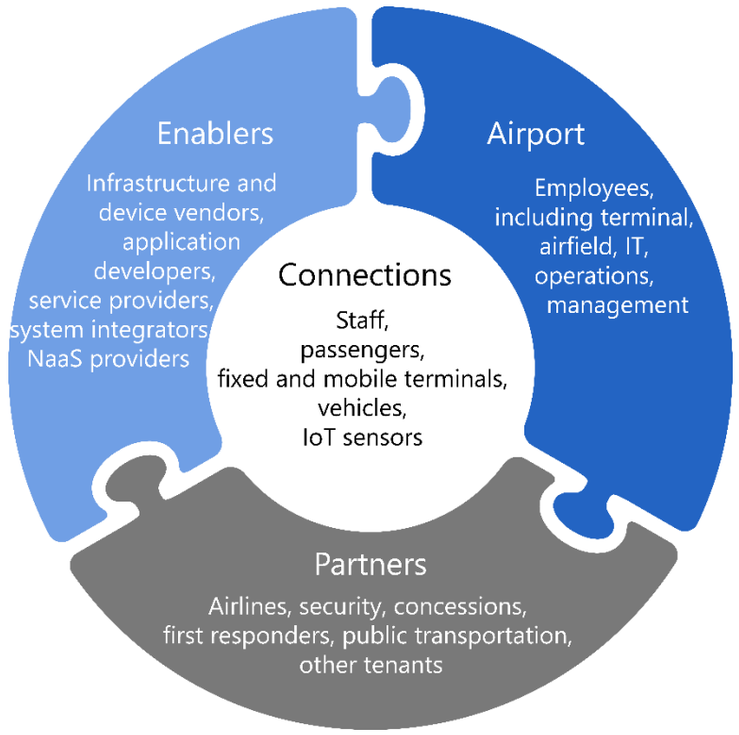
The airport 5G ecosystem keeps all connected

Much goes on in an airport. Passengers need to get safely checked in and boarded, retrieve their baggage, enjoy the food and other services in the terminal, and expect to be continuously connected and have a personalized, rich experience. Airlines have to ensure that flights depart and arrive on time and safely. Security agencies and first-responders have to maintain a safe environment. Concessions and other tenants offer a wide range of services to passengers and staff.

The volume and diversity of connections that airports need pose a challenge for wireless connectivity. Personal devices connect passengers and staff. Fixed and mobile terminals connect airport assets and provide services such as signage, surveillance, or traffic control. Vehicles are also connected for tracking, assisted or autonomous driving, and remote operations. IoT sensors need connectivity to monitor the environment and track moving goods, such as baggage and cargo.

Airport connectivity requires the support of a robust ecosystem that goes beyond the airport IT and communications team. It involves all the airport employees that work together to operate all the services that connectivity supports. Airlines and other partners can share the wireless infrastructure with the airport to run their operations and serve their customers.

The private 5G network ecosystem also relies on enablers such as infrastructure and device vendors and applications and service providers that work with airports to tailor their offerings to their needs. System integrators and NaaS providers also play a central role in planning, deploying and operating their private 5G networks.



Private 5G use cases

There is no shortage of use cases for airports. The table below lists only a selection of use cases that a private 5G network can support and that airports are exploring today. Further in the future, XR, automation, AI, ML, network slicing, 5G NR positioning, drones, and zero-touch and self-serve service provisioning will pave the way for new applications for passengers, partners and airports.

Because of the large number of use cases competing for funding and resources, airports will have to prioritize their rollout according to their digitalization strategy. Each airport may initially focus on different use cases, depending on specific needs or demand from partners. Technology maturity, terminal device availability and cost, and solution availability will also play a role in selecting the use cases deployed in the early stages.

As they select use cases, airports need a wireless infrastructure that can meet each use case's diverse set of requirements. Reliability and resiliency are crucial for security and emergency use cases. Low latency and continuous connectivity are required for vehicle and some tracking use cases. Video-based use cases need high throughput and low latency. IoT use cases may require ubiquitous connectivity but lower data rates.

Airport	Airlines	Tenants	Passengers
Runway traffic monitoring and management	Ramp connectivity	Public safety, TSA and first-responder connectivity	Self-service and assisted check-in and bag drop
Critical communications	Aircraft connectivity	Emergency management	Boarding
Parking management, dynamic pricing and payments	Telemetry data from aircraft	Ground transportation	Passenger mobile app
Body cameras	Flight operations and scheduling system	Concession staff connectivity and operations	Flight, gate and baggage information display systems
Vehicle tracking	Passenger management and customer service	Concessions' customer service and POS	Paging and public address system
Baggage tracking	Stand automation	Self-serve kiosks	Customer relationships
Environment, safety and asset management	Staff connectivity	Digital signage	Train and buses for terminal transportation
Staff voice, data and video connectivity	Asset management		Biometrics
Video surveillance			Security control
Passenger flow			Border control
Cargo management			

Moving past legacy to unlock new connectivity options

Most airports have started exploring, planning for, or deploying new wireless infrastructure. The limitations of the existing networks (see table on the right) have acted as a crucial call to action. For a long time, airports – as well as other enterprises – have felt that their wireless networks were slipping behind public wireless networks and failed to reach the cost and performance thresholds they needed and that they knew the technology could support. A combination of proprietary solutions and technologies and a siloed operational environment has created the need for a major renewal of the wireless infrastructure.

Yet, only with 5G – and more specifically with CBRS in the US – airports have become able to deploy private networks that use the same standards-based technology as public wireless networks. This is of paramount importance: with 5G, airports can deploy future-proof, scalable, open networks, avoid vendor lock-in, and benefit from the latest technology advances.

Limitations of legacy networks
Low data rates
High latency
Limited security options
Coverage limitations
Low reliability
Insufficient QoS
Limited visibility and control
Interference
Proprietary interfaces
Outdated technology
Multiple siloed solutions
Low scalability
Expensive to deploy and maintain

Wi-Fi and 5G

In most airports, wireless connectivity depends on separate networks that typically include public cellular networks, special-purpose networks such as LMR, and Wi-Fi. Wi-Fi is the most used access technology for data and video communications traffic, and airport-specific applications. While mobile operators deploy and operate their cellular networks, most airports own and control their Wi-Fi infrastructure. With Wi-Fi 6, Wi-Fi performance has improved, and with the availability of new unlicensed spectrum in the 6 GHz band, it has more capacity.

So why do airports need private 5G networks? Could they expand the existing Wi-Fi network that they are familiar with instead of deploying a separate private 5G network? The question stems from a false dichotomy: airports still need Wi-Fi, as well as public mobile networks, alongside private 5G to meet all their connectivity needs.

Wi-Fi and 5G complement each other, and, together, they can support the digital transformation in airports more effectively than they could on their own. Both technologies can support many use cases, but they do so differently. Wi-Fi can carry larger traffic loads and is preferable for video-intensive non-critical applications with many concurrent streams – for instance, in a dense webcam network in a terminal to track passenger flow. But private 5G networks are better suited for use cases that require mobility, reliability, deterministic performance, URLLC, high security, isolation, QoS, and outdoor coverage.

In some cases, both technologies can support the same use case, either for more efficient allocation of network resources or for redundancy. For instance, a surveillance system may use Wi-Fi for non-critical locations or switch to 5G during emergencies.

In addition, in many airports, the Wi-Fi spectrum is so heavily used that the network suffers from interference and congestion. In turn, this reduces the capacity and reliability, and increases the latency. Because Wi-Fi uses unlicensed spectrum, airports have limited ability to manage interference and prioritize traffic. While they control the network, they cannot control its performance as they need for many use cases.

