

2021 Private Mobile Networks Report: Separating Hype from Reality

RESEARCH BRIEF



Table of Contents

Executive Summary	1
The Private Mobile Network Opportunity – An Introduction	2
Enterprise IT Trends Behind Private Mobile Networks	2
Defining the Private Mobile Network	3
The Size of the Private Mobile Network Opportunity	4
Private Mobile Networks = Non-Public Networks (NPN)	4
CBRS, Shared License, and Unlicensed Spectrum	5
Complementary Technologies – WiFi and 4G/5G	6
Industries Benefiting from Private Mobile Networks	8
The Private Mobile Networks Ecosystem	10
Extending from Public to Private	10
Open Source Ecosystem for Private Mobile Networks	10
Magma	11
Aether and SD-RAN	11
FlexRAN and OpenNESS	11
Mosaic5G	11
Free5GC	12
Other Projects	12
Reality of Private Mobile Network Deployments Today	12
Deployment Complexities	12
Security Concerns	13
Device Compatibility	14
Expertise and Skill Gaps	14
SLAs and Assurance	14
Evolving Business Models	15

Table of Contents

Conclusion – Expectations for 2021 and 2022 15

Research Briefs are independent content created by analysts working for AvidThink LLC. These reports are made possible through the sponsorship of our commercial supporters. Sponsors do not have any editorial control over the report content, and the views represented herein are solely those of AvidThink LLC. For more information about report sponsorships, please reach out to us at research@avidthink.com.

About AvidThink™

AvidThink is a research and analysis firm focused on providing cutting edge insights into the latest in infrastructure technologies. Formerly SDxCentral’s research group, AvidThink launched as an independent company in October 2018. Over the last five years, over 110,000 copies of AvidThink’s research reports (under the SDxCentral brand) have been downloaded by 40,000 technology buyers and industry thought leaders. AvidThink’s expertise covers Edge and IoT, SD-WAN, cloud and containers, SDN, NFV, hyper-convergence and infrastructure applications for AI/ML and security. Visit AvidThink at www.avidthink.com.

ACCEDIAN



4G/LTE and 5G applications depend on critical requirements being met across complex, distributed infrastructures that often cross multiple operator domains.

Cloud-native, always-on performance monitoring with microsecond accuracy will be the assurance trust model that ensures performance expectations are met and that user experience is delivered.

**In the 5G age, slow is the new down.
Guarantee speed with Accedian Skylight.**

Accedian is the leader in performance analytics, cybersecurity threat detection and end user experience solutions, dedicated to providing our customers with the ability to assure and secure their digital infrastructure, while helping them to unlock the full productivity of their users.

[accedian.com](https://www.accedian.com)

Zero Touch Private 5G Management

5G will be entirely software driven. With 1,000s of applications across 10,000s of edge sites operating in a dynamic environment, the stress on network service and application management will multiply by up to 1,000,000x.

We solve this problem by providing an open source platform for orchestration, management, and automation of Private 5G networks and edge computing applications.

Try the Aarna Networks Multi Cluster Orchestration for free at:
<https://www.aarnanetworks.com/amcop>

Aarna
NETWORKS



2021 Private Mobile Networks Report: Separating Hype from Reality

Executive Summary

The arrival of 5G has brought opportunity to both public mobile networks and enterprise private mobile networks. In particular, private mobile networks are seeing an uptick in worldwide deployment, with hundreds of enterprises, municipalities, and educational institutions rolling out both private 4G LTE and 5G networks. Cellular technologies provide the reliability, security, performance, and user experience that many enterprise use cases demand but wired ethernet and WiFi cannot deliver. From improved spectrum efficiency to improved quality-of-service (QoS), lower latencies, and better coverage, private mobile networks provide a capable complement to today's WiFi deployments.

Shared licensing schemes such as Citizens Broadband Radio Service (CBRS) in the US, enterprise-friendly licensing schemes, and the arrival of unlicensed 5G NR-U worldwide have spurred interest in these private mobile networks. Across key verticals like manufacturing who are looking to realize their Industry 4.0 visions, healthcare looking for reliable and secure coverage, event venues looking to unlock new user experiences, airports and shipping ports seeking to fill coverage gaps, and mining installations wanting to ensure safety through anytime-anywhere communication, private mobile networks are a desired solution today.

At the same time, complexities in deploying private mobile networks (also called non-public networks or NPN in 3GPP specifications) need to be resolved. From complex deployment architectures that may or may not involve mobile network operators (MNOs) to lack of skills and expertise in integrating enterprise IT with mobile infrastructure, there are numerous opportunities for improvement, and potential monetization by both incumbents and new entrants.

The broad ecosystem for private networks includes the MNOs, hyperscale cloud providers, networking vendors, global system integrators, and managed service providers. With a sizable market, stakeholders are investing heavily to carve out a slice for themselves. Business models are being trialed, and the technology stack for private networks are evolving. Related initiatives like open RAN and mobile edge computing will also impact NPNs. And there's a healthy ecosystem in the open-source community targeting private mobile networks use cases.

Many companies are reaping the benefits of NPN today, and we expect over the next twelve to twenty-four months that the field will expand dramatically. AvidThink recommends that enterprises looking for private mobile network solutions do their homework in understanding the nature and pace of innovation in this arena and time their investments appropriately to maximize return on capital. There are promising startups focused on enterprise use cases today that may fit enterprise needs, even as MNOs and system integrators push to sell their private mobile network services. Regardless of which way enterprises are leaning, we advocate thorough due diligence as they evaluate options, and map their business needs to the offerings available.

Acknowledgements:

We thank the following organizations for sharing their perspective for this report: **Aarna Networks, Accedian, Celona, IBM, Linux Foundation, Nokia, Open Networking Foundation, Parallel Wireless, Telecom Infra Project.**

The Private Mobile Network Opportunity – An Introduction

The advent of 5G, accompanied by ongoing buzz and hype from carriers and other vendors in the ecosystem, has piqued enterprise interest in using 5G (and today's 4G LTE) technology for private networks.

Spurred by the virtualization and cloudification of mobile networks, the number of new entrants in the modern RAN market saw a further boost with the disaggregation and open RAN movement. In addition to targeting public 5G, many of these entrants realized the massive potential of the enterprise private 5G market and had made significant investments and inroads into this arena.

Major public mobile vendors including Ericsson, Huawei, Nokia are facing competition from other established firms such as NEC, Fujitsu, and Samsung in vying for the private mobile market. Other aggressive market entrants include startups and mid-sized players, including a number who have featured more prominently of late, such as Acceleran, Airspan, AltioStar, ASOCS, **Celona** (disclosure: a sponsor of this report), Expeto Networks, Federated Wireless, JMA Wireless, Mavenir, Parallel Wireless, Sercom, and Tango Networks.

