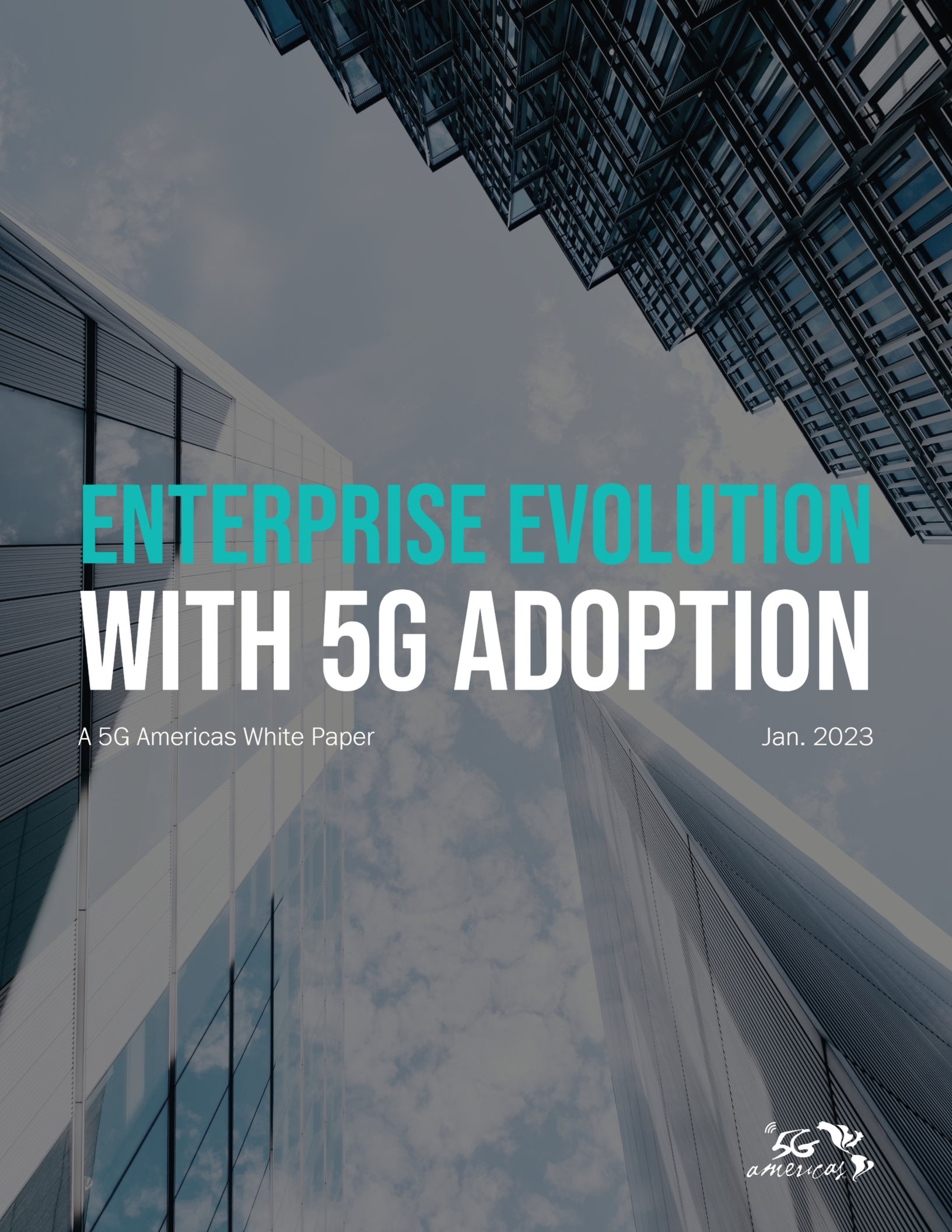


ENTERPRISE EVOLUTION WITH 5G ADOPTION

A 5G Americas White Paper

Jan. 2023

Contents

Executive Summary

In the last several years, we have witnessed 5G discussions move from idealized futuristic hype to a practical and relevant technology that holds promise for the future, while also providing immediate value. Of course, no other phenomenon in recent memory has helped a technology to deploy faster than the worldwide COVID-19 pandemic.

The global challenge has underscored the need for connectivity, specifically higher quality wireless connectivity, which has been demonstrated in virtually every corner of human existence - whether in public or private scenarios, be it for mission critical or general use. Wireless connectivity needs to be secure and provided at cost points that are acceptable by large sets of consumers. The accelerated demand for remote and hybrid work across industries like education, healthcare, commerce, and others still remains in effect and is expected to continue for the foreseeable future. These demands herald the emergence of a new era of improved internet access and enhanced cellular access for all communities.

The February 2022 GSA report on private mobile network uptake helps us understand where we are on the 5G adoption curve. There is clear and compelling growth in all categories. We are witnessing organizations deploying private 4G and moving to private 5G, many vendors building solutions, as well as launching a variety of offers. The future is bright with many market observers and analysts also reporting increased interest and demand for private 5G across almost all industry verticals, while also pointing out challenges. Overall, the wireless communications sector is bubbling with a healthy dose of energy and interest, which is currently translating into meaningful engagements between customers who need solutions and the vendors offering them. These engagements are continuing to refine knowledge about industry requirements that will lead to implementation and more offers of readily consumable services.

For industrial verticals, the promise of private 5G has been driving digitization trends as defined in Industry 4.0.While progress on Industry 4.0 has not been as fast as with other commercial 5G sectors deploying public network mobile broadband and Fixed Wireless Access (FWA), the vision painted by Industry 4.0 in 2015 still remains vivid and desirable. Overall, we are witnessing a dose of moderation and careful thinking applied to where and when which technologies are ready to be deployed effectively.

For example, smart manufacturing and factories of the future have been defined in great detail on paper. However, realizing and deploying these factories have not happened as fast as some have expected due to real world logistics issues such as lack of necessary equipment, delays in supply chain, as well as complexities of integration with brownfield production facilities. While these delays have not weakened the vision of Industry 4.0, it will still be a matter of time before many of the ideas that were introduced by Industry 4.0 can be realized.

On the other hand, emerging worldwide issues such as the pandemic and increase in cyber warfare have been pushing many innovative ideas to be realized even faster. Remote working capabilities to support hybrid work, as well as increased demand for secure infrastructure are examples of areas where faster overall development and deployment are happening.

In this paper, we will build on top of several past 5G Americas papers on Private Mobile Networks and will focus on how enterprise deployments of private cellular are evolving. In particular, we will focus on emerging deployment models, evolving RAN technologies, developing mobility requirements that are changing to meet enterprise requirements, as well as security and management needs that are being raised by enterprises. Below is a list of 5G Americas white papers, which we will be referring to in this document. We highly encourage you to review them for additional information we'll be discussing here:

- 5G Vertical Use Cases
- Private and Enterprise Networks
- 5G Technologies in Private Networks
- Transition Toward Open and Interoperable Networks
- Innovations in 5G Backhaul Technologies
- Commercializing 5G Network Slicing
- Security for 5G

Finally, this white paper is authored by a multi-vendor group of authors who are all active experts in 5G and private cellular technology and engaged with interested customers. The paper is made possible by 5G Americas, who provides a productive collaborative environment for like-minded experts to discuss, debate, and ultimately articulate a summary understanding of the state of technology and market. We'd like to thank both 5G Americas and the authors for their support and contribution.

1. Introduction

The term “enterprise” in this paper encompasses a large set of industrial and general service verticals with a very mixed set of requirements that are becoming increasingly more complex. Examples of enterprise verticals include manufacturing, transportation, mining, oil & gas, utilities, healthcare, education, hospitality, venues, banking, public sector, and gaming. Future wireless connectivity for these verticals is expected to include a mix of different wireless technologies and architectures. These will include both wireline and wireless access methods co-existing together in a complementary fashion to satisfy the demands of complex and data hungry applications, while allowing the enterprise network administrators to have full control over their network operation and data security. To face this challenge, vendors and providers that intend to serve the enterprise must implement sufficient performance and flexibility in their designs to meet enterprise demands at acceptable cost points.

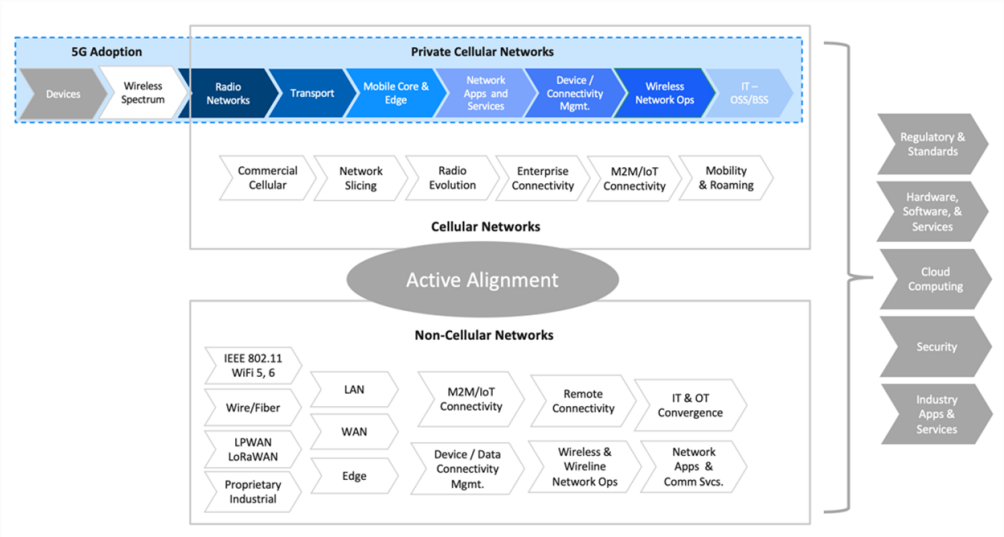
Wireless technology standard bodies, such as the Third Generation Partnership Project (3GPP) and the Institute of Electrical and Electronics Engineers (IEEE), have long been defining methods for improved signaling, lossless transport, lower power profiles, higher capacity, lower latency, more accurate location capabilities, better security, etc. These enhancements are being implemented and offered in various platforms, solutions, and deployment architectures. However, there is still much work to be completed for end-to-end integration across network, application, and service layers.

The following diagram provides a visual description of topics of interest that are under discussion and development in cellular and non-cellular networks, as well as overarching topics that span these two wireless categories and that need to come together to serve the enterprise.

In the cellular networks category, 5G adoption has been an ongoing track with sub-tracks in commercial and private networks. There are similar tracks of development in non-cellular, wireless and wireline, networks that are relevant to the enterprise. There are many alignment discussions underway given that enterprises, and consumers, are eventually in need of using all three methods: cellular, non-cellular wireless, and wireline, in a holistic manner to draw optimal benefit from connectivity. In addition, there are overarching topics as applications, end-to-end security, use of cloud computing, services architecture, and many more that are also evolving, which will need to be incorporated into emerging enterprise level networks and services.

This diagram is intended to illustrate the larger picture of topics under development that may be of interest to an enterprise decision maker as they consider private cellular solutions. In this paper we will touch upon a subset of these topics.

Figure 1: Topics under development related to Enterprise adoption of private cellular



2. Enterprise Deployment Trends of P5G

Deployment of Private 5G networks (P5G) in various enterprise verticals continues on a pragmatic trajectory possibly due to lack of device availability and completeness of end-to-end solution offers, particularly for more complex uses cases that require low latency and higher throughput. While interest remains high and proof of concept and trial deployments have been ongoing in almost all industrial verticals, a true and objective assessment of trends for broader enterprise adoption of private 5G cannot yet be fully established.

Meanwhile, cost conscious enterprises continue to solve their connectivity needs with "good enough" solutions based on Wi-Fi, and/or delay solutions that prove to be impossible or cost prohibitive with Wi-Fi. These scenarios are primarily outdoor use cases where Wi-Fi coverage is limited, and cellular radios can be more efficient. The category of use cases that have been successfully deployed to date include Fixed Wireless Access (FWA) and backhaul.

In previous 5G Americas white papers, we identified many enterprise requirements which are still very valid. Some of the use cases that depend on new technology at the application and device layers have matured. For example, in the case of Automated Guided Vehicles (AGVs) where low latency is a requirement for remote control of the vehicles, we are seeing AGV manufacturers putting control intelligence of the AGV in the vehicle itself as opposed to demand it from the network. This reduces the need for very low latency that is required for close control of the device by the network, limiting device dependence on the network to broader telemetry and video exchange.

Another example of application-level maturity is in the AR/VR space where a great deal of progress has been made in developing compelling application layer offers that can be consumed in enterprise verticals. Here too dependence on the low latency capabilities has been relaxed, at least for now, and more emphasis is made on availability of consumer-friendly goggles that can implement image processing at the rates that are acceptable to human consumption. With higher processing power at the headset and/or edge platforms, applications can distribute their processing demands and offloading the network. Smarter algorithms can also predict human user expectations and relax demand of low latency exchange with the network.

2.1 Enterprise Network Requirements relevant to P5G

Here we will provide an updated summary of enterprise requirements, technical as well as business related that are top of mind in all private cellular considerations. Many of these requirements have been mentioned in other papers as well.

2.1.1 Suitable Radio Frequency (RF) Spectrum

Availability of suitable and cost-effective spectrum continues to be the highest priority requirement for enterprise wireless use cases. Unlicensed spectrum, IEEE 802.11ax (Wi-Fi 6) and expanded 6GHz access with Wi-Fi 6E is the preferred choice for enterprises given that there is no license fee associated with these spectrum choices. The exception to this rule falls into use cases that cannot be satisfied with unlicensed spectrum ranges, typically outdoors use cases that require very large area of coverage.

Shared spectrum, as with CBRS in the US, and ISM bands in many parts of the world, are providing a new spectrum source which are attractive for use with 3GPP LTE based systems, but the use of these spectrum categories is still relatively new and deployment efficiency and overall cost are yet to be fully evaluated. For many industrial use cases, this category of spectrum can add extra boost to unlicensed spectrum with relative ease and moderate cost. We have witnessed a great deal of interest in CBRS in US, trial and early commercial deployments have been ongoing in many verticals.

Licensed Communications Service Provider/Mobile Network Operator (CSP/MNO) owned spectrum, while providing a very rich spectrum source, could be costly for enterprises when compared to unlicensed and shared spectrum. Nevertheless, a public spectrum business model is emerging that involves a public spectrum-for-private coverage value exchange, as providers are eager to engage their premium spectral holdings for private network cellular coverage. Internationally harmonized licensed spectrum is one of the important ingredients for MNOs to help them provide various applications and use cases to the Enterprise customer.

Industrial use cases that are deemed best implemented with private 5G have assumed use of millimeter wave (mmWave) range of spectrum (24 – 40 GHz). mmWave spectrum has the benefit of significant bandwidth in a limited geographic range. The opportunity for mmWave is especially relevant indoors where potential interference with a public network is minimized. The public spectrum-private coverage value exchange business model is especially relevant for mmWave. However, lack of mmWave supporting devices has been possibly preventing the market from fully evaluating effectiveness of mmWave performance versus unlicensed spectrum-based Wi-Fi 6 for indoor use cases. Some operators are performing value exchanges with private network owners for use of a public operator's mmWave spectrum.