Ultimately, the question airports face is not which technology to use but where it is more appropriate to use 5G or Wi-Fi. And to some extent, the answer will depend on the specific priorities of the airport, its deployed and planned infrastructure, and the set of required use cases. In all cases, however, each network will act as an

offload resource: Wi-Fi can free up capacity in the private 5G network; a private 5G network can reduce congestion in the Wi-Fi network and improve passenger access.

Private or public 5G networks?

Airports that want to use 5G can choose between public and private networks.

Public networks

Public networks are deployed and operated by mobile operators and airports have to share them with passengers and tenants. Because airports do not have to deploy their own infrastructure, they benefit from low capex and reduced complexity. However, networks access costs shift to opex, and they can be high because the high traffic volumes drive up prices. The high demand for network access may also limit the availability of network resources. Operators can offer SLA-based contracts that guarantee prioritized access and, in the future, dedicated access to a network slice, i.e., a virtual partition of the network resources, but airports would still have restricted access.

Perhaps more importantly, airports do not have control over network planning, deployment, operation and upgrades, nor visibility in the network performance. They may end up with a network with incomplete coverage or incapable of meeting throughput, latency or other requirements, and they may be unable to remedy these problems. In turn, this may prevent them from rolling out some use cases, either because of capacity, coverage, or performance limitations.

Private networks

The airport owns and controls private networks and hence can design them to meet specific performance, time and financial requirements set by the airport. This approach increases the capex, but it is less opex intensive. Because it controls the networks, the airport also allocates network resources to its tenants and other partners, enabling them to offer services that benefit them – and indirectly the airport as they will improve the passenger experience. Access to the network for third parties will also create a revenue source that will help offset the costs.

A private network requires not only a bigger upfront investment but also more effort in planning, operating and maintaining it, as well as supporting the selected use cases and managing third-party access. A private 5G network that supports use cases with stringent and varied requirements, covers a large indoor and outdoor area, and supports mobility will also be more complex than most enterprise private networks and the local Wi-Fi network. However, as we will discuss later in the report, airports don't have to run private networks in-house, relying on their staff or, most likely, hiring new staff. Instead, they can work with a system integrator or NaaS service provider that can manage the complexity while leaving control of the network to the airport.

Why private networks? Why now?
Existing wireless infrastructure is aging and difficult and expensive to update
5G technology is available and mature to meet the requirements of new use cases, increase operational efficiency and reduce costs
Digital transformation has become a priority, and covid is accelerating the process
Passenger expectations, airlines and other stakeholders' demand, and competition with other airports for passengers and cargo services are driving innovation
CBRS spectrum makes it possible to deploy private networks and give airports control and autonomy over the wireless infrastructure
Private networks are better suited at meeting security and safety requirements
Open RAN and standard-based solutions reduce complexity and avoid vendor lock-in
NaaS and other new business models reduce the complexity of private networks

Benefits of private 5G networks

The table on the right lists the main benefits of private 5G. 5G brings the performance and the ecosystem that the airport needs. The private architecture brings the control, flexibility and agility that allows the airport to tailor the network to its needs and maximize its value.

CBRS

CBRS in the US and other spectrum-sharing models in other countries are a game changer for private 5G because, for the first time, they make valuable 3.5 GHz spectrum available to airports. The use of CBRS spectrum is protected: airports do not need to pay for a license, but they need to request access to it. Unlike unlicensed access, however, only registered users can use CBRS access, so airports control who installs the infrastructure and effectively limit the deployment of competing CBRS networks within their footprint. Countries like the UK or Germany use different spectrum sharing models, but they also give airports protected access to spectrum without getting a license at an auction.

With CBRS, airports can use up to 150 MHz of midband spectrum in their private 5G networks. The band is used worldwide, mostly in public networks, ensuring that devices and equipment are available and affordable. Airports have the option to deploy LTE initially and later switch to 5G, as long as they choose upgradeable equipment. They may want to do so if some of the terminal devices they use do not yet support 5G.

Edge computing

If sharing a public network, it is difficult for airports to isolate their traffic or keep it within the premises. For security and performance reasons, airports may want to keep traffic within the same network and separate from other traffic (e.g., personal passenger traffic) and keep application data in a locally-hosted edge computing infrastructure. Private 5G gives them the option to do so and to select what data should remain local and what data should be hosted in a centralized cloud. Edge computing will increase security as data will remain within the airport. At the same time, the airport or some of its tenants will also be able to share some data with external agencies or units if they choose to do so. Other advantages of edge computing and isolation are lower latency and jitter, and higher reliability, which can be crucial to support the more demanding use cases.

The benefits of private 5G
Foundation for digital transformation
Control and autonomy over network infrastructure and data
Personalization of services
Self-service, zero-touch applications
Security and safety
Resiliency and redundancy
Edge computing and isolation
Network slicing
5G NR positioning
Future-proof technology
Open standards, multi-vendor ecosystem
Coexist with deployed Wi-Fi and DAS infrastructure
Move beyond legacy push-to-talk (PMR/LMR)

Open RAN

Open RAN was primarily developed with public networks in mind as a new RAN architecture that uses open interfaces and a virtualized architecture, promotes a multi-vendor environment, and gives operators flexibility and cost savings. Because Open RAN is still in its early stages, its adoption may initially add some complexity, but in the longer term, afford the same benefits it does in a public network. More specifically, it would make it easier for airports to use equipment from different vendors or switch to a new vendor when upgrading or expanding the network.

Network slicing

With network slicing, private 5G networks can create virtual partitions that are reserved for specific traffic types (e.g., URLLC for applications that require low latency), applications (e.g., vehicular applications), or tenants (e.g., an airline). Network slicing allows airports to allocate network resources more efficiently and ensure SLA compliance for specific applications or tenants.

5G NR positioning

5G provides precise positioning capabilities to locate devices with high accuracy (2-3 m today, with an expectation of 0.3 m and a latency of 10 ms with 5G Advanced), using NR, the new 5G air interface. Because 5G NR positioning does not require GPS or a satellite signal, airports can use it both indoors and outdoors. 5G NR positioning requires less power and set-up time than satellite-based solutions and supports mobile positioning more effectively than Wi-Fi or Bluetooth. Use cases that require navigation, drones, public safety, asset tracking, XR, and, generally, mobile devices will benefit from improved location capabilities.

Deploying and operating private 5G networks

A private 5G network gives airports the connectivity they need to digitalize services and operations, and transform their relationship with ecosystem partners and passengers. But deploying and operating a private 5G network that delivers on its promises is not trivial. Multiple factors require the airports' consideration for a successful private 5G network:

- An initial investment, which will take some time to generate a positive ROI from improved efficiency and new revenues from services and tenants' access
- Detailed planning, to ensure the network meets the airport's present needs and can be upgraded to meet its future needs
- Careful vendor selection, to avoid vendor lock-in and keep network future-proof
- Expert and quick deployment, to maximize the impact of investment and the benefits of the planned network
- Efficient operations, maintenance, monitoring and troubleshooting, to provide reliable and high-quality connectivity for the airport and its tenants
- Robust security, to protect the airport assets, employees and passengers
- Integration with existing wireless networks and legacy infrastructure, to preserve continuity of operations (e.g., with LMR) and benefit from network coexistence (e.g., with Wi-Fi)
- Flexible and agile management of third-party access, to extend the benefits of the

Innovative private 5G network brings digital transformation to Dallas Fort Worth International (DFW)

DFW is one of the largest US airports, covering 27 square miles, employing 55,000 workers, hosting 23 airlines, and serving more than 73 million passengers every year. Innovation is crucial to keep ahead of the competition, improve operational efficiency, support airlines and other partners, and improve the passenger experience.

The airport has established an innovation team tasked to identify what the airport needs, what technologies can meet these needs, and – perhaps most important – how to introduce digital transformation at the airport in practice. Who should the DFW work with? How should employees, airlines and tenants be involved to make its innovation strategy successful?