Further, hyperscalers like Amazon Web Services (AWS) are touting their **integration with private mobile networks** and Microsoft Azure **acquired mobile core provider, Affirmed Networks**, and a **mobile communications stack vendor, MetaSwitch**, hoping to provide enterprises with integrated private wireless solutions. Not to be left out, mobile network operators (MNOs) and global system integrators (GSIs) are jumping into the fray, offering managed private mobile networks as a service.

Given the frenzied level of activity, we hope to provide our enterprise and service provider readers with a snapshot of the state of the private mobile networks market and help sift out what's real and what's hype. The aim is to help our readers make informed decisions that lead to better business outcomes.

Enterprise IT Trends Behind Private Mobile Networks

Before we jump into a deeper discussion around private mobile networks, let's look at crucial enterprise drivers that help explain the interest in private networks.

Digital Transformation

We'll start with the digital transformation of businesses. Enterprises worldwide understand that **digitization of the industry can unlock additional value** through improved analytics, lower operational costs, increase agility, and reduce time-to-market. This was further reinforced during the pandemic, as evidenced by the varied performance of different businesses during this time. Digital-heavy companies proved more resilient than their counterparts, regardless of industry sectors.

IoT and IIoT

Associated with digital transformation is the adoption of internet of things (IoT) and industrial IoT (IIoT) platforms. Many manufacturing, logistics, and supply chain-related enterprises have embarked on a quest towards achieving **Industry 4.0** visions. These enterprises are converting devices and production processes to digital forms (IIoT devices) to be programmed, observed, managed, and optimized via digital automation. Making devices more intelligent, measuring critical indicators of manufacturing and production processes via intelligent sensors, and using AI and machine learning (ML) are key IT initiatives designed to help modernize and optimize businesses.

Mobile First

Another key driver for the business is a drive towards anywhere-anytime computing, which became a necessity during the pandemic. Work from home (WFH) and work from anywhere (WFA) initiatives accelerated dramatically and are now accepted as usual for many enterprises. A tenet of WFH and WFA is enterprise mobility – the use of mobile technologies to ensure that employees are always connected. After all, consumers customers today expect companies to engage on mobile channels, and it makes sense for an enterprise to adopt a **mobile-first** philosophy.

Edge Computing

Enterprises worldwide have benefited from adopting cloud computing. The cloud provides innovative software services, proven development frameworks, plus a flexible consumption model. However, many enterprises have applications that remain on-premises. These applications may have data residency or privacy constraints, or strict latency performance requirements, or need to directly connect to equipment on site. For workloads that generate a large amount of onsite data or that might be located in hard-to-reach places (e.g., oil rig in the ocean, remote mining operation), the high cost of data transfers to the cloud might mandate the use of local computing.

This is where **edge computing** – the use of cloud computing principles and technology in a local context – comes into play. On-premises edge computing promises to upgrade traditional server rooms and legacy systems into smaller form-factor cloud computing stacks, with the attendant operational and technology benefits that cloud platforms bring.

However, enterprise networks that connect applications hosted on these edge platforms to users and machinery are straining under increased data load from digital transformation and use of IoT. Wired networks provide performance but are difficult and expensive to upgrade or expand. Enterprise WLAN is cost-effective and easier to scale but can suffer from reliability, coverage, and performance challenges.

Within the context of these IT trends, private mobile networks can provide significant value by bringing a high-performance, secure, scalable, and flexible connectivity option to enterprise locations – both indoors and outdoors.

Defining the Private Mobile Network

5G is portrayed as the next generation of public mobile networks. 5G promises an order of magnitude faster speeds, greater coverage, increased reliability, and lower latencies. Like previous generations of mobile technologies such as 3G, 4G, and 4G LTE, the 5G standards are defined by the 3rd Generation Partnership Project (3GPP). What's significant this time is that the 5G standard (Release 16 and more in Release 17) encourages and supports the use of 3GPP standards in non-public deployments. These non-public networks (NPN) provide dedicated and private connectivity services for users and devices (or things in an IoT context). And like public 5G networks, NPNs support the same rich set of use cases from a quality of service (QoS) perspective, including enhanced mobile broadband (eMBB) for high bandwidth, massive machine-type communication (mMTC), and ultra-reliable low-latency communication (URLLC) for support of high-performance and large scale enterprise IoT deployments.

ENTERPRISE IT TRENDS DRIVING ADOPTION OF PRIVATE MOBILE NETWORKS

Digital
Transformation



IoT
Industrial IoT

Mobile
First



Edge
Computing



avidthink.com

The Size of the Private Mobile Network Opportunity

The impact of these NPNs on the enterprise connectivity market will be significant. As with any early market, analyst market size estimates vary. Nevertheless, the projected CAGR over the next few years ranges from 17% to 37%, with revenue estimates in 2027 spanning \$5B to \$12B. Given the level of uncertainty, we suggest using as context the enterprise wireless LAN (WLAN) market. IDC has measured **enterprise WLAN growth at 10.3% year-on-year in Q4 2020**, this follows **a 7.4% year-on-year growth in IDC's numbers for Q3 2020**. And despite COVID-19, the segment grew 1.9% for the full year of 2020, reaching \$6.35B worldwide.

We expect the NPN market to rival and potentially surpass that of the enterprise WLAN market. In any case, as we'll discuss later, private 5G (and 4G LTE) will not supplant WiFi but instead complement it.

Private Mobile Networks = Non-Public Networks (NPN)

With a sizable potential market, vendors have invested in bringing to market innovative NPN solutions. Recent technology improvements from vendors increased the need for wireless performance from corporations, and more open government spectrum policies worldwide have increased enterprise willingness to adopt these NPNs, which are more colloquially termed private mobile networks (PMNs) or private networks (PNs). NPNs will eventually be all 5G, though many of the early private networks today use 4G LTE technology due to the availability of cost-effective 4G equipment and compatible user devices.

NPNs fall into two main categories: standalone and public network integrated. The former, as suggested by the name, standalone NPN or SNPN, does not rely on any network functionality from a public mobile network (sometimes called a Public Land Mobile Network or PLMN). The operator could be the enterprise itself, a networking vendor, a hyperscale cloud provider, a GSI, or an MNO. The latter, a public network-integrated NPN (PNI-NPN), is deployed with the support of a public mobile network, usually with subscriber management and other mobile core services hosted and operated by the MNO.

There are different ways to deploy a radio access network (RAN) with NPNs. The RAN can be shared by multiple SNPNs, or even by numerous PNI-NPN, with different MNOs sharing the radio infrastructure. Likewise, with 5G, network slicing of a public mobile network can be used to provide PNI-NPN, with various enterprises offered parts of the public network and segregated from other customers with appropriate quality of service (QoS) and service-level agreements (SLAs) contracts.