2.1.2 Deterministic Behavior of System to Enable Higher Quality Connectivity

Improved determinism in system behavior usually leads to higher reliability and can be provided through many factors:

- Clean dedicated spectrum for a use case can provide interference protection from third party systems
- Improved scheduling mechanism in shared spectrum systems
- Improved data flow, buffering, and queuing discipline between application and network layers
- Fail proof reliability of all subcomponents
- Operational discipline to handle disaster recovery and scheduled maintenance

For most advanced use cases, such as industrial automation as in "factory of future", complete end-to-end system design is needed to ensure determinism. Cellular systems are more deterministic with predictable access delays, and therefore provide an upper hand for use of private cellular over Wi-Fi. However, with the advent of 802.11ax (Wi-Fi 6) this situation has changed, in the sense that more scheduled channel access management has been employed in Wi-Fi 6, increasing deterministic access, and, if applied in clean unlicensed spectrum (at 6 GHz, say), or in environments with strict device usage policy, for example on factory floors preventing usage of non-factory devices, then it is possible to reach the required levels of determinism needed for industrial use cases.

Other factors that can affect determinism when it comes to wireless connectivity is the end-to-end quality of connection. While scheduling mechanisms can enhance Over The Air connection quality, such as connection between the radio and user end points, other problems in the end-to-end application path can result in packet drops, delay, and jitter. As such, comprehensive system design and attention to end-to-end packet flow is needed to ensure quality.

Enterprises with mission critical use cases may also be considering parallel networks, such as a Wi-Fi network for their existing IT applications and a private cellular network for their mission critical applications that need strict resiliency and latency requirements that can only be met with dedicated clean spectrum. Given the trajectory of increased wireless demand, it is expected that both unlicensed and licensed bands will be in demand to satisfy various use cases in a few years. Alignment of these heterogeneous wireless network to enable end-to-end determinism across applications that use heterogeneous access networks is work in progress and is driven by use case needs.

2.1.3 Area of Coverage

Emerging enterprise physical footprints are varied and can include a combination of:

- **Campus** is a collection of buildings that are close enough to allow physical cable or fixed wireless connections. While indoor use cases for these campuses can be covered with Wi-Fi, outdoors remains a challenge for Wi-Fi due to its lower power profile. Larger, more powerful radios can cover broad outdoor spaces more efficiently. The private cellular coverage enabled by these radios can be part of a privately owned solution operated by the enterprise IT, or as a managed service offered by carriers.
- **Distributed remote sites** can be additional campuses, which need connection to the same Enterprise network. Each remote site can have indoor and outdoor needs like the main campus.
- **Branch offices** are smaller offices with limited connectivity needs but which also need to be connected to the main Enterprise IT network.

All combinations of the above are possible with locations spreading over municipal, national, and international

boundaries. Serving these locations with private cellular will depend on availability of fiber for direct wireline connection to the main campus, and/or through provider-based Wide Area Network (WAN) connections. In many use cases, carriers' presence and coverage capabilities provide opportunity to cost effectively extend the reach of the privately owned and operated option. Use cases that fall into diverse national and international boundaries must be considered in the context of local regulatory issues, including availability of spectrum in the geographical location and data privacy rules. Lack of uniform spectrum availability across multiple boundaries can cause a problem for multi-national enterprises that need to standardize on their enterprise architecture, tool usage, and compliance. Ultimately all the locations need to be brought under a security and access policy relevant for the enterprise use case.

2.1.4 Security

Any private cellular solution, be it privately owned and operated, or offered as a managed service, must be able to fulfill the requirements of the unique security policy of the enterprise. Enterprise data sovereignty is a high priority requirement and a major discussion in all private cellular considerations. Many enterprise IT managers prefer wired connections and even enterprise owned and operated connections to ensure data protection and prevent a costly data breach. Alignment of private 5G devices with enterprise identity management and access control engines is another key area of concern.

Additionally, enterprise IT managers prefer a single repository of user and device identity, so ideally the private 5G devices should be able to integrate with the enterprise identity engine and be able to get authenticated and authorized for access to enterprise applications in addition to the device authentication and authorization that is standardized by 3GPP. Other security concerns such as insertion of private 5G systems into the enterprise traffic segmentation policy, as well as integration with enterprise threat protection methodologies are also top of mind of enterprise IT managers.

2.1.5 Availability and Reliability

Most industrial and municipal venues that are considering private 5G tend to be a 365/24 operation, meaning that production or services are continuous throughout the year. Outages may have adverse financial or safety consequences (loss of sales, loss of security, delivery penalties, etc.). 5G technology and systems are designed to enable carrier-grade high availability and pervasive monitoring for reliability. As with security, many industrial venues have their own specific set of requirements for availability and reliability which need to be complied to.

2.1.6 Liability, Responsibility and Ownership

The responsibility and ownership of private cellular systems can become complicated in cases where not all components of the system are owned by one entity, e.g., spectrum and packet core may be offered by a CSP/MNO while the user end point and application may be owned by the enterprise. Liability and ownership issues surrounding these complex offerings may not be well understood by the market yet and may prove to be a roadblock for adoption.

2.1.7 Ease-of-Operation

Reducing complexity of operation of cellular systems and making private cellular system operation "as easy as" enterprise wireless networks is perhaps the most obvious ask from any enterprise IT manager who is considering private cellular. It is also highly desirable that these private cellular systems merge with, or at least align with, existing enterprise policy, security, and management systems. A related concern to operations is maintenance and support. Outsourcing maintenance and support to the vendors that provide the equipment is commonplace in enterprises. Providers of private cellular offers must be able to meet the support contract expectations of enterprises for their end-to-end offers.

2.1.8 Enterprise Considerations for Operating a Private Cellular Network

Having looked at enterprise requirements for any private cellular network, let's also summarize how an enterprise would go about evaluating and integrating a private cellular solution. These considerations are part of all private cellular deployment decision points.

2.1.8.1 Use case considerations

This is by far the most fundamental question to be answered when deciding on a private cellular deployment. A complete use case definition should include:

- What problem is being intended to be solved? E.g., operation of heavy equipment in mission critical venues such as mining or manufacturing floors, or improved remote connectivity of rural residents for better healthcare and education, or security surveillance of critical infrastructure

- What are components of the solution? User End points, radios, applications, spectrum
- What spectrum ranges are needed, and can these be used by the specified equipment? If licensed spectrum is needed, then which CSP/MNO can be a provider?
- What are performance requirements for the use case? Throughput, latency,
- What are the physical characteristics of the deployment venue? Coverage distances, indoor or outdoor, etc.
- What the targeted users of the network? What domains of the enterprise will they need service in? Will they be limited to the enterprise campus(es), or will they need to move/roam in between enterprise and public domains? Will they need connection to both multiple wireless networks concurrently? If so, are there any multi-path requirements to enable their applications to move from one network to another seamlessly?

2.1.8.2 Business level considerations for choice of a deployment model

Some of the factors that a Non-Public Network (NPN) operator will have to consider when selecting a management and operating model are:

Financial models: Lowering cost and complexity of a private cellular network is the highest priority challenge for vendors and providers. While enterprises are willing to pay premium price for private cellular deployments that can highly serve mission critical venues, these venues might remain limited in scope and can be isolated from mainstream enterprise IT. Broader and more pervasive deployments might require cost of deployment to come closer to other options such as Wi-Fi 6.

Cost reduction can be done in many ways. In the case of standalone private cellular in a box models feature sets can be drastically limited and very basic management tools provided for basic operations. In this case, expansion of 3GPP features and support of future releases, and integration with overall enterprise network, particularly for large multi-site enterprises, may prove challenging. In the case of cloud hosted models, 3GPP complexity can be offloaded to a cloud provider while capabilities such as low latency can be implemented using an edge platform on enterprise premise.

In these models, 3GPP-related feature and compliance support is centralized in the cloud provider, and as such, a significant amount of complexity is removed from enterprise IT. This level of simplification, together with subscription-based service pricing, may be attractive to many enterprises who are also considering moving other enterprise services into the cloud.

The macro slice model is by far the simplest from the enterprise deployment perspective. In these models, an expert group of cellular operators thoroughly familiar and adept in 3GPP specifications, take on the private cellular service offer. The only issue for these macro slice models is ability of the provider to fulfill highly demanding, and therefore costly, SLAs needed by the enterprise.

Support models: Who is ultimately responsible for quality of service? The standalone and cloud hosted models leave control of service quality by and large to the enterprise IT. For the macro slice model, CSP/MNOs have the Operations Support Systems (OSS) that can be extended or, if necessary, instantiated for specific deployments. This is particularly true for enterprises that already take advantage of other carrier services such as broadband fiber, Enterprise VPN, and others.

Being able to have a holistic troubleshooting view of the network for root cause analysis and remediation has a significant advantage, reducing mean time to repair and providing service continuity across the enterprise. This becomes even more critical in the case of large enterprises with complex WAN topologies. On the other hand, many existing enterprises already have a set of methods, tools, and mechanisms for performing these functions in their networks and will want to integrate the new 3GPP network into their established systems.

Data confidentiality and other security requirements: The ability to control which data stays local and control of devices and applications can both play a significant role in the decision to adopt a private deployment model. The standalone models are perceived as perhaps the most secure, however, it is increasingly clear that no amount of system isolation can provide enough security. Therefore, to satisfy cybersecurity sensitized enterprise IT, all three models need to provide a complete security framework for their implementation together with guidelines for integrating new private 5G service into enterprise IT security policy.

2.1.8.3 Consideration for Integration with existing enterprise network

Enterprises with established and complex networks (often with Wi-Fi as the primary wireless access), will need to address integrating an operator led model into their existing IT practices once they decide to add private cellular to their existing network. Example considerations for this type of integration include:

- **Network Security/Traffic segmentation:** How to integrate provider services into enterprise specific access control, traffic segmentation, and other enterprise led security monitoring and protection methods.
- **Identity and Access Management:** How to use enterprise identity engine to authenticate and authorize private cellular devices and services.
- **Device management:** How to enable enterprise IT to monitor and manage private cellular devices, particularly when the provider has full control over device life cycle management and health, but these processes need to be controlled by enterprise IT.

2.2 P5G deployment models being considered by enterprises

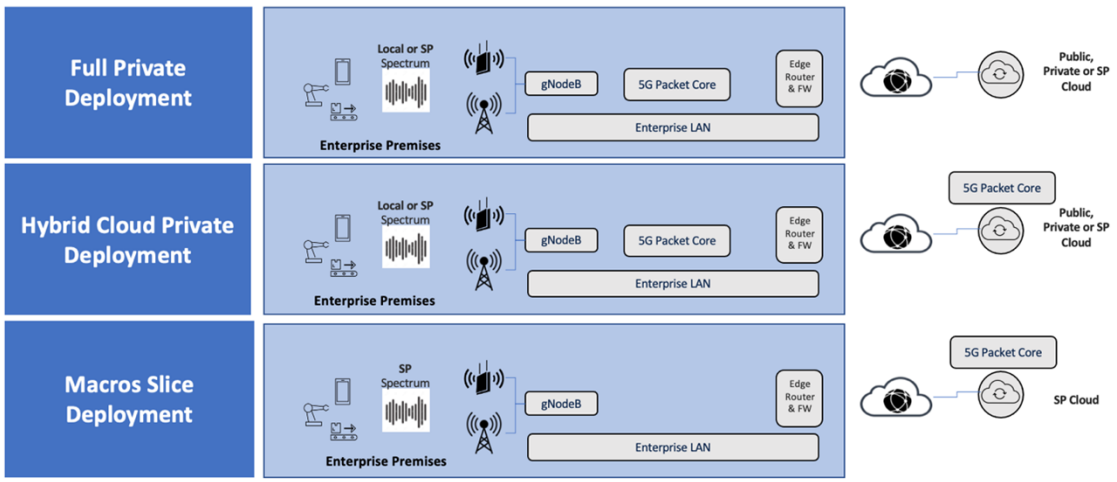
There are multiple ways to implement a 5G solution, including building and operating your own private network, contracting an MSP (Managed Service Provider) to install and operate a private network for you, or contracting with a CSP (Commercial Public Network Service Provider, aka "Mobile Network Operator" (MNO)) for general 5G service or a private network slice. There are advantages and disadvantages of each option, from a cost, complexity, and performance perspective.

For example, a healthcare facility operating its own 5G network has advantages that can be customized to meet its needs, such as the securing of data without leaving the premises, as well as no limits to data usage. On the other hand, the network may be limited to the coverage area that has been built, unless a roaming agreement is put in place. The same healthcare facility can contract a CSP/MNO to provide private cellular service through a nationally deployed network. Ideal solutions may involve a combination of offers depending on specific use cases.

Fortunately, there is a growing list of vendors that are optimizing complete solutions for the enterprise user, which vary in cost and capability to meet the exact needs of the enterprise.

As of today, there are three general deployment models that are trending in the market. Each model can have multiple variations and other models can still emerge. These current primary models are depicted in Figure 2.

Figure 2: Private Cellular Deployment models trending today



2.2.1 Standalone private deployment

In this model, a small standalone cellular network, complete with radios using leased or shared/local spectrum, packet core, user end points, and associated management and operations tools and applications, is integrated into the enterprise LAN and managed by enterprise IT or a system integrator service provider. There is usually minimal to no integration of this network with other enterprise network components, security and management of this private cellular network is usually handled independently.

Private 4G LTE networks have been, and continue to be, deployed using this model in venues that need cellular connectivity but lack cellular coverage through major providers, such as in mining. This model is being considered as the first option in many new private 5G deployment considerations. Most early proof of concept and trial deployments use this model to evaluate use case maturity and deployment possibilities. Larger more complex deployments, for example multi-site enterprises with multiple use cases for private cellular, may find this model limiting and too complex.

2.2.2 Hybrid cloud private deployment

Cloud hosted private deployment models have been emerging for the past few years as a response to enterprise demand for reduced complexity in managing a standalone private cellular network. In these models, a portion of the private cellular network is placed on the enterprise premise, on an edge platform, and managed remotely through the cloud. The exact mix of what stays on the premise and what is on cloud can differ depending on the architecture.

In the most basic case, the radio and user end points are on enterprise premises and packet core and management applications are in the cloud. Another option is to place the packet core, or key components of a virtualized packet core such as the User Plane Function (UPF), on premise. With each variation, demand for throughput and latency dictates the final deployment architecture, in both Over the Air (OTA) as well as end-to-end scenarios, as data traverses the cloud. Flexibility that is introduced through 5G virtualized packet core and edge platform enhancements allow for these models to be designed in innovative ways.

The cloud hosted options are attractive for enterprises as they can offload complexity of operations of a standalone cellular network to the cloud provider operator. However, they suffer from the same drawback as the standalone models, as they depend on leased or shared/local spectrum availability, unless enterprises or system integration partners own spectrum that can be used in these models.

