Case Study

Metropolitan Airports Commission

Minneapolis · Saint Paul
INTERNATIONAL AIRPORT
msp

Private Wireless Network Proof of Concept

Prepared For:

Metropolitan Airports Commission
Eduardo Valencia / Glenn Hutt
August 1, 2022

Table of Contents

Table of Figures

Executive Summary

After years of work to develop an innovative new spectrum model, the Federal Communications Commission (FCC) authorized 150 MHz of mid-band wireless spectrum for commercial use in January of 2020. Known as the Citizens Band Radio Service (CBRS), the “innovation band” ushered in a new era of enterprise connectivity. The adoption of LTE and 5G mobile platforms using this newly licensed spectrum enables enterprises to deploy Private Wireless Networks (PWNs) that provide the flexibility and simplicity of Wi-Fi-like operations with the quality of service and predictable performance of wired networks.

As a leader in the aviation industry, the Metropolitan Airports Commission (MAC) commissioned a PWN Proof of Concept (PoC) at Minneapolis-Saint Paul Airport (MSP) to investigate several aviation operations use cases. The use cases range from general-purpose mobile device data connectivity to high definition moving maps for workforce automation, to industrial Internet of Things (IoT) for infrastructure monitoring and maintenance. Requirements varied from low bit rate (e.g. sensors), to high throughput (video surveillance, HD mapping), to ultra-reliable performance for mission-critical applications (e.g. infrastructure IoT), to highly secure operations (e.g. gate agent passenger processing).

In each case, the CTS PWN PoC met or exceeded the performance of current networking technologies while also identifying opportunities to increase operational flexibility, reduce time to deploy/relocate services and applications, and decrease operational costs.

Background

As an innovator in the aviation industry, the MAC commissioned a PoC study to validate the functionality of certain airport operational use cases over a Private Wireless Network. MAC is a public corporation established by the Minnesota State Legislature to provide aviation services to the Twin Cities metropolitan area. MAC manages the operation of MSP and six smaller airports in the area. The PWN PoC study was performed in laboratory and production environments at MSP.

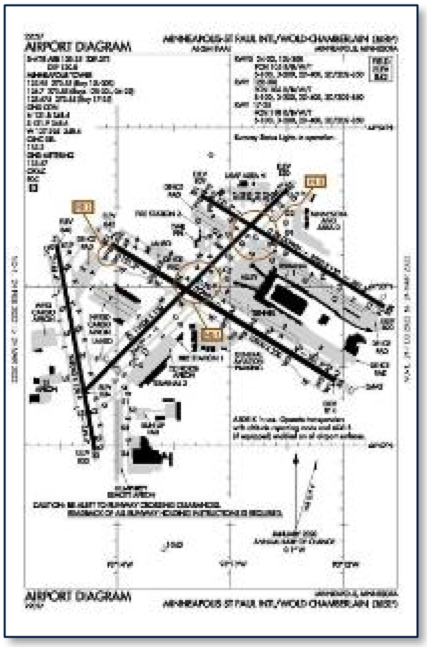
AIRPORT DIAGRAM
MINNEAPOLIS-ST PAUL INTL/WOLD-CHAMBERLAIN (MSP)
AIRPORT DIAGRAM
MINNEAPOLIS-ST PAUL INTL/WOLD-CHAMBERLAIN (MSP)

Figure 1 Diagram of MSP Airport (Federal Aviation Administration)

MSP is a joint civilian-military public use airport surrounded by the twin cities of Minneapolis and St. Paul as well as the suburbs encompassing Bloomington, Eagan, Mendota Heights and Richfield, Minnesota. MSP is home to Sun Country Airlines, a major hub for Delta Airlines, and a Joint Air Reserve Station serving the Air Force Reserve Command and Air National Guard. MSP also handles cargo for FedEx, UPS DHL and Amazon; MSP was named Amazon's fastest growing air cargo operator in 2021. MSP is the 17th busiest airport in the United States in terms of passenger traffic with over 25.2M travelers served in 2021. In addition, MSP ranks 12th for aircraft operations serving 303,850 passenger and cargo flights in 2021.

MSP covers 3,400 acres and supports more than 86,000 jobs in the region. The airport features two terminals with 131 gates serving flights to 163 markets, 136 domestic and 27 international destinations. MSP has four runways that serve both commercial and military traffic. MSP uses a variety of networking technologies for onsite voice and data communications for operations and guest services including cellular (macro and Distributed Antenna System (DAS)), Wi-Fi, 900 MHz unlicensed and wired Ethernet.

The MAC is a recognized leader in the aviation operations industry as evidenced by MSP being named the top North American airport for efficiency excellence in its size category by the Air Transportation Research Society from 2016 through 2019 and then again in 2021. MAC is constantly on the lookout for new technologies that can further improve airport operations and the customer experience to extend its leadership position in the industry. PWNs are an emerging technology that enterprises can use to improve airport efficiency and the overall passenger experience while reducing operational costs.

Throughout MSP and its six-reliever airports, the MAC finds opportunities in technology and sustainability to provide innovative solutions and improve the customer experience.

Use Cases

CTS tested and verified six discreet use cases during the lab trial to assess the Private Wireless Network's coverage and performance, and to assess the co-existence of the PWN with the other existing wireless networks in the MSP airport facility. The use cases were:

1. Federal Aviation Administration (FAA) Part 139 Airside Maintenance Tracking
2. Common Use System Equipment (CUSE) carts
3. Digital signage
4. Video surveillance
5. Infrastructure monitoring
6. Mobile application usage

FAA Part 139 Airside Maintenance Tracking

Cityworks is a cloud-hosted Global Information Services (GIS) application used for asset and work order management, and for maintenance scheduling and tracking on the airport grounds and runways. The primary Cityworks functions used by MSP include:

- Airfield management system
- Logging
- Inspections
- Site maintenance
- Moving map function

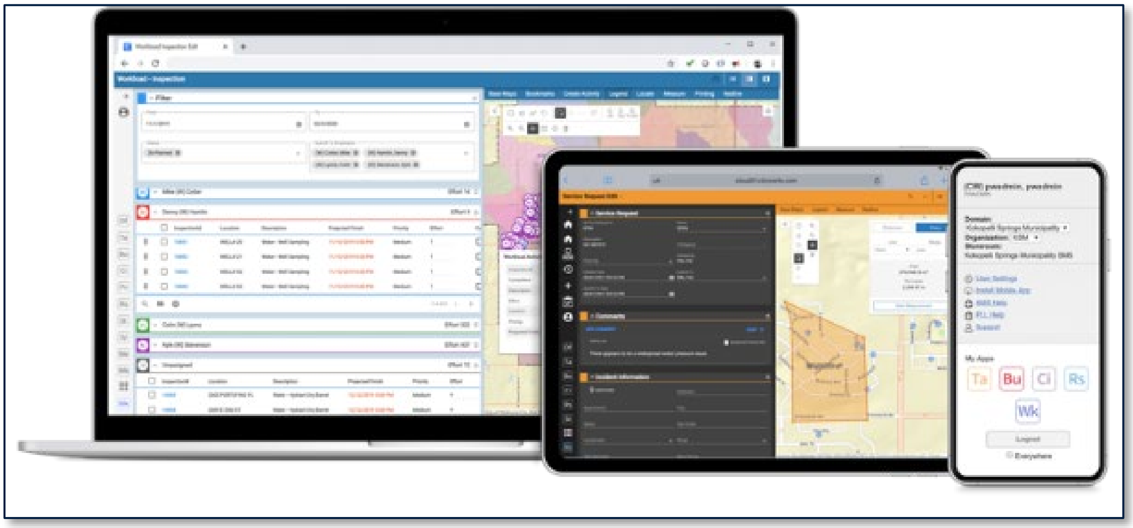

Figure 2 Cityworks application (Source: Trimble)

