5G TECHNOLOGIES IN PRIVATE NETWORKS

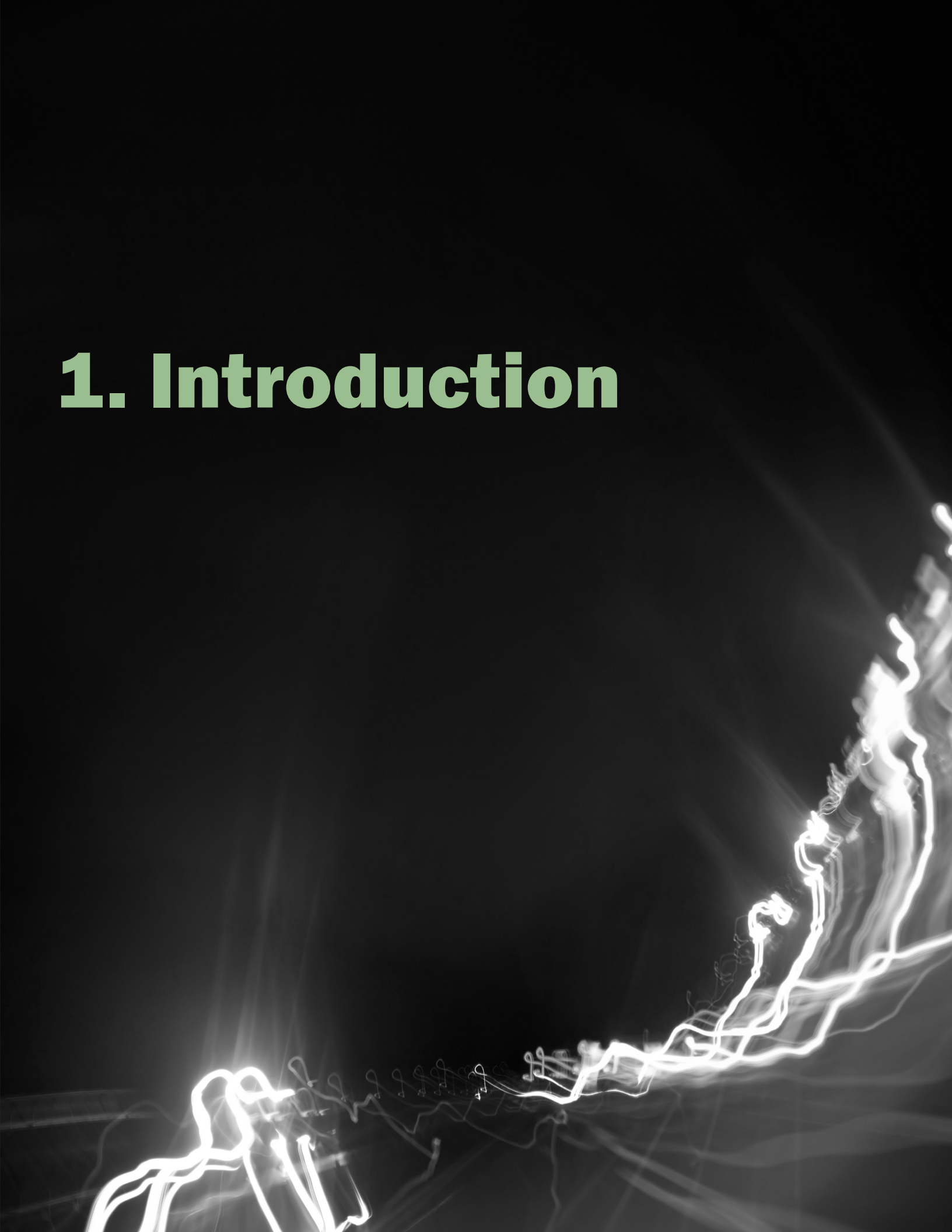
5G Americas
White Paper

OCTOBER 2020

5G americas™

Contents

1. Introduction



1 Introduction

5G is here with a lot of promise. It is heralding a wave of new applications and use cases of wireless communication technologies for vertical industries that have never been entertained or possible. The power of 5G enables a range of new and improved capabilities, like massive increases in broadband speeds, ultra-low latency, support of massive numbers of IoT devices and mission-critical use cases requiring the highest levels of reliability and security. These capabilities are tied to a myriad of factors, a convergence of various old and new technologies, different vertical markets and eco-systems, and different deployment architectures.

There is a growing trend of companies expressing interest to build their own private 5G networks for various advantages. This includes manufacturing, ports, airports and other sectors looking forward to using private 5G networks for high-level, granular enhancements in performance and reduced operational costs. A private 5G network is a local area network that provides all the features of a 5G network including reduced latency, higher speeds and all the advantages in terms of efficiency and security.

The high level of bandwidths offered by a 5G network is ideal for various use cases and advantages for industries that have become a major driving factor for the IIoT. Private networks, or Non-public Networks, have been gaining tremendous momentum for use cases, including industry automation, IoT, AR/VR and for new communication services in many enterprise scenarios. Though it started with 4G, it is no surprise that 5G has become the hottest topic as a new vehicle considered to provide the capabilities, advantages and efficiencies required for these applications.

It is important to recognize that many of these new verticals and applications are widely used in indoor scenarios. When it comes to indoor networks, 5G allows new experiences for consumers, new technical features and performance advantages with IoT, industrial automation and new communication services. However, there are many questions surrounding the unique challenges and opportunities in bringing 5G indoors.

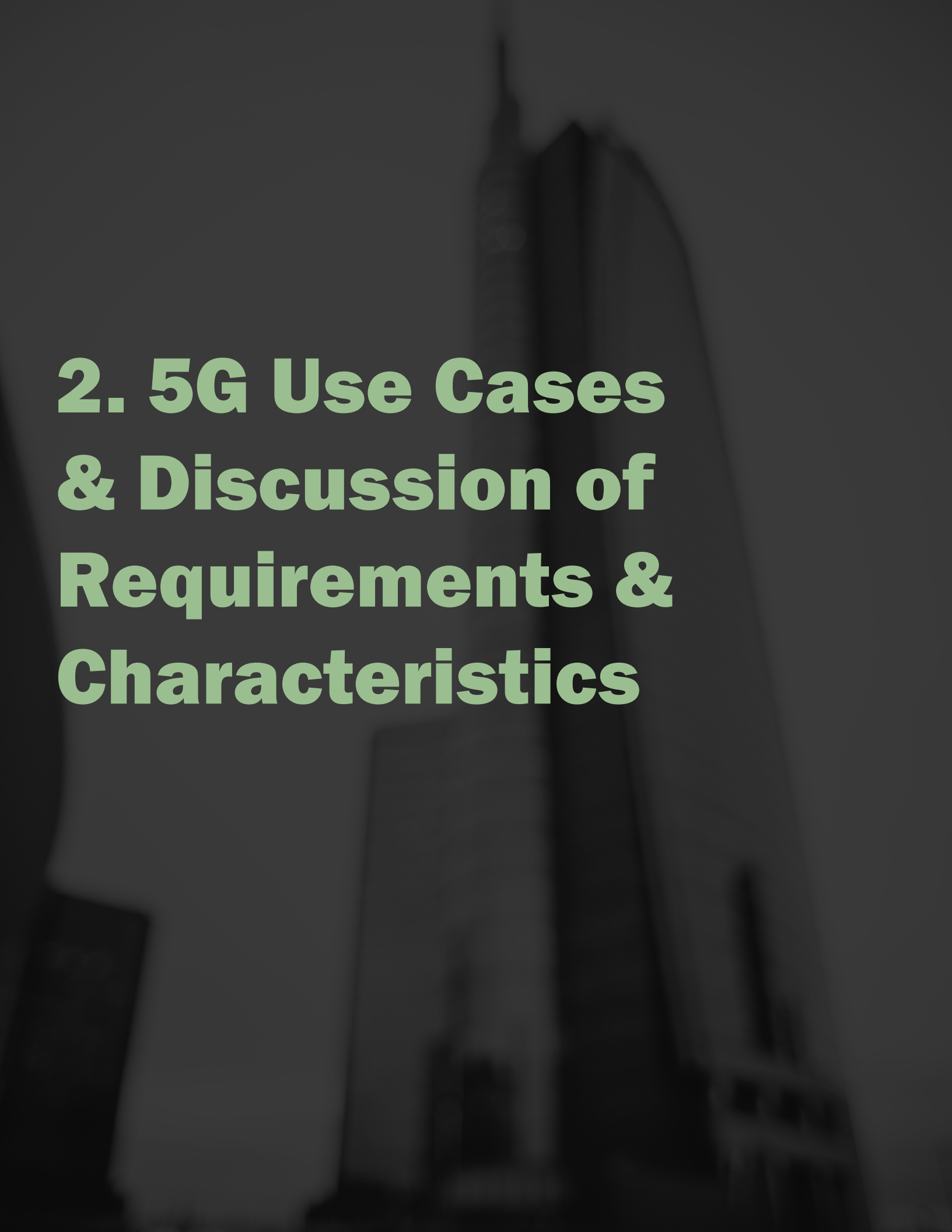
Essentially, private cellular networks are tailor-made to address specific needs of an enterprise or any such entity where these networks can provide a higher degree of mobile connectivity. Private cellular networks enjoy the enormous advantage of an extensive ecosystem of technology suppliers, system integrators and service providers compared to proprietary solutions. Additionally, the already existing market of cellular devices that can roam seamlessly onto global mobile networks conveniently fosters the use of 4G or 5G based private network deployments as opposed to new proprietary solutions. As new spectrum is made available and usable for 5G, enterprises and such entities can leverage private network modes of deployments for several general, business-critical, and mission-critical connectivity needs.

This white paper intends to provide a window into private 5G networks. This paper discusses how 5G private networks are suitable for different groups of applications and details the specific architectures that are applicable in building a private network. The paper also analyzes how different types of spectrum (licensed, unlicensed, and shared) can be utilized in building private networks.