Paul Puopolo, Executive VP of Innovation at DFW, shares his experience on the DFW private 5G network POC and his plans for the commercial deployment to follow in a conversation that is part of this report.

These are the main highlights from our conversation with Paul:

- DFW conducted an extensive research project to identify service and operational needs, goals, technologies, and business models.
- The project results defined the scope of three POCs: ramp, cargo and terminal services.
- A CBRS private 5G network was selected because it gives DFW control over the network and the data, and it establishes a network that DFW can share with airlines and tenants.
- DFW worked with partners to deploy and operate the wireless infrastructure and services, but it closely monitored how the connectivity levels affected airport and airline services and staff operations.
- Coverage, throughput, latency and reliability improvements fundamentally improved the efficiency of services such as baggage handling.

network to airlines and other tenants
- Continuous innovation, to update and expand the network to improve performance on existing use cases and to support new ones

Most airports – large and small – do not have in-house staff resources to execute on all these dimensions. This is equally true of most enterprises: they are not connectivity experts, and they should not be required to have such expertise to use and benefit from new technologies such as 5G.

Airports have multiple options to get assistance as they deploy and operate their private 5G networks, which vary depending on how much work they want to do on their end, and how much control they want to have over the network. The more they do on their own, the more control they have of the network and the more in-house resources they need. They can also relinquish control and keep out of deploying a private network if they choose to use a mobile operator's public network. But even if the operator creates a virtual private network with network slicing, the airport has to share the network with other users and has limited, if any, control over the network.

Between these two borderline cases – complete control and no control over the wireless network – there is a growing set of options that allow airports – and more generally, enterprises – to retain control over the network without having to do all the work internally. This is nothing new: airports have been working with system integrators to deploy cellular, Wi-Fi, LMR and other wireless networks for a long time. They may continue to do so with private 5G networks, although they may select a specialist system integrator (e.g., different from the one they work with for Wi-Fi).

Airports can also move to new deployment and business models such as NaaS, where a new breed of managed service providers not only perform the system integration but also offer a turn-key, end-to-end solution. From a deployment perspective, with NaaS, the airport retains control of the network, but its level of direct involvement is lower. As a result, the airport needs to dedicate fewer resources to manage connectivity. Instead, it can direct the available resources to support the services that use the private 5G network's connectivity. From a business model perspective, NaaS supports (but doesn't require) contractual agreements that are shifted more towards opex than the ones with traditional system integrators. As the network becomes a service, the operating costs become primarily a service cost. Depending on the agreement, this may reduce the cost variability and risk, making the investment in the private 5G network easier to budget for.

The table below presents the advantages and disadvantages of some examples of deployment and business models. Many variations of these models are possible, and airports will negotiate an agreement specifically tailored to their requirements. For instance, a mobile operator may act as a NaaS or system integrator, or a system integrator may offer a NaaS solution. The models listed in the table present the differences across models and the tradeoffs that airports face as they choose the most appropriate model.

Does 5G interfere with air traffic in airports?

Ensuring air traffic safety is the highest priority for airports. Wireless networks – public or private – deployed within the airport grounds that interfere or negatively impact air traffic are not acceptable. Regulation and certification from the FCC, FAA, and other public agencies ensure safe wireless transmissions.

The dispute about the potential interference of 5G with altimeters used for aircraft landing illustrates how to promptly address safety concerns and how to safely manage the coexistence of 5G with other wireless devices.

Aircraft altimeters operate in the 4200-4400 MHz band and cellular midband networks operate in the 3200-4200 MHz range. The FAA concern is specifically over the 3700-3980 MHz range, a licensed band mostly allocated to mobile operators. It does not affect the CBRS band – the band that US airports have access to and typically use for private networks.

Altimeters and 5G bands do not overlap to avoid interference. In other countries, the coexistence of altimeters and 5G in the same bands is deemed safe by local transportation and communication regulators, airlines, and airports. As long as the equipment is certified and in good working conditions, 5G does not appear to cause harmful interference to the air traffic or, more generally, other airport operations.

The standoff between the FAA and airlines, worried about the safety risk, and the FCC and wireless operators, eager to deploy 5G networks, has been disruptive to all. To avoid similar issues in the future, all ecosystem partners must ensure that the infrastructure equipment and devices conform to regulation and operate correctly. Equally important, any potential source interference should be thoroughly assessed ahead of any deployment, and the necessary measures should be taken to ensure safety.

	Airport	Mobile operator	Neutral host	System integrator	NaaS
Network type	Private, airport owned	Public, shared access	Public, shared access	Private, airport owned	Private, airport owned
	The airport independently operates the network with its staff and resources	The operator gives access to its public network to the airport. The airport shares access with passengers and airport tenants	The neutral host operates a DAS that multiple mobile operators use. The airport can use the DAS through arrangements with operators	The system integrator assists the airport in building the network	The NaaS provider builds and operates the network on behalf of the airport. The airport pays for and owns the network
Spectrum	Unlicensed spectrum, shared spectrum (e.g., CBRS)	Licensed spectrum, but in most cases shared with public networks		Unlicensed spectrum, shared spectrum (e.g., CBRS)	
Control	The airport controls technology, coverage, performance, security, vendor selection, network evolution, and cost	The operator controls the network. The airport has some control if investing in the network	Operators control the network operations. The airport has some control if investing in the network	The airport controls technology, coverage, performance, security, vendor selection, network evolution, and cost	
Visibility	Full visibility into the network	No visibility into the public network. Airport may have visibility into its traffic and/or slice		Full visibility into the network	
Internal resources	High need of internal resources	Very limited		Limited internal resources needed	Minimal internal resources needed
Edge computing, isolation	Airport decides what to keep on-premises and how to integrate private 5G with other networks. Network traffic is isolated from the public network	Traffic is shared with the public network. Integration with airport wireless networks is difficult. Virtual isolation will be possible with network slicing in the future		Airport decides what to keep on-premises and how to integrate private 5G with other networks. Network traffic is isolated from the public network	
Partner access	Managed and owned by the airport	Managed by the mobile operator		Managed and owned by the airport	
Revenues	Airport gets revenues from airlines and other tenants	Mobile operator gets revenues from airlines and other tenants		Airport gets revenues from airlines and other tenants	

Takeaways

Airports need ubiquitous, reliable, low-latency, high-speed and secure connectivity to digitalize and automate their operations, support airlines and other partners, and provide a personalized passenger experience. They need to connect with everybody that works in airports, passengers, and an increasing number and variety of IoT devices.

Private 5G networks can deliver the connectivity that airports need to support many existing and new use cases, in the terminals, in the ramp, in the airfield, and in the cargo areas. Tracking assets and goods, biometrics, security and safety, baggage tracking, check-in, and boarding are the highest priority use cases.

Retaining control over the wireless infrastructure throughout its lifecycle, from planning and deployment, to operations and technology upgrades, is crucial for airports.

Private 5G networks give airports more control over the network architecture, coverage, performance, security and technology evolution than public 5G networks, which airports have to share with other users and which are deployed and managed by mobile operators.

With CBRS, Open RAN, network slicing, and edge computing, 5G supports an open, multi-vendor, standards-based, future-proof environment that gives airports flexibility and protection for their investment.

Private 5G networks will not replace Wi-Fi, and Wi-Fi is not an alternative to 5G. Airports need both technologies to support their use cases efficiently, with each technology playing a different connectivity role.

A private 5G network requires experience, expertise and resources that most airports do not have internally and do not want to acquire. Instead, a system integrator may deploy the network for the airport, or a NaaS service provider may deploy and operate the network on behalf of the airport.

A NaaS service provider offers an end-to-end solution that gives airport control and access to the private 5G network but does not require an active role of the airport in deploying and managing the network. With NaaS, airports do not have to deal with the complexity of 5G and can focus instead on its benefits.

Why do airports need private 5G networks?