NPN-related technology development, system and deployment architectures, management and operation processes, and business models are in flux. In our work with MNOs, hyperscalers, and networking vendors, we observe that key parameters defining NPNs continue to evolve:

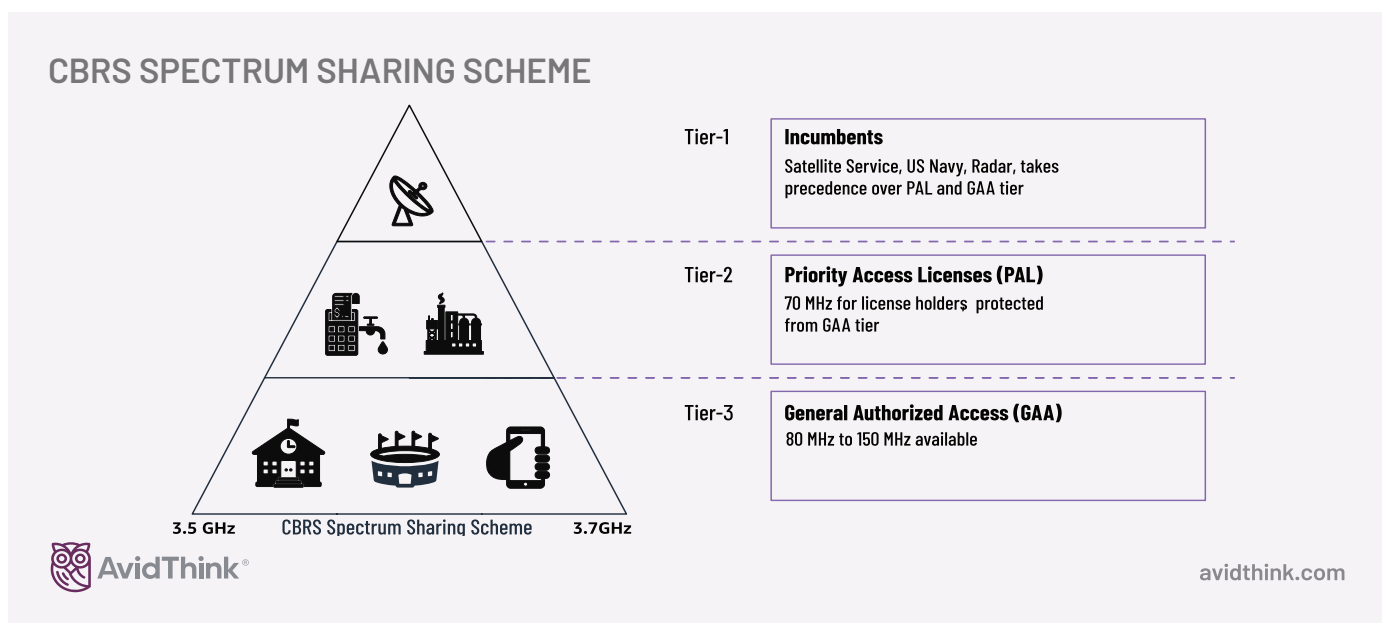
- **Design and deployment** – Who designs, pays for, deploys the infrastructure – RAN and core? Depending on the nature of deployment and business model, different entities from the enterprise or even the MNO might pay for the equipment and installation. We're seeing subscription models where an integrator provides a private network as a service, with no upfront capital outlay from the enterprise. In multi-tenant deployments, we observe shared RAN or a neutral host arrangement where a property owner contracts with multiple MNOs for integration between an NPN and a public mobile network.
- **Operation and management (O&M)** – Who operates the service? In standalone NPNs, enterprises may choose to pay for the equipment upfront but count on a GSI, MNO, or third-party to operate the service. SNPN-focused solution providers like Celona offer cloud-hosted and managed O&M, akin to the cloud-based enterprise WiFi solutions from Cisco Meraki and HPE Aruba, reducing the complexity of managing NPNs.

Private mobile networks can provide significant value by bringing a high-performance, secure, scalable, and flexible connectivity option to enterprise locations – both indoors and outdoors.

- Public network integration** – This is currently an area of complexity. How particular devices on an NPN interact with a public network can range from having multiple-SIMs (or eSIMs) to roaming arrangements between the NPN and the public network to more integrated PNI-NPN that use gateways (e.g., multi-operator core networks or MOCN) for mobility. In certain instantiations, the private network is a private slice of a public network. Issues abound: from assuring consistent and predictable behavior from devices, to the flow of money in different business models, to ensuring security and privacy across the boundaries of public and private networks. While 3GPP Release 16 (and future releases) offer techniques for how user devices can navigate in between both, with mechanisms like closed access group (CAG) cells, there is still a level of sophistication required that’s not implemented in many today’s devices yet. And in situations where SLAs matter, accountability, control, and visibility continue to be debated and negotiated between stakeholders. For this reason, many of the early successful NPN deployments are SNPNs, which allow enterprises to gain immediate benefits while avoiding the public network integration complexity until it matures.
- Spectrum considerations** – Multiple spectrum options exist for NPNs, from using unlicensed bands (which may differ across different geographic regions), using shared licensed bands, obtaining license bands directly, or with the aid of an MNO. Considerations here will depend on the specific use case and required bandwidth, QoS requirements, the location of deployment, how crowded the bands at the site already are, and the costs of using licensed spectrums.

CBRS, Shared License, and Unlicensed Spectrum

Spectrum is an important consideration in NPNs – spectrum availability and bands determine capacity and potential interference and congestion. In the United States, a shared spectrum scheme, the Citizens Broadband Radio Service (CBRS), is a 150 MHz-section covering 3550 MHz to 3700 MHz that’s available for commercial use in a spectrum sharing arrangement. CBRS provides for a general authorized access (GAA) tier that’s available to everyone, a county-by-county priority access license (PAL) option that anyone can bid for in a federal auction, and an incumbent user band that’s protected for US Department of Defense use, and fixed satellite services. In order to ensure that the shared access is appropriately protected, CBRS systems in the US have to communicate with a Spectrum Access System (SAS) – a cloud-based service that governs what frequencies are available at a locale. CBRS devices (CBSD) will need authorization from a licensed SAS before they broadcast. As of publication of this report, there are five approved SAS administrators: Amdocs, Commscope, Federated Wireless, Google, Sony and Keybridge. This scheme, and cost-effective and easier-to-obtain enterprise licenses in countries like Germany, France, and Japan, and the availability of 5G NR-U (5G unlicensed bands), help drive enterprise adoption of private 5G and 4G. We should note that prior to wide interest in CBRS, there was an earlier 4G LTE-initiative called MulteFire, promoted by the **MulteFire Alliance** (MFA), which continues to promote private mobile networks today.