2.2.3 Macro Slice deployment

The Macro Slice deployment model is where an CSP/MNO dedicates a "slice" of their existing commercial cellular network to an enterprise. A slice can include a set of radios, spectrum bands, fiber network capacity, 5G Core, and other collaterals as defined by the CSP/MNO. In this model, the operator will continue to operate the slice of the network that is dedicated to the enterprise for a cost and will integrate the slice into the enterprise network enabling the enterprise to co-manage the slice through CSP/MNO operations portal that will be offered.

The level of control, security, and management of the slice is specified and agreed to through Service Level Agreements (SLA) that will be made between the provider and the enterprise. While SLAs can be customized by each provider for each enterprise customer, a generic SLA template has been defined to provide a framework for these agreements (Generic Slice Template 2.0). This Macro Slice model is very exciting as it can open the vast resources of cellular providers: spectrum, footprint, coverage, expertise, to enterprises. However, it remains to be seen how providers can successfully monetize this model as it may be in direct competition with lucrative consumer cellular use cases that providers traditionally prioritize.

Slicing is covered in more detail in 5G Americas' white paper, Commercializing 5G Network Slicing.

2.3 P5G functionality defined in 3GPP

3GPP Release-16 introduces two specific sets of capabilities for private networks:

- **PNI-NPN:** "Public Network Integrated - Non-Public Network" is a 5G network assigned for private enterprise use, which nevertheless enables people and mobile objects to maintain connectivity outside the 5G network, (e.g., campus, industrial site, or hospital) by accessing the public network. PNI-NPN interfaces are defined clearly by 3GPP and a PNI-NPN can be run from the cloud. Slicing allows CSP/MNOs to separate and dedicate a portion of their RAN, packet core, and transport network resources to an enterprise. The enterprise slice can be permitted or restricted from various service aspects including roaming. 3GPP defined mobility restrictions can be used to bound a private service offering.
- **SNPN:** A 5G "Standalone Non-Public Network" differs from a PNI-NPN in that it is completely isolated, with no connectivity outside of the 5G network. SNPNs generally come at a higher cost, since all the hardware and software need to be deployed and operated on site. This is not the case for PNI-NPNs, which can be run from the cloud.

These 3GPP Release-16 definitions and their refinement going forward into future releases will enable different deployment models, as described above. In the following sections we will go through considerations that apply to all deployment models.

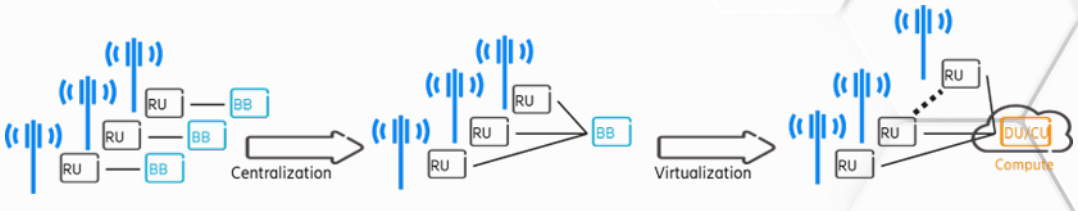
3. RAN Considerations for Enterprise Deployment of P5G

Complexity of a cellular Radio Access Network (RAN) is one of the major roadblocks for faster adoption of private cellular technology in the enterprise. Enterprise IT are used to the ease of deployment of Wi-Fi and expect a similar level of ease for a private cellular deployment. As such, effective and efficient design of a Radio Access Network, which can also be easily operated by enterprise IT, is perhaps the most fundamental part of any private cellular network design. While 5G's set of technology enhancements have been very focused on improving the radio, ease of use, flexibility, and enterprise "friendliness" that is expected for private use is still a work in progress for 3GPP and other standard bodies.

Technically speaking, the RAN technology segment has been undergoing similar disaggregation and virtualization transformations as seen in other cellular components such as the packet core. These transformational architectures are covered in various industry forums under topics of disaggregated RAN, Virtualized RAN, Distributed RAN, or open RAN, versus traditional RAN. These trends are allowing a more flexible RAN architecture to emerge where logical RAN components can be separated from physical components and placed on compute platforms in different configurations. This increased flexibility can eventually provide benefits for both public and private cellular deployments. Many of these topics are still in development.

RAN disaggregation and virtualization is covered in more detail in the 5G Americas white paper "Transition Toward Open and Interoperable Networks". Table 1 briefly summarizes RAN evolution trends that are now culminating in virtualized RAN.

Figure 3: Radio Access Network evolution



Enterprise	Distributed RAN	Centralized RAN	Virtualized RAN
Rationales	• Reduce transport cost • Smaller outage units at equipment failure • Reduced latency for end-user services • Data centers are limited by floor space and power supply	• Pooling of hardware resources (optimization) • Fewer nodes/sites leading to reduced CAPEX/OPEX • Competence consolidation • Energy efficiency	• Vendor agnostic comericial off-the-shelf (COTS) hardware to enable innovation across a range of a software ecosystem
Benefits	• Flexible backhaul • Use at most locations and scenarios	• Maximum radio coordination • Flexible baseband configuration and dimensioning/pooling	• Virtualization on General Purpose Processors (GPP i.e., x86)
Challenges	• Baseband dimensioning	• Strict delay requirements (i.e., fiber fronthaul) • Fronthaul/baseband single point of failure	• GPP inefficient for real time baseband processing (~1/10) • Diminishing returns on pooling

In the following sections we will take a closer look at RAN needs of enterprise and how RAN virtualization can benefit private 5G deployments for the enterprise.

3.1 RAN Requirements for Private Cellular Use

Industrial private network use cases present different challenges to the RAN compared to the usual mobile broadband application use cases that are focal point of commercial cellular.

3.1.1 Coverage

Even though many private networks are currently deployed as outdoor networks, many deployments are expected to focus on campus area and indoor coverage in the future. Indoor areas may include factory floors and warehouses with high ceilings, large open spaces, and large metal infrastructure that are used in production lines. Installing radio antennas in high ceilings can cause cell coverage to extend over the desired area, outside of the building, and interfere with adjacent cells that may be active in the neighborhood. Intercell interference can also occur in large open spaces as in warehouses which lack walls to limit cell coverage.

Another challenge of industrial indoor scenarios is the presence of metal infrastructure or equipment that can block propagation of radio signals and cause dead spots. In scenarios involving moving robots or automated guided vehicles (AGVs), dead spots can appear dynamically as the AGV, or robot moves. In a similar way in factories, the reorganization of a production line implies moving metal equipment that can block the radio signals and change the cell coverage. These complexities are usually studied carefully during an initial “site survey” to determine how cellular radios can be installed effectively, and continued monitoring will be necessary to ensure optimal signal availability for demanding applications.

3.1.2 Device-centric use cases

Private cellular deployments usually include fewer devices that need higher throughput and lower latency performance to serve demanding industrial applications, whereas in mobile broadband cases there are larger number of devices dealing with people-oriented applications that are not as demanding. This focus on demanding applications on a single device will require a different way of tunning of spectrum and radio being used than is normally done in commercial people oriented cellular environments.

3.1.3 Performance per device

QoS requirements for data paths from different vertical scenarios, use cases, and applications vary for each vertical. There may be multiple demanding data paths in play for control of complex machinery, as for example in mining or manufacturing. The available radio and spectrum must be tuned to satisfy these data paths to achieve effective performance. For example, many private network applications may need higher uplink throughput than is normally allocated in commercial cellular networks, and this implies a different radio and spectrum allocation for private network use than for commercial network use. Also, low latency and redundancy requirements are more demanding in private networks than in commercial networks.

3.1.4 Enterprise-friendly profile

Enterprises are typically looking for an easy-to-deploy, easy-to-integrate, and easy-to-maintain type of solutions that are designed to allow and deliver sustainable business value, and scale as they need. In many public venues the size and appearance of the radio antenna can also play a role in decision making.

3.1.5 Enterprise owned and operated radios

Many enterprises are considering private cellular deployment as an opportunity to consolidate all active radio collaterals on their premises into one offer that is owned and operated by the enterprise.

Removal of CSP/MNO managed Distributed Antenna Systems (DAS) and transfer of DAS functionality onto privately owned and operated radios is top of mind for many large enterprises that require CSP/MNOs to install DAS systems in their campuses. In these scenarios a Neutral Host configuration, where the enterprise can serve various CSP/MNO subscribers and route the CSP/MNO traffic through enterprise owned radios is highly desirable. Radios that can support multi-tenant and sharing features (MORAN and MOCN) are increasingly attractive options for private deployment.

3.1.6 Transport considerations

All wireless systems will have to eventually be supported by a wireline network, as every radio connects to some wire. Availability of rich and flexible wireline for enterprise use is a critical consideration that sometimes does not get noticed as early as it should during considerations.

3.2 Spectrum Related Requirements

5G Radio-access technology can be deployed in two frequency ranges:

- **Frequency Range 1 (FR1):** 450 MHz – 7.125 GHz, commonly referred to as "sub-6 GHz"
- **Frequency Range 2 (FR2):** 24.25 GHz – 52.6 GHz, commonly referred to as "millimeter wave"

Different frequency bands have complementary characteristics, with low bands being ideal for coverage and availability and having the most diverse device support (though with typically smaller bandwidths), mid bands offering significantly improved capacity with a good balance of coverage, and high bands delivering a major capacity boost (though with limited coverage).

There are two types of LTE Frequency Bands - FDD and TDD. "FDD" stands for Frequency Division Duplex, as each of the FDD-LTE bands consist of a pair of frequencies, one for the uplink and another for the downlink. On the other hand, TDD (Time Division Duplex) LTE bands require only a single band which is used for both the uplink and downlink.

For TDD bands, there are trade-offs to consider between capacity, latency, and coverage, depending on the choice of the TDD transmission pattern. Additionally, when using a TDD band, an important aspect is synchronized TDD patterns with respect to networks on the same or adjacent spectrum. The mmWave bands have better isolation than mid-bands due to the radio wave propagation characteristics and, consequently, have relatively relaxed TDD coexistence constraints.

Private wireless networks will be deployed in frequencies allocated by regulators in various countries and network radio nodes will comply with power level authorized by the regulators. The choice of radio network solution can vary according to deployment choice.

Radio Units (RUs) typically supported include 2T2R, 4T4R, 8T8R, 32T32R, 64T64R and are selected for deployment based on throughput and coverage requirements. RUs are expected to support full instantaneous Bandwidth (biwa) and occupied Bandwidth (oBW) with the solution supporting both contiguous and noncontiguous channels. Channels will be deployed in 5, 10,20,40, 60, 80, 100 MHz bandwidths for FR1 bands.

Harmonizing the use of spectrum bands across geographies is essential to achieving mass-market conditions which in turn enables cost-efficient and competitive industrial devices. The mobile wireless communications industry has flourished with each generation of technology in part due to the international standards and internationally harmonized licensed spectrum allocations. The approaches to spectrum allocations differ widely between regulators, and the allocated bands are in some cases shared with incumbents. 5G Americas has been consistent in advocating for more internationally harmonized licensed spectrum for the mobile wireless communications industry to support the various applications and use cases as the industry enters the 5G era of innovation. Enterprises can acquire spectrum directly from CSP/MNOs or in some countries directly from the government/regulators. The CSP/MNO allocated spectrum can be limited and could possibly have cost constraints causing the enterprise to not be able to acquire enough spectrum to match their actual requirements.

Spectrum options for enterprises are described in Table 2.

Table 2: Spectrum options for use by enterprise

Public/Private LIcensed Spectrum	New Regulated Licenses	Unlicensed Spectrum
• Spectrum Use Agreements - Lease • Owned Spectrum (e.g., 600MHz, C-Band) • No interference, most secure, reliable • Unique CSP/MNO asset if owned • Monetizable value, SLA ready • MOCN/5G slicing	• CBRS GAA (rules based unlicensed) • CBRS PAL (licensed owned) • 900MHz (realigned 6MHz) • New, but subjected to limits • Highly reliable, strong value, low chance of limits, SLA potential • Mostly focused on utilities	• 2.4, 5, 6GHz (also some mmWave) • Freely available • Useful, but can't offer full SLA • Risk for costly outages • Extra high-capacity cases with LAA, carrier aggregation • Lowest cost alternative, best effort

Local spectrum can facilitate the access to the spectrum required by industries, but with certain limitations:

3.2.1 Availability of Devices and Chipsets

Regarding the locally licensed/leased spectrum considered by administrations, these diverse allocations pose challenges to building a device ecosystem for industrial applications. Device chipsets need to be supported not only by an ecosystem of traditional mobile broadband devices but also by an ecosystem that includes industrial devices of varying complexity on different spectrum bands.

3.2.2 Suitability of the Spectrum for the Required Application

Unlike mobile broadband, the industries' connectivity needs are extremely diverse. Requirements can go from low throughput and long battery life devices to time-critical communication for data delivery within specific latency targets with guaranteed levels. Because frequency bands have different characteristics which can make them more suitable for one application or the other, it is important to understand if the local spectrum available matches the enterprise requirements. As an example, FDD bands are better suited for Cat-M/NB-IoT access but are not usually available to enterprises as local spectrum.

3.3 RAN Offers for Private Cellular Use

There are variety of radio solutions available for supporting 5G RAN deployment.

3.3.1 All-in-One (AiO) Small Cells

These are indoor or outdoor units where the Radio and Baseband functions are integrated within a single unit. The output Effective Isotropic Radiated Power (EIRP) of these units can range anywhere from 1W to 20W and are usually deployed in indoor venues for indoor coverage or outdoor environment to provide additional capacity or address coverage issues from macro radios. These small cells connect directly to the core network.

3.3.2 Classical RAN

This type of radio access network constitutes Distributed RAN Micro/Macro Remote Radio Head (RRH) with Common or Enhanced Common Public Radio Interface (CPRI/eCPRI) to Baseband Unit (BBU) Distributed Unit/Centralized Unit (DU/CU), where the Radio Unit (gNB RU) and baseband unit (gNB DU/gNB CU) are separate entities with an Ethernet-based eCPRI connection between them.

A wide variety of radio solutions, including low, medium, and high-power operations are supported. The gNB DU/CU functionality is hosted in vendor specific custom hardware platform. The capacity and scaling differ from vendor to vendor and is widely used in current deployed CSP/MNO networks worldwide. Vendors can leverage their innovation to support variety of functionalities to provide better spectral efficiency and optimal usage.

3.3.3 Virtual RAN

This type of radio access network constitutes RAN RU (Remote Unit) with eCPRI to virtual Distributed Unit (vDU), RAN RDU with F1 interface to vCU. The gNB DU, gNB CU functions are virtualized to run on a Commercial Off-the-Shelf (COTS) hardware platform, where the Radio Unit (RU) connects to gNB vDU via Ethernet-based eCPRI connection. The gNB vDU further connects to gNB vCU.