A conversation between Johan Bjorklund, CEO, Betacom, and Monica Paolini, Principal, Senza Fili

Why do airports need private 5G networks?

A conversation between Johan Bjorklund, CEO, Betacom, and Monica Paolini, Principal, Senza Fili

Airports are on the brink of a transformation toward automation, increased operational efficiency, and more effective services for passengers and tenants, driven by the pressure for higher cost-efficiency, competitiveness, reliability and security. Private networks have a big role to play in this transformation.

In this conversation, I talked with Johan Bjorklund, CEO at Betacom, about how their 5G-as-a-Service (5GaaS) approach makes it possible for airports to deploy CBRS private networks without having to operate one on their own, yet retain full control.

Monica Paolini: Johan, Betacom has been in wireless for a long time. Can you tell us what is special about what you do?

Johan Bjorklund: Betacom has been around for 30 years, doing mostly large wireless construction projects. Today, we design, we build, and we operate wireless private wireless networks for airports and for other enterprises. We do everything in-house.

Our customers do not have to be experts at building or running wireless networks. They do not have to be experts in 4G or 5G. We are the experts, so they do not need to add one single headcount to get their own private wireless network working. We do everything from soup to nuts, and deliver a turnkey solution to our customers to make it very easy for them.

Monica: How does the recent work you are doing in airports fit Betacom's activities?

Johan: We have worked with many airports, and we have built the wireless infrastructure in several of them. In the last nine months, we have ventured into something we call 5G-as-a-Service (5GaaS), where we are offering enterprises, including airports, a wireless private network using CBRS spectrum. We are enabling airports to take advantage of 5G services – or 4G services, for that matter – using dedicated spectrum and a private network within their own firewalls.

Monica: What makes airports one of the best environments to prove the viability of wireless technologies?

Johan: Airports are like small cities – there are so many different applications within an airport. And those applications need a robust and secure network to run properly.

Today, most of them use Wi-Fi. And Wi-Fi comes with many challenges. There is often quite a bit of congestion in Wi-Fi networks. Sustainability can also be an issue – Wi-Fi was not built with sustainability in mind.

With private wireless, we can address many of these challenges and make business-critical airport applications run smoother.

Monica: From a technology point of view, airports are the perfect showcase environment because there you face most of the challenges you find in wireless deployments, and you need to support almost any use case you can think of.

At the same time, an airport may want to deploy one or more wireless networks, but they may not want to do it themselves. They may not have the capability in-house, and they may not want to hire people to run their networks. In fact, this could be a showstopper. So having someone who can do that for them can be crucially valuable to the airport, and also accelerate the adoption of private networks in airports.

We have recently seen a sudden growth in interest from airports to test and deploy private wireless networks. What is driving the change?

Johan: There are several reasons. One reason is that with COVID, everything went from being very, very busy to everything shutting down more or less

Watch the conversation

overnight. During this period, airports and airlines have restructured and, in some cases, have been forced to reduce personnel. Now that traveling has started to pick back up again, there are many areas that are understaffed. This creates a huge need for automation, for both above-wing services and below-wing services – for instance, for baggage and cargo handling and tracking, or for boarding services.

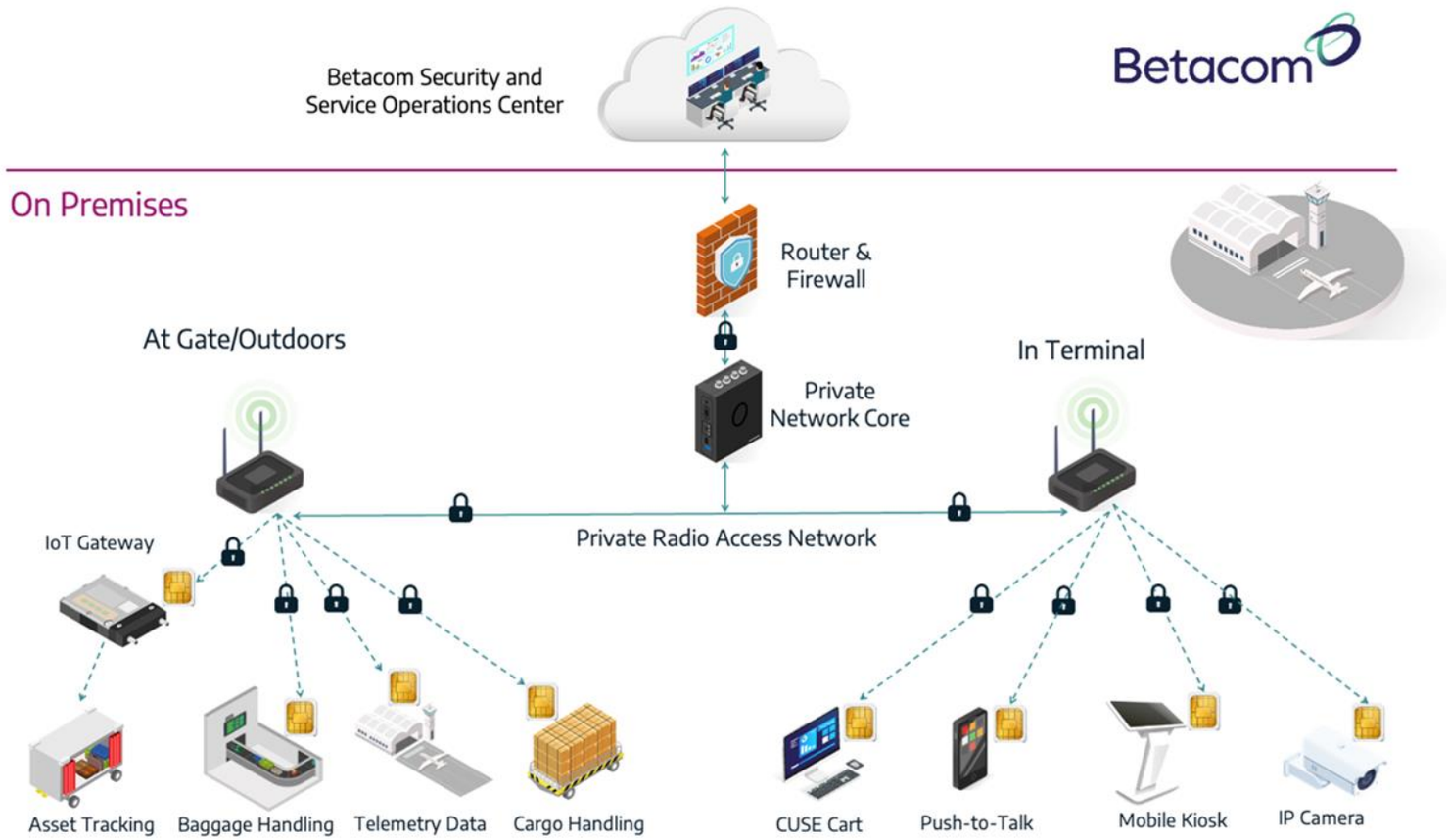
With the currently tight labor market, hiring new people and training them to take care of this onslaught of demand can be challenging. After the COVID shutdowns, there is a big need to effectively automate many processes. You need to connect everything wirelessly, and, to do so, you need a robust network.

One of the challenges we are seeing is that airports are struggling with the capacity limitations of Wi-Fi. I was at an airport a couple of weeks ago, and the Wi-Fi network was working just fine. But then a large aircraft came in from Japan. You could see almost everybody on that flight powering up their phones at the same time and logging into Wi-Fi. And the network went down.

The airport has business-critical applications that require reliable connectivity, and Wi-Fi is insufficient to provide that capacity for operations.

The ability to have separate networks where the airport can run these business-critical applications is something that has been getting more attention from airports, and the new challenges brought on by COVID have only escalated the need.