For CBRS, the **OnGo Alliance** (formerly CBRS Alliance), an industry group, aims to help promote LTE-based CRBS solutions. They have developed certification programs similar to what the **WiFi Alliance** has done for WiFi, hoping to ease industry adoption of CBRS by providing education and reducing friction and uncertainty via their certification programs.

Private 4G LTE and 5G networks, like WiFi, are isolated from public mobile networks. However, the NPNs have performance characteristics that allow them to replace wired networks and augment enterprise WiFi. As we shared, the majority of private networks today are 4G LTE, but they will transition to 5G over the next few years as the technology matures.

Complementary Technologies – WiFi and 4G/5G

Hundreds of enterprises, municipalities, state and local governments worldwide have deployed private 4G and 5G networks. These NPNs operate similarly to WiFi, where mobile radios (named eNodeBs/eNB or gNodeBs/gNB) are deployed in an office, factory, or outdoor enterprise setting. These eNBs or gNBs are similar to enterprise WiFi access points (APs). However, these radios tend to be more complex and expensive than WiFi APs, adding to capital costs. Some of these costs can be offset by reduced cabling needs (less mobile base stations can provide same coverage and performance as WiFi) and installation costs.

In addition, these mobile radios are connected to a 4G or 5G mobile core that provides the control and data management for mobile traffic. Again, the mobile core stack, with its multiple components and sophistication, tends to be harder to deploy and manage than enterprise WLAN controllers. Nevertheless, as we discussed earlier, vendors like Celona, Expeto and others are trying to simplify deployments of private 4G and 5G networks.

Compared to WiFi, private mobile technology provides improved security, better traffic isolation, better spectrum efficiency, and improved handoff between radio cells. We will note that newer versions of the WiFi specifications, notably WiFi 6 and 6E, borrows performance-enhancing techniques from mobile technologies such as multiuser multiple input multiple output (MU-MIMO) and orthogonal frequency division multiple access (OFDMA) to improve capacity and performance under congestion. As WiFi 6/6E sees wider deployments, these techniques may help close WiFi's performance gap.

Here's a quick comparison of both technologies:

Attribute	4G/5G	WiFi
Spectrum	Able to use dedicated license spectrum, shared license, unlicensed spectrum. However, the need to manage spectrum use and licenses may require spectrum planning, and in the US, CBRS needs a SAS system to protect licensed and incumbent users.	Uses unlicensed spectrum, which may be crowded, but increased bandwidth availability in countries like the US mitigates some 5G advantages.
Ease of Deployment	Historically complex to deploy with multiple core components in addition to RAN (open RAN further integration).	Easy to deploy, with most enterprise WLAN using convenient cloud controller for management, enabling zero-touch plug-and-play setup.
Management	Historically hard to manage, with complexity around radio planning and many functional components in the core. AI/machine learning to optimize is in infancy.	Enterprise indoor and outdoor configurations well-understood, standard templates available with simple point-and-click. AI/machine learning to maximize performance in use.
Procurement	Less available and harder to procure from distribution chains, usually need a reseller or integrator involved.	Available from multiple retailers, resellers, distributors. Online configurators and direct-to-enterprise purchases.

Attribute	4G/5G	WiFi
Device Compatibility	Requires more expensive modems and, therefore smaller set of compatible enterprise devices. For CBRS and new unlicensed bands, it will require time for more devices to support (e.g., only newer model mobile phones support CBRS).	Enterprise IoT devices support WiFi (varying versions), and all end-user computing devices have built-in WiFi support. Low-cost devices generally only support WiFi.
Performance	Rich support for different QoS requirements, mMTC, eMBB, critical IoT, time-sensitive workloads with URLLC. Better predictability under high loads. Improved coverage per radio (4X or more indoors and even better outdoors). Handle devices moving at speed.	Improving with newer versions (WiFi 6/6E) and can provide good bandwidth but prone to drops and poor handling of device handoff between radios. Limited QoS support.
Public Network Mobility	Support for devices seamlessly attaching to a public mobile network as they leave enterprise premises (while retaining the same device ID). However, it requires improvement in management policies and user device software upgrades.	No easy handoff, but intelligent routing or overlay software can provide application-layer mobility between multiple connection types.
Enterprise IT Integration	Work-in-progress today through early deployment architectures provide local breakouts that can be connected to enterprise networks (after 5G N6 or 4G SGi interface). Tie-ins to enterprise user directories, IP address management systems, network security systems are being worked out. Some vendors are touting early solutions that are more integrated than incumbent 5G/4G systems.	Enterprise WiFi has been an integral part of IT systems for decades.
Skills	Limited availability of specialized skills needed for private mobile networks, though vendors are attempting to wrap complexity and simplify with new software solutions and cloud-based management.	Enterprise WiFi deployment skills are readily available, and a robust ecosystem has been built.
Costs	Viewed to be more expensive from both capital outlay and operational costs. However, costs are use-case dependent since fewer 5G/4G radios (and therefore shorter cable-runs and lower installation costs) are needed when compared to WiFi APs (especially outdoors). New upstarts in this space are lowering costs through new approaches and technologies.	Perceived to have lower costs on both WiFi infrastructure and end-devices. Both capital and operational costs are believed to be lower.

While the WiFi versus private mobile networks discussion invariably comes up at most enterprises contemplating rolling out an NPN, the reality is that both will coexist for the foreseeable future. The focus will need to be on what use cases each will serve and how to seamlessly integrate both in a way that supports enterprise IT initiatives.


Industries Benefiting from Private Mobile Networks

The benefits of NPN stem from improved performance and SLA support, better predictability and scale, and potentially better security. In particular, there are select verticals for which private mobile networks can solve a significant number of problems. In many of these situations, existing wired ethernet networks may meet the needs for performance and throughput but are rigid and expensive to expand or reconfigure. And for numerous use cases, WiFi rollout can be expensive due to cable runs and installation costs to place the larger number of APs needed to cover an indoor or outdoor area. This is in addition to private mobile's support for tighter QoS and better default security.

SELECTED VERTICALS FOR PRIVATE MOBILE NETWORKS

Industrial Manufacturing Transportation Hubs Mining Oil and Gas Healthcare

Sports/Performance Venues Education Retail Utilities

 **AvidThink**[®] avidthink.com

Verticals that can benefit from NPN deployments include:

- **Industrial Manufacturing** – In factories and warehouses, the rollout of industrial IoT and the digitization and automation of previously manual processes require a reliable network fabric. Private 4G or 5G can bring improved coverage and reliability close to wired networks, but with the same flexibility as WiFi. These NPNs can reliably connect autonomous mobile robots (AMRs) and automated guided vehicles (AGVs) on the manufacturing floor to edge computing facilities that host control modules or computer vision (powered by AI/ML). Likewise, private mobile networks can enable the centralization of manufacturing control systems on edge computing server racks without compromising safety by supporting reliable low-latency (multiple milliseconds) links to manufacturing lines. Other NPN-enabled use cases include powering push-to-talk (PTT) for employees on the factory floor, facilitating real-time communication, and reliably carrying surveillance video feeds for inventory, safety, and health applications.