Cityworks functions as both a web application and through a suite of mobile applications available on iOS and Android tablets and smartphones. Cityworks incorporates HD-quality visuals as an optional feature through a partnership with Nearmap. MSP also enriches the experience with their own-hosted high-resolution aerial imagery.

Common Use System Equipment Carts

MSP employs Common Use System Equipment (CUSE) carts inside the airport for shared use by airlines operating within the facility. The CUSE platform enables multiple airlines to leverage the same hardware platform at a gate or in the airport while still using their own independent systems for administration. Each MSP CUSE cart consists of a multiuser Microsoft Windows-based PC, keyboard, monitor, mouse, ticket printer and desktop printer mounted on mobile pedestal carts.

Digital Signage

Digital signage from the attached Windows 10 workstation is used throughout the airport to display content for various purposes including wayfinding, flight and entertainment information, and advertising.

Video Surveillance

MSP employs an Integrated Video and Information Systems Network (iVISN) that connects video feeds from approximately 4,000 video surveillance cameras distributed throughput the indoor and outdoor footprint with MSPs Security and Access Control System. The primary camera utilized by MSP is the Panasonic WV-S4550L, a 5 Megapixel IP video camera. The video cameras are currently multicasting a 450Kbps video stream at 640x480 resolution via a wired LAN connection to the iVISN.

Infrastructure Monitoring

As part of MAC's Energy Conservation program, MSP uses an Intelligent Monitoring and Control System (IMACS) that connects all the energy-related systems and equipment at the airport using controllers from Honeywell and Siemens. The controllers communicate with sensors for each energy system using a variety of legacy machine protocols (e.g. SCADA, MODBUS) over a wired network. The sensors collect monitoring data which is transmitted to the IMACS and controllers for management and operation of various systems including heating, ventilation and air conditioning (HVAC) systems; power quality meters; escalators; elevators; moving walkways; baggage carousels; airfield sensors; and retention ponds located on the perimeter of the airfield.

Laptops and Smartphones

MAC employees also use corporate-issued Apple iPhones from Verizon as well as both Apple and Android mobile devices authorized under MAC's Bring Your Own Device (BYOD) to access IT services including Microsoft Teams and Microsoft Office 365. In the future, employees may also access mobile application variants of the use cases above (e.g. Cityworks). The airport is also exploring using tablets to access operations applications including Cityworks.

Network Overview

What is a Private Wireless Network?

The wireless industry is beginning a transformation as important and wide reaching as the introduction of Wi- Fi was two decades ago. Using recently released FCC CBRS spectrum, individual organizations can create their own Private Wireless Networks, taking advantage of the reliability, quality of service and security of 4G/LTE and 5G cellular networks.

Unlike Wi-Fi, which uses unlicensed spectrum, PWNs use FCC-licensed spectrum to deliver a network with high availability, reliability, QoS and true mobility that delivers where Wi-Fi falls short. However, planning, deploying and operating private wireless networks is far more complex than Wi-Fi. Specialized software tools and certified professionals are required to design and install the network for optimum operations. Network radios connect to an evolved packet core or 5G core to control the network. Mobile Network Operator (MNO) level of expertise is required to manage both the core and radio access networks to deliver peak application performance. So, while the advantages of private LTE and 5G are many, so are the number of deployment and operational challenges for those lacking expertise in mobile network management.

A Private Wireless Network, shown in Figure 5 below, consists of three primary components:

1. Radio Access Network: The Radio Access Network (RAN) is the physical infrastructure that enables connectivity to the end user applications using low-cost CBRS spectrum allocated by a Spectrum Access Service (SAS) approved by the FCC. Specifically, it includes Citizens Band Service Devices (CBSDs) that are the active radios used for data transmission connected by cabling, switches and routers.
2. Mobile Network Core: The mobile core is the intelligence that powers the RAN; it is responsible for subscriber management, authentication, and policy management to enable optimized performance for each individual application. The mobile core can be deployed onsite (on an edge compute node), in the cloud, or in a hybrid model that keeps the user data onsite while realizing some scale efficiencies of processing the control plane in the cloud.
3. User Equipment: The User Equipment (UE) are the devices the connect the application to the RAN. UEs include smartphones, tablets, mobile routers and other devices with embedded LTE chipsets that access the CBRS band.