Monica: And when the passengers all get to check their phones after they land, it is also a peak time of activity for the airport. This is also the time when the luggage comes in. The increase in passenger traffic is correlated with an increase in airport activities.



Source: Betacom

But would not it be sufficient – as well as cheaper and less complex – to expand the Wi-Fi network, rather than building a private network using CBRS or licensed spectrum?

Johan: Upgrading the Wi-Fi network to meet all the airport requirements is not necessarily easy to do. You only have a few unlicensed spectrum bands that you can run Wi-Fi on. You can always add another Wi-Fi network, but eventually you run out of spectrum resources.

When you suddenly have all these passengers coming in and they are firing up their phones at the same time, they are all competing for the same spectrum, even though it may be over different Wi-Fi networks.

There are many challenges with optimizing Wi-Fi networks. And airports – especially large ones – are so dynamic because they have so many people coming and going for hours and hours each day.

Monica: To meet high traffic demand, airports need

more than a Wi-Fi network. But can they shoulder the costs of the initial deployment?

Johan: Private wireless networks, the way we are pricing them, are not much more expensive than Wi-Fi. And bear in mind that Betacom offers a turnkey service. The airport does not need to add any staff. It is pretty easy for the airport IT organization to add a private wireless network if they use Betacom's 5G-as-a-Service because we are doing everything end-to-end.

Monica: What, then, are the overall cost savings and revenue opportunities for an airport to deploy a wireless private network?

Johan: There are many cost savings and revenue opportunities. To give you a concrete example, biometric scanning systems for passenger boarding are becoming an increasing trend with COVID as airports pursue touchless technologies. In some Wi-Fi biometric scanning systems, the problem is that after about 16 or 17 scans, the scanner has taken up so many resources from Wi-Fi that it causes the Wi-Fi network to shut down. And the way the system is configured, the application has to restart, and that takes about 30 minutes. So if you can only scan 16 or 17 people to board an aircraft, and then you have to wait 30 minutes to restart the application to continue boarding, the value is completely lost. So you need to be able to fall back to the old system, and this means going back to having many gate agents again. In this situation, there are no cost savings.

If instead you have a private wireless network that works 100% of the time, or close to that, you do not need as many gate agents – maybe you need one instead of three – and you do not need to fall back to the old system when you use this reliably automated onboarding process.

In fact, the current situation may add costs. The airport may have this new, cutting-edge biometric scanning system, and it needs a new person at the gate to take care of the system and restart it all the time, as well. So the airport has to add a gate agent, and this is quite counterproductive.

In addition to cost savings, operational efficiency is a key business driver at airports. For instance, what matters is how fast you can run your processes – what is your turnaround time. When you have to manage planes at the gate, the cost savings go beyond reducing the number of agents at the gate.

Monica: In an airport, the value of getting things done on time is huge. If a plane departs late, there may be a domino effect on other flights as well.

What role does CBRS play in making a private network much easier and more compelling for an airport or other enterprises to have a private network? With CBRS, airports now have midband spectrum they can use without paying for a license or even applying for it.

Johan: The CBRS midband spectrum dedicated by the FCC in the 3.5 GHz band is ideal for airports. Opening up that spectrum allows enterprises such as airports to have their own networks without having to purchase licensed spectrum because it is public spectrum that is shared and managed to ensure that the airport is not going to have performance issues because they do not use licensed spectrum. And this allows airports and other enterprises to own their private wireless networks in a way they could not before.

Monica: With CBRS, airports have access to unlicensed, but protected spectrum. With Wi-Fi, anybody can plug in an AP – tenants, but also passengers. This is not something that can happen with CBRS, because you need to be granted use by a SAS.

Let's consider the use cases. It is not just the airport that can benefit from a wireless network: airlines and all the other tenants can benefit from it too. What do you hear from airports on CBRS?

Johan: Airports want to launch business-critical applications on CBRS spectrum on their own private wireless networks. By business critical, I mean applications that need to be up and running all the time, such as baggage tracking.

Airports need to track baggage all the way from when you check in your luggage to when it gets loaded onto the aircraft. But right now, a bag gets scanned when you check in and again when it gets on the aircraft, but it is not scanned from the time it leaves the belt to when it goes into the aircraft. And that is when there is a risk for luggage to get lost. There are IoT applications that can make that tracking continuous. And for that, you need a wireless network that is available without interruption as the bag moves from the belt to the ramp to the plane.

The ability to track baggage and cargo continuously is quite important for the airport and for the airlines. And to do so, you need those applications to be up and running all the time. If those applications have a lot of downtime, they are not going to be useful to you.

Automated boarding and credit card payments are other examples of applications that need to run continuously to be useful.

These are the operational applications that we see airports migrating to private wireless networks.

Monica: What do you recommend to airports that want to have a CBRS private network? Should they go for LTE or 5G?

Johan: It depends on the end-user devices. At this point in time, many devices are not available for 5G, so 4G may be the better option to start with, and then upgrade the network to 5G once the 5G ecosystem matures.

Really low latency is the biggest advantage of 5G. But LTE latency can be quite low, especially when you have everything, including your core, on-prem. So we do not see a latency issue for most of the applications that airports want to run.

However, once airports get used to the capabilities of 4G, there will be a lot of innovation, with more applications requiring 5G, both for speed and latency. And as that happens, there will be more and more demand for 5G.

And we see the ecosystem for devices catching up within the next year or so for 5G, and then we will see more 5G versus 4G CBRS networks.

Monica: And airports can gradually transition their CBRS networks from 4G to 5G when it is time. And that may take some time for devices not only to support 5G but also to reach 4G-level price points.

How can an airport get some revenues from giving access to its CBRS network – or to applications running on it – to airlines, retailers, or other tenants?

Johan: Airports have to be careful. They have to work closely with their biggest customers – the airlines. To support this, we get SIM cards for the airports, and they can distribute them to airlines and other tenants. So for airports, it is pretty easy to give them access to their own network.

At the end of the day, though, the network is owned by the airport, and the airport controls who gets on that network through the SIM cards. Because the applications run on its network, it has better control of the performance of applications.

Monica: You mentioned the work you are doing with major US airports. What are some of the new applications and use cases you are deploying for the private networks with airports and airlines?