For certain deployments, the RU and DU functionality is often built into a single entity within a physical box and can be made to connect to gNB vCU via F1 interface. Typically, a vDU will support multiple RUs and vCU will support multiple vDUs making scaling of the solution fit for purpose. The actual capacity of the solution varies according to the OEM. The RAN RU, DU, CU functionality/solution is provided by same vendor in classical RAN and Virtual RAN solution. Where applicable, virtual RAN components can also be deployed on Cloud Infrastructure.

3.3.4 Open RAN

This constitutes disaggregated RAN functionality built using open interface specifications, defined by Open RAN organizations, that can be implemented in vendor-neutral hardware and software-defined technology based on open interfaces and community-developed standards. O-RAN Alliance is an example of a specification group defining next generation RAN infrastructures, empowered by principles of intelligence and openness. O-RAN standards-based deployments allow use of RU, RDU and vDU/vCU from different vendors where RAN RU and DU interworking is standardized according to IoT profile for a given Radio type. The vDU, vCU functionalities are often containerized and can be hosted in a variety of platforms (COTS, AWS, Azure, Anthos) subject to testing and conformance supported by the provider. FCAPS/Orchestration support is provided through O1 and O2 interfaces.

All vendors generally comply to 3GPP compliance and advanced software features. Some key attributes which are generally evaluated while considering the radio node include:

- Compact form factor with carrier grade reliability
- Aesthetic appearance (ease of zoning)
- Power Over Ethernet and backhaul
- Timing Over Packet IEEE 1588V2, External GPS support
- Integrated/external antenna
- Indoor and outdoor hardened, IP65/IP68 Rated
- iBW/oBW fit for purpose
- Power level, with permissible EMF exposure for installation at a given height
- Single/dual and multiband support
- Ease of installation and options (wall mount, book mount, ceiling mount, pole mount etc.)
- Plug and Play
- Secure and reliable operation, Operations and Maintenance (O&M)
- Mean Time Between Failures (MTBF) and Mean Time to Repair (MTTR) within industry norms

Future RAN enhancements expected in 3GPP Releases 16, 17, 18 include:

Mobility enhancements:

- Conditional handover for improved robustness
- Mobility solutions for reduced handover interruption time
- Fast failure recovery mechanisms
- Slim mobility for fast cell switching
- Machine learning for mobility

Dual Connectivity, Carrier Aggregation (DCCA) enhancements:

- Early measurement reporting
- Secondary cell activation time improvements
- Conditional SN addition and change for fast access
- Activation of secondary cell group

3.4 RAN Virtualization and Relevance to Private Cellular

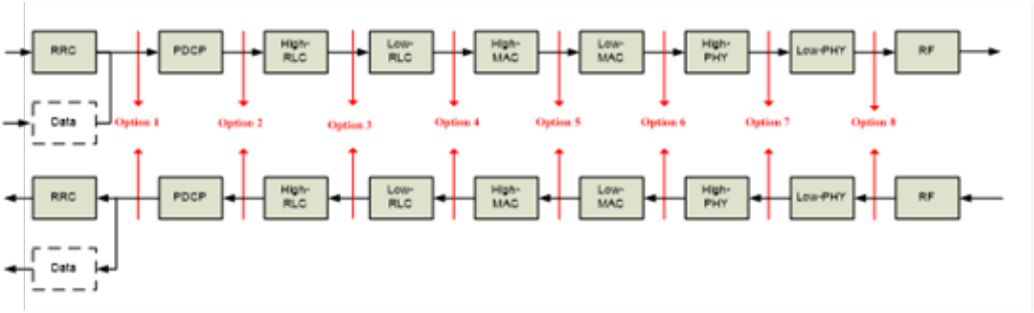
The Radio Access Network has traditionally been a closed and complex system with its own multi-layered architecture, each layer being responsible for various aspects of radio signal processing. With RAN disaggregation and virtualization this closed system is being opened and modularized to enable a more flexible system that can leverage cloud computing, scale in many different forms and eventually lower cost for consumer and operator.

With disaggregation, the full RAN processing set of functions, which are traditionally built into an all-in-one gNB, can be split at different functional layers, disaggregating the architecture into a Radio Unit (RU), DU (Distributed Unit) and CU (Centralized Unit). Each of these units can then constitute different hardware or software components of the overall RAN system with the option of being placed in separate locations in the architecture at various scales, e.g., multiple RUs can be served with a single DU/CU.

3.4.1 RAN Split Options for Enterprise

Each split type has its own pros and cons which RAN experts have been analyzing and debating for several years. Figure 4 summarizes different potential splits.

Figure 4: Functional Split options for disaggregated RAN architecture



Splits 2, 6 and 7 are gaining traction thanks to the support of strong associations like 3GPP, Small Cell Forum and O-RAN Alliance.

The key question here is which type of architecture should we use for a specific private network deployment. To solve this, we need to understand the pros and cons for each split in the context of enterprise deployment. There are two main metrics here: transport requirements and features supported.

On the transport side, the lower the split used, the higher the bandwidth and the lower the latency requirements. If we look at Split 7.2, having a 2.4 Gbps radio cell throughput will translate to four times more bandwidth required (using BW 100MHz, 30KHz SCS, 256QAM, 16 Ant Ports, 4 layers, Block Floating Point compression). Lower layer splits also drive tighter transport latency requirements, with Split 7.2 typically requiring less than 200µs for LTE based RANs.

On the feature side, the lower the split, the more advanced features supported such as Dual Connectivity (L3), Carrier Aggregation (L2) and Up Link Coordination Multipoint (L1). Split 7.2 can support all the features, Split 6 can support CA and DC and Split 2 will support only DC. AiO gNB won't support any of these features since there is no disaggregation of the software. Split 8 (CPRI) could support all three features but given the short latency and high bandwidth requirements, it would be hard to group many radios.

Looking at these factors, we can start matching some specific use cases to RAN functional splits. For example:

- **Large venues** (e.g., football stadium) are best served with Split 7.2 which will reduce the interference between radios, it will also allow to group radios as one single cell using the O-RAN defined Fronthaul Multiplexer (FHM).
- **High number of indoor radios** (e.g., factory floors) are best served with Split 6 or Split 7.2. Depending on the transport capabilities, Split 6 will reduce the need of having optical fiber and provides a good set of inter-cell features like Carrier Aggregation (CA) or Downlink Coordinated Multi-Point Transmission/Reception (DL CoMP). If Uplink (UL) interference mitigation is required, then Split 7.2 would work best although increasing transport requirements.
- **mmWave deployments** are best served with Split 2. The radiation pattern of mmWave signals is very short, so the primary need involves creating narrow beams to increase its coverage. There is no need to go to low layer splits since the transport requirements will increase significantly with a minimum performance advantage. Therefore, a Split 2 should be sufficient for this type of deployment.
- **Scatter outdoor deployments** are best served with Split 2 or AiO gNB. VRAN can reduce the overall cost of the solution where there is a high resource pooling, meaning that many radios are connected to the virtual infrastructure (CU/DU). If just a few radios are connected to the DU or CU, the price of the overall solution increases due to the price of the servers. Therefore, for a scatter outdoor deployment, a high-level split is preferred. In this way, the latency requirements of the transport are much more relaxed (>10ms, assuming this can meet use case latency requirements), allowing many radios to connect to the CU and decreasing the overall cost of the deployment. There is also no need to support advanced features due to the scatter nature of the deployment, where there is little interaction between cells.

In summary with a virtualized RAN, it is possible to move every RAN functional component freely in the network to suite enterprise requirements. Other considerations for these moves include:

- Organizations and responsibilities within the enterprise
- Long lease-terms for sites infrastructures
- Cost for network redesign when functions move in the network for future virtualization

Given the flexibility and multiple variants of virtualized RAN, there is a need for selection guidelines and reference solutions to support the right choice for deployment and accelerated service delivery. Most networks will likely consist of a combination of both distributed and centralized RAN deployments, mainly depending on availability of transport and capacity/performance needs.

3.4.2 Challenges of RAN Virtualization

RAN virtualization presents several significant challenges as the processing and timing requirements are very high on certain critical functions in the lower parts of the RAN stack. Table 3 compares vRAN with a pre-integrated purpose-built All-In-One gNB solution that is delivered today:

Table 3: Virtualized RAN vs. Purpose built RAN

Rationale/ Benefits	Purpose-built RAN	Virtualized RAN
Efficiency	Purpose-built RAN hardware will likely provide a higher level of efficiency in terms of size and power consumption. This is due to the optimization of network functions that are implemented in custom hardware rather than on generic processors.	A fully virtualized RAN could bring significant benefits of harmonization: one single uniform hardware platform across the core network, RAN and edge. This could simplify the management of the complete network, reducing operations and maintenance costs.
Cost	The cost of custom-built hardware will be lower compared to vRAN. However, over its lifetime, a COTS-based platform could become increasingly cost efficient due to hardware manufacturing volumes across multiple industries.	In vRAN, the network functions are separated from the processing hardware. This means that RAN network functions from multiple vendors could run on the same shared hardware. In sharing use cases, the hardware could even be shared between service providers.
Integration	The purpose-built RAN solution is a verified and pre-integrated end-to-end system, whereas in many cases, a virtualized system—if not procured from a single vendor—will require additional system integration efforts and costs that need to be considered.	vRAN offers an opportunity to embrace established solutions, available in today's public cloud technologies, for non-RAN-specific functions. By agreeing to use industry-established components for common tasks, the need for costly adaptations of vendor-specific solutions can be removed. If this is achieved, it can allow the RAN ecosystem to focus on business-critical components.
Flexibility	In a pre-integrated end-to-end solution from a single supplier, the system performance accountability is preset but clear. With a virtualized solution—comprised of hardware, software, and service elements from multiple suppliers—accountability needs to be clearly assigned.	A vRAN holds the promise of increased flexibility as functionality and capacity could be more easily deployed where and when required. Cloud technologies can facilitate this type of flexibility.

A widely adopted open platform will lower barriers for cross-domain innovation, facilitating the development of new use cases and services. However, the question remains if and when potential operational benefits and flexibility offered by vRAN for private networks can outweigh and compensate for the hardware, power, and system integration costs, while attaining the same high level of system network performance. One key aspect will be the cost evolution of custom-built hardware compared with generic COTS hardware and the emerging COTS-based accelerated compute platforms.

3.4.3 Shared Cell, Shared ORU, and Potential Relationship to DAS

Shared Cell and shared Open Radio Unit (ORU) are enhancements enabled by RAN virtualization which can improve Distributed Antenna System (DAS) deployments in enterprises. Shared Cell is defined as the operation of the same cell over multiple RUs. Benefits of shared cell include:

- Cost-effective scaling of deployment by enabling increasing coverage without the need to scale base band processing capabilities
- Improved mobility experience by eliminating interruption time and reducing signaling overhead when users move within the shared cell

Front Haul Multiplexing (FHM) is one of the implementation modes supported on O-RAN Alliance split 7.2. FHM is a third-party element which copies and forwards the data packets to the different RUs in the downlink and combines them in the uplink.

Figure 5: Fronthaul Multiplexing

Shared O-RU is supported on O-RAN Alliance Split 7.2 and can be seen as blurring of the boundary between RAN and DAS, enabling an O-RU to operate with multiple O-DUs, where those O-DUs can be operated by separate CSP/MNOs.

- First included in version 10 of O-RAN's Open Fronthaul specification, shared O-RU includes support for neutral-host deployments and enhanced role-based access control for individual tenants.

The combination of shared O-RU together with Shared Cell features can dramatically decrease the cost of deployment compared to DAS and provide a superior performance thanks to the multiple cell deployment, which increases capacity.

3.4.4 Private Versus Public Spectrum and MOCN/MORAN Features

Public networks have two options with regards to sharing RAN infrastructure to make the economics of indoor or outdoor deployment more appealing: MOCN (Multi Operator Core Network) and MORAN (Multi Operator Radio Access Network). MOCN is fully defined by 3GPP and enables a common cell/frequency to provide coverage for multiple operators. With MORAN, each operator uses a unique cell/frequency to support their service. This means radios for MOCN deployments are simpler but negotiating third-party access to dedicated spectrum is more complex. In contrast, the radios for MORAN deployment are more complex, but there is no need to negotiate third-party access to dedicated spectrum.

A Neutral Host solution is similar to MOCN, but instead of using an CSP/MNO licensed frequency, a shared access license is used, such as Citizens Broadband Radio Service (CBRS) in the United States. In this example, the cost of deployment and management lies with the system integrator or the venue. These entities deploy a small-scale private network to provide indoor or outdoor coverage, with the option for CSP/MNOs to connect to it and offer their services. This accelerates indoor and rural coverage by passing the economic burden of deployment to a system integrator, with CSP/MNOs connecting to these networks by paying a monthly fee.

In another approach, with O-RAN's newly defined shared O-RU capability or Small Cell Forum's (SCF) network Functional Application Platform Interface nFAPI service, the neutral host can deploy a shared O-RU (or SCF Physical Network Function (PNF)) and enable simultaneous operation with the O-DUs or SCF Virtual Network Functions (VNFs) of different operators. Here the deployment is more like MORAN, as each operators' O-DU is used with a dedicated cell using the operator's own spectrum.

3.5 Transport Considerations for Private RAN

There are many technologies that have traditionally been used to create the Transport Networks of CSP/MNOs. Many of these have been focused on transporting large volumes of traffic over long distances with minimal delays – the so-called ideal transport (3GPP TR 36.932 sec 6.1.3). Private Networks may not have access to ideal transport due to several factors, including availability and accessibility, costs, time to deploy, and more.

A number of alternative transport technologies have been considered for Backhaul, Midhaul and Fronthaul (see "Innovations in 5G Backhaul Technologies" and these could be used for deployment of Private Networks. These technologies include:

- Integrated Access and Backhaul (IAB)
- Hybrid Fiber Coaxial Cable (HFC)
- Ethernet
- Passive Optical Networks (PON)

Proof-of-Concept studies for vRAN fronthaul that covered Non-ideal transport technologies have also been performed, for example by Telecom Infra Project (TIP). PON, HFC,

and Ethernet have been shown to be viable transport technologies for vRAN Midhaul Upper Layer Splits (ULS) and, with some enhancements, even Fronthaul Lower Layer Splits (LLS).

The availability and capabilities of the various transport technologies will factor into which RAN split options can be used on a given deployment. Key deciding factors will be bandwidth, latency, and jitter requirements of the RAN split option and if the available transport technology can meet them. In the following sections we investigate some of these transport options.

3.5.1 Integrated Access and Backhaul (IAB)

The key concept of IAB involves re-using the existing spectrum of the 5G New Radio (5G-NR) access link for the backhaul as well, by efficiently multiplexing access and backhaul in the time, frequency and/or space domain. Two key use-cases for this technology involves providing backhaul and extending coverage footprint, as shown in Figure 6 and Figure 7.