Ultimately, this white paper provides an overview of the current industry considerations in deploying private networks in terms of the radio aspects, network architectures, access and connectivity and the supporting technical features. The white paper also discusses the evolutionary and revolutionary changes compared to previous generations. This raises questions of how to best to bring these new capabilities to the market, and the benefits of different network architectures, like Open RAN, Cloud or Virtualized RAN and evolved small cells supporting multiple split structures.

The white paper is further organized as follows:

- **Section 2** discusses the requirements and characteristics of use cases where private networks can be deployed to reap the best of benefits.
- **Section 3** discusses the emerging market landscape for the private networks in different spectrum and the various factors driving the adoption of private networks for indoor and outdoor scenarios.
- **Section 4** provides an overview of the various deployment models and details the network architectures and technical features of private networks.
- **Section 5** presents the technology features of private networks defined by the industry for CBRS 3.5 GHz shared spectrum.
- **Section 6** examines confidentiality aspects of major enterprise considerations and technologies that address secure private networks.
- **Section 7** covers economic value and modeling for private networks and provides an overview of various business perspectives and the funding and operational models.
- **Section 8** provides a summary of conclusions and recommendations for private networks.



2. 5G Use Cases & Discussion of Requirements & Characteristics

2 5G Use Cases and Discussion of Requirements and Characteristics

2.1 Overview

Ecosystem activities concerning Private Networks have increased in recent years. This is mostly due to market enablers, like spectrum availability such as Citizens' Broadcast Radio Spectrum (CBRS) and 5G capabilities but more importantly, due to digital transformation and sophisticated IT needs of enterprises. Robust, reliable, secure, and compatible connectivity is required to address the growing needs of enterprises.

On the other hand, Wi-Fi is still a dominant solution for connectivity. IEEE 802.11 protocols are also evolving to enhance Wi-Fi performance; it is likely to expect coexisting and complementary connectivity solutions in the early days.

2.2 Summary Business Requirements for Use Cases

The growing enterprise needs are concentrated around common requirements such as improved coverage and control, and increased performance, reliability, and flexibility. Table 2.1 lists the summary of the needs and illustrating the underlying expectations.

Table *2-1* List of Enterprise Requirements

Coverage & Control	Enterprises need improved coverage while maintaining control of data and user policies. Specifically the ones that have large number of locations, distributed across the nation and into rural areas, with growing number of devices and users.
Performance & Reliability	Increasing number of users and devices requires reliable and high performing connectivity depending on their needs. Considering machine to machine communication has less limitations compared to human capabilities, serving true potential of machines requires a more robust link between them.
Operational Flexibility & Integration	Every enterprise have different needs and resources therefor they expect flexibility in terms of choosing which operational model works for their needs. The ability to integrate with their current IT infrastructure is also important for lessening the complexity of operations and maintainance.

These requirements and how they can be met with respective technical 5G capabilities will be explained in detail in later sections.

2.2.1 Indoor and Outdoor Scenarios

Currently, most use cases of private cellular have involved both large indoor and outdoor venues with inadequate public cellular coverage. Leased license (or individually owned) spectrum has been used to drive privately operated LTE or specific business needs in these isolated venues. In addition to traditional small cell coverage, Fixed Wireless Access (FWA) solutions can be an excellent alternative for enterprises that do not require support from national operators.

Isolated Private Networks with a dedicated or shared spectrum is one option to provide such connectivity and ability. Still, in the early days, complimentary private networks working with existing Wi-Fi, IoT, or public cellular networks will likely be a popular alternative.

2.3 Sample Use Cases

2.3.1 Retail Robotic and Automated Deployments

Today's retailers use remote, automated devices like inventory robots, automated guided vehicles, automated forklifts, and many more for inventory management, asset tracking, and for performing many routine work tasks.

In all the automated use cases, data transmission in uplink and downlink is identified as high priority and processed on a local server to ease the complexity on the UE side. Most automated devices that need ultra-low latency with high reliability require high signal-to-interference-plus-noise ratio SINR which is possible only in 5G based private network deployments.

Other sectors of industry like manufacturing and government (for example, first responder-supporting MCPTT-like services) need high-resolution video cameras and advanced detection technology to identify and capture any life-threatening incidents or errors and defects in industry applications. The camera is continuously monitoring and relaying its UHD video feed through the air-interface. This data communication needs high bandwidth, latency sensitive, secure transmission processed in a secure private server. Such industries (private and government) do not prefer the data to be shared with public cellular provider for such processing. 5G private networks can address such design by spectrum efficient 5G waveforms, multi-spectrum support, flexible deployments and by placing intermediate UPF-like nodes, or by branching in UPF alongside to edge server. These use cases represent an excellent example for enterprises that require high performance because a more reliable network can be controlled and modified as needed.

2.3.2 Smart Factory, Smart Office, Smart City, Gaming Industry

5G is often collocated with Wi-Fi and used in complementary modes to enable a richer experience. Certain industrial sectors need extensive bandwidth, with low latency in the range of <1 ms, as well as multi-connections for reliability with micro and macro supported mobility among private-private and private-public networks for session continuation. 5G based private network topology eases such use cases because of control user split, support of multi-connectivity via multi-radio access technology through single-core, support of multi-profile devices, ability to integrate RAN and Core with non-3GPP (Third Generation Partnership Project) technology with cloud-native interfaces, and evolved device capability itself. Other important capabilities that enable private networks with 5G in enterprises such as Smart Factory, Smart Office, Smart City and Gaming Industry includes the following:

- Consistent bandwidth and experience in or out of office
- Higher density workforce sites (for example in real-time game)
- Seamless workforce mobility and device rationalization
- Richer collaboration with high definition multi-media and AR/VR with reliability and latency for both
- Optimized access across 5G and Wi-Fi 6
- Consistent policy and security with intent-based networking
- 5G high assurance wireless for critical production efficiency and quality
- Connectivity platform for closed-loop AI/ML processes

Some poignant use cases in this sphere include the following:

- **Supply chain**: Autonomous Vehicles, AI inward goods Inspection
- **Assembly:** AR guided assembly, Remote Engineering
- **Testing:** AI QC Inspection, Autonomous functional testing, AR guided inspection

2.3.3 Healthcare Applications

With the global pandemic, the healthcare system needs to rely on connectivity to maintain critical and routine patient operations while maintaining front line workers' security and safety, such as doctors and nurses. In addition, many healthcare facilities, such as dentistry practices and hospitals, are harnessing the power of virtual reality (VR) to help ease patient discomfort and assist in pain management. VR headsets are providing welcome relief to patients undergoing otherwise stressful or even painful procedures and recoveries. However, as this technology becomes more popular and the library of streamed virtual experiences grows, standard network architecture cannot support VR devices without siphoning off bandwidth from other critical data processing tasks or causing your patients' stream to lag.

The patient interacting with the VR headset browses and selects a virtual experience from the library stored on the local server. The headset then transmits this data to the local network. The VR headset receives and acts on locally processed, low-latency data and can stream patients' selected virtual experience with minimal lag.

2.3.4 Fixed Wireless Access: IIoT, Residential/Enterprises, Rural America, Small WISPs

One of the outdoor use cases for a Private Network with 5G as an access and core topology is Fixed Wireless Access (FWA). It enables the service provider to deliver ultra-high-speed mobile broadband to suburban and rural areas. Besides, it is a potential alternative for fiber-based broadband at residential and school broadband (EBS – educational broadband services). FWA can be used for supporting home and business applications where fiber is not feasible to maintain in the long run. These days, there is less dependency on a public network for such use cases because of the free spectrum like CBRS and Heterogenous Networks (Het-Net) design flexibility. Another advantage is network sharing and neutral host integration with the public network, especially when combined with Open RAN deployment and 5G converged core with open stack, container, and virtualized platform that provides flexibility and openness.

Moreover, the RAN Baseband Unit (BBU) has been a consolidated HW/SW (hardware/software) solution, and it was entirely dependent on proprietary technology and interfaces were not supporting open architectures. Today, decoupling and virtualization are a step toward more custom and open solutions fitting different needs. Above all, interfaces were not supporting open architectures.

3. Market Landscape & Current Developments

3 Market Landscape and Current Developments

3.1 Market Drivers for Private Networks

Private Networks have become one of the telecom industry's most promising growth sectors with analysts estimating it to become a $60 billion industry in the next five years. By focusing on specific IoT applications and services, Private LTE/5G networks are the ultimate solution for organizations who need an independent enterprise-grade outdoor or indoor wireless network with all the benefits that LTE/5G can offer, such as: data privacy, enhanced security, network flexibility, low latency, quality of service, network resiliency, and cost effective solution. The new era of private LTE/5G can open multiple opportunities for multiple applications with a different class of service. Global enterprise organizations, utilities and mining industries, airports, ports, sport facilities, campuses and more are already adopting this amazing technology, reducing costs, and increasing efficiency.

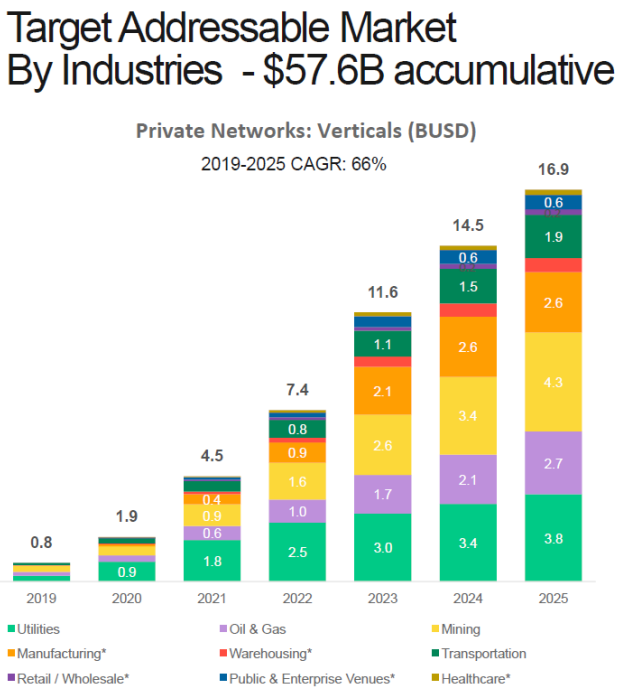


Figure *3-1* List of Enterprise Requirements

Business owners are used to managing a relatively simpler Wi-Fi network or relying on wireless services provided by an operator. With the recent growth of the performance, reliability, and security needs of enterprise, private LTE networks have become more attractive and manageable to the enterprise. However, many enterprises are still trying to figure out what commercial mobile networks can do for them and how it is different from what their enterprise-class Wi-Fi network can do.