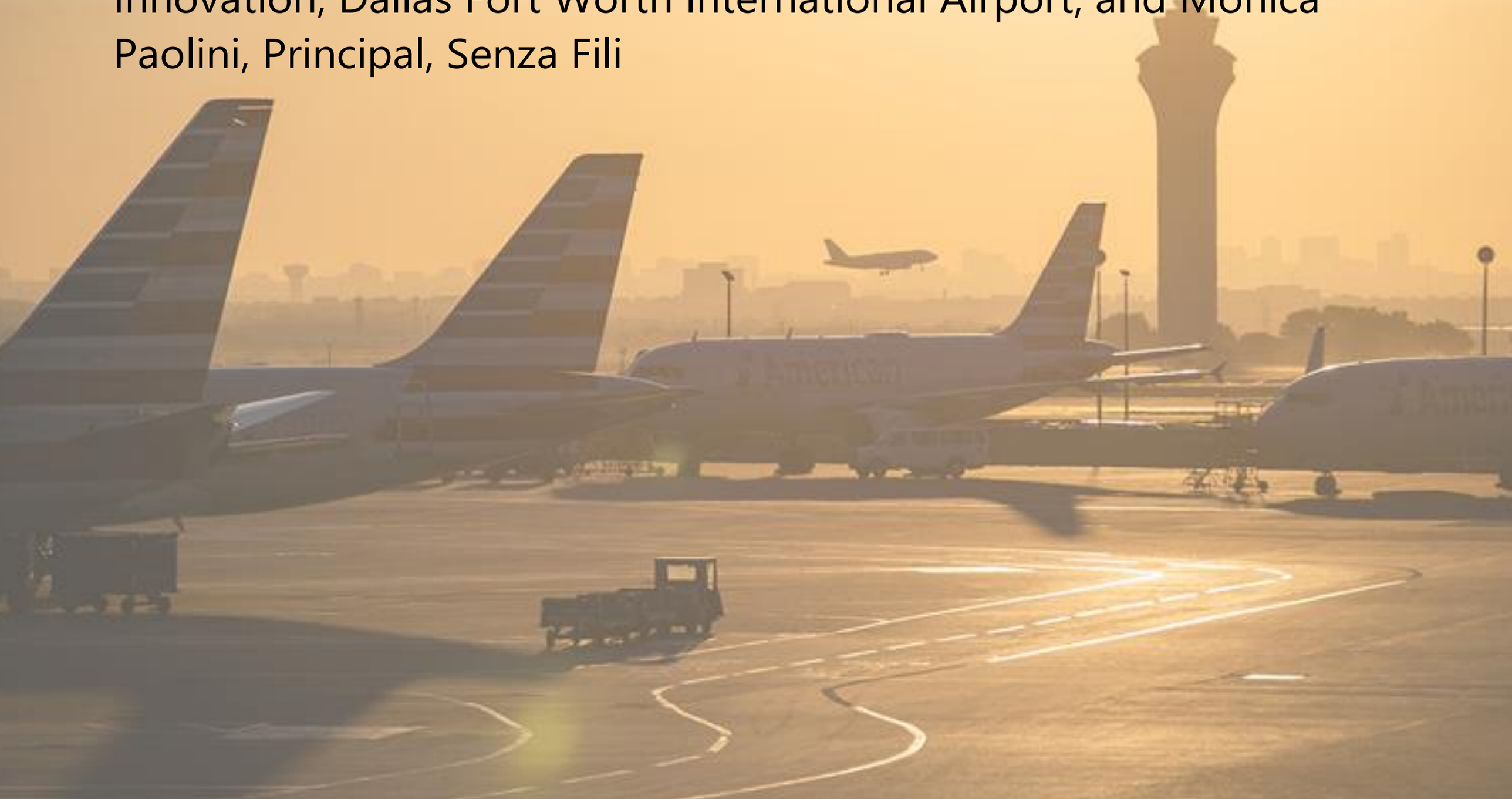
Johan: We are working with several airports and airlines across the country right now, with a focus on improving efficiencies for baggage and cargo handling, and for airplane maintenance.

Terminal gates are sometimes owned by the airlines and sometimes owned by the airport. That poses a potential problem because the responsibility of airlines and airports can differ from airport to airport. This is why we are working closely with both the airlines and the airports to roll out our solution and to evaluate the technology and the applications they would like to put on to the private wireless network.

So far, it is looking very promising. There is much interest out there, and we are keeping extremely busy. We would like to thank these airport leaders for pioneering private wireless technology and paving the way for other airports to innovate in this space.

DFW: The airport of the future, enabled by a private 5G network

A conversation between Paul Puopolo, Executive VP of Innovation, Dallas Fort Worth International Airport, and Monica Paolini, Principal, Senza Fili



DFW: The airport of the future, enabled by a private 5G network

A conversation between Paul Puopolo, Executive VP of Innovation, Dallas Fort Worth International Airport, and Monica Paolini, Principal, Senza Fili

Innovation is crucial for airports to improve their operations and to meet the needs and expectations of passengers, partners and tenants. Innovation also requires a lot of work, a supportive partner ecosystem, and the adoption of new technologies.

In this conversation with Paul Puopolo, Executive VP of Innovation, Dallas Fort Worth International (DFW) Airport, we talked about the vision and the plans for the digital transformation at DFW using 5G private networks to connect everybody and everything within the 27 square-mile footprint of the airport. We also talked about the hard work, lessons learned, and results achieved during the initial proof of concept (POC).

Monica: Paul, it is great to hear about your work at DFW to improve wireless connectivity. Can you give us an introduction about your role and the team you are heading at DFW to start?

Paul: I am the Executive Vice President of Innovation at DFW, and I have been here for three years. I lead an innovation program where our responsibility is to design new services, solutions and products, to operationalize them, and to build a culture of innovation for the airport.

We also spend a lot of time assessing new technologies. And that is why we got into 5G and private networks.

Monica: As I was preparing for this interview, I learned that 55,000 people work at DFW. I know the airport pretty well, but I would have never thought there were so many people, and all of them need connectivity. And this does not even include all the things you have in the airport that need to be connected – it is not just planes. So getting connectivity to all of these people and things is not a trivial task. And managing this connectivity requires a transformation that is not trivial either.

This does not consider the connectivity needs of the passengers – and there are many of them going through DFW daily.

Paul: You are right, and we are quite large. We have five terminals, and the airport itself is 27 square miles. There are a lot of people, a lot of partners, a lot of tenants, a lot of passengers that use and need connectivity.

Monica: What is your vision for innovation in wireless connectivity in an airport setting?

Paul: My vision is to build an integrated innovation program. And that means that we need to have a clear strategy, a clear process, a clear focus on what we are doing for the airport, as well as building a culture of innovation across all the airport divisions.

Technology is moving too fast. Companies or organizations that do not spend the time or the effort to put resources into the future will find themselves less competitive. Innovation is hard to do because the operational challenges of today always get in the way of tomorrow's opportunities. So it is easy for us to kick the can down the road. But when that happens, you end

Watch the conversation

up missing a competitive advantage, or you end up missing being a leader in your industry.

An organization that does not spend time thinking about innovation or figuring out what the company's role is 3-5 years down the road could find itself to be irrelevant.

5G private networks are an emerging technology. We are working very closely with our IT group to figure out how this new technology applies to what we do. That is the role of rapid learning in our innovation program. And that is why we ended up with this project in our portfolio.

Monica: How will 5G help you realize this vision?

Paul: The airport of the future is going to be highly connected. And that means it is going to need a very flexible network strategy, one that meets the needs of our business partners and the expectations of the traveler.

From an efficiency standpoint, we know that IoT is going to grow. We know that autonomous vehicles will be a future mode of transportation, and we know that robotics, AR and VR are going to take a more active role in the future. Automation will be used below the wing and above the wing and in the terminals and to move packages around for our cargo business or people through the airport. These new technologies require better connectivity – and this means more bandwidth, lower latency, and appropriate security.

This is why we started to look at what private 5G networks can do for the airport. 5G provides the level of flexibility and customization we need. It opens opportunities that the airport would not have had in the past because the technology was not available.

Source: DFW

We are trying to get better coverage and better control over the infrastructure and how the network operates. We are also looking at lower costs and higher efficiency.

Monica: Can you give examples of things that do not work quite well or areas where you see scope for improvement?

Paul: Every airport is different. But we have horseshoe-type terminals, and we have five of those. We have large, concrete support structures. Connectivity on the ramp can be challenging for our partner airlines, particularly when they move between inside and outside.

We want to make sure we can manage and provide continuous connectivity, for example, for bags moving from outside to inside. We want workers on the ramp to stay connected. Autonomous ground-support equipment that goes in and out of tunnels and around terminals between gates cannot lose connectivity.

Monica: How urgent is the need to change? And what happens if you do not change? What are the risks?

Paul: The first downside is that we would not meet our partners' expectations, whether it is a concessionaire or an airline, to provide the right amount of connectivity so that they can support their business.

The second downside is that if passengers do not have the right connectivity, this can reduce customer satisfaction.

Travelers expect things to happen immediately, just like we all do. When we buy things or interact online, we expect things to happen fast, and we do not like to wait. Passengers have this expectation too, and we need to provide the right level of connectivity and latency in the terminal.

Monica: Once you have all the connectivity you need, what does the airport of the future look like?