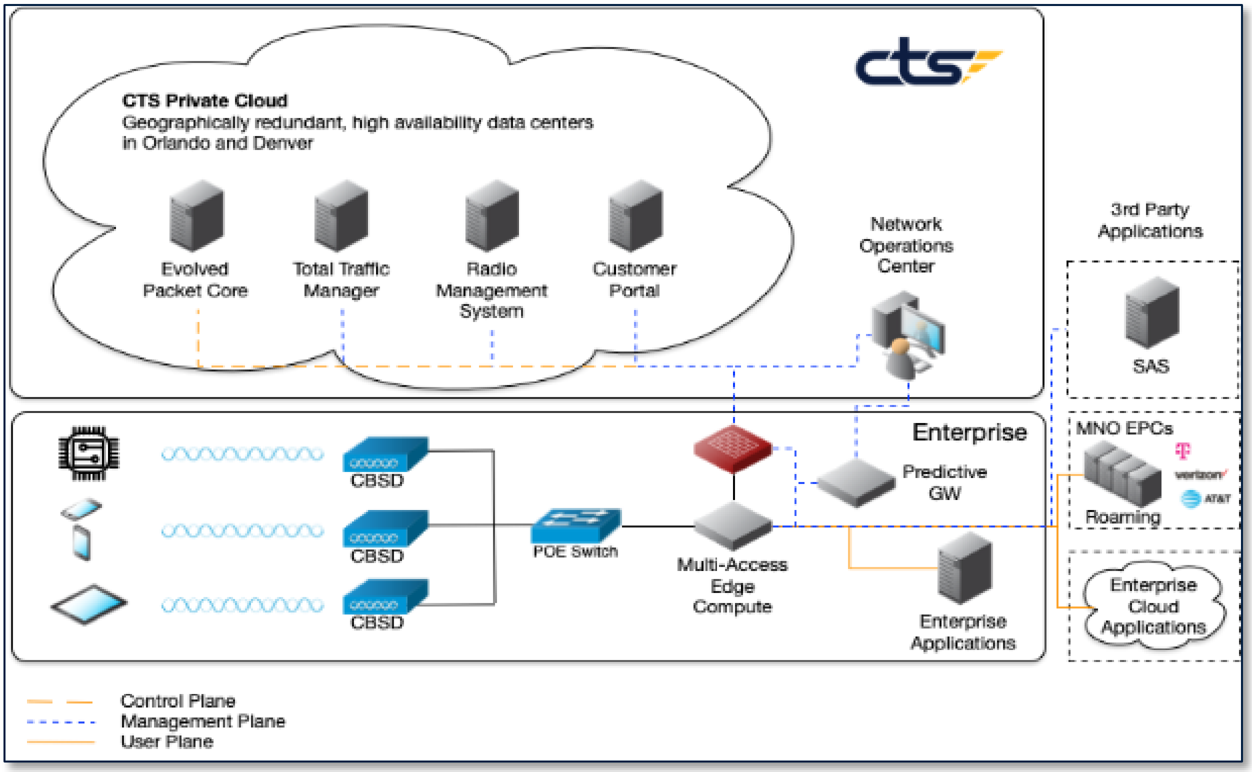

Figure 3 Private Wireless Network architecture

MSP Private Wireless Network Overview

A PWN using 4G Long Term Evolution (LTE) cellular technology was installed at MSP as a test bed for validating the performance of a variety of operational use cases. The network included the following components, depicted in Figure 6 below:

- RAN featuring (3) Nokia Flexi Zone Multiband Indoor Pico BTS (MBI) CBSDs and (1) Nokia Flexi Zone Multiband Outdoor Micro BTS (MBO) CBSD;
- An on-site edge compute node with a CTS Evolved Packet Core (EPC) for subscriber management, authentication, and basic policy management;
- The CTS Total Traffic Manager (TTM) managed service, with a data collection agent that resides on the MEC and operates out of the CTS private cloud. TTM provides detailed network traffic analytics and advanced policy management;
- The Spectrum Access Service (SAS) from Google for CBRS frequency licensing;
- Remote monitoring and maintenance from the CTS Network Operations Center (NOC) in Greenville, SC; and,
- A firewall appliance for external system access to the network including the CTS NOC, Spectrum Access Service (SAS), customer applications and public internet access.

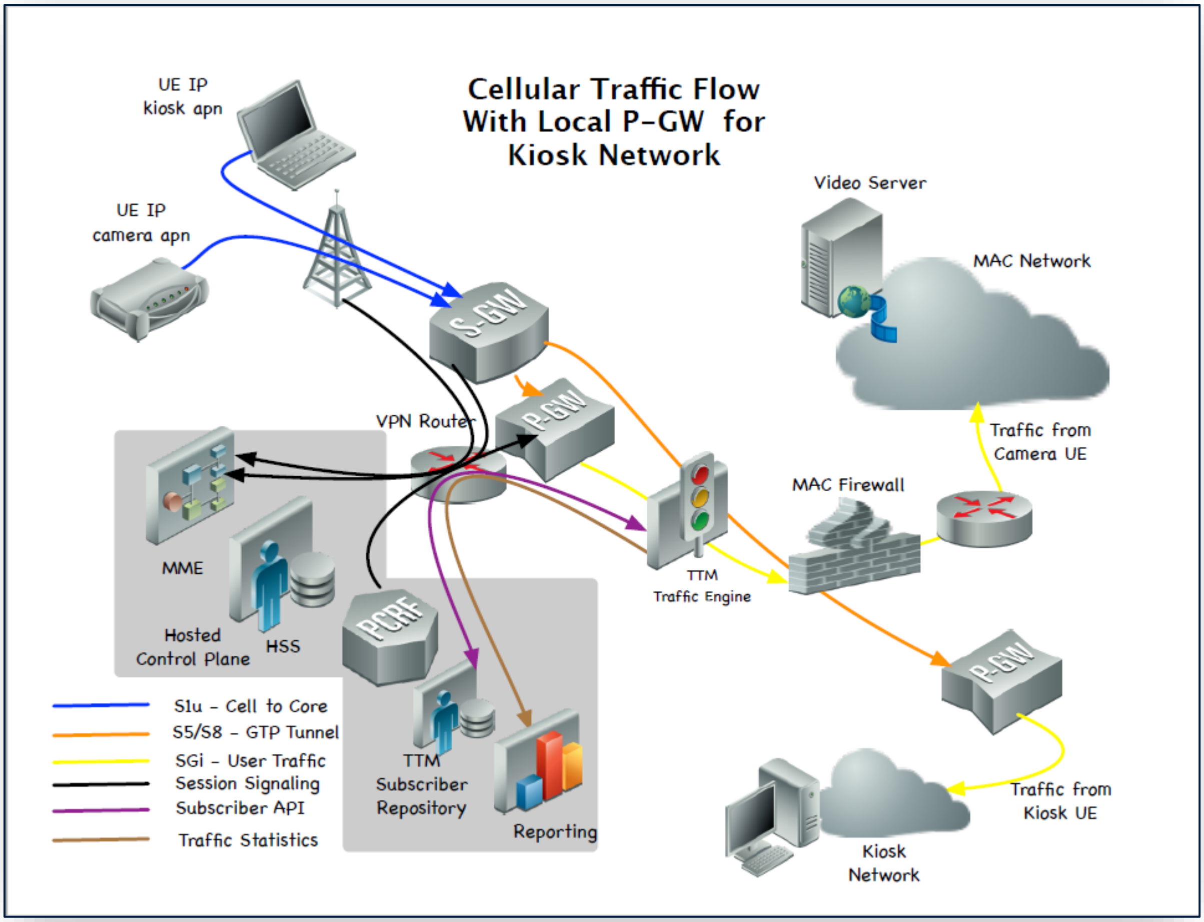

Figure 4 MSP Private Wireless Network architecture

Radio Access Network

For the purposes of the PoC network, the RAN design covered the MAC IT laboratory in Concourse C including the lab office space and adjacent hallway used to access the lab. The network coverage was provided by (3) Nokia MBI CBSDs with 2 x 20MHz channels broadcasting at 50mW. One of the CBSDs was placed inside the IT Lab and two were in the hallway outside the lab, as noted in Figure 7 below, with the letters “SC” within a blue circle marking each CBSD.