There are several key aspects and driving factors for Indoor Wireless and Private Networks:

- **Work is changing:** More employees are working over mobile networks than IT managed networks
- **Private networks towards 5G**: Multiple private network models based on 5G application and use cases
- **Private networks enable a win-win for both wireless services providers and indoor enterprises:** Private network will enhance indoor coverage for national mobile operators beyond current capabilities
- **Private networks spectrum and OnGo certification strengthens the ecosystem**: Licensed spectrum and shared spectrum (CBRS) opportunity

3.1.1 Work is changing

Today, more employees are working over mobile networks than IT managed networks. Digital transformation is exposing the "best efforts" of Wi-Fi and the challenges it faces with application performance. Workforces around the globe are becoming increasingly tech-savvy, which has made wireless far more critical, but causing those workforces to become far more reliant on indoor wireless networks. Since the rise of the Local Area Network (LAN), Wi-Fi has understandably become the foundation of all company networks. Connecting PCs, printers, and multiple other resources around the office that use thousands of meters of cables in an office has always been a major part of the IT department's responsibilities, and probably accounts for far too much of their financial budget. As the world progresses, workforces are starting to move more business to the wireless network

and cloud-based management, including critical applications, which heighten the demands for increased mobility and throughput.

It is no doubt that wireless and private networks are not just a value resource but also a vital one. As the need for wireless spectrum has increased, it is clear the demand for data is limitless. In office buildings and facilities across America, 77 percent of Americans currently own a smart phone (Pew Research Center) and 80 percent of mobile traffic starts and ends indoors (CommScope Research).

Figure *3-2* Traffic distributions in indoor wireless services

3.1.2 Private networks towards 5G

5G technology can possibly be superior in performance to other wireless technologies such as 4G and Wi-Fi and is more flexible than wired networks. However, with recent innovative technology developments in automation and IoT, applications in a variety of broad business sectors require added privacy. 5G private networks are becoming both more tangible and inevitable for companies to remain competitive. 5G not only delivers superior indoor and outdoor range, as well as seamless mobility compared to Wi-Fi, it also provides improved interference characteristics that enable new wireless use cases.

5G is still evolving in upcoming 3GPP standard releases 16 and 17 in terms of low latency and ultra-reliability, massive machine connectivity, and support for unlicensed spectrum. Significant to this evolution are its expansion towards supporting business use cases such as enterprise offices, research campuses, manufacturing plants for automation, logistics ports and warehouses, health care facilities, shopping malls, and venues for much better productivity and higher security. 5G's broad reach has implications for important aspects for different types of business sectors and facilities. Depending on the applications they need, the required performance varies widely. An industrial automation business may need a URLLC type service while some amusement parks and retail stores may remain centered on mobile broadband connections.

Indeed, CBRS is expected to have a smooth transition to 5G in coming years, because the technology and its entire ecosystem are already well established with proof of applications for LTE mobile wireless to enterprises. Regulatory developments are also bringing new energy to the industry by setting forth rules for the development of uses for new spectrum for 5G, as well as cultivating new ways of allocating, localizing, and sharing them, as has been done for CBRS. Operators regard CBRS as a strategically important tool

for entering the private LTE market and widening their enterprise services – an area where mobile operators would like to have a stronger presence.

Mobile operators can offer their experience operating 4G and 5G networks to help the enterprise deploy its own private networks. Initial CBRS applications are mostly focused on well-understood building and enterprise remote control applications, customer services, surveillance, and voice services with 4G. However, going forward, applications that depend on high reliability, mobility and low latency will become more prominent with 5G in use cases, like automation, AR/VR, and vehicular applications. This is where mobile operators can offer their experience operating 4G and 5G networks to help the enterprise deploy its own private networks.

Other advances in wireless networks are also changing the landscape for private wireless network development. The combination of 5G and edge computing is bringing unprecedented potential access to enterprise infrastructure. Additionally, while private data centers in the enterprise were very cumbersome before the recent implementation of cloud computing, recent disruptive advances in cloud computing can be paired with enterprise communications to bring cellular networks inside a private network and treated at parity with the rest of the infrastructure. During early 5G deployments, traditional Wi-Fi and wired ethernet will continue to coexist, but in the long term, 5G will most likely to replace these technologies in more demanding environments where reliability, low latency and flexibility are mandatory and connecting thousands of machines and sensors is required.

Since 1998, 3GPP has evolved wireless cellular standards continuously from 2G GSM. However, of all the generations of cellular wireless to date, 5G is emerging as the most disruptive technology, extending its capabilities into business sectors with intrinsic capabilities to support existing and emerging business models. Initially, adopting private 5G may simply mean changing or replacing cable lines and Wi-Fi with 5G technology but will ultimately become much more enriching when redesigning processes and business model follows. Therefore, it becomes possible by introducing private 5G networks, 5G can become an innovative Industry 4.0 initiator.

Recent milestones in private networks include:

- Deutsche Telekom to build LTE-based standalone campus network using spectrum from its public network for drone deliveries to hospitals in the city of Siegen, Germany and it is known that 5G will be considered as well as the project unfolds and seeks a blueprint for a fully autonomous drone 'shuttle' service.
- Verizon's five-year contract with German pharmaceutical firm Bayer will build a cloud-based "next-generation global network infrastructure" in the context of the products and solutions integrating its NB-IoT, LTE-M, and 5G networks, plus its availability of mobile and multi-access edge computing (MEC) technologies.
- Affirmed Networks will partner with Netmore Group to deliver Private LTE enterprise networks and infrastructure, enabling Netmore to also deploy 5G enterprise services. The company seeks private enterprise networks to serve as the foundation for supporting the company's continued expansion to enterprises and locations across Europe.

3.1.3 Private Networks enable a win-win for both wireless services providers and Indoor enterprises

Private networks can enhance indoor coverage and benefit both enterprises and mobile operators by deploying both private wireless networks and public wireless networks. For office buildings and venues, basic amenities like power, water, heating and cooling are essential components that are planned and constructed. Reliable in-building wireless coverage is a new amenity to be planned or added by building owners. Today, CBRS makes it easier for the enterprises to deploy indoor wireless network by transmitting private PLMN (Public Land Mobile Network). Mobile operators working with

premise owners and enterprises to implement a CBRS wireless network provide an opportunity to enable public PLMN in these facilities for their customers. Additionally, it is easier for mobile operators to deploy the guarantees of licensed access points along with CBRS. By taking this approach, mobile operators can provide better user experiences with carrier aggregation for enterprise employees.

If enterprises want to deploy CBRS in house, they can work directly with an original equipment manufacturer (OEM) to procure the equipment. In many cases, equipment suppliers will be bundling in the backend services for the Evolved Packet Core (EPC) and the Spectrum Access System (SAS), which are both critical enabling components. However, these enterprises are required to develop some expertise with RAN and EPC architecture. Fortunately, many of these industrial companies, and even some large companies, already possess these types of IT capabilities. Enterprises can work with a managed-service provider or national mobile operator to manage their private EPC if they are not familiarized with radio, baseband, SAS, Mobility Management Entities (MME), Serving Gateways (SGW) and Packet Access Gateways (PGW), and how subscription management works in an LTE or a 5G network.

3.1.4 Private network spectrum and OnGo certification strengthens the ecosystem

CBRS creates a framework for 4G and 5G deployments in this band, which is currently under used in the US. In many other countries, the 3.5 GHz band is reserved for 5G deployments. CBRS spectrum can be shared by multiple PLMN at each location by enabling a Multiple Operator Core Network (MOCN) or Multiple Operator Radio Access Network (MORAN). For indoor wireless networks with only CBRS spectrum, Priority Access License (PAL) users will have reliable access to their allocated channels, with PPA (PAL Protection Area) and the use of the 3.5 GHz band is reserved to incumbents. General Authorized Access (GAA) users will share the remaining spectrum using mechanisms for fair coexistence. For national mobile operators, CBRS provides an opportunity to combine the freedom of unlicensed access with the guarantees of licensed access. Moreover, it is feasible to combine CBRS with unlicensed spectrum such as 5GHz License Assisted Access (LAA) and unlocked Gbps peak rates even when only 10MHz CBRS spectrum has been assigned. It will open considerable, additional capacity for indoor deployment. However, this combination will require standards, RAN (Radio Access Network) and handsets to support it. This is technically possible but will depend on market demand.

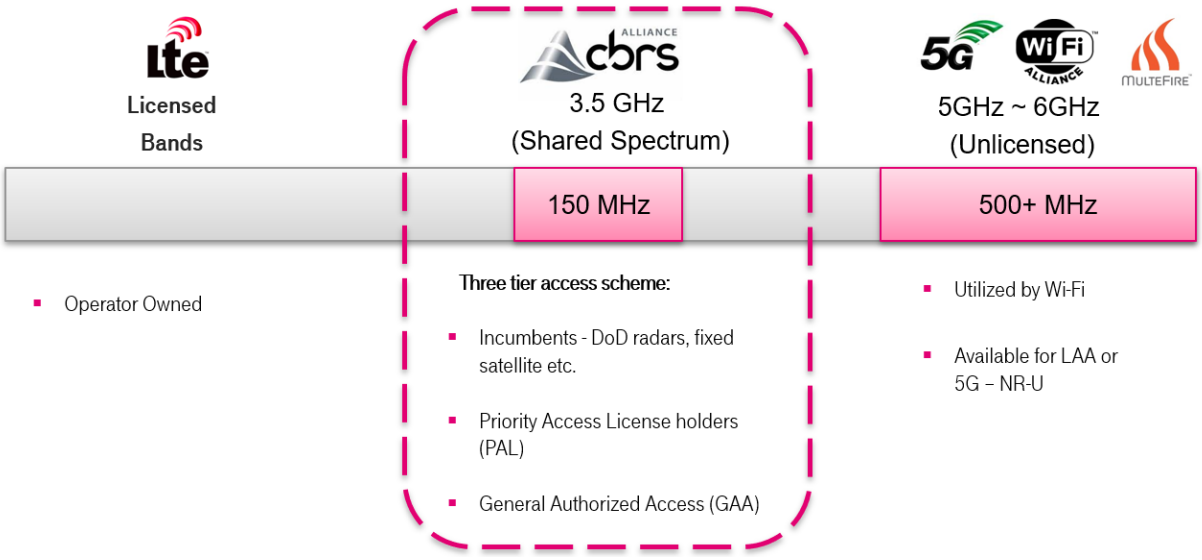


Figure *3-3* CBRS 3550-3700 MHz Spectrum Framework

Private networks are expected to become one of the telecom industry's most important growth areas, making private networks more attractive and manageable to the enterprise. With support from CBRS Alliance member companies, CTIA, and global test labs, the CBRS Alliance has developed the OnGo Certification Program to ensure seamless integration and deployment of OnGo wireless solutions, and to support widespread market adoption of OnGo technologies. With the OnGo commercial launch on September 18, 2019, CBRS RAN devices and end user devices are live in enterprises. One of the best attributes of CBRS and OnGo is that the system has been designed to be compatible with 5G. This means all private networks deployed today will be able to take full advantage of the accelerated speed and low latency of 5G.