Paul: When I say future, I am not being a futurist – I think about the next three to five years. Much of the work that we are doing with biometrics and digital ID, for example, will require a network. Sensors tracking passenger flow and trying to understand the movement of people and things through the airport require a certain amount of connectivity. Again, autonomous vehicles, whether they are ours or somebody else's, will need low latency and reliable connectivity.

That is where we see mobility going. That is where we see technology going.

The pace of technology will not get any slower than it is today. During the pandemic, we have seen how digital transformation has accelerated.

To support all that technology requires a very flexible network strategy. And that is what we are working on at DFW Airport with our IT group.

Monica: Technology is an essential ingredient, but you also need to embed it into your ecosystem – employees, tenants, airlines, passengers. How are you going to do this?

Paul: It is a journey, and we are all trying to understand emerging technologies. People might say 5G is not that new. Well, it is new when you are trying to implement an unfamiliar technology or a different network model.

It all works well when you have good partners – whether it is a partner who is going to help you roll out the technology, or who is going to work with you on a POC.

Monica: How is this working out in your private network POC?

Paul: We are partnering with American Airlines. And it is great that they are working together with us to understand how this POC should work. We have to understand the technology. We have to make sure that whatever we put in will work for us in our environment.

Putting a 5G network in a building is one thing, but putting it in five terminals and across 27 square miles is a big decision.

We want to make sure we understand the technology – we want to understand the good and the bad. We want to make sure we design it the right way for our environment – in a way that works for us. We are not the experts, so having technology partners helps us understand how to leverage the technology.

In the airport, we are asking people to disrupt their operational environment to test something. That requires a lot of good collaboration and a lot of good discussions. And you have to have an innovation mindset to get that done. That is our approach. And I think we have been pretty successful at it with the POCs we are doing right now.

Monica: Before we dive into the POC, let me ask you about security and privacy. When you start tracking people, things or events, questions about privacy and security arise. How do you address them?

Paul: 5G is more secure than other wireless technologies. So if you are going to pay for something with our concessionaires, 5G will provide the level of security required for that transaction.

From the airport's standpoint, we do not hold or capture any personal information. But we want to facilitate the exchange of information between, let's say, the airline and the passenger, or the passenger and the concession. We believe that is our role. And providing a secure environment to have that happen is essential.

The decision to share that information is up to the passenger. The network has to be secure so that we can protect the flow of information.

As far as the operational environment goes, the airport would not necessarily have access to information that belongs to partners and tenants. But we need to make sure we provide a secure network for our airline partners, for instance, to transfer information to and from their devices to support their operations and their customers.

Monica: You mentioned that the POC is key to understanding the technology before rolling out a network covering the entire airport. You want to make sure that the network will work for you. How is the POC helping you get the information you need?

Paul: We are doing three POCs that include ramp, cargo and airline in-terminal applications. The first

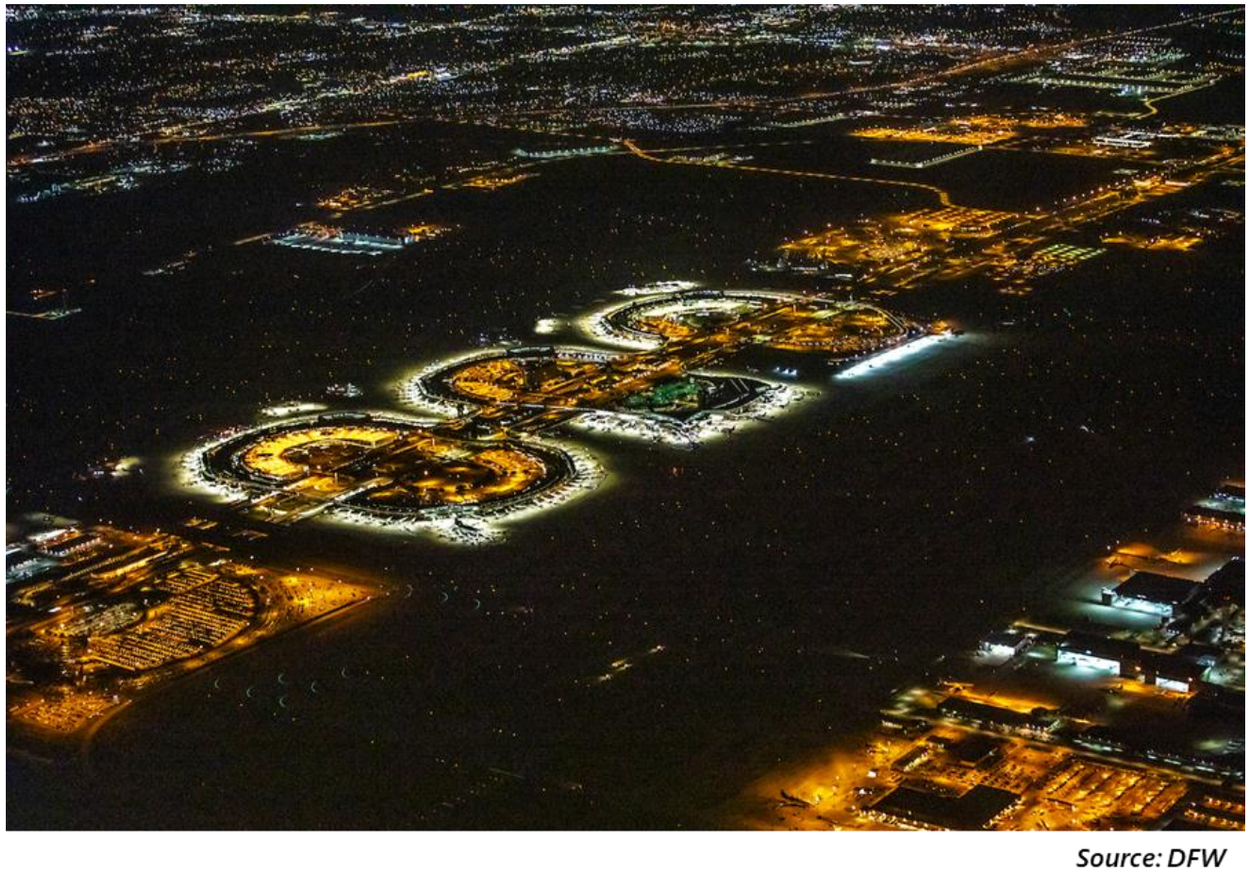
two are ongoing, and the third one is still in the planning stage.

For the first POC, we put 5G at one ramp location. We are working with American Airlines to test out the connectivity for bag handling – tracking bags as they move from the plane underneath the structure and into the baggage system – and the effectiveness of American Airlines' devices. One of the challenges we face as you move around the ramp is the loss of connectivity because of the physical infrastructure. But the beauty of 5G is that it provides low latency and great coverage. We see coverage across seven gates, with one access point – which is great.

And we are learning. For instance, how many of these access points do we need per gate? Because again, in our horseshoe environment, we need to think through how much hardware will be required. We are also learning a lot about whether the network we plan to build will meet the needs of American Airlines – will it do what they want it to do?

We are also learning how to install a network. A POC is different than an operational rollout. Some of the things we are putting in place for the POC may be temporary. We are putting in hardware to test something, and it may or may not stay after the POC is over. During these six months when the POC is running, we are learning how much we need to do, whether we have the right hardware to cover the right areas, and whether our users and clients are getting what they need.

Once we get all that done, we will know how to multiply this approach across 35 gates per terminal. That is a big decision, and this is why it is so important for us to understand the requirements, the implementation issues, and the implementation costs. Will the network do what we said it was going to do? This is a big investment for us to move forward.



Source: DFW

Monica: It is a big investment and a big change in how you and your partners will be using wireless connectivity in your operations with a private network.