- **Transportation Hubs** – Compared to WiFi, private mobile technologies provide improved range and penetration in shipping ports, airports, bus terminals, and other hubs. For critical use cases that require dedicated bandwidth, NPNs offer the option of using licensed spectrum obtained directly by an enterprise (CBRS PAL in the US, enterprise licenses in other countries) or licensed from an MNO. The private network can power AGVs, enable PTT and carry surveillance video feeds for processing by AI/ML systems. The NPN integrates well into IoT use cases, tracking devices, and carrying feeds from sensors to localized compute for processing, enabling predictive maintenance to ensure low failure rates of machinery and vehicles (ships, planes). Video feeds in ports carried over the private network can be used to detect safety issues or to assist with inventory and maintenance. Finally, as augmented reality (AR) becomes more available, private mobile networks can enable real-time overlays that help technicians with troubleshooting essential equipment or provide quick look-up for key information in repair or technical manuals.
- **Mining** – A popular industry for NPNs in regions and countries like South America, South and West Africa, China, and Australia. Private mobile networks (4G LTE and 5G) have stronger penetration and performance, even in underground deployments, requiring fewer base stations to cover the same area and providing higher reliability of signal than WiFi. PTT, video surveillance for health and safety, and IoT sensor use cases dominate this industry. Unique use cases include using precision location capabilities in cellular networks to enable geofencing for safety. In addition, many of the NPNs can operate standalone in remote regions where a public mobile network might not be built out.
- **Oil and Gas** – Like the mining industry, oil and gas and other energy companies operate in remote locations that sometimes have poor or no mobile coverage. Private mobile networks operated by the enterprise or a system integrator can provide a high-performance, corporate-controlled network that ties into IIoT sensors, process management systems. Other everyday use cases include PTT, video surveillance, and monitoring of critical equipment and locations. NPNs provide more cost-effective coverage, especially outdoors, for the industry when compared to alternatives.
- **Healthcare** – Private mobile networks can provide reliable and more secure connectivity across hospital campuses, tying together internet of medical things (IoMT) devices with edge computing stacks that provide analytics, AI/ML capabilities. Likewise, these NPNs can carry medical records and scans over higher capacity links for real-time diagnostics, possibly powered by AR soon. And when hospitals need to expand into overflow capacity, private cellular technology can provide a critical and secure network extension that is an improvement over WiFi. Other healthcare-related use cases include PTT and video surveillance processing for safety and health – monitoring at-risk patients who may have mobility challenges and raising alarms when accidents are detected.
- **Sports Arenas and Performance Venues** – In crowded arenas that tax today's WiFi systems, private 5G networks promise higher capacity and increased density. NPNs can power augmented in-person experiences (AR) for concerts, and sports events, carrying high-definition video feeds for local edge processing before near real-time distribution to an in-venue audience. Real-time replays from user-selected angles, follow-me footage of favorite players are all potential use cases that private mobile networks can support. This is in addition to the standard video surveillance use case for safety and health.
- **Education** – University campuses that may find WiFi coverage challenging and insufficiently reliable are trialing private mobile networks. Running a parallel, secure private network segregated from the semi-public WiFi systems that most universities have, is appealing to many IT departments. In addition, school districts (sometimes rural) are looking to private networks as an alternative to keep lower-income students connected to the internet. During the pandemic, a few school districts in the US set up CBRS networks in their neighborhoods and provided LTE modems to students, allowing them to connect to the school network and the internet, providing cost-effective and safe browsing.
- **Retail** – Private networks as deployed in warehouses, stock rooms, and stores can provide a more reliable foundation on which to carry video traffic for surveillance, IoT sensors that aid with health and safety checks or that assist with inventory. AMRs that stock shelves can be powered off the same private networks. Likewise, point-of-sale terminals running off private cellular networks may gain greater flexibility through improved coverage, allowing them to be dynamically placed as needed to facilitate fast and convenient checkout.

- **Utilities** – Utilities are different from the other verticals in that they have a wider service area. While utilities could depend on public mobile networks for coverage for their IoT sensors and for their communication and collaboration in the field, some utilities in the US bid on PAL licenses in recent US FCC auctions. Utilities can use these PALs to erect and build wide-area networks across the counties they cover using the CBRS spectrum. These private networks can be used for critical sensor traffic, process and operational controls, video surveillance, and communications.

There are other verticals of interest but these are the main ones we've encountered in our engagements with MNOs, hyperscalers and networking vendors to date. Next we'll switch from the demand side of the market to examine the supply side.

The Private Mobile Networks Ecosystem

Many of the initial players in the private mobile network ecosystem are incumbents for the public mobile network – Huawei, Ericsson, and Nokia. All three vendors have made a significant investment in pushing private network solutions to the market, with Nokia taking both a direct-to-enterprise and carrier-led approach. Ericsson and Huawei lean towards a carrier-led or at least carrier-involved philosophy. With Nokia leading the way with a stated 260+ private networks customers worldwide, there are multiple hundreds of companies who have rolled out private mobile networks today. However, based on our conversations with carriers and vendors, many of these are pilot projects with few radio base stations.

Extending from Public to Private

All the incumbents, along with the host of competitive vendors listed in the early part of this report, are aggressively trying to simplify private network deployments. Whether taking the path of a "private mobile networks in a box" approach, or a fully-managed "private mobile networks as-a-service" approach, the goal of these vendors, MNOs, SIs is to make cellular technology as easy to deploy as WiFi.

They are assisted by other vendors in a value chain that is seeing opportunity in both private networks and public networks, given the trends of disaggregation and open RAN. Innovations are coming rapidly, from improved silicon (base station on a chip, integrated systems-on-chip for open RAN) from vendors like AMD/Xilinx, ADI, Broadcom, startup EdgeQ, Ericsson, Intel, Marvell, Nokia, Qorvo, Qualcomm, and Samsung, to an opening up of the radio ecosystem, to open-source options for the mobile core, to integrated edge computing stacks with pre-loaded mobile cores. Meanwhile, orchestration and software vendors are simplifying their software stacks and optimizing them for open RAN in both private and public settings.