Figure *3-4* OnGo Certification Benefits

More favorably, CBRS is an economic solution compared to conventional mobile transmissions thanks to low spectrum acquisition cost, and lowered cost for the equipment and devices by its worldwide ecosystem of 3.5GHz spectrum currently in use. The most crucial factor of CBRS is made possible by sharing the base station among the operators because CBRS spectrum is supported by all the major operators. Figure 3-5 shows the comparative unit economics of outdoor and indoor deployments [1].

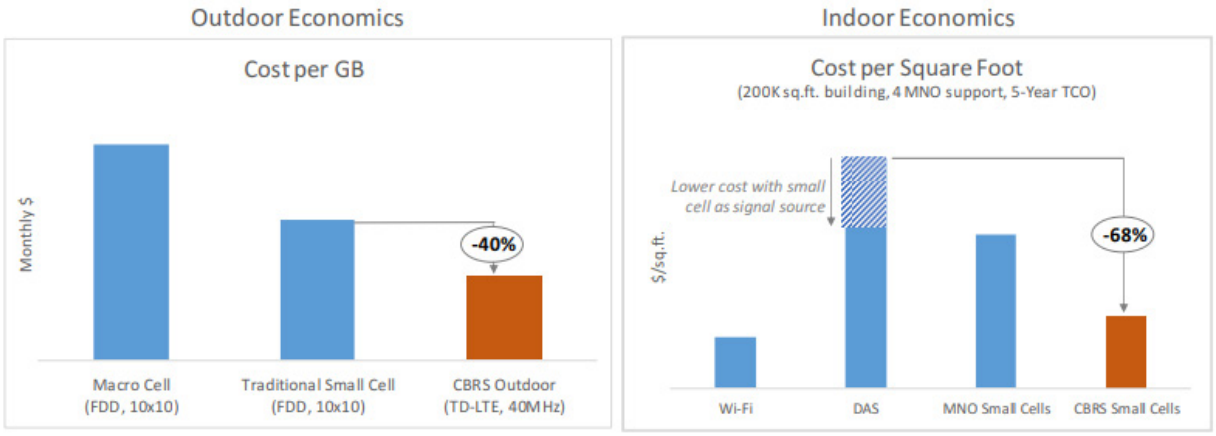
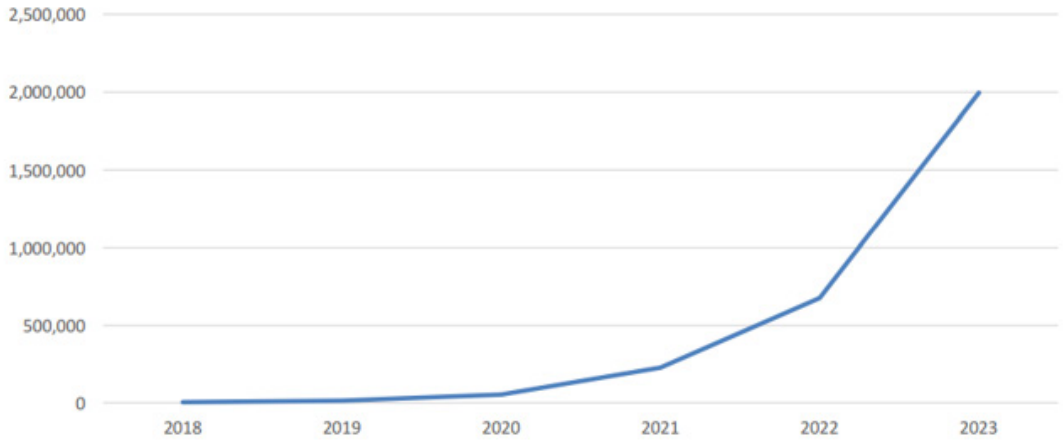


Figure *3-5* CBSD's economics vs traditional LTE network

An interesting forecast in the number of indoor CBRS nodes in commercial buildings in an iGR market study [2] in which it predicts most of these deployments will primarily be private LTE networks.

	2018	2019	2020	2021	2022	2023	CAGR
Indoor Nodes, Commercial	3,747	15,176	53,145	227,514	674,822	1,997,474	251.0%

Source: *iGR*, 2019



Source: *iGR*, 2019

Figure *3-6* Predicted growth of CBSD deployment in North America

4. Private Networks: Deployment Models & Technology Features

4 Private Networks: Deployment Models and Technology Features

4.1 Private Network: Non-Public Network Overview

In simple terms, a "private standalone network" is a network which can provide the access and connectivity to its private users, like free Wi-Fi in a shopping mall that can work independent of any service provider. A 3GPP based private network started from LTE having key capabilities with split core design (CUPS), OFDMA waveform for better spectral efficient, SON/carrier aggregation, and more LTE-Advanced features providing high throughput, high reliable and low latency.

5G came with new concept of "non-public networks" intended for the use private entity like enterprises private wireless (3GPP) solution. The key difference from 4G is that new use cases which bring very stringent requirements in terms of latency, reliability, and high accuracy with positioning. 4G was not business friendly or efficient enough to meet the performance. The combination of 5G technology with enterprise network solutions becomes crucial to satisfy these requirements in private environments. 5G came with new bands that make this new topology of private networks:

- increased capacity,
- a split control user plane of RAN and core,
- unified and programmable user planes (like I-UPF/UPF),
- UE (user equipment) and session context storage in UDSF (unstructured data storage),
- service based architecture design of the 5G core,
- and the concept of edge and fog computing with content awareness.

These combined factors make the new topology of private network is very important.
Although 3GPP Release 15 was mainly for public use, there was high interest to make such 5G networks re-designed for private topology. 3GPP releases 16 and beyond address this new network with two models:

1. **PLMN mode:** Macro and MNO centric for nationwide coverage
2. **NPN (Non-public network) mode:** Intended for solely for vertical domains, like private or large businesses, shopping malls, hot-spots or special events, and Industrial IoT (IIoT) with heterogeneous device ecosystems.

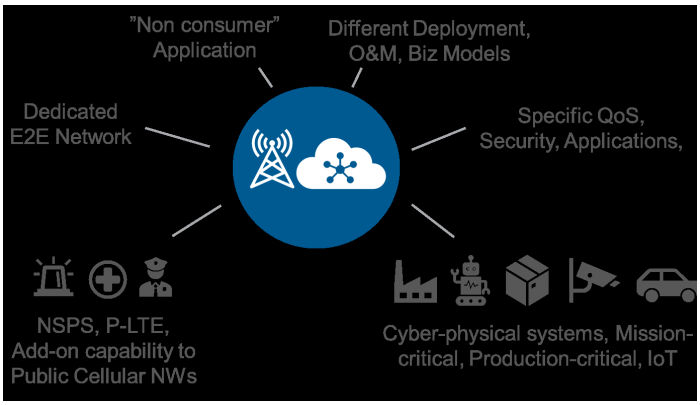


Figure *4-1* Private Network – Use Cases

Every NPN use case comes with different network and transport requirements on the network. Hence, data networks disperse into many smaller private networks addressing their requirements shown in Figure 4-2:

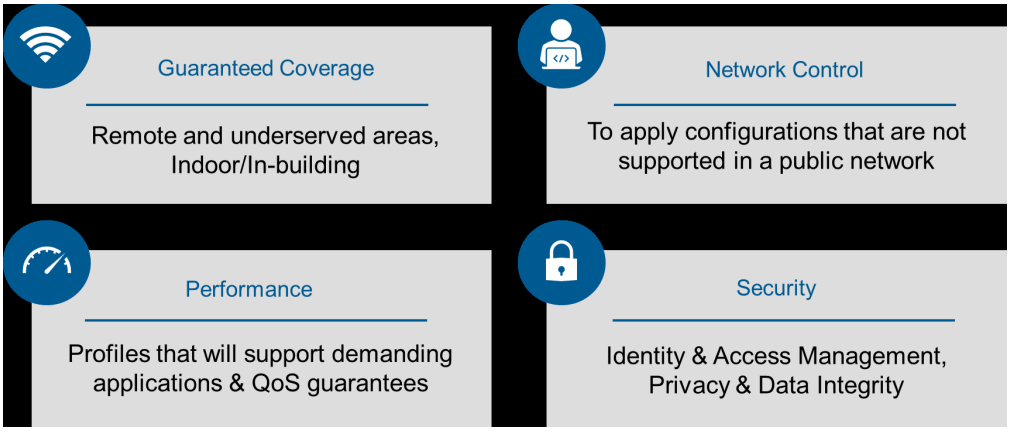


Figure *4-2* Key drivers for Private Networks

Special application functions are required depending the NPN usage for these drivers. Most importantly needed are:

- cost effective ease of deployment like zero- touch provisioning,
- a unified network management system,
- possible integrated NPN packages of 4G and 5G RAN and Packet Core solutions with a centralized traffic steering,
- voice/video capability,
- a common Subscriber Management,
- policy and privacy,
- and above all, a cloud native deployment model as shown in Figure 4-3.