Figure 6: Providing wireless transport where no fixed transport infrastructure is available

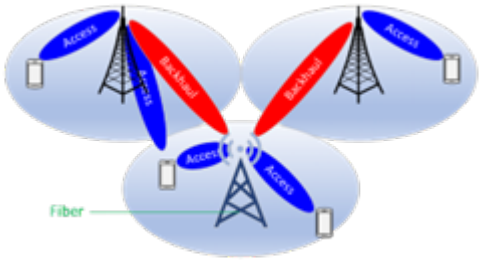
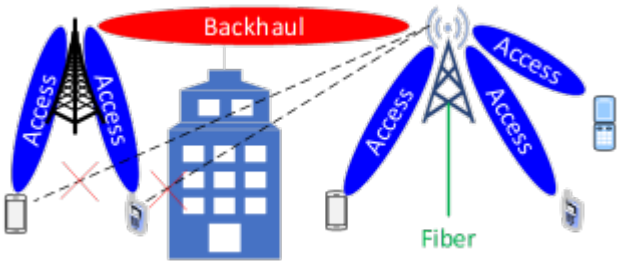


Figure 7: Deployment of gNB in locations of poor coverage using IAB backhaul



IAB has been studied earlier at 3GPP in the scope of LTE Rel-10, under the label “LTE relaying”. However, because the existing LTE spectrum was considered too valuable to be used for backhauling, only a few commercial deployments were ever done and those were limited to single hops.

IAB work in 3GPP was re-initiated in 2017 with a study item followed by a normative phase in Release 16. The key features to be supported by the first release of 3GPP IAB network for NR backhauling (Rel-16), are:

- **Multi-hop backhauling** to enable flexible range extension
- **QoS differentiation and enforcement** to ensure that the 5G QoS of bearers is fulfilled even in a multi-hop setting
- **Support for network topology adaptation and redundant connectivity** for optimal backhaul performance and fast adaptation to backhaul radio link overloads and failures
- **In-band and out-of-band relaying** for the use of the same (for in-band) carrier frequency or different (for out-of-band) carrier frequency for the access. An example is the link to User Equipment (UEs) and backhaul links (i.e., link to other network nodes) of the IAB node
- **Support for legacy terminals:** the deployment of IAB nodes should be transparent to UEs. For instance, no new UE features/standardization should be required.

3GPP Release-17 aims to enhance Release-16 IAB in terms of robustness, spectral efficiency, latency, and end-to-end performance.

Integrated Access and Backhaul (IAB) is a promising transport solution for private networks, especially where mmWave bandwidth is available. While IAB can be used in FR1, the main focus is on FR2 where there is less contention for bandwidth by access and backhaul. Therefore, of key interest is the use of IAB in conjunction with unlicensed spectrum such as NR-U on the upper end of the FR1 band (5GHz-7GHz), and V and E bands (60GHz-80GHz) in the mmWave/FR2 band.

For the United States, the Federal Communications Commission (FCC) is also looking at opening the Lower 37GHz Band for shared usage and is currently investigating coordination schemes for such sharing.

As mentioned previously, IAB multiplexes access and backhaul in three domains: time, frequency and/or space. The use of Orthogonal Frequency-Division Multiple Access (OFDMA) in LTE and 5G-NR is well suited to provide multiplexing in the time and the frequency domain. In addition, the use of beam steering capability in massive MIMO radio solutions may be used to provide spatial separation between the backhaul and the access allowing multiplexing in the space domain and increasing spectrum efficiency.

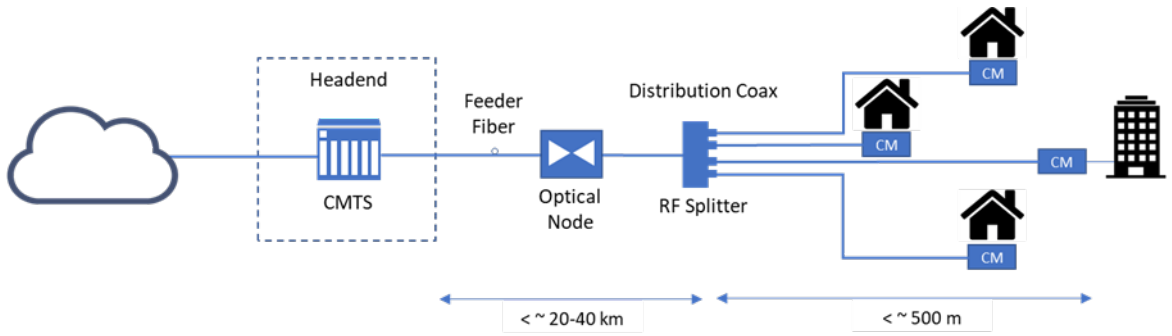
A wireless backhaul solution, such as IAB, allows the rapid deployment of a cellular network, without having to lay down a fixed transport infrastructure or, at least, delaying the costly investment of laying down a complex infrastructure. In this way, IAB facilitates and reduces the costs of private networks and enterprise deployments, particularly where cellular coverage is needed for low traffic or low bandwidth use-cases, such as sensor networks, IOT, and small numbers of subscribers/ customers/devices.

3.5.2 Hybrid Fiber Coaxial (HFC)

One of the most ubiquitous transport technologies in North America is Hybrid Fiber Coaxial. HFC networks have been deployed by many cable operators, sometimes referred to as “Multi Service Operators” (MSO).

A high-level architecture of a HFC network can be found in Figure 8.

Figure 8: HFC/DOCSIS Network Architecture



HFC networks use fiber optic technology to transport video, voice, and data traffic from a centralized headend (or data centers) to optical nodes located in the surrounding neighborhoods. At the optical node, which is typically less than 500 meters from the customer or business, the optical signal is converted to a radio frequency (RF) signal and carried over robust, shielded coaxial cables to customer premises. Similarly, RF signals travelling in the opposite direction are converted to the optical domain and sent to the headend.

It is unlikely that any single enterprise or private network will deploy a HFC network, but it is very likely that MSOs will start providing hosting services from their datacenters which are usually within 20-40km from their enterprise customers. This opens the possibility of enterprises accessing virtualized private or shared packet cores, telephony services, and even vRAN without having to deploy their own servers on-premises.

While HFC is considered a non-ideal transport, significant advancements have been made which have improved the usefulness and suitability of HFC to provide backhaul and even fronthaul to LTE eNBs and 5G gNBs. For example, Data Over Cable Service Interface Specification 4.0 (DOCSIS 4.0) is expected around 2023 and plans to significantly improve US speeds to 3.7Gbps. Downlink speed is also improved to 10.8Gbps, which will further increase HFC usability for 5G networks.

Another advancement is low latency xHaul (LLX) technology. LLX may significantly reduce the DOCSIS latency and make mobile network traffic less suspectable to HFC network loading.

While today’s HFC deployments can achieve a minimum latency of 5ms which is acceptable for backhaul, LLX will offer latencies of 1-2ms which will allow HFC to be used for midhaul (Option-2) and perhaps even fronthaul (Option-5 or Option-6) and facilitate vRAN deployments.

Both LTE and NR have timing and synchronization requirements, but phase synchronization is a must specifically with TDD deployments (including CBRS). The required frequency and time synchronization is achievable with the current DOCSIS standards, but phase synchronization can only be achieved with additional LLX enhancements to the DOCSIS protocol. This will make HFC particularly useful when private networks are deployed in areas that cannot receive good GPS signal (for instance indoors).

Another advantage of an HFC network is the ability to deliver limited and shared power. Typical 90V power supplies can provide around 1000W on a single cable strand which can be shared to the end customer equipment such as a low power small cell or radio, eliminating the need to route a power source to the device.

3.5.3 Ethernet

The most ubiquitous transport technology in use today is Ethernet. As discussed in Section 3.2, enterprises will look to make use of their private Ethernet networks primarily in their LAN infrastructure to drive down the total cost of ownership of a private cellular network as best as possible. This infrastructure depends on the base technology, such as Precision Time Protocol (PTP), Synchronous Ethernet (SyncE), or Time Sensitive Networking (TSN), as well as the equipment used (i.e., switches, PoE, Grand Master Clocks and Telecoms Boundary Clocks) and the network design. This LAN infrastructure may be able to support fronthaul, midhaul, and backhaul for their private cellular network.

While Ethernet may use optical fibers, the most common variants of Ethernet use copper cables. These cables are rated in categories, from Category-5 (Cat-5) to Category 7 (Cat-7) which support various speeds. However due to the physics of copper conductors, the distance of a single cable run is limited to about 100m (330 feet).

The most common variants found in Enterprises are: 100Mbps Fast Ethernet standard (IEEE 802.3u), Gigabit Ethernet (IEE 802.3), and 10-Gigabit Ethernet (IEEE 802.3ae).

In terms of bandwidths and capacity, 100Mbps-1Gbps is suitable for backhaul and 10Gbps potentially being able to support LLS (Option 6 and Option 7-x) depending on the 5G cell bandwidth and number of radio transmission layers.

Just like HFC, Ethernet has the added benefit in that it also offers the possibility of providing power to a small cell or radio. The Power-over-Ethernet (PoE) standard defined by the IEEE 802.3 working group, is the primary standard in use today. The highest power that can be delivered today is 71.3W with the 802.3bt Type 4 (4PPoE or PoE++) certified switches and power injectors.

As previously mentioned, fronthaul networks of today are typically implemented using dark fiber (or ideal transport technologies) with semi-proprietary protocols such as CPRI. For enterprises, these transport techniques are prohibitively expensive to build and maintain and therefore solutions that use Ethernet are needed. Development focus in this area has been firstly, the encapsulation of data over Ethernet Frames, and secondly strict timing and synchronization requirements.

There are two encapsulation methods for fronthaul defined to date:

- **Enhanced Common Public Radio Interface (eCPRI)** - which isn't a fully open standard and therefore has some inter-vendor operability issues
- **Radio-Over-Ethernet (RoE)** - defined by the IEEE 1914.3 working group is an open standard effort to specify a transport solution for time-sensitive wireless radio data.

A key requirement for both encapsulation methods is strict latency and packet delay variation (PDV) control. The typical latency requirements for fronthaul vRAN LLS RAN splits is in the order of 100-300 µs, including the fiber propagation delay. To achieve these requirements, the main solution proposed is Time Sensitive Networking (TSN). The IEEE TSN Task Group has published a new standard (IEEE 802.1CM) that addresses TSN for fronthaul networks that are capable of transporting fronthaul streams that are time sensitive.

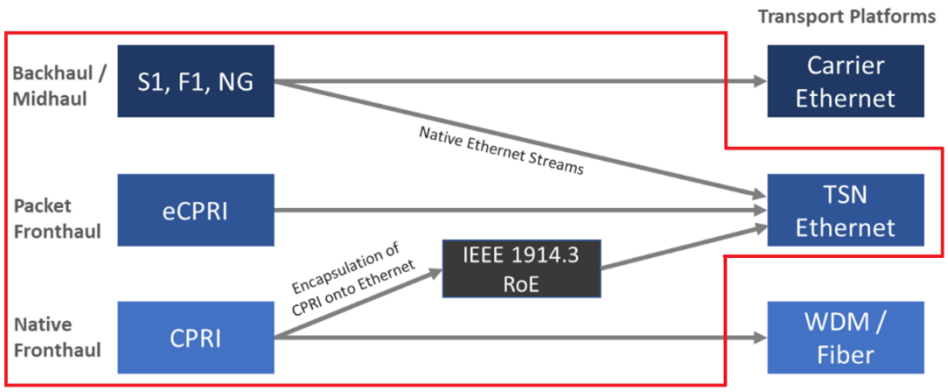
Ethernet networks complying with IEEE 802.1CM will provide deterministic transport of eCPRI and RoE streams by controlling traffic scheduling, timing synchronization, and system reliability.

Figure 9 shows the relationship between the various xHaul interface types (e.g., F1, CPRI, eCPRI), radio encapsulation techniques such as Radio over Ethernet (RoE), and TSN Ethernet and other transport platforms. The elements within the red border are of specific interest in the discussion of the use of Ethernet for Private Networks.

The O-RAN Alliance specifies that all fronthaul systems support Ethernet transport, with support of IP-defined transport being optional. Ethernet is used to transport the eCPRI frames which carry the fronthaul control and user-plane traffic. O-RUs can be attached to Ethernet switches using access ports or trunk ports, such as if multiple VLANs are used across the fronthaul.

As Ethernet is an open standard and devices supporting it are readily available, it is susceptible to un-authorized access and snooping, therefore the use of encryption and secure protocols is important. The O-RAN Alliance has defined the use of IEEE 802.1X and Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) for helping secure the fronthaul network. The approach follows the same procedures that private enterprises may already be using for securing access to the enterprise LAN infrastructure.

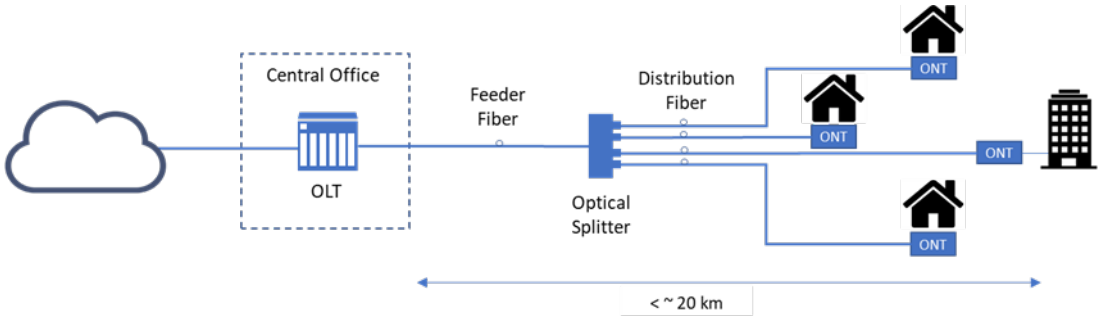
Figure 9: xHaul transport options



3.5.4 Passive Optical Networks (PON)

PON is a fiber-optic network technology that uses a very similar architecture as HFC. PON uses a point-to-multipoint topology and optical splitters to deliver data from headends where Optical Line Terminators (OLT) are located, to Optical Network Terminals/Units (ONT/ONU) where users are located. Figure 10 shows the architecture of a PON Network.

Figure 10: PON Architecture



Unlike HFC, all the elements on the path are passive, hence the range from the headend to the user is more limited to about 20 kilometers. However, there is an advantage to using “all-fiber”, sometimes referred to as Fiber-to-the-Home (FTTH), compared to HFC as it is capable of higher and more symmetrical throughputs in both the Downstream (DS) and Upstream (US).

Both International Telecommunications Union – Telecommunications Sector (ITU-T) and IEEE have specifications for PON. PON’s throughput capabilities are better than HFC and this makes it a better solution for the vRAN midhaul and fronthaul interfaces. In terms of latency, PON has better performance than HFC, but LLS RAN Splits (Option 6, Option 7, and Option 8) require a maximum latency of a few hundreds of µs, which is currently not possible with most PON variants, especially in the Upstream.