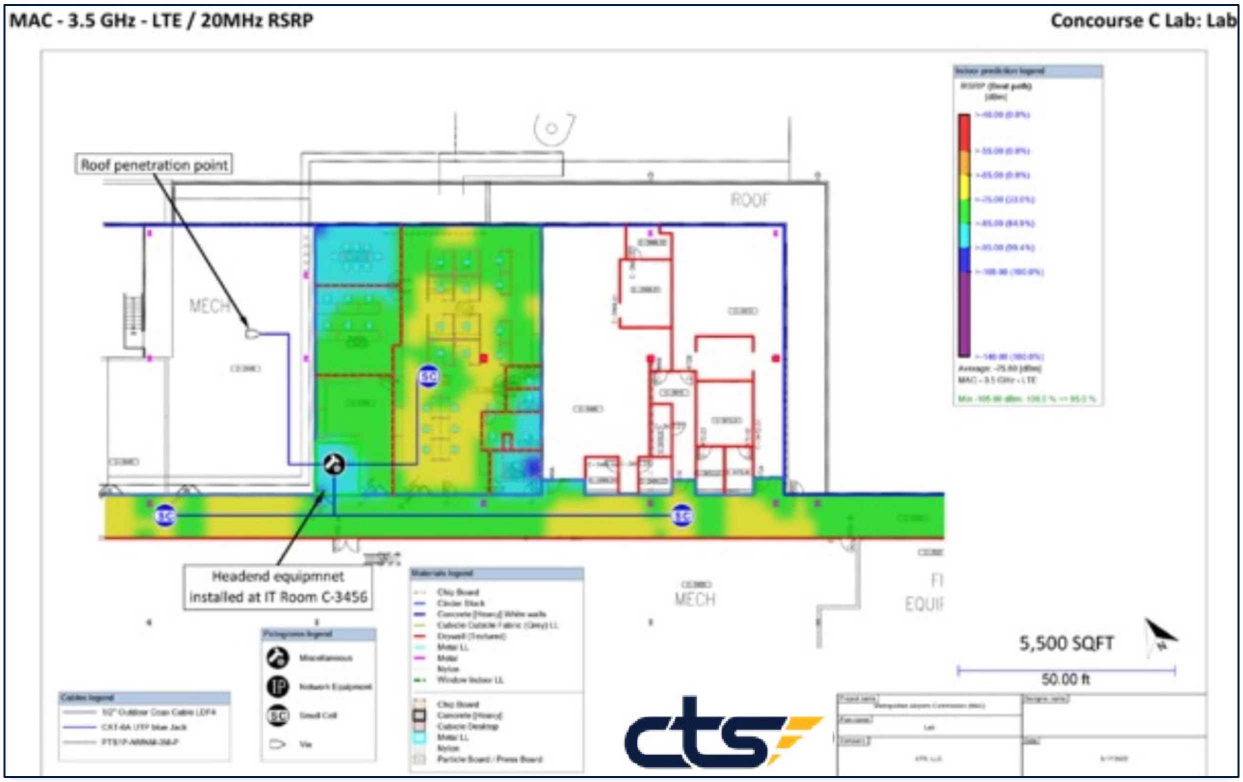

Figure 5 MSP PoC indoor coverage map

Indoor Network

The Nokia MBIs were mounted on the ceiling in the lab and the hallway as shown above in Figure 8 shows one of the Nokia MBIs mounted on the hallway drop ceiling.

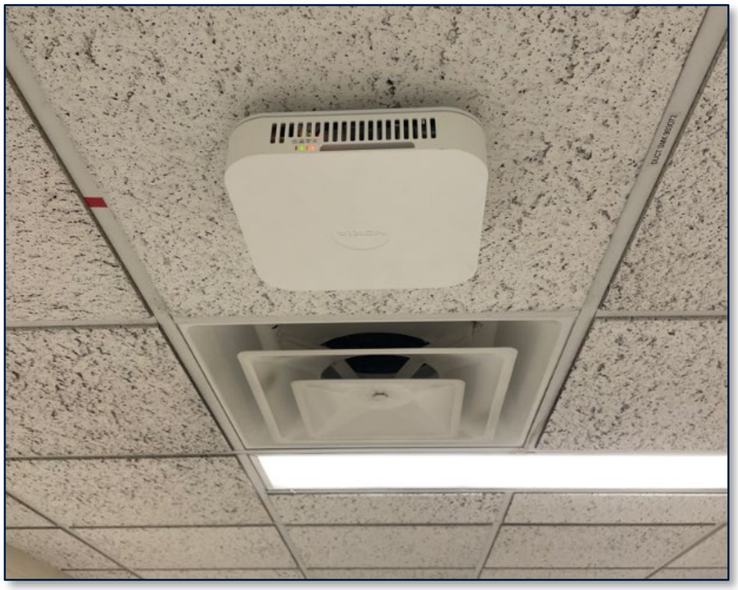

Figure 6 Nokia MBO and antenna mounted on the roof of Terminal 1

Outdoor Network

The RAN also covered the terminal gates outside Terminal 1, full coverage of runways 12L/30R and a portion of runway 22, shown in Figure 9. The outdoor network coverage was provided by (1) Nokia MBO CBSDs with 2 x 20MHz channels broadcasting at 2W using two antennae.

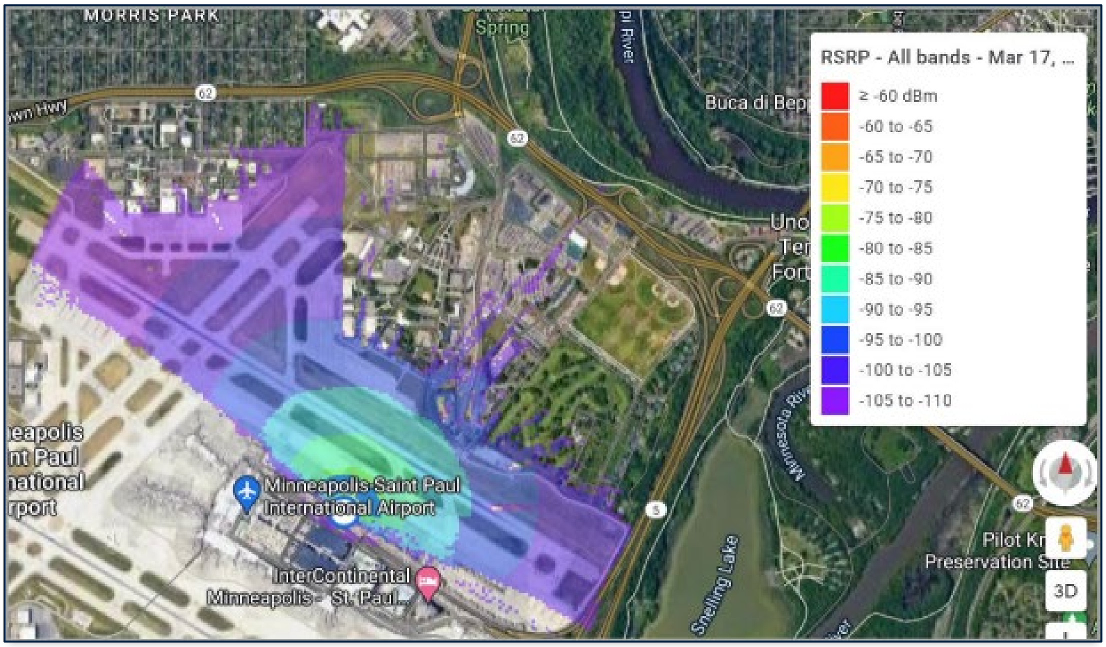

Figure 7 MSP PoC outdoor coverage map

The outdoor radio and antenna assembly was mounted on the roof of Terminal 1 as shown in Figure 10.