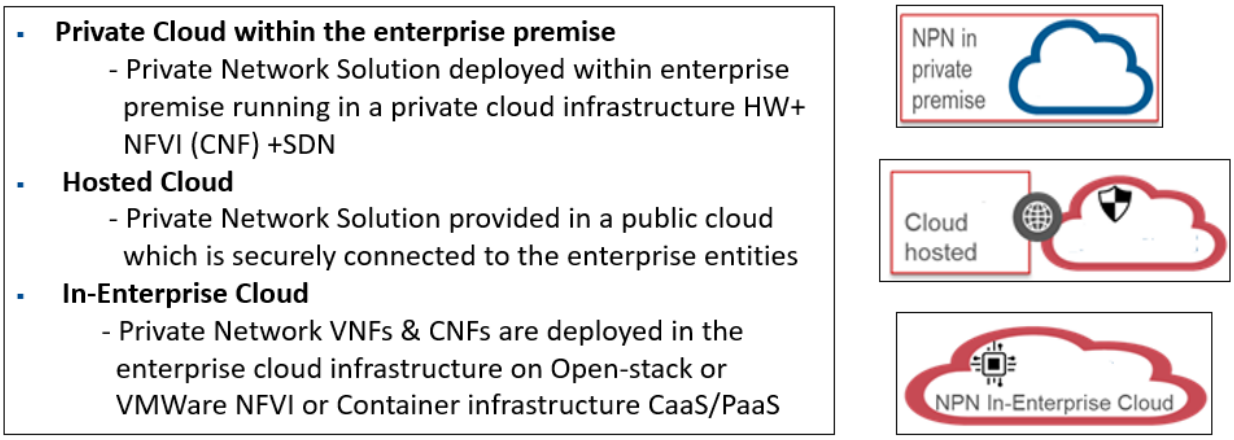


Figure *4-3* Private network with cloud native models

There are two deployment models defined in 3GPP TS 23.501 R16:

1. **Standalone Non-Public Networks (SNPN):** A SNPN private network is operated by an NPN operator which is different from a Public Network (PLMN) operator. 5G enables the non-telecom providers like Wireless Internet Service Providers (WISP) who want to have 5G services in their cluster or premises without a large macro centric infrastructure. A stand-alone NPN is an isolated and private network that does not need to interact with a traditional LTE or PLMN like 4G/5G network; instead, the NPN is deployed

on capacity centric network infrastructures. Such private networks consists of its own Radio Network with preferred spectrum, packet core, and policy enforcements that manage the devices and users with customized network Quality of services.

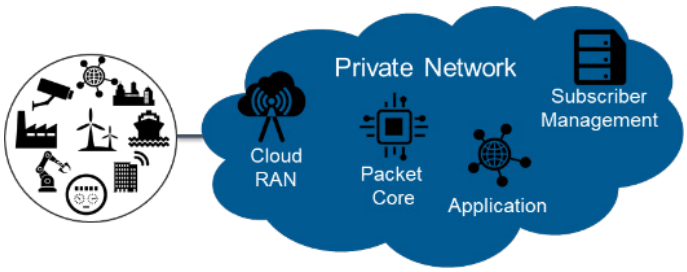


Figure *4-4 Isolated Private Networks*

A private network with its own PLMN ID could also implement roaming connectivity with special arrangement with national macro MNOs.

2. **Public Network Interface** - Non-Public Network (PNI-NPN): This is public network with integrated NPN is deployed with the support of a PLMN. A private network can work in conjunction with a public macro network operated by an MNO. In this case, the MNO can centrally manage access credentials for the private network by allowing mobility between the private and the macro networks.

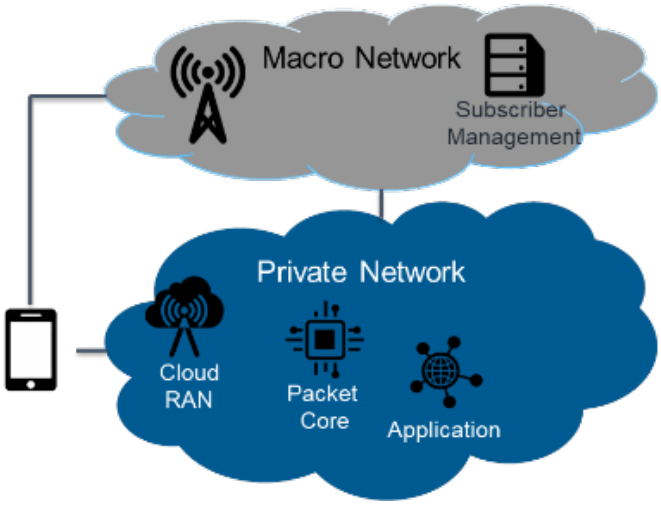


Figure *4-5* Private Networks in conjunction with a macro network

The Subscriber Data Management (SDM) in Figure 4-5 is in the macro network. The private network can authenticate access against the macro network's SDM via S6a interface for a 4G NPN or N8/N12 for a 5G NPN. For resiliency of the NPN, a local SDM can be deployed inside the private network.

4.2 Detailed View of SNPN

A stand-alone NPN private network is based on new release 5G RAN and core specifications where integration with public networks is optional. Key differentiators from the PLMN based approach are:

- the use of unique identifier for the NPN, for example, NID (network identifier), which can be independent as well as combined with PLMN ID,
- a dedicated RAN and Core with all network elements like spectrum assets, RF/CU/DU/RRM/5GC,
- and an end to end network elements like 5GC (5G Core), SDM (HSS/UDR/UDM).

4.2.1 Network Architecture

To meet the low latency and high reliability -objectives, licensed spectrum is highly preferred for the NPN. This licensed spectrum can be directly obtained from the regulator, or sub-leased from the MNO. An unlicensed spectrum like CBRS in the GAA mode can be used with access restrictions in similar topology. Different RAN deployment models can reduce the Capex like shared spectrum, shared RAN, split spectrum on single RAN, or like in a neutral host (MOCN) type of deployment. RAN based network slicing, with or without bandwidth part (BWP) or dynamic spectrum sharing (DSS), plays a major role in such disruptive deployments so existing service providers can integrate many services profiles. By introducing network slicing, customized authentication can be implemented for slice selection and access. These slices will have special charging, control functions, QoS profiles, and other features that make network management easier, and deployment faster.

NPN similar to NG-RAN architecture has all network components of control and user plane with a central management plane, or in a hosted cloud container-based deployment with shared (DU/CU)

server for a small to medium business. Local edge and core processing are commercially available now. A private solution comes with dedicated support in operation and management, security, trust and isolation, and device connectivity when it comes to service coverage.

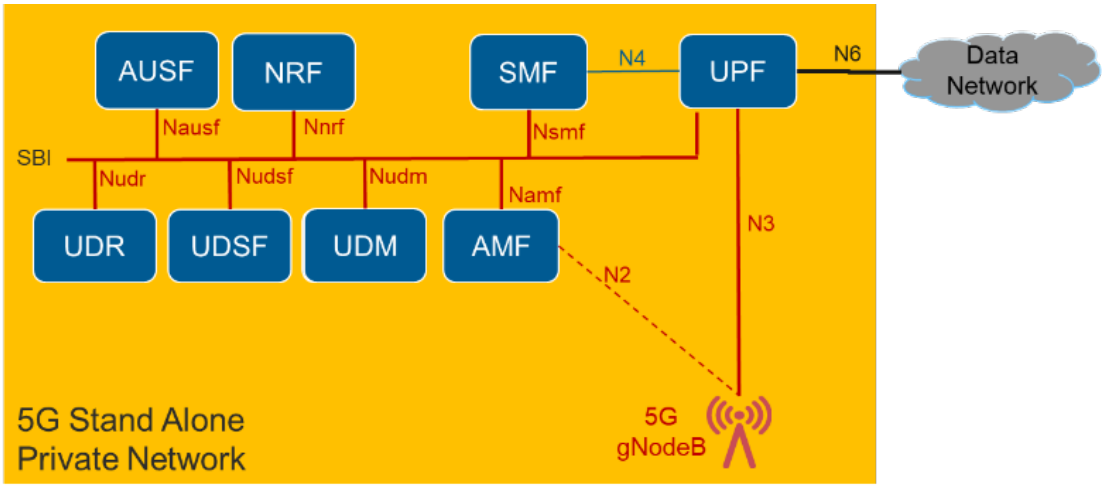


Figure *4-6* Private Networks in 5G SA with SBI

A deployment model will need the several enhancements that are discussed in following subsections.

4.2.2 Network Identifiers

It is possible to have the combination of a PLMN ID and Network identifier (NID) for SNPN. Existing MNOs can use existing PLMN IDs for SNPN(s) along with NID(s). 3GPP agreed on two assignment models:

1. **Self-assignment:** NIDs shall be chosen by SNPNs at deployment time as defined in TS 23.003.
2. **Coordinated assignment:** NIDs are assigned using one of the following two options:

- A unique and agnostic to PLMN ID or,
- only a combination of the NID and PLMN ID that is globally unique.

4.2.3 RAN's PHY layer enhancement: PBCCH enhancement

A 5G RAN needs updates on broadcast messages in broadcasting twelve NIDs (3GPP TS 38.331). This includes:

- One or multiple PLMN IDs,
- an overall list of NIDs per PLMN ID identifying the NPN networks through NG-RAN,
- and an optional human-readable network name per NID, though such NID is only used for manual SNPN selection. The mechanism for either broadcast or unicast of such NID is defined in 3GPP TS 38.331.

4.2.4 UE selection mode

A supported UE must be pre-configured with subscriber identifier (SUPI) and credentials for each subscribed SNPN identified by the combination of PLMN ID and NID. A subscriber of an SNPN is either:

- identified by a SUPI containing an IMSI, or,
- identified by a SUPI like the form of a Network Access Identifier (NAI) as defined in 3GPP TS 23.003.