Vendors who have embraced disaggregation and open RAN are using the private mobile network as a route to market – smaller deployments, potentially shorter sales cycles, limited exposure during early testing of yet unproven technology. These include RAN and core vendors and orchestration vendors, and integrated edge stacks (involving virtualization vendors like VMware and Red Hat, or newer Kubernetes-distribution vendors).

At the same time, given the potential size of the private mobile opportunity, there are new vendors focused on the private networks experience, such as Celona, which is recreating the enterprise WLAN-as-a-service experience with private mobile technologies while pushing prices into the same envelope.

Open Source Ecosystem for Private Mobile Networks

As with all major networking initiatives today, the open-source ecosystem plays a significant role. While there aren't separate open-source ecosystems for private versus public networks, some open-source projects (like Project Magma) are more focused on private mobile use cases. Regardless, we expect to see more enterprise-specific features such as integration with enterprise directories, or improved local-breakout support, be better supported in the codebase to ease NPN deployments.

Magma

Magma Core is a project initially seeded by Facebook as part of their **Connectivity initiative**. Today, it is linked to multiple open source organizations, notably Linux Foundation, which is its main and legal home, together with Open Infra Foundation (OIF), **Telecom Infra Project (TIP)**, and the **OpenAirInterface Software Alliance (OSA)**. Magma provides a mobile core (4G LTE today, 5G in progress) that can be easily deployed to power a private 4G LTE network. Former founder of Mirantis (a popular virtualization platform previously based on OpenStack), Boris Renski, has started a company, FreedomFi, that's packaged Magma for consumption by enterprise IT teams, and is seeing strong market interest.

Aether and SD-RAN

The **software-defined radio access network (SD-RAN)** project at the Open Networking Foundation (ONF) is focused on providing an open RAN implementation that can be used in an ORAN Alliance-compliant deployment. SD-RAN includes multiple software components from ONF's library of software projects, including μ ONOS (their software-defined networking controller). SD-RAN has demonstrated a white-box open RAN full-stack solution hosting an end-to-end call. The ONF aims to make the development of xApps (software that can interact closely with and control the RAN) more convenient with their SD-RAN platform and the SDKs that come with it. They anticipate innovation in the areas of the near-Real-Time and non-Real-Time RAN Intelligent Controller (RIC) – a more detailed topic best discussed in the context of open RAN (a future report from us).

ONF also hosts the **Aether** project, which utilizes their SD-RAN solution as part of a 5G/LTE connectivity service. Aether is a platform designed to bring edge cloud to enterprises and encompasses a computing edge based on Kubernetes and Linux Containers, a software-defined networking fabric based on their ONOS software-defined networking platform, and a connectivity service based on SD-RAN attached to mobile cores (either ONF's 4G LTE OMEC EPC, or the open-source Free5GC NG-Core). In addition, Aether includes a cloud-based management platform that provides lifecycle management and orchestration. ONF Aether is essentially a private mobile network and edge platform integrated stack for enterprise deployment.

ONF Aether is essentially a private mobile network and edge platform integrated stack for enterprise deployment.

FlexRAN and OpenNESS

Intel's **FlexRAN** platform is a virtualized reference implementation of LTE Advanced RAN with a modular eNB (eNode-B) software stack that runs on white box hardware (assisted by FPGA hardware accelerators). Open Network Edge Services Software (OpenNESS) is another Intel-supported open-source effort that provides a cloud-native MEC software toolkit to provide high-performance edge platforms. While not targeted only at private mobile networks, FlexRAN and OpenNESS combine to power edge-hosted use cases in concert with NPNs, and Intel has shown various proofs-of-technologies that target NPN use cases.

Mosaic5G

Mosaic5G is a community initiative between academics and industry to foster the development of 5G. Mosaic5G hosts a series of projects that are relevant to both public and private mobile deployments, including LL-MEC – a low-latency edge computing platform with a mobile network core network controller and FlexRAN (not related to Intel's) – a software-defined RAN platform. It also includes a Juju-based 5G slicing orchestrator called JOX and a Kubernetes-based platform called Kube5G that supports both VNFs and CNFs through Kubevirt and Docker.

Free5GC

The **free5GC** is an open-source implementation of a mobile 5G core. Seeded initially by the National Chiao Tung University (NCTU) in Taiwan, it has the support of other parties, including Chunghwa Telecom, ONF, Fujitsu, Edgecore Networks, Wistron NeWeb Corp, and EstiNet.

Other Projects

Beyond the projects above, there are many other open-source projects of relevance to private networks (often linked with open RAN and ongoing white box disaggregation of the RAN). They include the data plane development kit (DPDK), vector packet processor (VPP), open vSwitch (OvS), P4 (a network programming language), ONAP (orchestration platform hosted by Linux Foundation), and EMCO (formerly ONAP4K8S, another orchestration option).

In addition, the **Open Compute Project (OCP)** and TIP are driving forward efforts on this front. While OCP's products tend to be more focused on public 5G hardware server and data center infrastructure, TIP has a private network solutions group focused on building integration, automation, and deployment infrastructure to assure and deploy an end-to-end private networks stack built from open-source and white-box components. This builds on top of TIP's open core network (OCN) initiative, aiming to develop an ecosystem that can take to market cloud-native and converged core offerings tying together 4G, 5G, and WiFi. Recently, TIP unveiled their OpenWiFi initiative to unlock the enterprise WiFi market and painted a vision of a future hyperconverged wireless system that provides integrated 5G and WiFi.

Reality of Private Mobile Network Deployments Today

The expected market size of the private mobile network market, coupled with PR buzz around public 5G and edge computing, has led to inflated expectations for the market. We have had conversations with carriers worldwide who are eagerly touting their private mobile wins and rolling out their enterprise private 4G/5G design, implementation, and management services. MNOs view this as a natural revenue stream extension to their public 4G/5G mobile services.

TIP has a private network solutions group focused on building integration, automation, and deployment infrastructure to assure and deploy an end-to-end private networks stack built from open-source and white-box components.

Announcements of "private 5G in a box" or "private 5G in a box with MEC" (mobile edge computing) conjure visions of stepping up to a fast-food counter, grabbing a to-go package, and bringing home a complete turnkey private 5G (with MEC) solution. Carriers (e.g., SK Telecom with Dell and VMware), hyperscalers (e.g., AWS with Verizon, Microsoft Azure with Verizon and AT&T), and virtualization and server vendors (e.g., Red Hat, HPE, VMWare) are driving towards turnkey, integrated, pre-validated offerings. Early efforts and deployments are promising, but there's still significant investment and efforts for private mobile networks to be deployable by many enterprises, particularly those that involve public network integration. This means that upstarts like Celona, Expeto, JMA Wireless, who have set out to simplify enterprise deployment have a chance to provide a value proposition that enterprises will appreciate.