Paul: It is a major change. Managing a private network is completely different from what we have done before. 5G is positioning us to do things we normally would not have done in the past. We will be working with partners we have never worked with before because the technology is different. And those partners are helping us understand what we can and cannot do, and what their expertise is. New business models are created from a new approach that we hope will be more cost-effective for us in the long run.

Monica: Other than being cost-effective, what are the other benefits of a private network? Why do you think you need a private network?

Paul: A private network gives us more control over connectivity. Having control over the network alleviates the bandwidth challenges we have had in the past.

And it gives us more flexibility to have different types of connectivity for the airport. Just because we have a private network does not mean we are giving up on other connectivity strategies. It is

just one element of our overall connectivity strategy.

The private network can do a lot for our partners. And having access to licensed and unlicensed spectrum that we normally would not have had before is a great benefit.

Now we can work with somebody to help us slice that network. We could not slice networks before. We are moving away from a one-size-fits-all approach to making sure we provide the right connectivity and the right latency to support use cases that a business partner or passengers may have. We never had that flexibility.

This is why I go back to flexibility and control. This is why we are exploring private networks: 5G allows us to have the flexibility and control we need.

Monica: With network slicing, not only do you control the network, but you also control the network in a much more granular way than you could have done a few years ago.

Paul: Correct, and that is exciting for us. But again, this is going to require many partners, many discussions.

Monica: How will your private network coexist with your existing Wi-Fi network? Will you still use it?

Paul: Yes, we will still have our public Wi-Fi network already available to the public. The private network will augment our public Wi-Fi network.

Today, everybody is using the same network. And with a private network, we will be able to separate users and traffic among networks. This means that the public will have more bandwidth, and that will help us on public Wi-Fi. And we will be able to push more of the operational traffic to the private network.

Monica: What do you plan to do once you complete the POC?

Paul: These three POCs will help us understand what we need. We will run these POCs for about another four months to make sure we get good data. After that, we have to put a business case together that recommends how we want to roll this out.

At the same time, we have to make sure that our airline partners and our tenants are interested and have access to the network. We also need our partners to help us execute it, and this all has to come together in a business case.

So that is the plan. And we are committed to doing it. We know that IoT will only get bigger, and we know autonomous vehicles are coming within the next three years. We need a phased approach to implement a comprehensive private network across our entire ecosystem.

Monica: And you will need both indoor and outdoor coverage, right?

Paul: Correct. And that is part of the discussion we need to have. What makes sense now? What makes sense next year? What makes sense the year after? This will depend on the results and learnings from the POCs.

Monica: The POC is still ongoing, so you will keep learning more from it. But to date, is there something that you learned that you did not expect and that surprised you?

Paul: On the tactical level, it was the coverage and the quality of that coverage. I was not expecting that with a single access point we could cover seven to nine gates. And the people who did the implementation made this possible.

I am also learning, though, that, on the other side, it is tough to implement in an operational environment, particularly when you introduce a new network. So the POC itself is teaching us how to get better at moving quickly to do a test and not overthink things. But there are rules and regulations we have to follow. So testing something in an operational environment has been eye-opening, particularly for the implementation team.

Monica: How do you see this changing your relationship with the ecosystem – employees, tenants, airlines, contractors?

Paul: As with any new technology, relationships are going to change. No matter what technology we put in place, it enables the roles to change and allows people to do things they would not have done in the past. That is why the discussions we are having are good.

It is a big change for us as an airport to manage our network. While we may manage it through partners, we will be taking a more active role in our ecosystem than in the past. Both technology and customer expectations are forcing us to do that. And that makes it a fun and challenging space to be in.

Glossary

AI Artificial intelligence

AR Augmented reality

CBRS Citizens Broadband Radio Service

DAS Distributed antenna system

FAA Federal Aviation Administration

FCC Federal Communications Commission

IoT Internet of things

LMR Land Mobile Radio

ML Machine learning

NaaS Network as a service

NR New radio

PMR Professional mobile radio

POC Proof of concept

POS Point of sale

QoS Quality of service

RAN Radio access network

ROI Return on investment

SLA Service-level agreement

TSA Transportation Security Administration

URLLC Ultra-Reliable Low Latency Communications

VR Virtual reality

XR Extended reality

About Betacom

Betacom offers the first fully managed private 5G network, building on its long history as a wireless infrastructure provider to AT&T, T-Mobile, and Verizon. Founded in 1991 and headquartered in Bellevue, Washington, the company has regional offices throughout the country. Having completed more than 800 large-scale design and deployment projects, Betacom inspires confidence among their customers who have worked closely with them to meet their pressing high-performance connectivity needs. Its private 5G wireless service is the first managed service of its kind in the United States. For more information, visit http://www.betacom.com.

About Johan Bjorklund

Johan Bjorklund is the CEO of Betacom. Johan is a senior executive leader who combines rich telecommunications industry experience with a strategic and operational focus on building and growing businesses. Having previously held a number of leadership roles in his 18 years at Ericsson, Johan has gained broad international market expertise leading business success in the US, APAC, and EMEA with a record of creating profitable business models in emerging business segments. His broad functional background includes executive P&L management, business development, mergers and acquisitions, strategic partnerships, customer service, vendor management, and integration and business optimizations.

.

About DFW

Dallas Fort Worth International (DFW) Airport is the most connected airport in the world. Centered between owner cities Dallas and Fort Worth, Texas, DFW Airport also serves as a major job generator for the North Texas region by connecting people through business and leisure travel. For more information, visit the DFW website or download the DFW Mobile App for iOS and Android devices. Follow @dfwairport on Facebook, Twitter, Instagram, and LinkedIn.

About Paul Puopolo

Paul Puopolo serves as Executive Vice President of Innovation at Dallas/Fort Worth International Airport. He leads DFW's Innovation function to identify, assess, and drive the collaborative development of new solutions and business models to create new growth and competitive advantage. Mr. Puopolo joined the DFW staff in August 2018. Mr. Puopolo is an experienced "intrapreneur" with multi-industry innovation, emerging technology, and direct to consumer background. Throughout his career, he has built and led corporate innovation teams within large, complex organizations. Prior to DFW, he served as the VP of Innovation at MetLife Inc., VP of Business Innovation & Development at Highmark Inc., and Director of Consumer Innovation at Humana Inc.. In these roles, he was accountable for developing business innovation strategies and portfolios and their strategic implementation to increase profitable growth, improve the consumer experience, and champion an innovative culture. Mr. Puopolo served as an active-duty officer and pilot in the U.S. Navy (retiring after 22 years of service) and holds a Bachelor of Science in Comprehensive Science from Villanova University and a Masters degree in National Security Affairs from the Naval Postgraduate School.

About Senza Fili

Senza Fili provides advisory support on wireless technologies and services. At Senza Fili, we have in-depth expertise in financial modeling, market forecasts and research, strategy, business plan support, and due diligence. Our client base is international and spans the entire value chain: clients include wireline, fixed wireless, and mobile operators, enterprises and other vertical players, vendors, system integrators, investors, regulators, and industry associations. We provide a bridge between technologies and services, helping our clients assess established and emerging technologies, use these technologies to support new or existing services, and build solid, profitable business models. Independent advice, a strong quantitative orientation, and an international perspective are the hallmarks of our work. For additional information, visit www.senzafili.com.

About Monica Paolini

Monica Paolini, PhD, founded Senza Fili in 2003. She is an expert in wireless technologies, and has helped clients worldwide to understand technology and customer requirements, evaluate business plan opportunities, market their services and products, and estimate the market size and revenue opportunity of new and established wireless technologies. She frequently gives presentations at conferences, and she has written many reports and articles on wireless technologies and services. She has a PhD in cognitive science from the University of California, San Diego (US), an MBA from the University of Oxford (UK), and a BA/MA in philosophy from the University of Bologna (Italy). You can contact Monica at monica.paolini@senzafili.com.