Emergency services as well as voice support are not considered in current version of 3GPP. Network enhancement with support for voice is part of 3GPP release 17 (work item: FS_eNPN). If a certain UE does not support SNPN access modes, such UE will not select SNPNs.

4.2.5 Network selection mode in SNPN access mode

As defined in 3GPP TS 23.122, UEs must read the available PLMN IDs and list of available NIDs from the broadcast SIB for network selection. In automatic network selection, UE selects and register with available and configured SNPN (identified by PLMN ID/ NID). For manual network selection, UEs will be provided the list of NIDs of the available SNPNs for selection. During Initial Registration to an SNPN, the UE will indicate the selected NID and the corresponding PLMN ID to NG-RAN. NG-RAN will inform the AMF of the selected PLMN ID and NID.

4.2.6 Initial Access control: During network congestion

For overload start and overload stop, busy hour congestion, and other critical stages, SNPN is configured to support the authorized UE(s) because Unified Access Control information is configured as a part of UE's subscription information in UDS/ HSS.

4.2.7 Cell (re-)selection in SNPN access mode

UEs operating in SNPN access mode only select cells with a configured and allowed cell broadcasting for both PLMN ID and NID of selected SNPN. In 5G-RAN, such idle mode behavior is applicable to RRC-inactive states.

4.2.8 Access to PLMN services via stand-alone non-public networks and vice versa

A UE that is registered in a PLMN can perform another registration to an SNPN through the PLMN user plane. This is an "over-the-top" architecture whereby in a first step the dual-subscription UE uses the PLMN subscription to get a data connection to the Internet. Then, the UE uses an SNPN subscription to get access to the 5G Core Network of an SNPN using the architecture for "Untrusted non-3GPP access" defined in 3GPP TS 23.501 [2], for example, by establishing an IPsec tunnel with an N3IWF (Non-3GPP Interworking Function) node of an SNPN. This case is illustrated in Figure 4-7.

Similarly, a UE that is registered in an SNPN can perform another registration to a PLMN through the SNPN user plane.

The firewall may be good option to integrate between NPN operator (for example, the vertical) and the PLMN operator (for example, the MNO). Privacy of the UE identity is preserved by registering to the serving network with a subscription concealed identifier (SUCI), a one-time useable identifier created from the subscription identifier (SUPI).

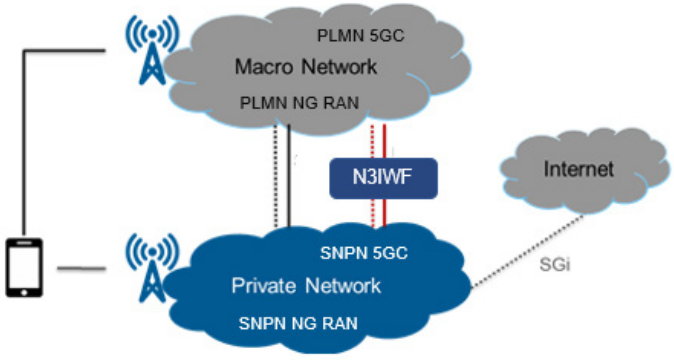


Figure 4-7 Access to SNPN services via PLMN vs direct access to SNPN

Another representation 5G stand-alone core is the reference point architecture illustrated in Figure 4-8.

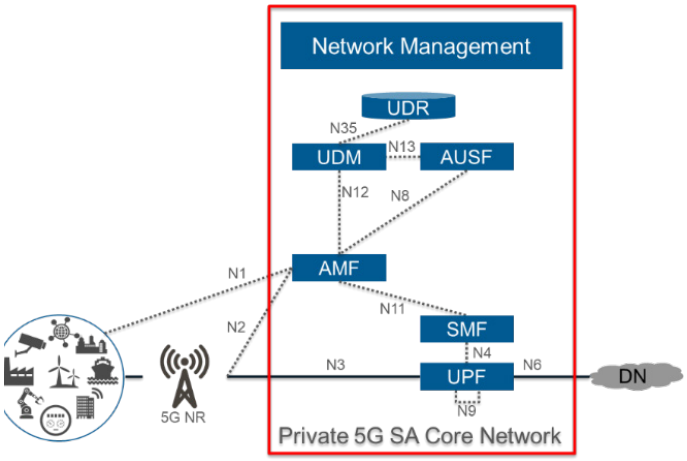


Figure *4-8* Stand-Alone 5G NPN – Reference Point Architecture

Figure 4-8 illustrates the basic 5G Private Network design providing N6 interface to Data Network. It can be expanded to accommodate more use cases and functions. Below lists are extension options:

- Short Message Service Function (SMF) to support for narrow-band SMS based Internet of the Things (IoT) services and applications functions implementing SMPP.
- Policy Control Function (PCF) if user/device specific data traffic policies (QoS) is required.
- Network Slice Selection Function (NSSF) in case multiple SMF or UPF slices are required.
- Network Exposure and NB-IoT application functions implementing REST based interface N33.
- Security Edge Protection Proxy (SEPP) to interconnect to other 5GC networks via SBI based HTTP/2 using N32 interface.

4.3 Detailed view on Public network integrated NPN

PNI-NPN is another category of NPN with aid from MNO's PLMN. 3GPP Release-16 also specifies the ability for UE to obtain PLMN services while camping on the Stand-alone Non-Public RAN when the UE has a subscription and credentials to obtain services from both PLMN and SNPN. It is supported using network slices or Closed Access Group (CAG) cells or a combination of both.

PNI NPN operation may optionally make use of the concept known as Closed Access Group (CAG) which enables the control of UEs' access to PNI NPN on a per cell basis (CAG cells), and for which a UE may be configured with CAG information on a per PLMN basis.

Network slices are network instances for individual customers using the same infrastructure to be dynamically shared by different tenants. They are composed of capabilities from multiple network segments from the access to the core as well as applications.

In the case of 'Public Network Integrated-Non-Public Network (PNI-NPN)', the PLMN ID identifies the network, and the CAG ID identifies the Closed Access Group (CAG) cells. A CAG cell broadcasts one or multiple CAG Identifiers per PLMN. CAG is used for the Public (for example, it is used for authorization at network/cell selection independent from network slice selection). The UE can move between CAG and non-CAG cells unless it is restricted by configuration to only access CAG cell. Service provider can have below two scenarios:

- **Scenario 1:** The private network is deployed isolated from the macro network. There is no mobility of subscribers to or from the macro network. There can be only a roaming agreement in place to support mobility and session management as an option.
- **Scenario 2:** Subscribers have mobility between macro networks and private networks. The subscribers can use the same device and SIM card in the private networks and macro networks. Conversely, the macro network subscribers will be able to use the private network as if it were the macro network. A roaming or other service agreement is assumed to support such scenario.

Network selection and reselection is based on PLMN ID. Cell selection and reselection, access control based on CAG ID. The CAG cell shall broadcast information such that only UEs supporting CAG are accessing the cell.

There are few deployment options available for integrating PLMN with NPN and such options will be covered in next section. Key enhancements on a basic PNI-NPN network are addressed in the following sections.

4.3.1 UE enhancements

UE needs to be pre-configured with allowed CAG list or with a CAG indication where the UE is only allowed to access 5GS via CAG cells. In presence of a PLMN, the UE shall only consider the CAG information provided for registered PLMN in System Information Block (SIB) broadcast.

4.3.2 RAN enhancements

A 5G RAN needs more upgrade to support such topology. Some of them are listed below:

- CAG supporting capability indicator; Broadcast Control Channel (BCCH) must broadcast for supporting UE for accessing the cell
- 5G RAN must continue to use C-Plane load control, congestion, overload control, access control, access barring, Extended Access Barring (EAB) and Unified Access Control to prevent access to NPNs
- Standard procedure for automatic and manual network selection in relation to CAG, TS23.122, TS 38.304
- Mobility Restrictions impacting the UE's mobility according to the Allowed CAG List, like Source NG-RAN shall not handover the UE to a non-CAG cell if the UE is only allowed to access CAG cells
- UE transition from CM-IDLE to CM-CONNECTED: UE is accessing the 5GS via a CAG cell, UE shall provide the selected CAG Identifier to NG-RAN and NG-RAN shall provide the CAG Identifier to AMF
- In transition from RRC Inactive to RRC Connected state: After UE initiates the RRC Resume in a CAG Cell then NG-RAN shall reject the RRC Resume request if none of CAG Identifiers supported by the CAG cells are part of the UE's Allowed CAG list

4.3.3 Network selection mode in PNI-NPN access mode

The following are the principles for network and cell selection in PNI-NPN, as well as for access control:

- CAG cell broadcasts CAG identifier(s) for UE to decide on "cell suitable" to camp. (TS 38.304)
- In transition from idle to connected state: NG-RAN forwards the CAG identifier(s) to AMF. AMF matches the user's subscription and allowed CAG identifier(s) of the CAG cell and share any Mobility Restrictions information to the NG-RAN.
- In mobility procedures NG-RAN takes care to never hand over the UE to a target CAG cell that is not allowed for this user according to the user's Allowed CAG list.

4.3.4 Deployment options: NPN is hosted by Public network (MNOs)

A private network does not necessarily need to have all core network functions in this mode of integration; instead, MNO can leverage the existing infrastructure. Only a private user plane function to accommodate special traffic handling is required by the private network.

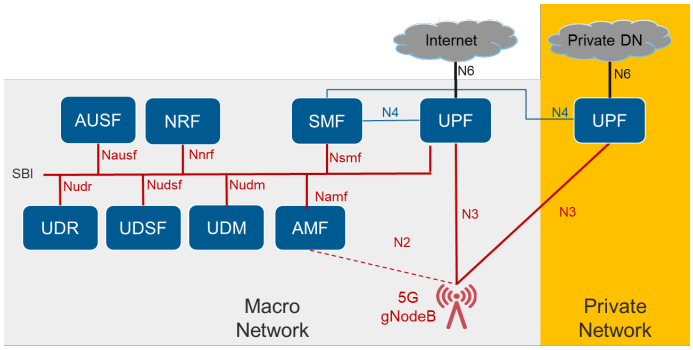


Figure *4-9* Private User Plane Function

To allow also private control and user plane being part of the NPN, the SMF function can be moved to the private network interconnecting with the AMF of the macro network using N11.