The two main latency inducing factors in the US are Dynamic Bandwidth Allocation for multiple users and the quiet window during ONT activation. The IEEE Next Generation Ethernet Passive Optical Network study group (IEEE NG-EPON) have improved latency with various techniques and now PON should be able to support these RAN Split options even in US.

PON networks can decrease 5G transport costs by more than 50 percent compared to microwave and P2P dark fiber for both operators that own the PON network as well as enterprises that intend to lease PON networks. As such, PON can be an attractive option for implementations of vRAN xHaul.

4. Mobility Considerations for Enterprise Deployment of P5G

Mobility can refer to a large set of capabilities that usually get bundled together, but need to be considered independently. For certain enterprises, particularly industrial verticals such as manufacturing, that are looking to deploy private 5G to take advantage of the high reliability and low latency features, an isolated network with no roaming capabilities to other networks may be sufficient. In fact, some enterprises may demand isolation as a requirement. Most private cellular networks that have been deployed as of today fall into this category.

On the other hand, many enterprises, such as healthcare, logistics, transportation, will need to allow their devices to roam freely between private and public networks. There is also always a need to consider movement across different networks, like from Wi-Fi onto a private cellular network served with CBRS and then onto a public network served with 4G or 5G.

All mobility actions involve a device requesting a connection to a network and a network allowing connection and service to the device. The concepts of “home” network and “visited” network are used to distinguish where the device is currently registered versus the network to where the device is moving. In the public cellular context, the home network is the network that is responsible for subscriber management and billing for the cellular service. The visited network is expected to recognize the device but only serve it if there are existing agreements between the home and visited networks for a roaming service.

How home and visited network operators implement their mutual business agreements, like revenue exchange for serving visiting subscribers, is a complex topic and proprietary to the CSP/MNO operators. With the introduction of private cellular, there is an expectation that similar types of roaming agreements can be established between public and private network operators, even if they are not easily accomplished. This section will attempt to uncover some of these complexities and directions being considered for possible solutions.

4.1 Mobility Concepts Overview

4.1.1 Subscriber and Device Identity

In public cellular networks the Subscriber Identity Module (SIM) holds device identity which can also be equivalent to the Subscriber Identity, where subscriber definition represent cellular services that are associated with a user and billing entity. Multi-SIM devices can consist of multiple physical SIM modules and/or use the eSIM technology which enables programming of multiple identities in a physical SIM device.

In all cases each SIM instance represents a service instance. In addition to device information SIMs can also hold a great deal of other information, such as usage metrics, location info, etc., which may need to be protected per security policy of the “owner” of the device and provider of the service. In private networks, or “non-public networks” as per 3GPP, the Extensible Authentication Protocol (EAP) can be used to authenticate a Network Access Identifier (NAI)-based (i.e., user@realm) subscriber identity. 3GPP specifications include example of using certificate-based authentication using EAP-TLS, but other EAP methods may be used, subject to device support.

In enterprise networks, a User Identity is associated with access control policies for a user who may have multiple devices registered to their name. Access control mechanisms can be simple, username and password, or complex, such as encrypted certificates with two factor authentication, etc. The enterprise security policy decides which user on which device can access to what resources in the enterprise.

Private cellular networks using SIM-based identifiers need to somehow map SIM information to username and associated security policy information for that user in the specific enterprise. Other private cellular networks using NAI-based identifiers can enable a common identity type to be used across different enterprise systems.

Coordinating the security policy associated with a device and subscriber between multiple networks is an active topic of discussion. A clear and unified set of definitions for these topics can be very useful for enterprises who are almost always needing to use multiple access networks together but under one single security policy and methodology.

4.1.2 Network Identity

Cellular networks use a globally unique Public Land Mobile Network (PLMN) code, assigned by ITU, to identify their networks. These codes are used in roaming situations that allow traffic to traverse cellular networks. Any private network that intends to "roam" with a public network needs to have access to a valid PLMN code, either assigned to it or assigned to the entity that will handle roaming for that private network.

Public providers that offer private network services can use their PLMN code(s), as well as provisions defined in 3GPP for Non-Public Network (NPN) configurations, in order to roam between private networks that they serve and public networks. Private networks that are deployed independently by an enterprise or served through a cloud provider that does not happen to be an CSP/MNO have to devise a method to use a valid PLMN code for their roaming transactions. Many Cloud providers that offer private cellular network services have allocated PLMN codes that they can use in roaming transactions.

Note that allocation of a PLMN code to a single enterprise is not practically possible as PLMN codes do not scale. Also, establishing roaming agreements between a large CSP/MNO and small enterprise is not something CSP/MNOs are willing to consider. These limitations are being discussed actively to enable easy to deploy roaming for private networks.

4.1.3 Handoff

As devices move from one radio to another, they go through a process called "handoff". Handoff is a foundational feature in any wireless or cellular network and usually refers to movement across radios still within the same administrative domain. Improving speed and reliability of handoffs to reduce latency has been happening and continues to evolve in all wireless networks.

Handoff between different network types, such as Wi-Fi to cellular, is usually handled in the application layer and involves a temporary disconnect as application moves data path from one network to another. Devices that would support these applications are expected to have multiple connection interfaces for each network type. Handoff between public and private cellular networks can also happen at the application layer if the device supports multiple SIMs. In single SIM cases the handoff interaction is equivalent to roaming.

4.1.4 Roaming

Roaming refers to maintaining connection as a device moves from one administrative domain to another, such as moving from a private network onto a public network or moving from a public network served by an CSP/MNO to another public network served by a different CSP/MNO. Roaming always involves interactions between multiple packet cores.

Roaming depends on established agreements between the network providers to "permit" device connectivity as devices move onto and request connection in the provider's domain. Roaming agreements are complex business level legal agreements that are created between public CSP/MNOs and involve CSP/MNO's subscriber management processes, billing, rate plans, etc. Public CSP/MNOs allow subscribers to connect to their networks, but also ensure usage measurement and billing to be "settled" between providers in the background. As private cellular networks evolve it is desirable to enable simpler roaming methodologies between private and public networks.

4.1.5 Mobility Restrictions

Mobility Restrictions are methods that commercial cellular networks use to limit mobility handling or service access of a subscriber. There are multiple categories including Radio Access Technology (RAT) restriction, Forbidden Area Restriction, Service Area Restrictions, Core Network type restriction and Closed Access Group information. These features are implemented on the device, the radio, and the packet core. These restrictions can be over-ridden when accessing network for emergency services.

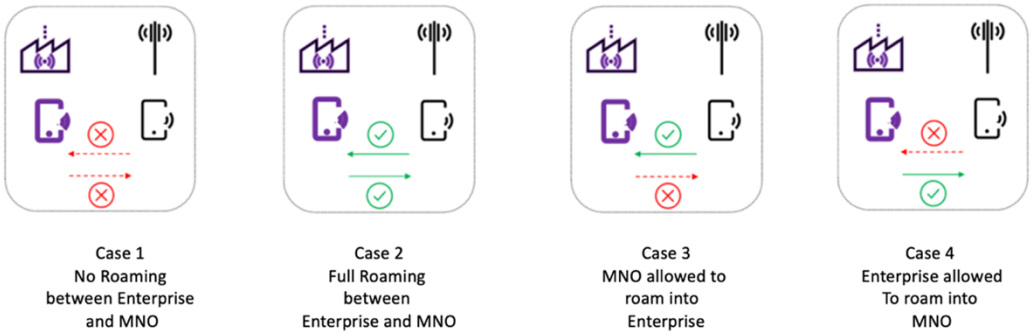
For example, forbidden area restriction can be implemented to limit the mobility for users/devices in restricted areas based on subscription. The device behavior, in terms of cell

selection, RAT selection, and PLMN selection, depends on the network response that informs the device of forbidden area list as defined by 3GPP. Mobility restrictions provide a separate layer of access control which needs to be considered carefully along with private network access control criteria and methods when deploying a private network.

4.2 Mobility Scenarios Relevant to P5G Deployments

Mobility scenarios between private networks and public network operators fall into four general cases as described below. These cases are highly generalized, and variations will emerge.

Figure 11: Possible Roaming scenarios between private and public networks



Case 1: Isolated private network where private devices do not need to be used outside the enterprise premises. In this case, no roaming is needed between the private and public networks. Devices can be managed by the local Enterprise IT in identity databases that are owned and managed by the enterprise, or by public provider through SLAs that are agreed to for the service. The security credentials of the device, i.e., SIM/eSIM or EAP credential, must be provisioned only in the private 5G network. These "private network only" devices will only be able to connect under the wireless coverage of the private network.

Case 2: Private network with full mobility access to public networks. Devices can be smartphones that run special applications that can only be utilized under enterprise coverage (e.g., sensitive data, machine control), while also providing general applications such as email, workflow, and voice communications outside the enterprise. This case requires the private device to connect to the private network while on enterprise premises and to CSP/MNO's public network when outside the private premises. This can be achieved with a dual SIM device or through roaming enabled with the public network and vice versa.

Case 3: A potential use case for this scenario is if a CSP/MNO owns the private network, such as private networks set up for events and venues, and allows "handovers" from the public network to the private network for that specific venue location only. Another relevant use case can be when CSP/MNO extends its radio footprint into a private premise to improve connectivity at the private site using Distributed Antenna Systems (DAS).

Case 4: In this scenario coverage of the private network can be extended into the public network to enhance capacity limitations in the private network.

Comprehensive and flexible mobility and roaming architectures that can allow private networks to integrate with CSP/MNO networks with ease and at scale is a work in progress. Currently, most private network deployments, such as in industrial verticals, do not enable full mobility/roaming. However, as devices and use cases mature, this will change. Use cases that do need full mobility/roaming, like in healthcare, venues, or transportation, can be served with multi-SIM devices as well as features that are already defined through 3GPP in CSP/MNO networks that dedicate access to private networks through service definitions and capabilities that are offered by the CSP/MNO, these include Slicing, Public Network Integrated Non-Public Network (PNI-NPN) as well as Mobility Restriction features.

4.3 Cellular Identity Onboarding in the Enterprise Context

With privacy and identity theft a top issue, 5G has made significant progress in protecting subscriber identity and providing options for enterprises to manage identities. Conventional 5G public cellular service is based on International Mobile Subscriber Identity (IMSI) public cellular identities that use unique E.212 number ranges allocated to the public cellular operators. Roaming systems enable the devices with public cellular identities to be able to operate on visited networks. The PNI-NPN approach to non-public networks re-uses the same approach, whereby a unique PLMN code is embedded in the identity used by enterprise devices.

The Standalone Non-Public Network (SNPN) approach enables third party credential holders to manage device credentials used by the enterprise devices. These credentials may be conventional SIM-based or, by leveraging 5G SNPN support of the EAP framework, non-SIM based, for example with 3GPP describing how to use certificate-based identifiers in SNPNs. SIM based devices, including eSIM devices, can have their SIM profiles remotely provisioned using standardized interfaces. Such remote provisioning requires the enterprise device to be provided with IP connectivity so that it can access remote provisioning systems. In public cellular systems this is achieved by enabling an initial provisioning and/or operational profile.

3GPP has defined how to onboard UEs for SNPNs, allowing the UE to access an Onboarding Network (ONN) based on default UE credentials for the purpose of provisioning the UE with SNPN credentials and any other necessary information. Authentication using the default credentials requires that either the credentials are stored in the SNPN, or the SNPN allows access to authentication via a remote Default Credential Server (DCS). After establishing connectivity with the default credentials, the UE accesses a Provisioning Server that can provision new credentials.

4.4 Cellular Mobility in the Enterprise Context: PNI-NPN, SNPN

Public cellular service has transformed businesses, offering ubiquitous coverage that enables enterprise users and devices to be constantly connected. The 3GPP defined Public Network Integrated Non-Public Network (PNI-NPN) approach augments the existing wide-area cellular coverage with localized Non-Public Network functionality. PNI-NPNs leverage network slicing and closed access group (CAG) functionality, delivering access control at the cell level. The closed access group identity is configured in the operator's SIM cards used by enterprise devices and on the NPN network. When the device subscription permits access on non-CAG cells, this offers seamless access using the local NPN and wide area public networks to the PLMN provided 5G service, such as with an enterprise dedicated Data Network Name (DNN).

In contrast, stand-alone NPN have not been designed to be integrated into a broader public network. Whereas PNI-NPNs leverage operator managed identities corresponding to SIM subscriptions, SNPNs enable enterprise to manage their own identities. Existing enterprise identities with EAP-based authentication can be used to authenticate devices onto the SNPN. However, as the enterprise identity cannot roam onto the public network, then SNPN use cases can be focused on scenarios where isolated coverage and capacity is sufficient to meet the business requirements, where the SNPN provides access to a private DNN.

When enterprise devices are permitted to access via non-CAG cells, the PNI-NPN deployments offer the ability of authorized enterprise devices to seamlessly connect to an enterprise dedicated DNN via both the NPN and wide area cellular networks. If the enterprise use case requires connectivity support for devices from third parties, such as contractors and visitors, then the network needs to be configured with a non-CAG cell. Similarly, if the enterprise use case requires connectivity for devices, irrespective of carrier affiliation, then the network will need to be configured with multi-operator support.

For SNPN, 3GPP has not defined the ability to roam onto the SNPN from a third party PLMN. In Release-17 however, 3GPP has defined how the credentials used in the SNPN can be owned by an entity separate from the SNPN. 3GPP defines scenarios where the Credential Holder (CH) simply operates an EAP-server, such as an enterprise, or where the credential holder operates an Authentication Server Function or Unified Data Manager (AUSF/UDM), such as a CSP/MNO. Such capability may permit the ability of an SNPN to integrate with multiple credential holders, effectively delivering a multi-operator deployment.

4.5 Application Based vs Network Based Mobility Control

With increasing drivers for heterogeneous wireless environments, the application environment is switching from "handover-centric" propositions, where only a single access is available at any instance in time, towards "multi-access" propositions, where multiple access types

are simultaneously available to support the application flows. The key challenge is to realize how best to use the multiple accesses available at any instant to best serve enterprise application requirements. There is substantial fragmentation in approaches for supporting services delivered in heterogeneous multi-access environments. At a high level, these different approaches can be characterized as either "tightly coupled", whereby a converged network architecture is defined that encompasses multiple access-types, or "loosely coupled", where parallel networks are used to support different access-types.

In loosely couple approaches, the device, including application client functionality, is typically responsible for handling mobility between heterogenous access types. Device operating systems include APIs that enable application to learn whether certain network paths are expensive or constrained as well as other APIs that allow applications to use the multiple paths available. The multipath functionality can enable ability for handover, improved low latency performance, or enhanced throughput. Client and server application ecosystems supporting HTTP/3 can now leverage native support for client-side connection migration from different IP networks, to enable application flows to be "handed over" from an isolated stand-alone NPN towards a public cellular network.