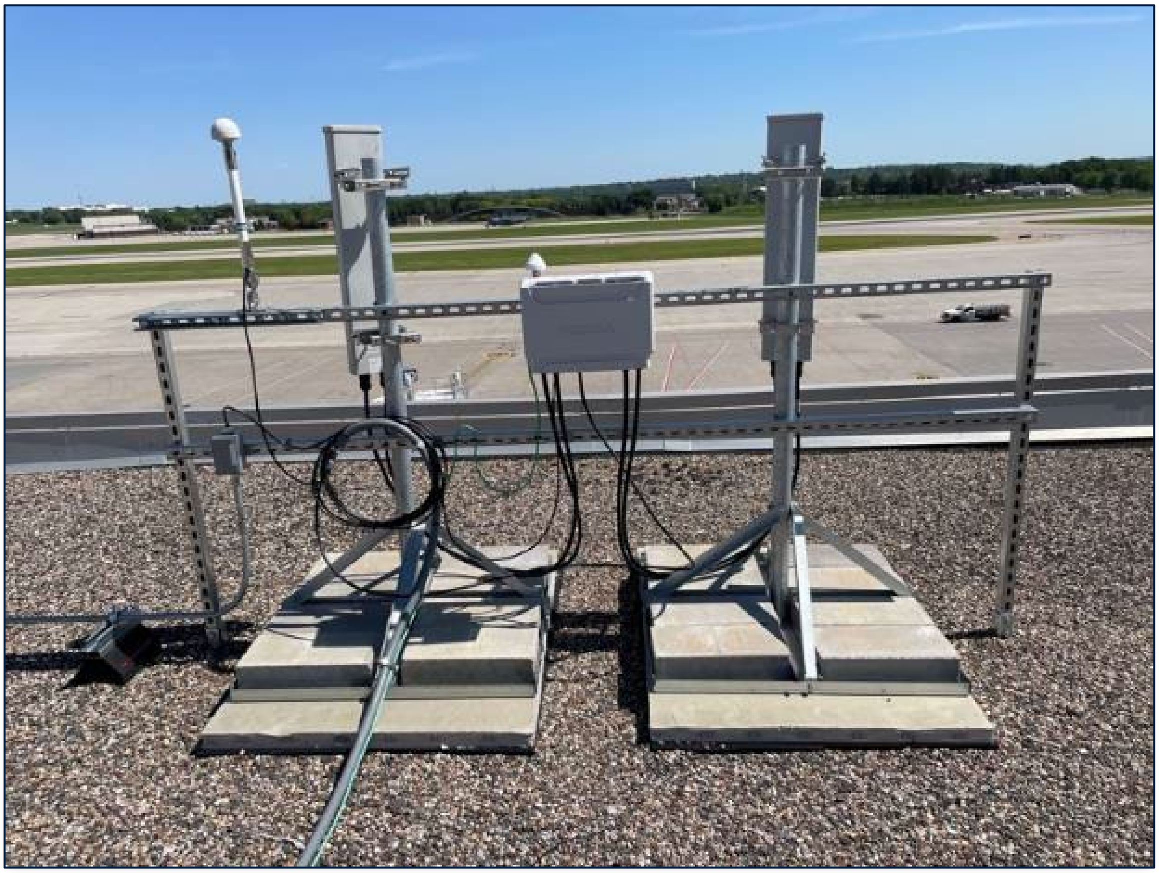

Figure 8 Nokia MBO and antenna mounted on the roof of Terminal 1

Use Case Testing

The primary use cases tested in the indoor coverage area include the Integrated Video and Information Systems Network, Intelligent Monitoring and Control System, CUSE Cart, digital signage, laptops, and smartphones.

The Cityworks application was tested in the outdoor coverage area.

User Equipment

The UEs used in the MSP Private Wireless Network PoC provided data connectivity to a variety of onsite and cloud-based applications supporting MSP airport operations.

Three major classes of UEs used for the CBRS PWN were:

- Bridges/routers – Provide cellular connectivity to wired assets with Ethernet ports
- LTE USB data cards – Enable LTE connectivity for laptops and computers with USB ports and no wireless capabilities or Wi-Fi only
- Embedded devices – Devices with built-in CBRS LTE support such as smartphones, tablets and laptops

Below is a list of the specific UEs used in the trial to support different use case applications:

- Apple iPhone 13 smartphone
- BEC MX240 Enterprise CBRS Gateway
- Cradlepoint IBR1700 Ruggedized LTE Router
- Cradlepoint MC400 Modular LTE Modem (for the Cradlepoint IBR1700)

Detailed specification sheets for each UE are attached in the Appendix.

Apple iPhone 13

The Apple iPhone 13 is a smartphone that can support a variety of mobile applications for workforce productivity. The iPhone 13 supports dual Subscriber Identity Module (SIM) cards, with one connected to the public cellular network (in this case, Verizon) and one connected to the PWN PoC network. Connection to the preferred network is configured in the device settings. MSP uses Microsoft Teams for workforce collaboration in addition to Microsoft Office 365 for documentation and storage. Both Teams and Office 365 were tested as part of the trial using two iPhone 13s.

BEC MX240 Gateway

The BEC MX-240 Enterprise CBRS Gateway features a compact, ruggedized enclosure with embedded CBRS and gigabit Ethernet WAN connectivity to bridge IoT devices lacking an LTE Band 48-embedded capability to the PWN. A detailed specification sheet can be found in the Appendix.

The MX-240 was used in the PoC to connect with the CUSE cart, infrastructure monitoring, and surveillance camera use cases.

Figure 9 BEC MX-240 Gateway

Cradlepoint MC400 Modular LTE Modem

The Cradlepoint MC400-1200M-B Modular LTE Modem extends the functionality of a Cradlepoint IBR1700 in a vehicle router to include the CBRS frequency band. The Cradlepoint IBR1700 Ruggedized Router is currently in use by MSP with a Verizon SIM operating on the public cellular network.

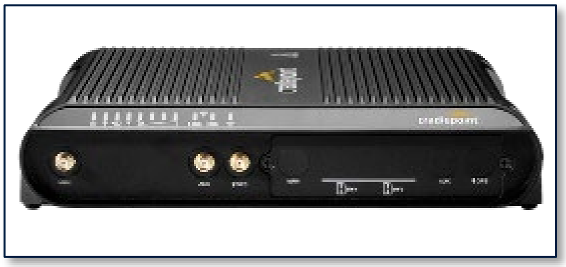

Figure 11 Cradlepoint MC400 Module

Figure 10 Cradlepoint IBR1700 Ruggedized Router

A detailed specification sheet for the MC-400 can be found in the Appendix. The integrated Cradlepoint IBR1700 with MC-400 modem was used to test the Cityworks application in the lab and on the airfield. The unit was mounted and connected to a ruggedized laptop in one of three service vehicles used in tarmac operations.