A further evolution providing even more private network implementation cases is the availability of a converged 4G and 5G core as illustrated below.

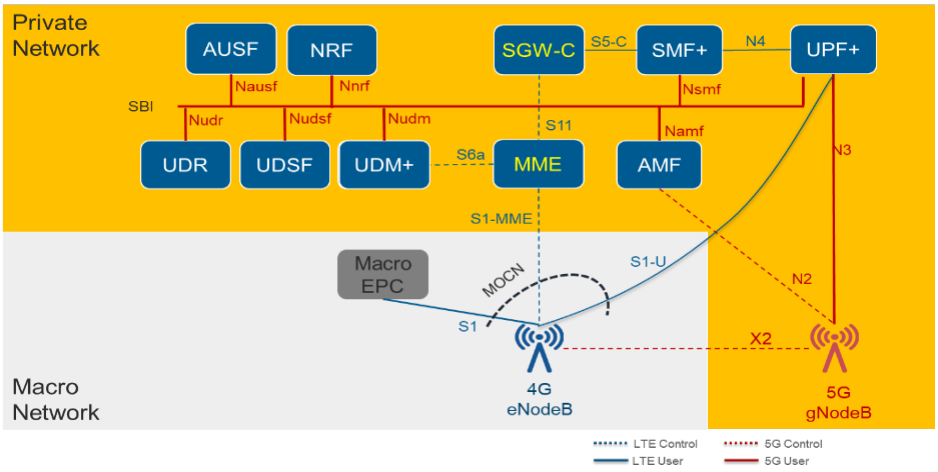


Figure *4-10* Converged 4G and 5G Core

4.4 NPN ORAN (or vRAN) deployment and Transmission Requirements

For private network deployment it is assumed that fiber connectivity between the Radio Unit to the NPN data center. That allows the Distributed Unit (DU) to be deployed on the same NPN data center hardware. In specific cases DU can be also deployed at cell site or at some aggregation point depending -on the distance between cell site and data center or extraordinary capacity demands at the cell site.

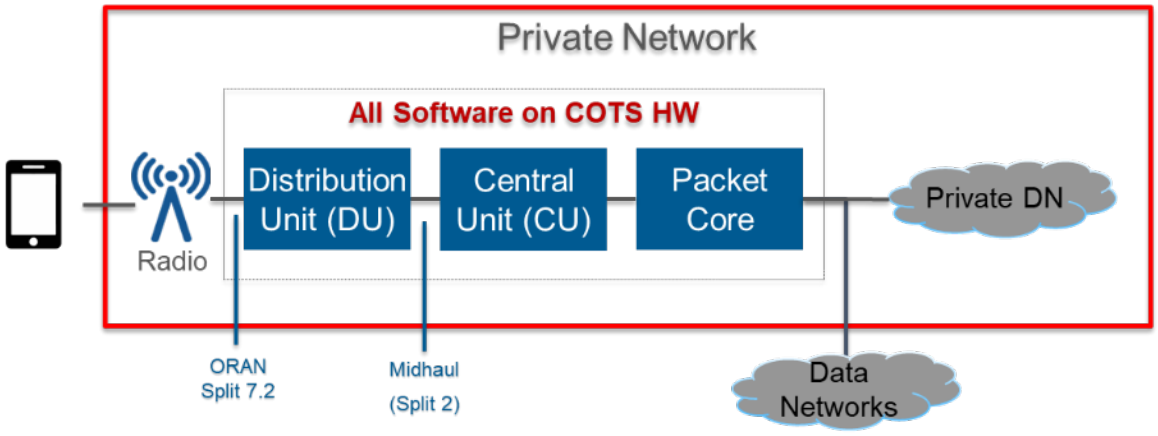


Figure *4-11* ORAN (or vRAN) Deployment for NPN

To achieve excellent network performance (KPIs) there are several requirements on both transmission networks, which need to be kept:

Table *4-1* Transmission Requirements for Network Performance

Transmission	Protocol	Physical req.	Max distance	Max RTT	Bandwidth
Split 7.2 RU – DU Cell site to data center	Ethernet (L2/(L3))	Fibre	10km	200µs	10Gbps
Split 2 DU – CU	Ethernet (L2/L3)	Fibre or metallic	In tolerance	20ms	10Gbps
N2/N3 – CU – 5GC X2 – network eNB (anchor eNB)	Ethernet (L2/L3)	Fibre or metallic	In tolerance	20ms	1-10 Gbps – Depending the use case

If fiber connectivity from the radio unit to the DU is not available, the DU needs to be to the placed closer to the radio unit. For that purpose, a ruggedized COTS hardware is available to host the DU.

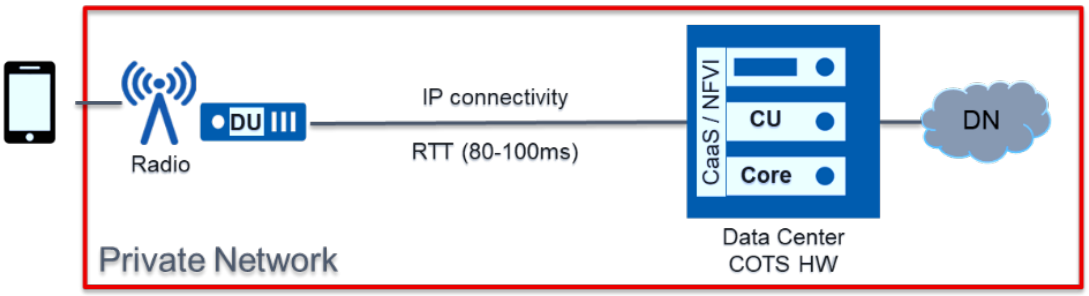


Figure *4-12* Latency constraints for NPN in RAN split topology

The below illustration shows the connectivity requirements of the data center running the 4G or 5G Core as well as the ORAN or vRAN like components.

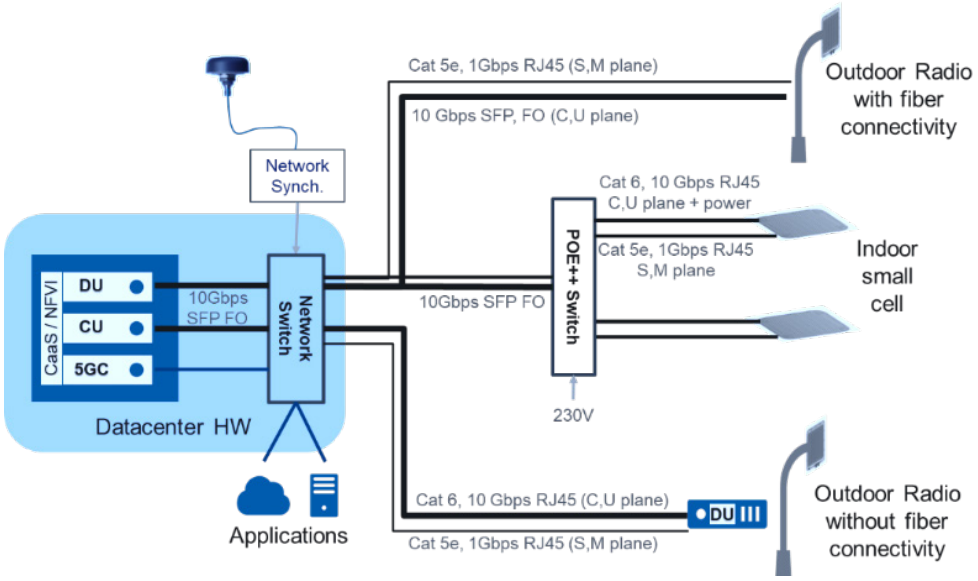


Figure *4-13* NPN Connectivity – RAN full view

As mentioned earlier, the Packet Core is key subsystem of the NPN. The evolved packet core with split control and user plane (CUPS) and SBA architecture (5GC) enabling the following different network architecture options agnostic to RAN model:

- 4G Package Core based private network
- 5G Core based private network

Table *4-2* NPN deployment model - end to end LTE/Option 3x Connectivity

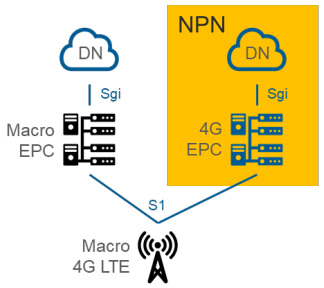
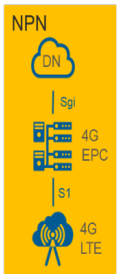
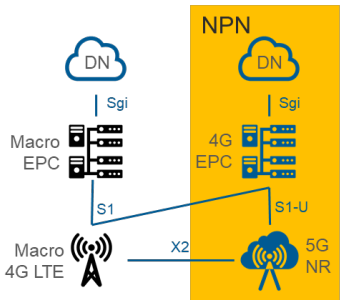
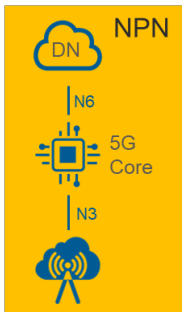
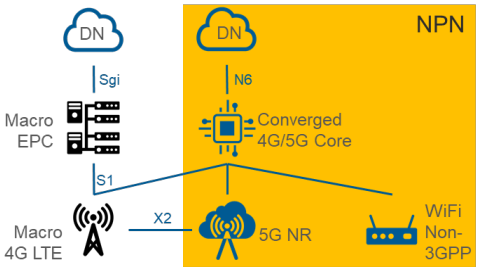
4G Package Core based NPN Option		
Radio	Description	Illustration
Sharing 4G Macro Radio	4G based NPN using Macro Radio coverage Private 4G EPC sharing macro radio using DÉCOR or MOCN to select the network. Capable to provide user security and privacy, full session and mobility management	
Private 4G Radio	4G based standalone NPN with private 4G Private Stand Alone 4G Packet Core Private Stand Alone 4G RAN Licensed/Unlicensed/ or combination of both (LAA/CBRS)	
Sharing 4G Macro Radio + Private 5G Radio	5G NSA based NPN with private 5G Radio and macro 4G Radio coverage Private Non-Standalone Packet Core supporting 4G and 5G NR. 4G Macro network can use DÉCOR or MOCN to select the network.	