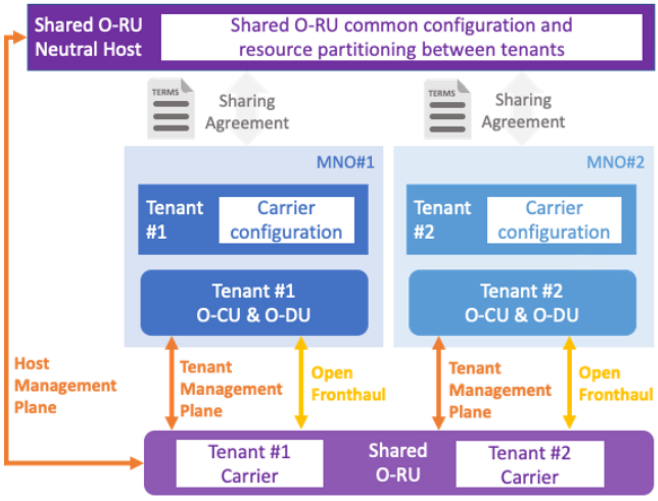
4.6 Shared Networks

Private networks with network sharing give the possibility of sharing RAN equipment to better utilize the equipment and infrastructure. Out of several benefits of RAN sharing, spectrum sharing is a key benefit which enables the private networks and mobile network operator to use the same spectrum in the same geographical area.

Established sharing approaches faces key challenges. MOCN simplifies the RAN functionality but is operationally complex as exclusively licensed spectrum needs to be shared. MORAN simplifies operations as each CSP/MNO uses their own spectrum but adds complexity to the base station. Finally, DAS simplifies interoperability based on attenuated RF interfaces but is complicated by having to bring multiple base stations into the enterprise's communications room.

O-RAN's shared O-RU capability offers a best of all worlds to address these issues. It offers a simplified O-RU using fully specified multi-vendor interoperable interfaces enabling integration with separate CSP/MNO remote O-DUs transported over a packet based fronthaul network. Additionally, it offers OAM functionality that enables an enterprise or neutral host to partition the shared O-RU's carrier resources between separate CSP/MNO tenants, with each CSP/MNO operating carriers using their own dedicated spectrum, as well as role-based access control permitting those tenants to only configure and receive performance data from their own partitioned resources.

Figure 12: Shared ORU as defined in O-RAN



While much of the focus on Open RAN has been on the transformation of the macro network, the compelling case for multi-vendor interoperable open RAN must include supporting those indoor enterprise deployments that necessitate multi-operator capability. Version 10 of O-RAN Alliance's Open Fronthaul specification enables the accelerated deployment of shared multi-operator networks, using fully standardized shared O-RUs.

4.7 Roaming Between Public and Private Networks

The 5G enterprise evolution is triggering a shift in buying centers from carriers to businesses and this shift is challenging traditional scale optimizations that are built into cellular networks. Cellular 3GPP- based networks are designed to accommodate very large sets of subscribers who are served by a rather limited set of providers.

With the 5G shift to enterprise, cellular networks are required to serve a large set of businesses, each of which are in turn serving their respective devices and applications as an autonomous private entity. The number of devices served per enterprise will be much smaller, each device demanding more throughput and resources, but number of private networks needing to be served will be much larger, with each private network needing similar sets of capabilities, such as roaming, as a provider network.

The current N32-based roaming systems assume fully decoupled signaling between the Security Edge Protection Proxy Initiator (SEPP-initiator) in the NPN and the SEPP-initiator in the Home Public Land Mobile Network of the Credential Holder (HPLMN/CH), for example when used for signaling based on subscriptions to callback URIs. This means the inbound CH initiated signaling to an SNPN can originate from a source IP address independent of the destination IP address used for outbound SNPN initiated signaling, necessitating the configuration of specific firewall rules by the SNPN to permit in-bound CH initiated signaling.

Today's PLMNs have a centralized database of IP addresses of all operator nodes that connect to the inter-PLMN IP backbone network, including AAA Servers/Proxies. This information is used for firewall and Border Gateway configuration. Signaling connections between VPLMN and HPLMN are long-lived (Diameter and N32f) and support bidirectional signaling. However, in private networks such as SNPNs, there is no centralized IP address database. Private networks configure the firewall to enable outbound connections to Credential Holders. In this case, signaling connections between VPLMN and HPLMN are short-lived. Signaling connections between VPLMN and HPLMN can be terminated if no signaling needs to be exchanged.

Some forecasts predict there will be 1 million SNPNs by the end of the decade. In Europe alone, that equates to a 1,000x increase compared to the number of public networks. A recent communication from the Wireless Broadband Alliance to 3GPP indicates that signaling scaling from roaming using non-public Wi-Fi networks can experience signaling scaled at 1/1000th of the load experienced by public networks. Hence, one future scenario has the N32 roaming reference points being required to support 1000 times more networks, each with 1/1000th of the signaling scale of a conventional public network.

5. Security Considerations for Enterprise Deployment of P5G

Security demands of enterprises continue to increase, particularly as cyber-attack surfaces expand due to increased digitization. Emerging wireless technologies need to align themselves with security requirements of the venue in which they are to be deployed. These requirements are defined in various forums under the general topic of Zero Trust, examples including the National Institute of Standards and Technology's NIST Zero trust (SP 800-207) model and Industrial Security in Purdue Model ISA-99 (now also known as IEC-62443). Additionally, 5G specifications have built in a rich set of security measures which are covered in several 5G Americas papers.

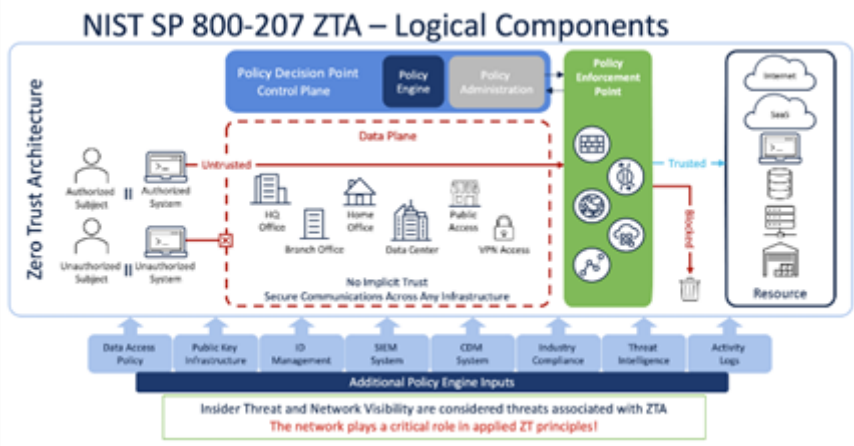
Enterprises are paying close attention to these models to lower their cybersecurity risks; however, most are only implementing a subset of these architectures, due to limiting factors of cost and complexity. Security discussions for private networks usually involves a coming together of these two large topics: 5G security and enterprise zero trust security and how the two can be aligned to meet enterprise needs at appropriate cost and operational ease of use.

Zero Trust security models are based on "ubiquitous least privilege access," such as granting access but requiring that it be made specific. Assumptions for this approach include:

- The network is always assumed to be hostile
- External and internal threats always exist on the network
- Network locality is not sufficient for deciding trust in a network
- Every device, user, and network flow need to be authenticated and authorized
- Policies must be dynamic and calculated from as many sources of data as possible

Figure 13 depicts logical components of the NIST zero trust model:

Figure 13: NIST Zero Trust model



According to the NIST guidance, any organization that intends to implement zero trust should articulate their access policy rules in a centralized policy engine which orchestrates policy enforcement through various enforcement points throughout the organization. All access will be subject to policy assessment, there will be no "implicit" trust assigned to any internal access.

The enterprise monitors and measures the integrity and security posture of all owned and associated assets, collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture. All data sources and computing services are considered resources. All resource authentication and authorization are dynamic and strictly enforced

before access is allowed. Access to individual enterprise resources is granted on a per-connection basis and determined by dynamic policy. All communication is secure regardless of network location.

This model includes the following elements in a comprehensive data/network security strategy that meets zero trust principles:

- **Identity**—Role and privilege definitions for user/account access
- **Credentials**—Authentication controls, such as passwords and keys
- **Access management**—Controls and policies that govern what assets and services can be accessed, and from where
- **Operations**—The overarching tools and processes needed to define, implement, maintain, and monitor zero trust architectures
- **Endpoints**—Distinct systems and workloads that are part of a zero-trust environment
- **Hosting environments**—The environment where a zero-trust architecture is implemented (for example, a data center or cloud provider infrastructure)
- **Interconnecting infrastructure**—Tools and platforms that facilitate connectivity to and from assets both within a zero-trust architecture and external to it

There are other security models and certifications that are relevant to enterprise deployments, which are like or derive from the NIST Zero Trust model. These include:

- SOC 2® – SOC for Service Organizations: Trust Services Criteria
- ISO IEC 27001:2013 – Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27017:2015 – Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2019 – Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27701:2019 – Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- ISO 22301:2019 – Security and resilience — Business continuity management systems — Requirements
- Esquema Nacional de Seguridad (ENS)
- Infosec Registered Assessors Program (IRAP December 2020)
- Payment Card Industry Data Security Standard (PCI-DSS v3.2.1)
- Information System Security Management and Assessment Program (ISMAP)
- Cloud Computing Compliance Controls Catalogue (C5)
- EU Cloud Code of Conduct (CoC)
- Third Party Cybersecurity Compliance Certificate (CCC)
- The Federal Risk and Authorization Management Program (FedRAMP LI-SAAS/Tailored)
- IEC 62443

Ultimately decisions on how much security to deploy in an enterprise private 5G system is in the hands of the Enterprise IT who will be responsible for deployment of the service, either directly operating the service, and/or acquiring service from various operators and establishing contractual SLAs for operations outcome. In this section we outline some of the more nuanced aspects of securing private 5G deployments for the enterprise.

5.1 5G Security

Security in 5G networks is standardized by 3GPP at every network interface level, where user data is decrypted and encrypted in different functions within the network. Signaling and user data is, in most cases, encrypted in transit over the network but processed in cleartext in many functions at the individual network nodes in a secure environment. The air interface is encrypted, and integrity protected between the device and the gNB.

From the gNB over the backhaul network to the core network normally via an edge router, the 3GPP defined IPSec-based NDS/IP security framework is used to protect the integrity and confidentiality of the user plane and control plane between the device, the gNB and the core network. The UE is expected to support integrity protection and ciphering of RRC, NAS signaling and user data to ensure confidentiality as required by the regulations permit.

A broader look at 5G security can be found in the 5G Americas 2022 white paper, "Evolving 5G Security for the Cloud" and 5G Americas 2021 white paper, "Security in 5G" and the various white papers discussing security available at the 5G Americas website (www.5gamericas.org).

5.2 Enterprise Security Policy

Enterprise security policies will include methods for placement of firewalls, definition of traffic segmentation, device, and user admission control, as well as many other details that may be necessary to conform to specific local regulatory and industry specific requirements of the vertical. Insertion and alignment of the private 5G service into the

enterprise security framework is one of the essential steps in the deployment phase.

Enterprise networking security policies are usually defined around a Wi-Fi use model, and Wi-Fi systems have evolved to provide easy to use methods to conform to typical enterprise security policies. System architecture and security mechanisms that are defined for a private cellular solution are originally designed for carriers and must be scaled down and adapted to the needs of enterprise. Complexities of insertion into enterprise increase with the cloud deployment and macro slicing models where some parts of the private network deployment can reside in enterprise premise while other parts remain in the provider domain.

How should end-to-end security be considered in these models? How can providers ensure enterprise IT have control over all their critical assets and can implements their specific security policy? Is it even possible to provide a unified set of guidelines that can cover all enterprise use cases or should each use case be looked at independently? These questions are being discussed and addressed by providers as deployments mature.

On a positive note, given the high priority of security across the board in enterprise and service provider domains, there are plenty of mature methods that can be used to secure the most complex service offers spanning multiple administrative and cloud domains and applications. Most discussions of this topic ultimately gravitate towards ease of use and total cost of implementation.

5.3 Enterprise Data Protection

In public cellular wireless networks, data forwarding is handled by the base station and the packet core. Many enterprise IT managers are leery of using public cellular services because it can cause their enterprise specific data to need to pass through a public provider's network. With packet core virtualization as defined in 5G, in private 5G deployments it is possible to keep the User Plane Function (UPF), which is responsible for data forwarding, within the Enterprise security boundary to ensure enterprise data remains within the enterprise domain. Other network functions can also be placed flexibly in different locations, at enterprise site, in regional data centers managed by Carriers or other providers, or in central data centers. These virtualized functions can also be aligned and integrated with existing enterprise-specific functions to provide tighter security and easier operation and visibility for the enterprise.

The flexibility of a virtualized packet core where different components can be residing in different clouds that span multiple geographical domains, is raising General Data Protection Regulations (GDPR) related issues that are relevant to the enterprise. Providers are being asked to conform to all geographies where they offer service, and each geographic domain may have its own specific security and regulatory requirements. In many cases, the location of service provided to an enterprise site, may be in a different country or even continent. In these cases, providers are being required to establish a footprint that ensures service origination points fall in the same regulatory domain as service consumption with ability to conform to local regulatory requirements. These factors are applicable to many other popular cloud hosted service offers.

5.4 Identity Management and Access Control

5G standards define comprehensive identity management, authentication, authorization and subsequent encryption and integrity protection of all traffic between the device radio modem to the network functions in the 5G core network. Also, security for communications between the virtualized network functions in the 5G core are provided in the 5G standards.

Per 5G standards, all devices accessing the 5G network perform mutual authentication and authorization with the authentication server in the 5G network. The device has two identities, one is the primary identity used to access the 5G core (this is the permanent identity, e.g., associated with a SIM card) and the other is the identity of the device itself, this is the secondary or linked identity since SIM cards can be moved from one device to another.

Authentication to the 5G network is performed using the primary identity and credentials. Subsequent authorization checks are performed based on subscription information stored in the packet core to ensure that only those 5G network features, such as quality of service and access control to different sections of the private 5G core, are allowed which are contained in the authorization profile of the device. Private 5G core can provide automation rules that can check for a change in permanent identity in the SIM and the identity of the physical device. On detecting such a change, the automation engine takes whatever action is specified. This can be used to effectively tie SIMs to devices as desired, ensuring only authorized devices are allowed access to the 5G network.

After authentication, session keys are derived to encrypt and protect the integrity of traffic between the device

and the P5G network. The signaling traffic and the data traffic are encrypted over the radio interface. While encryption as defined in 5G can increase protection of the data and control path, it can cause a problem for highly secure environments that need full visibility to perform threat protection. The topic of efficient firewall placement in encrypted paths for private 5G deployments is a work in progress. Many enterprises choose to not use encryption for their internal 5G devices primarily for performance reasons but also to enable internal firewalls to inspect traffic.

5.5 RAN Security

RAN security is a well-defined topic for traditional All-In-One gNB implementations, as listed below. Applying these requirements to a virtualized and disaggregated RAN architecture that can be laid on different enterprise network architectures is an active topic of discussion and work at the O-RAN Alliance security task group.