Proof of Concept

Over a three-week period, CTS installed, configured, and operated the six use cases on the Private Wireless Network with support from the MAC IT and operations staff. Overall, the applications performed well over the PWN, at par or better than current methods of connectivity. Following are the details of the specific use cases and the results of their evaluation.

FAA Part 139 Airside Maintenance Tracking

Current State

Currently, the MSP operations team utilizes a Cradlepoint IBR1700 mobile router to provide connectivity via the Verizon public cellular network. An IBR1700 is mounted inside each of twenty-one vehicles that currently utilize the Cityworks application to provide support for the Airside Operations, Field Maintenance and Trade teams. The mobile router is connected to ruggedized laptops that access the Cityworks application using a web browser once the user has authenticated via MAC single sign-on.

Figure 12 Courtesy of MSP Airport

Proof of Concept

The PoC testing used two different setups:

(1) Indoors in the IT lab and,
(2) At various locations along the airfield in the intended coverage area from Outdoor Radio Nokia MBO around Terminal 1.

For the lab setup, Cityworks was tested in a fixed location using the Cradlepoint MC400 Modem Module installed into a Cradlepoint IBR1700 connected to a laptop via USB. A CTS PWN SIM was also installed in the MC400 to access the PoC PWN. The PWN was integrated with the MAC IT LAN to provide in-network capabilities without a VPN service. The performance over the PWN was consistent with the performance of the application of the local LAN connection.

For the outdoors, the IBR1700 with the MC400 module was mounted in one of the six Airside Operations vehicles, using a 12V cigarette lighter power connection and an external magnetic mounted antenna. The in-vehicle mounted ruggedized laptop was connected via Ethernet cable to LAN 1 port of the Cradlepoint IBR1700. Once the connection to the PWN was successful and GPS lock was observed, access to the Cityworks application was established via the device browser with appropriate location tracking from the GPS network overlaid on the map.

Beginning at Terminal 1, Gate C12, drive testing was conducted in a counterclockwise direction toward the perimeter of the outdoor coverage area. The vehicle was stopped multiple times along the drive to verify coverage and throughput against an OpenSpeedTest server installed at the SGi interface of the PoC PWN.

Results

Local Network Integration

The ability of the PWN to integrate with the MAC LAN was important as both the laptop and Cityworks application rely on single sign-on for end-user authentication. Because the PWN was integrated into the IT LAN, the end user did not have to use a VPN to access the network and Cityworks functionality, which simplified the user experience.

Coverage for the Enterprise

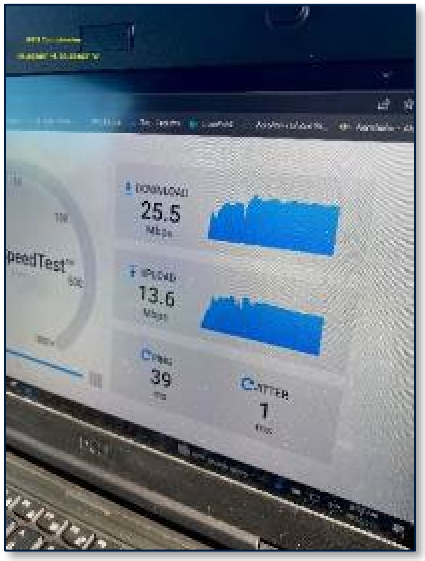

Figure 13 OpenSpeedTest results for drive testing

Currently, many locations throughout the airfield lack adequate coverage from Verizon, making it difficult to use the Cityworks application and the HD mapping function. The shortfall is expected because the Verizon macro network was designed for customer coverage rather than the specific customer's design requirements. One benefit of a PWN over public cellular networks (e.g. Verizon, AT&T and T-Mobile) is that the network is custom-designed for and completely controlled by the enterprise, delivering mission-critical coverage where required.

Reliable Network Performance

Drive testing verified consistent uplink and downlink speeds throughout the predicted coverage of the outdoor PWN. The throughput was far greater than the 20 Mbps that MAC IT staff said was the minimum speed required for a smooth mapping experience. The PWN PoC coverage area was designed to support a single outdoor radio covering a subset of the ongoing airport operations on the airfield. The coverage area included locations where users previously had a poor experience using the Cityworks application on the Verizon network due to inadequate public network coverage. The MAC operations team stated that the performance and HD mapping were more consistent over the PWN.

Video Surveillance Camera

Current State

Figure 14 Panasonic WV-S4550L IP video camera

Today, MSP has approximately 4,000 video cameras connected via fiber or Ethernet cable to the iVISN. IT staff estimates that the cost to deploy a single camera is approximately $11,000, including conduit, cabling, camera, programming, design, project management, and construction management. There is a growing need to expand the surveillance network and, given the high cost of current methods and budget constraints, a lower cost solution would enable MSP to reach more areas, more quickly.

Proof of Concept

One goal of the PoC was to demonstrate that the video cameras can be reliably connected over the PWN to the Central Security System (CSS), reducing the time-consuming and cost-prohibitive deployment of additional wired network video cameras.

For the PWN PoC, a single video camera was installed in the IT lab and connected to the PWN using the BEC MX-240 CBRS Gateway. A dedicated network slice was created on the PWN for the camera application to assign the required priority over other applications in use.

Results

Quality of Service

QoS was ensured through the combination of dedicated network resources, configurable traffic priority levels, advanced traffic analysis and the high-speed connectivity of the PWN-enabled video from the video camera. Video surveillance was delivered with the appropriate priority and required latency for the application to perform at the highest level, consistent with the current performance over the wired iVISN Closed Circuit Television (CCTV) network.

Coverage

Deploying video cameras to unserved areas of the airport using a wired network would take a lot of time and money, if facilities were available. As a result, the perimeter of the MSP property and the tram that connects the terminals remain unserved by video surveillance.

Since power is often easier to get to a location than fiber connectivity, a wireless network has the potential to decrease the time and cost to deploy video surveillance in areas currently unserved within MSP airport. MSP cannot rely on a public cellular to network video cameras back to the CSS due to inadequate coverage and unreliable performance, as evidenced by the current gaps identified by users of the Cityworks application. Even if the public network did provide adequate performance, the cost to backhaul the traffic over the public wireless network would be cost-prohibitive due to the high volume of data.

A PWN covering the entirety of the MSP operations footprint would provide an ideal backbone to expand the surveillance network to include the entire airport perimeter as well as mobile applications such as the tram.

CUSE Cart

Current State

Currently, MSP uses eight CUSE carts to provide flexibility to different airlines operating within the airport. The carts can be moved around the airport terminal from gate to gate or run standalone as kiosks. The carts are connected via a wired Ethernet or Wi-Fi connection today, depending upon the location.

Once the gate agent logs on, the workstation runs a series of airline-specific scripts to configure the local PC environment with the appropriate proprietary airline applications. The breadth and depth of functionality varies by airline, but can include a mix of browser-based or virtual applications, such as VMware or Citrix. The cart's ticket printer prints boarding passes and the laser printer prints various items including itineraries and receipts.