Deployment Complexities

Enterprises or system integrators looking for a do-it-yourself (DIY) approach for private networks found their early days challenging — though improvements are around the corner. Much of the mobile technology development in the past was focused on carrier-scale deployments, with skilled personnel that had a strong understanding of RF, spectrum planning, complex operations, and systems. Unlike enterprise WiFi, with simple pick your APs, cloud-based web interfaces, and one-click deployments, rolling out an NPN requires more planning and thought. While spectrum complexities are being

reduced with CBRS in the US and 5G NR-U (unlicensed) globally rolling out, many private mobile solutions from major incumbent vendors aren't designed for end-user installation. This might not be an issue if the solution is offered as a managed service, and some incumbents like Nokia have seen early success on this front. Likewise, we've seen vendors like Celona invest R&D in simplifying and automating spectrum planning and management.

Independent of enterprises and SIs, many MNOs have limited experience in rolling out indoor, small-cell-based 4G LTE and 5G networks integrated with enterprise networks and IT infrastructure. Our conversations with local and global SIs indicate the same, with the market split between players with strong enterprise IT expertise (with WiFi) and those who have familiarity with distributed antenna systems (DAS) previously relied upon to improve indoor coverage, and sometimes indoor small cells rollouts, but limited enterprise IT knowledge. The rare few that can cross these boundaries are finding early success in the market with their unique skillsets.

Nevertheless, we recognize that some startup vendors covered in this report have made significant gains in simplifying both the enterprise experience, and potentially the operator/SI experience as well. One notable relationship is the Celona-HPE Aruba distribution relationship, which points to a recognition by a major enterprise WiFi vendor of a private mobile solution that potentially achieves the simplicity that enterprises are looking for.

Architectural Variations

Complicating deployments is a variety of deployment architectures for NPNs that are evolving. In many SNPNs, all the components of the mobile core, along with the RAN, are deployed on-premises. Even with open RAN in SNPNs, we can constrain the complexity by placing the centralized unit (CU), distributed unit (DU), and radio unit (RU) on-premises.

Some networking vendors now provide cloud-based management UIs that connect to the on-premises components to provide a simple web UI to manage the deployments – akin to enterprise WiFi. In remote deployments with poor internet connectivity, these management UIs may need an on-premises option.

However, even with SNPNs, there are deployment options that host portions of the core within carrier or other external infrastructure (co-location facilities), with user plane functions or select portions of the core deployed locally. These can offload the number of components on-premises, but add to the complexity of deployment.

And in PNI-NPNs, where an MNO or multiple MNOs are involved, architectural decisions can get more complicated. The enterprise and MNOs will need to decide whether to use single or multiple SIMs/eSIMs, whether roaming is involved, who handles subscriber management and where that is hosted, which bands of the spectrum are used (licensed/unlicensed/shared), whose PLMN (public land mobile networks) IDs are broadcast and on which bands, how to configure device policies in terms of which networks to attach and more. The sophistication of the user devices may constrain the flavors of deployments supported. Other considerations include: whether the NPN a dedicated slice of a public network as well as the type of gateway integration required – multi-operator core network (MOCN), multi-operator radio access network (MORAN), or other methods.

Security Concerns

One of the strengths of private mobile networks is the stronger context around identity (when compared to WiFi). However, simple questions like who manages SIM provisioning and how identities are integrated with existing enterprise directories can tie up deployment. Different vendors take different approaches to solving this, with some solutions reflecting a more enterprise-friendly foundation, and others reflecting their operator-centric roots.

Inadequacy in understanding how to best enforce enterprise security at the transition points between mobile and enterprise networks is also an issue. Based on the deployment architecture, the data breakout points may differ – most will likely be on-premises, but it is possible for an MNO-managed private network to have data network interfaces (4G LTE S-Gi or 5G N6 interfaces) that are located in a nearby mobile service center. How and whether these exit points are connected back to an enterprise are areas of consideration, and whether firewalls or other security devices are needed are open questions.

Further, in cases where an MNO uses the private network infrastructure to extend their indoor coverage, the MNO may need assurances about the underlying infrastructure to ensure that their subscriber traffic is not exposed or compromised. MNOs involved in these types of multi-MNO or neutral host implementations may also request additional visibility to help troubleshoot subscriber problems — there's open questions on how best to limit visibility to the network segment and relevant subscriber data.

Device Compatibility

Most enterprise equipment and devices support WiFi. While CBRS has been a boon for private mobile networks in the US, the number of enterprise computing devices or IoT devices that support that band is limited but growing. In our discussions with enterprises contemplating NPNs in factories or transportation hubs, the topic of device support invariably comes up. Today's POCs still involve picking a set of devices from a list of phones, tablets and cellular modems that support CBRS.

Nevertheless, with the popularity of CBRS and promise of 5G NR-U, the situation is changing, and the list of compatible devices is multiplying. Many new phones, like iPhones 11 and later, and other mobile devices sold today support the appropriate bands. There's still work required on network access policies, fallback logic and handling of network transitions, which will come in time as an increasing number of enterprises push device manufacturers to increase the sophistication on this front.

Expertise and Skill Gaps

Many organizations involved with enterprise IT are unfamiliar with cellular technology. WiFi resellers used to performing enterprise WLAN site surveys will need to adapt and understand the RF characteristics of low, mid, ultra-high bands for cellular, and familiarize themselves with CBRS, 5G NR-U, and licensed bands (CBRS PAL or MNO spectrum) as well as RF tuning and optimization. MNOs already have that expertise in-house and use sophisticated planning and monitoring systems, but their processes and tools are not always easily scaled down for enterprise use.

In addition, while vendors are simplifying mobile core and RAN setups, early deployments require careful orchestration of the various components of a 4G LTE or 5G core. A from-scratch installation involves familiarity with a virtualized infrastructure manager for VM-based deployments or Kubernetes for container deployments and setting up clusters. Enabling high availability involves yet more complexity.

On the other side, MNOs and other cellular specialists familiar with mobile technologies might have a limited understanding of the enterprise IT landscape. Enterprise directory systems like Microsoft Active Directory, enterprise firewalls and network security solutions, corporate IP address management (IPAM), and other systems that do not usually interact with mobile networks will come into play.

We envision two parallel trends: one, networking vendors like Celona, Expeto and others pushing to simplify their NPN products and utilizing analytics and AI/ML to enable convenient self-optimizing private mobile network systems for enterprises; and two, system integrators, enterprise resellers, and MNOs plugging their respective knowledge holes rapidly and developing best practices and blueprints for successful deployments across different industries and use cases.