5.5.1 Security Requirements for the RAN

- Support ciphering of user data between the UE and the gNB.
- Activate ciphering of user data based on the security policy sent by the SMF.
- Support ciphering of RRC-signalling.
- Implement the ciphering algorithms: NEA0, 128-NEA1, 128-NEA2, 128-NEA3
- Confidentiality protection of user data between the UE and the gNB is optional
- Confidentiality protection of the RRC-signalling is optional
- Confidentiality protection should be used whenever regulations permit.

Any part of a gNB deployment that stores or processes keys in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then keys in cleartext shall be stored and processed in a secure environment. Keys stored inside a secure environment in any part of the gNB shall never leave the secure environment

5.5.2 Security Requirements for the RAN setup and configuration

Setting up and configuring RAN by Operations, Administration and Maintenance (OAM) systems shall be authenticated and authorized by RAN so that attackers shall not be able to modify the RAN settings and software configurations via local or remote access. 3GPP defines OneAPI, XSD and YANG-based data models for managing functions. O-RAN Alliance defines the use of NETCONF/YANG for managing the functions in the disaggregated RAN.

- The certificate enrolment mechanism specified in TS 33.310 [5] for base station should be supported for gNBs and RUs. The decision on whether to use the enrolment mechanism is left to operators.
- Communication between the OAM systems and the RAN shall be confidentiality, integrity and replay protected from unauthorized parties. The security associations between the RAN and an entity in the 5G Core or in an OAM domain trusted by the operator shall be supported. These security association establishments shall be mutually authenticated. The security associations shall be realized according to TS 33.210 [3] and TS 33.310 [5].
- The gNB/RU shall be able to ensure that software/data change attempts are authorized.
- The gNB/RU shall use authorized data/software.
- Sensitive parts of the boot-up process shall be executed with the help of the secure environment.
- Confidentiality of software transfer towards the gNB/RU shall be ensured.
- Integrity protection of software transfer towards the gNB/RU shall be ensured.
- The gNB/RU software update shall be verified before its installation.

6. Management and Operations Considerations

Management and operation of enterprise networks is dominated by ease of use and automation. Tools are increasingly cloud hosted, operational steps for most platforms are streamlined and automated to reduce OPEX. In this spirit. any private 5G system being considered for enterprise use must comply with a similar level of simplicity and automation.

Different deployment models can provide management efficiency in their own ways. Isolated private 5G networks can provide a simplified management interface to the small packet core being deployed, cloud hosted models can offload complexity to cloud providers, macro slice models can offer management services through SLAs to relieve the enterprise IT of the complexity of 5G. Some of the key metrics that any enterprise will expect from any management service includes:

- Secure access for enterprise IT to access and control private 5G assets
- Deployment configuration information
- Secure Access of Device and SIM Authentication credentials
- Secure management of subscriber data
- Full Life Cycle Management of private 5G devices
- Detailed Usage records
- KPIs and Metrics
- Location information

6.1 Enterprise IT and OT expectations

In current enterprise networks, both information technology (IT) and operational technology (OT) management use Wi-Fi in wireless networks is dependent on the size of the enterprise and industry application requirements. If there are no conflicts, both IT and OT can operate independently. However, it is challenging when they do have a conflict, particularly for large enterprises.

One example is when more capacity is required from adding more people or departments in IT. Another is when additional service requirements are necessary with the inclusion of new equipment (like self-driving AGVs in the warehouse). Also, a large facility that requires multiple Wi-Fi hubs might also need to add 5G coverage for mobile endpoints, whether they are autonomous vehicles or people walking around. Some facilities might even need to track individual products or containers, and the movement of things from one Wi-Fi hub coverage area to another can disconnect the session.

5G has standardized mobility management features that can sustain those requirements. To meet SLA requirements, companies may create or design new tools to fulfill SLAs, meeting most key requirements like high capacity, low latency, reliability, interference management and mobility. The IT and OT management solution can build up a centralized department to manage both IT and OT, or use OT to manage IT. This would be dependent on both operation service/application requirements as well as enterprise operation size.

One solution to the question of how to manage IT and OT and share resources to meet IT or OT requirements involves centralized management.

6.2 GTM and Operational Models

As 5G networks evolved from a Business to Consumer (B2C) model to more of a Business to Business (B2B) operations model, several areas of work have become highlighted. These include distributed deployment of core networks, evolution of converged networks, lightweight deployment of network

equipment, and “co-management and co-dimensionality” collaborations between operators and vertical industries. Many of these broad topics are currently in development and how they are approached will differ based on different deployment models that were described earlier in this paper.

Let’s review the Go to Market (GTM) aspects of these models here with management functions in mind.

6.2.1 Buy Public 5G Services from a Mobile Operator

One way of obtaining 5G services is to contract them from a public 5G mobile network operator. In terms of connectivity, this option provides businesses exactly what they have with 4G: the ability to call or be called from anywhere. Public 5G services are great for capacity and mobility driven 5G use cases. However, being on a public 5G network means 5G security will be terminated in the public network and enterprises will have to use these services in the same way a commercial 5G service is deployed. If an organization is satisfied with application-level security and doesn’t need anything more comprehensive, public 5G services are the right choice.

6.2.2 Lease a 5G Network Slice

Another method of 5G procurement is to lease a network slice, which is a virtual network within a public 5G network that isolates organizations from other users and traffic. Network slicing targets the security benefits of 5G, but it also may enable enterprises to tune the specific characteristics of their 5G service and target latency by using QoS to prioritize traffic.

The important point about a network slice is that an operator provides it, which means it is available only within the service area of that operator. Operators will have to decide how to offer a slice in a way that does not interfere with their commercial services. Enterprises may have to work out how to connect slices provided by multiple operators, either through the operators themselves or using their own tools. If organizations want broader geographic coverage, they need to decide whether their network slices connect in any way to the public network.

1.1.1 Build a 5G Network

The third way to obtain 5G services is for an organization to build its own 5G network. This means it must obtain radio frequency spectrum, procure antennas and transceivers, and deploy the various elements of 5G infrastructure. Large use cases with critical need for service quality and security can consider this option. Building a 5G network is neither cheap nor easy, but enterprises that can justify it will find it is the ultimate path to having a highly reliable and effective network to use for their mission critical use cases.

Whatever an organization’s 5G justification and whatever service option it takes to the procurement phase, the path to becoming a 5G enterprise involves many other players, including infrastructure providers, public cloud 5G hosts, 5G telecom vendors and mobile operators that can provide network slices.

6.3 How to Fulfill SLA Expectations for Enterprise

Industry application requirements can be filled into customized SLA templates which are built by industry standards and enterprise specifications. Creation and operation of SLAs is currently a custom manual task that is different from provider to provider. However, in the future, industry customers can order network services by signing service agreements automatically. This level of automation is being discussed in relevant industry forums.

Evidence-based SLA commercial agreements can help industry customers measure network service quality, focusing on Key Performance Indicators (KPI). Implementation and enforcement of the SLA requires intelligent and secure telemetry and assurance systems that can provide: (1) high precision operations data with one-way target measurements accuracy reaching microseconds level, (2) automation tools that automatically start measurement and analysis, (3) Correlation and AI/ML based tools to detect end-to-end connection and network health. Four key performance indicators, which are delay, jitter, packet loss, and bandwidth, are typical KPIs being considered today, however many other criteria can be added to a service definition. Additionally, centralized system management and control, automatic analysis of SLA data, intelligent abnormal detection, intelligent fault prediction, and intelligent analysis fault root causes can be provided.

Conclusion

Within the last few years, a great deal of progress has been made in enterprise understanding of what private cellular can offer. Similarly, private cellular requirements and deployment options have also been evolving to fit enterprise needs. 5G continues to make significant technical and deployment progress. However, there is still much to do to ensure optimal and efficient private cellular solutions for various enterprise needs. Several areas of work that stand out as being bottlenecks preventing faster deployment include:

- **Lack of ready to use User End points, devices, and related applications.** Most 5G device development is still focused on commercial cellular offers (cell phones) with traditional voice/data rate plans that carriers have been offering. The performance of these devices in private cellular context where general "data services" dominate is still sub-optimal. More complex devices that must rely on a 5G modems to be integrated into a larger system are still within proof of concept and trial phase. mmWave devices are rarely available for even lab tests. We are witnessing many networks that are designed and ready to be used awaiting devices to connect to them.
- **Spectrum availability** and the need to be streamlined and aligned with what is consumable and efficient for enterprise use cases. Private 5G Enterprise network applications and use cases are expected to require significant spectrum to meet the various applications and use cases of the entities. The availability of CBRS and its shared spectrum model has also prompted interest in the enterprise community in the United States The increased availability of harmonized licensed spectrum, and more efficient use of spectrum, e.g. improved aggregation, licensed, unlicensed and sharing methods across different bands, will help enable more demanding complex use cases to be implemented more efficiently.
- **Total Cost of Ownership (TCO) of private 5G systems**, as compared to WiFi6 based systems is still considered possibly higher. TCO consists of cost of equipment as well as complexity of operation. While WiFi6 systems may not be able to provide a "perfect" solution to many enterprise problems, their ease of use and lower cost profiles might motivate enterprise IT to consider them as "good enough".

In closing, future wireless could be defined by a coming together of multiple wireless modalities that can together solve complex problems. Private 5G has emerged as an exceptional modality that can provide carrier grade performance to enterprises and continues to evolve and improve as use cases are better understood, and various aspects of end-to-end solutions mature.

Acronyms

AAA: Authentication, Authorization, Accounting

AGV: Automated Guided Vehicle

AiO: All in One

BBU: Base Band Unit

CA: Carrier Aggregation

CAG: Closed Access Group

Cat-M: LTE Category M (low powered wide area technology)

CBRS: Citizens Broadband Radio Service

CH: Credential Holder

CoMP: Coordinated Multi Point

COTS: Commercial off-the-shelf

CPRI, eCPRI: Common Public Radio Interface, Enhanced CPRI

CSP: Commercial public network Service Provider

CU, vCU: Centralized Unit, virtual CU

DAS: Distributed Antenna Systems

DCS: Default Credential Server

DL: Down Link

DNN: Data Network Name

DOCSIS: Data Over Cable Service Interface Specification

DU, vDU: Distributed Unit, Virtual DU

EAP-TLS: Extensible Authentication Protocol – Transport Layer Security

EIRP: Effective Isotropic Radiated Power

EMF: Electromagnetic Field

ENS: Esquema Nacional de Seguridad

EPC: Evolved Packet Core

FCAPS: Fault, Configuration, Accounting, Performance and Security

FDD: Frequency Division Duplex

FHM: Front Haul Multiplexing

FWA: Fixed Wireless Access

GDPR: General Data Protection Regulations

GSA: Global Mobile Suppliers

HFC: Hybrid Fiber Coaxial

HPLMN: Home Public Land Mobile Network

IAB: Integrated Access and Backhaul

IDMZ: Industrial Demilitarized Zone

IMS: IP Multimedia Subsystem

IMSI: International Mobile Subscriber Identity

IoT: Internet of Things

IP: Internet Protocol

IRAP: Infosec Registered Assessors Program

ISM: Industrial Scientific & Medical

IT: Information technology

ITU: International Communication Union

KPI: Key Performance Indicator

LAA: Licensed Assisted Access

LAN: Local Area Network

LLX: Low latency xHaul

LLS: Low Layer Split

LTE: Long Term Evolution

MIMO: Multiple Input Multiple Output

MNO: Mobile Network Operator

MOCN: Multi Operator Core Network

MORAN: Multi Operator Radio Access Network

MSO: Multiple Service Operator

MSP: Managed service provider

MTTR: Mean Time To Recovery

NAS: Non-Access Stratum

NB-IOT: Narrow Band Internet of Things

nFAPI: network Functional Application Platform Interface

NIST: National Institute of Science & Technology

NPN: Non-Public Network

NR: New Radio

OAM: Operations, Administration, Maintenance

OEM: Original Equipment Manufacturer

ONN: Onboarding Network

ORU: Open Radio Unit

OSS: Operations Support Systems

OT: Operational technology

OTA: Over the Air

PII: Personally identifiable information

PLMN: Public Land Mobile Network

PNF: Physical Network Function

QoS: Quality of Service

RAN: Radio Access Network

RAT: Radio Access Technology

RF: Radio Frequency

RRC: Radio Resource Control

RRH: Remote Radio Head

RU: Radio Unit

SAR: Specific Absorption Rate

SCF: Small Cell Forum

SEPP: Security Edge Protection Proxy

SIM: Subscriber Identity Module

SLA: Service Level Agreements

SMF: Session Management Function

SNPN: Standalone Non-Public Network

TDD: Time Division Duplexing

UE: User Endpoint

UL: Up Link

UPF: User Plane Function

URI: Uniform Resource Identifier

VNF: Virtual Network Function

VPLMN: Visited Public Land Mobile Network

VPN: Virtual Private Network

WAN: Wide Area Network

References

[1] https://gsacom.com/paper/private-mobile-networks-summary-february-2022/

[2] https://www.networkworld.com/article/3658471/enterprise-private-5g-has-a-stage-but-challenges-remain.html

[3] https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution

[4] https://www.5gamericas.org/private-and-enterprise-networks/

[5] https://www.cisco.com/c/en/us/products/collateral/wireless/white-paper-c11-740788.html

[6] https://www.gsma.com/newsroom/wp-content/uploads/NG.116-v2.0.pdf

[7] https://www.ieee802.org/1/files/public/docs2008/as-garner-1588v2-summary-0908.pdf

[8] https://telecominfraproject.com/vran/

[9] https://www.federalregister.gov/documents/2018/07/20/2018-14807/use-of-spectrum-bands-above-24-ghz-for-mobile-radio-services

[10] 3GPP Technical Specification # 23.501 https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

[11] 5G Americas white papers: Evolving 5G Security for the Cloud, “Security for 5G”, all white papers

[12] www.o-ran.org

Additional Resources:

https://www.5gamericas.org/white-papers/

https://gsacom.com/

https://www.3gpp.org/

https://www.ieee.org/

https://www.o-ran.org/

https://www.smallcellforum.org/

https://csrc.nist.gov/publications/detail/sp/800-207/final

Acknowledgments

5G Americas' Mission Statement: 5G Americas facilitates and advocates for the advancement and transformation of LTE, 5G and beyond throughout the Americas.

5G Americas' Board of Governors members include Airspan Networks, Antel, AT&T, Ciena, Cisco, Crown Castle, Ericsson, Intel, Liberty Latin America, Mavenir, Nokia, Qualcomm Incorporated, Samsung, Shaw Communications Inc., T-Mobile USA, Inc., Telefónica, VMware and WOM.

5G Americas would like to recognize the significant project leadership and important contributions of group leaders Yi Huang, Senior Staff Engineer, Qualcomm Incorporated, Tingfang Ji, VP of Engineering, Qualcomm Incorporated, Mark Younge, Distinguished MTS, T-Mobile USA Inc., and Jun Liu, Manager, Systems Architecture, T-Mobile USA Inc. along with many representatives from member companies on 5G Americas' Board of Governors who participated in the development of this white paper.