Proof Concept

The lab setup consisted of a Dell Workstation with Microsoft Windows 10 OS connected via Ethernet cable to the BEC MX-240 CBRS Gateway that connects to the PWN.

Gate agents process payments for upgrades and additional charges levied at the gate through CUSE carts. For the CUSE carts to successfully operate with minimal network impact, the workstation must access the existing PCI-compliant security processes and procedures. To satisfy this requirement, CTS implemented a local Packet Gateway (PGW) on the MSP LAN that securely tunneled native traffic to the CUSE cart over the PWN. In addition to leveraging existing security, the added layers of authentication, access control, and over-the-air encryption offered by the private cellular network provided a superior solution to the existing Wi-Fi solution in place at MSP today.

Since MSP requires that the carts operate with a static IP, CTS configured a dedicated network slice on the PWN to implement a static IP address for the workstation through a passthrough configuration on the BEC gateway.

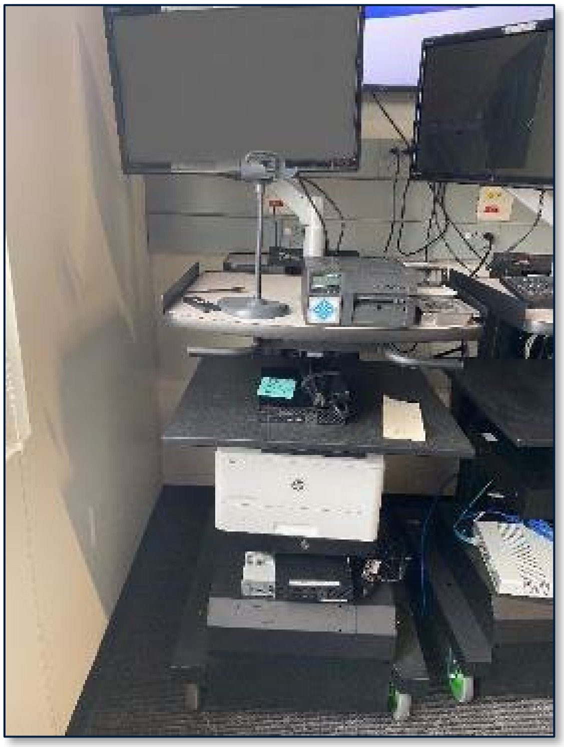

Figure 15 CUSE cart lab setup

Results

Initial configuration of the workstation was noticeably slower than configuration over the LAN, consistent with Wi-Fi. That said, a slower startup had a negligible impact on operations and could likely be reduced by creating a higher speed connection using additional CBRS spectrum. Once setup was complete, there was no noticeable difference in operations between the performance on the PWN and performance on the wired connection.

Reliability

Overall, the PWN provided performance that was comparable to the wired network connectivity utilized today for CUSE carts. Connection reliability should also be significantly improved over Wi-Fi because of the use of licensed spectrum for the PWN and the dedicated network slice allocated within the core network for the application.

Security

The authentication, access control and over-the-air encryption inherent to the LTE technology used in the PWN provide a foundational level of security to ensure that the payment data is transmitted safely between the CUSE cart and the payment processing infrastructure. While the network still needs to be designed for PCI compliance, a PWN based on LTE technology provides a stronger foundation for PCI compliance than an open Wi-Fi network.

Mobility

The mobility afforded by the PWN provides greater operational flexibility over a solution relying on wired connectivity. At the same time, it is more cost-effective and less time-consuming to deploy a PWN than a wired network.

Infrastructure Monitoring

Current State

Approximately 300 sensors are connected directly to the IMACS; additional sensors are connected through approximately 300 controllers on the network. Currently many of the sensors and controllers are networked via Ethernet or fiber. The exception is that a few remote locations on the airfield perimeter are connected via a point-to-point 900 MHz wireless link located on top of the parking garage. Data is collected on a centrally-located server on the property and can be viewed, managed, and configured via a PC application.

Proof of Concept

As shown in Figure 16, the lab setup consisted of a Honeywell Controller (Tridium JACE8000) connected via Ethernet to a BEC MX240 Gateway that connects to the PWN.

A dedicated network slice was configured on the LTE network for the controller with a static private IP address from the MSP subnet allocated to IMACS. In addition, several ports needed to be opened in the PWN firewall to enable the UDP traffic from the controller to pass through to the production network.

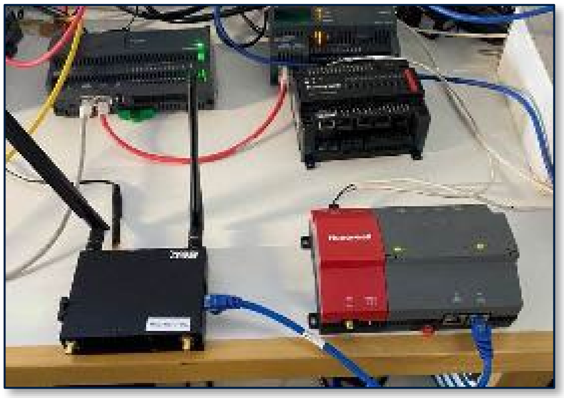

Figure 16 Honeywell controller lab setup

Results

Once configured correctly, the lab's Honeywell controller was able to transmit and receive data from the centralized server. The IMACS IT administrator reported that application performance and system response was consistent with the performance on the wired network currently used in production.

Reliability

Overall, the PWN provided performance that was comparable to the wired network connectivity utilized today for IMACS. Connection reliability should also be significantly improved over unlicensed spectrum (e.g. Wi-Fi, 900 MHz) because of the use of licensed spectrum for the PWN and the dedicated network slice allocated within the core network for the application.

Security

Wi-Fi is not currently used in the solution because of network security and reliability concerns. Security is of paramount importance due to the mission-critical nature of many of the systems connected to the IMACS platform. The authentication, access control and over-the-air encryption inherent to the LTE technology used in the PWN provide a foundational level of security to ensure that the management and operations data is safeguarded as it is transmitted across the wireless network.

Wireless

The wireless connectivity afforded by the PWN provides a significant degree of operational flexibility over the current solution, which primarily relies on wired connectivity. At the same time, deploying new sensors and controllers on a PWN is more cost-effective and less time-consuming. Many mission-critical systems run on the IMACS and unpredictable performance is unacceptable. The predictable performance of the LTE technology used in the PWN ensures mission-critical operations can be supported with stringent SLAs.

Digital Signage

Current State

Today, MSP operates approximately 800 digital signs throughout the airport using wired connections to approximately 600 Microsoft Windows 10 workstations. In some cases, multiple digital signs are attached to one workstation. While the signage is fixed today, MSP is investigating the future implementation of mobile displays. Displayed content consists primarily of scrolling text, images and video that changes throughout the day. Background images and videos change with the seasons.