SLAs and Assurance

One of the critical differences between NPNs and WiFi is the improved performance characteristics of NPN. Many early deployments are looking for that lower latency, more stable bandwidth in the face of congestion, or better handoff behaviors. Beyond installing and operating a mobile network, operators need to assess and monitor the KPIs of the NPN. The same performance statistics could be used by network automation and analytics to provide ongoing real-time optimization of the NPN or to troubleshoot and heal the network autonomously. Unsurprisingly, we're seeing established assurance vendors like **Accedian**, Keysight, Spirent, and Viavi, who provide mobile assurance solutions, extending their public mobile testing and monitoring products to fit private networks use cases.

Assurance is essential because private mobile business agreements will increasingly involve SLAs or QoS performance guarantees.

Assurance is essential because private mobile business agreements will increasingly involve SLAs or QoS performance guarantees. Early deployments are focused on coverage, but as we evolve SLAs on public 5G network slices for performance-sensitive workloads (like connected cars, critical IoT), we expect that private mobile networks will become subject to the same type of SLA guarantees with financial motivators not to violate KPIs. Vendors that build in SLA and performance monitoring into their solutions will stand a better chance of success in the enterprise.

Evolving Business Models

For SNPNs, we have observed deals where enterprises pay for capital equipment and installation upfront, with a recurring charge and sometimes software license fees for managing and updating the NPN. Other arrangements include all-in-one subscription models with multi-year agreements. The enterprise pays a fixed fee per month per base station/square footage covered that includes management of several SIMs/devices. Whether networking vendor-led or reseller/integrator-led, these appear to be the current working business models. We envision a simplification of pricing as popular blueprints are developed per vertical per significant use case. We could see a near future where enterprises pick from a selection of low, medium, high-density options, with add-ons for real-time performance SLA guarantees. SaaS-type billing and pricing systems would then calculate a fixed fee per device/user or a cost per square foot covered for indoor/outdoor.

NPNs also promise to be a boon for property owners of multi-dwelling units (MDUs), where they can set up private networks for use by multiple business tenants and charge them for access. Whether SNPN or PNI-NPN, property owners can leverage 5G network slicing capabilities to provide segmented access, with different SLAs to different tenants, providing a better wireless access solution than what WiFi offers today. Even transportation hubs like airports are contemplating building out NPNs and charging airlines, airport retailers and other on-site businesses for network access.

When MNOs come into play in PNI-NPN scenarios, the business models are in flux. Who pays whom for network access? What about spectrum licensing? Who pays for the equipment infrastructure? These are questions that aren't always easy to resolve. Should carriers pay to access the installed infrastructure in a neutral host situation, viewing it as a cheap way to get in-building coverage without erecting a DAS? Or do enterprises provide free integration with MNOs, so tenants and visitors in their buildings get 5-bar coverage regardless of carrier? One could imagine this to add value to consumers in a healthcare or a sports venue setting. Perhaps MNOs could pay for the installation and operate a private network for free in exchange for in-building public coverage and thousands of corporate-liable mobile subscriber revenue. Given that MNOs have had a slow start into the NPN space (only **16% of tracked NPN deployments** in 2020 were carrier-led), they might need to take a more aggressive route to market. Regardless, we view NPN as fertile ground for new and creative business models.

Conclusion – Expectations for 2021 and 2022

We'll wrap up with what we expect to see from the various stakeholders in the private mobile ecosystem.

- **Network equipment providers, silicon merchants** – We expect more players to enter the private mobile networks fray, particularly open RAN and ORAN-compliant solutions. We're hopeful that enterprise-friendly cloud-powered solutions like Celona and Expeto will continue to gain traction and expect others to follow. At the same time, we predict that there will be advances on the platform and silicon front that make private wireless solutions much more cost-effective. As was unveiled at the recent **TIP OpenWiFi event**, hyper-converged solutions involving integrated WiFi/cellular systems will show up in the next few years, with a cost envelope that eliminates the WiFi/cellular debate.
- **Mobile network operators** – MNOs are scrambling to ensure that they aren't left out of a market they view as rightfully theirs. When a major vendor like Nokia takes a direct path to enterprises, MNOs need to be careful not to miss this opportunity. It does require MNOs to be more agile than they previously have been and to find appropriate partners with whom to enter the enterprise market. We aren't sure that the incumbents powering MNO networks are always the best choices and recommend MNOs look closely at the upstarts as alternatives. Nevertheless, MNOs will continue to engage their customers in private 5G/LTE conversations, but we would caution that MNOs need to revisit business models and be more creative.

- **Hyperscale cloud providers** – Private networks with edge computing are a strong match to solve numerous enterprise challenges. Many use cases and verticals we described earlier require a joint private network and MEC combination. We expect an ongoing collaboration between the hyperscalers and MNOs but anticipate hyperscalers will also take a direct path into the enterprise market – like Microsoft Azure who owns mobile software stacks (Affirmed Networks, Metaswitch)
- **System integrators, value-added resellers, managed service providers** – This is a wonderful revenue and managed services opportunity for this class of stakeholders. Many will need to pick the right private mobile solution vendor to partner with in their go-to-market. We anticipate that resellers and managed services providers will likely go with a non-mobile incumbent initially, in particular solutions focused on deployment and management simplicity. Larger GSIs might invest in more complex integrated stacks for specialized deployments at enterprises that need a larger scale or have unique requirements.
- **Enterprises** – As the ultimate end-user, it's important to be educated prior to making a decision. Many enterprises are experiencing enough pain with their current infrastructure that they are seeking alternatives to WiFi and wired Ethernet. There are use cases for which private 4G LTE is a natural choice – transportation hubs, mining, manufacturing – and enough successful deployments to warrant early investment. Private 5G (versus 4G LTE) is still early and the ROI model is not yet proven. That could change rapidly over the next twelve to eighteen months as new solutions arrive, especially those based on disaggregated, open RAN that promise lower costs. Picking the right deployment partner: MNO, GSI, local reseller, and managed provider will be a critical decision. For standalone NPNs, it will be worthwhile for enterprises to evaluate the new generation of enterprise-centric private mobile network providers mentioned earlier who have streamlined the deployment process and determine if they fit their needs.

There's gold in 'em private mobile network hills. But who plays the role of Levi Strauss? Who will sell pans and shovels? And who are the prospectors in this private networks gold rush? We'll find answers to these questions as winners are minted and losers are identified while we light up enterprises globally with private 5G networks.



AvidThink, LLC
1900 Camden Ave
San Jose, California 95124 USA
avidthink.com

© Copyright 2021 AvidThinkI, LLC, All Rights Reserved
This material may not be copied, reproduced, or modified in whole or in part for any purpose except with express written permission from an authorized representative of AvidThink, LLC. In addition to such written permission to copy, reproduce, or modify this document in whole or part, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced. All Rights Reserved.