Figure 17 Courtesy of MSP Airport

Proof of Concept

For the lab setup, a BEC MX240 Gateway was used to connect a workstation to the PWN CBRS network. The PWN is integrated to the MAC IT network to allow connectivity from the existing sign management system to the sign, including using the MAC’s private DNS.

Results

Overall, digital signage is an ideal use case for a PWN. The low-bandwidth requirements with infrequent updates are easily solved by the PWN. The PWN provides added benefits since mobility increases operational flexibility over the current wired networking. Increased flexibility includes reducing time to deploy new signs and allowing for easy sign movement for pop-up advertising, new traffic patterns or emergencies.

Mobility

The mobility afforded by the wireless technology inherent in a PWN provides significant operational flexibility for the deployment of digital signage throughout the MSP campus. Rather than being confined to fixed locations, digital signage can be deployed where it is needed to meet pop-up demand, optimize advertising placement to increase revenue and test new airport traffic flow configurations.

Mobile Devices

Current State

Today, MSP staff use Apple iPhones on the Verizon network to access a variety of applications, most importantly to enhance workforce productivity. These applications include email, messaging, Microsoft applications (e.g. Teams, MS Office 365, MSP) and mobile extensions of operations applications such as Cityworks. Mobile device connectivity today is through Verizon and Wi-Fi.

Proof of Concept

An iPhone13 was used to check uplink and downlink speeds on the PWN LTE network; the test consistently showed downlink speeds in excess of 180 Mbps and uplink speeds approaching 20 Mbps.

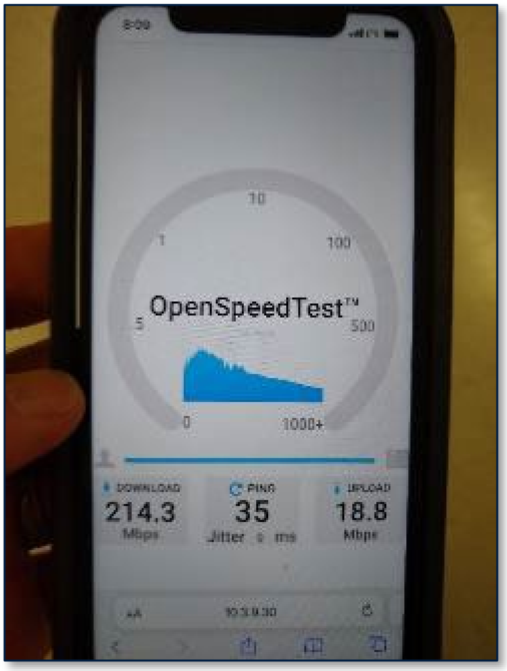

Figure 18 Mobile device speed test

Results

As expected, Band 48-capable mobile devices accessing the PWN experienced performance consist with that experienced on a high-performing public LTE network. The major benefit of the PWN over the public network is that PWN coverage is determined by the enterprise, ensuring network availability in mission-critical operation zones.

Coverage and Reliability

Both the public cellular and Wi-Fi networks onsite at MSP could be improved to increase mobile device user productivity.

- Public cellular networks are costly to use with per bit pricing; public cellular networks are also limited by coverage issues in mission-critical areas of the operations facilities.
- Wi-Fi coverage is primarily in-building and suffers from decreasing performance as the network load increases.

Security

Cellular networks are generally considered to be more secure than Wi-Fi networks, even though they can be designed and deployed to be private and password-protected with user authentication and data encryption.

LTE and 5G networks authenticate the user with either a physical or embedded SIM (eSIM) and data is encrypted out of the box. The SIM is a smart card that is programmed with network-specific information that defines the networks and services available to the user. Cellular networks require a SIM card in order to access the network; without a SIM, a device will only be able to access Wi-Fi.

Further, PWNs are more secure than public cellular networks because the end user data stays within the corporate firewall. The data is not traversing the public network with security policies defined by the carrier. Rather, the data security is defined and enforced by the enterprise.

Workforce Productivity

Many additional mobile device use cases highlight the performance, privacy, and security advantages of the PWN. They include mission-critical communications (e.g. Push-to-Talk, Push-to-Video) and location services (e.g. employee tracking, asset tracking).

The low latency afforded by the onsite mobile core components ensures that mission-critical communications get there in time; the ability to define QoS on the LTE/5G network ensures that the communications connect; and the throughput of the network satisfies real-time video communications.

The precision accuracy delivered by LTE/5G network technology enables employee tracking for worker safety and workforce optimization applications. Location services also enable asset tracking to increase asset use while also preventing loss and theft.

Summary of Findings

The Proof of Concept at Minneapolis-Saint Paul Airport demonstrated the benefits that can be realized through a wide-scale deployment of an enterprise Private Wireless Network across the airport campus, indoors and outdoors. In particular, the PoC demonstrated that a PWN delivers complementary benefits over existing networking solutions utilized by MAC, including improved LAN integration, coverage, reliability, security, and mobility.

- **LAN integration**: Unlike public wireless networks from Verizon, AT&T and T-Mobile, the architecture of the PWN enables tight integration with the local MSP IT network. Integration improves application performance, extends existing IT infrastructure and policies, and maintains network security over a wireless network that increases operational efficiency.
- **Coverage**: Like Wi-Fi networks, PWNs are designed to deliver the coverage and connectivity needed to meet unique enterprise requirements. It is unlikely that Verizon, AT&T or T-Mobile will extend their macro network coverage based on an individual enterprise’s coverage needs. With a PWN, MSP can be assured of robust network coverage to ensure network availability for mission-critical operations by staff and infrastructure within the entirety of the MSP operations footprint.
- **Reliability**: PWNs use a combination of licensed spectrum from the FCC and proven cellular networking technology to deliver a wired network performance with the flexibility of wireless operations. The high availability and reliability of a PWN is critical to maintain mission-critical operations for a Tier 1 airport such as MSP.
- **Security**: The architecture of PWNs enables enterprise data to stay onsite, reducing data security risk. In addition, the authentication, access control and over-the-air encryption inherent to the LTE technology used in the PWN provide greater security over Wi-Fi. The enhanced security afforded by a PWN is essential for mission-critical infrastructure operations as well as PCI compliance for payment processing by gate agents.

- **Flexibility**: LTE mobile technology increases operational flexibility by reducing the cost to deploy operations infrastructure. Wireless networks reduce costly wired installations and shorten the time to deploy mission-critical infrastructure such as video cameras and controllers/sensors.

PWNs provide the best benefits of public wireless networks, Wi-Fi, and wired networks in a flexible networking platform. PWNs are custom-designed to meet specific enterprise requirements, and they perform better than a wired network for mission-critical applications. A comprehensive PWN deployment at MSP has the potential to deliver significant operational improvements to help MSP extend its leadership position in efficient airport operations, improve the employee and customer experience, and ensure future-proof innovation.

Appendix

Exhibit 1: Technical Specification for BEC MX-240

Exhibit 2: Cradlepoint MC400 Data sheet

Exhibit 3: Nokia MBI Indoor SC spec sheet

Exhibit 4: Nokia MBO Outdoor SC Spec sheet