Table *4-3* NPN deployment model - end to end 5G Connectivity (with converged core)

5G Core based NPN Option		
Radio	Description	Illustration
Private 5G Radio	5G Core based NPN with private 5G radio.	
Sharing 4G Macro Radio + Private 5G Radio + Wi-Fi (Optionally)	4G and 5G Combo Core Converged LTE and 5GC supporting 4G Option 3 and 5G Option 2. Optionally support for non 3GPP access.	

4.5 Key Technology Features applicable to Private Networks:

4.5.1 URLLC

Typical use cases in 5G are e-MBB, m-MTC, and very challenging one ultra-reliable and low latency control (URLLC). Most demanding applications, like motion control, require the communication service availability of as long as 99.99% and the end-to-end latency of as short as 500 µs. The URLLC challenge is not merely limited to enabling a low-latency or an ultra-reliable link. It is also about the end-to-end implications and tradeoffs, in providing an available, efficient, and sustainable service. Use cases are considered only if their requirements on low latency or high reliability targets or both cannot be compromised.

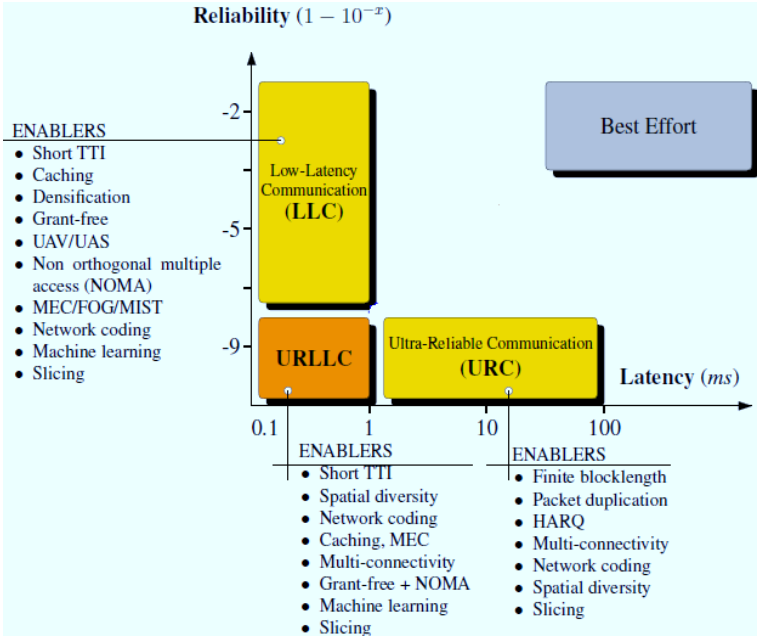


Figure *4-14* Enabler for low latency and low reliability

Transmission of multiple control signals via "multi-TRPs" may be beneficial to improve reliability of the URLLC. High frequencies (for example, mmWave) in 5G facilitate deployment of a large number of small cells with large antenna array elements (beamforming and massive-MIMO) for multi-TRP technology, which are not currently supported by 4G. LTE came with "CoMP" (coordinated multi-point concept) but 4G CoMP cannot sufficiently support practical scenarios, such as non-ideal backhaul, and therefore cannot provide deployment flexibility (for example, non-collocated TRPs). CoMP requires a highly detailed feedback (for example, channel state information) and close coordination between the TRPs. When multiple TRPs are connected with a non-ideal backhaul, the joint scheduling among the TRPs may not be feasible due to delay or limited backhaul capacity, resulting in a poor link adaptation, or performance loss. 5G in mmWave though has high signal loss and blockage issue, but if used in multiple independent links via multi-TRPs provides a robust against blockages and beam failures.

Relaxing the backhaul and synchronization requirements in the multiple TRPs will enable non-coherent joint transmission because each TRP can independently schedule a transmission without exchanging channel state information, scheduling information, for example, with other TRPs.

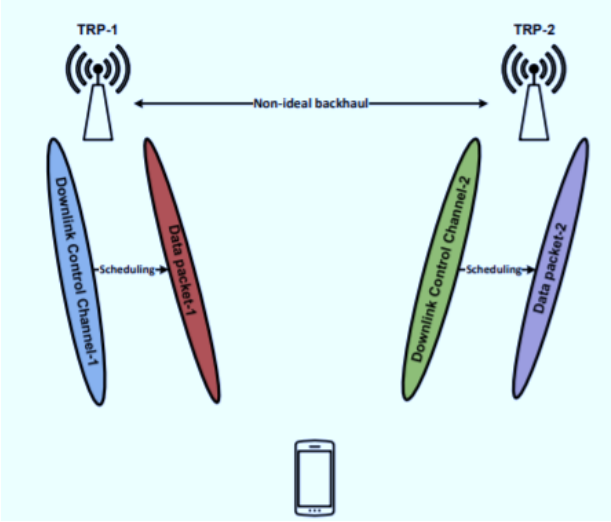


Figure *4-15* Multi-TRP in 5G-NPN

4.5.2 Low latency in 5G NR

The process in radio access network is comprised of gNB/UE processing and DL/UL control/data transmission as it could be seen in below figure that illustrates the latency components in each step of a downlink (DL) data transmission and the corresponding mechanisms to reduce the latency:

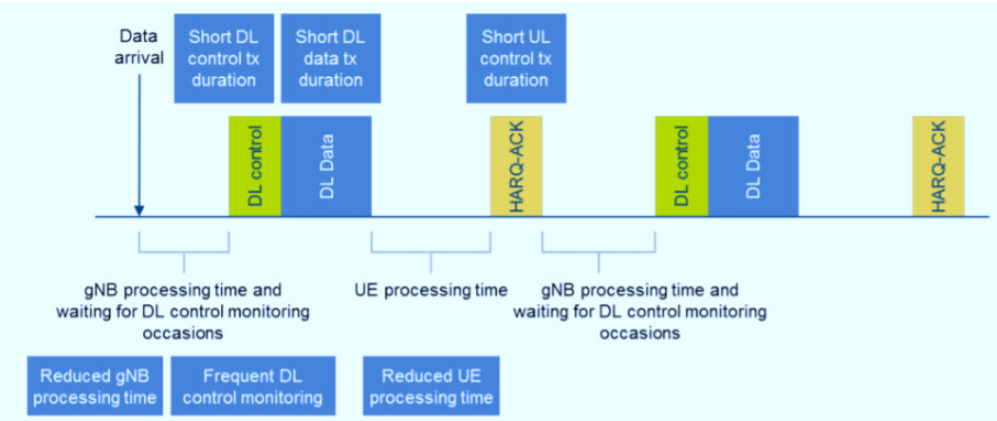


Figure *4-16* Enabler for low latency

To address the latency reduction in 5G NR changes in PHY/MAC, layers are required reduce the latency, but are easily manageable because of 5G Split RAN design and shared DU in private 5G solutions as discussed in the following subsections.

4.5.2.1 Frequent transmission opportunities that minimize waiting time

Utilizing preemptive scheduling when there is ongoing eMBB traffic, scheduling more than one PUCCH for HARQ ACK in a slot to support simultaneous eMBB and URLLC and supporting out of order HARQ feedback/traffic channel for URLLC over eMBB.

4.5.2.2 Flexible frame structure for Time Division Duplexing (TDD) and Flexible transmission duration (short duration for both data and control channel)

5G NR supports several subcarrier spacings (SCS) and transmission time interval (TTI) can be less than a slot unlike LTE. TTI is normally one time slot but can be a few symbols of 2, 4 and 7 which is called mini slot in 5G NR. For example, the TTI can be as little as 35.7μs by 2 symbols with 60KHz SCS.

4.5.2.3 Short UE processing time and Short gNB processing time

DMRS is front loaded so that the reference signal can be processed in one symbol duration and following data can be immediately demodulated. Also, LDPC (Low Density Parity Check) is newly applied channel coding in 5G NR to facilitate its parallel processing that results in faster processing.

4.5.2.4 Grant-free (or configured grant) UL transmission

SPS (Semi-Persistent Scheduling) can be configured for DL per bandwidth part to reduce the scheduling latency by UL grant request and DL transmission grants. UL grant free scheme is similar to DL SPS in UL.

4.5.2.5 RRC Inactive mode

A new state called RRC Inactive mode is introduced in 5G NR. In this mode, all the contexts related to the UE is reserved in base station while they are removed in RRC Idle mode. It enables to facilitate faster activation time to transition to RRC Active mode compared to transition from RRC Idle mode to RRC Active mode and help to save the energy of the UE.

4.5.2.6 High reliability in 5G NR

To address the high reliability with low latency, air interface channel needs to be re-designed with a high reliability target. URLLC requires lower spectral efficiency when reliability and low BLER is addressed. At the 5G NR PHY layer, the following techniques aspects have been defined in 3GPP used to improve reliability:

1. **Data channels:**
   - Channel coding: To facilitate efficient HARQ support and designed with error floor optimization
   - Channel State Information (CSI) report enhancements: Lower BLER target for scheduling, CSI reporting and the corresponding CQI table
   - Frequency/spatial diversity: Frequency and spatial diversity to improve the reliability. Spatial diversity method for reliability by non-collocated Transmission Points (multi-TRP).
   - New CQI/MCS table: The UE can be configured to report CQI using a separate CQI table targeting lower code rate to support URLLC traffic with very high reliability requirements for target BLER of 10^{-5}. Special MCS tables for traffic channels are also defined in 3GPP Rel16.

2. **Control channel:**
   - A compact Downlink Control Information (DCI) with small payload size is useful for improving the reliability. In addition, higher aggregation levels can be supported for the DL control channel to reduce the effective code rate

3. **Repetitions for data and control channels:**
- When there is not sufficient time for the UE to process and provide HARQ ACK
- Packet Duplication at the RAN Layer: Using packet duplication at the RAN layer allows the packet to be transmitted with two independent radio paths in the air interface.

5G Core also supports provision of end to end latency reduction and reliability. Selection of local area data network , flexible placement of UPF, local routing and traffic steering, redundant tunnels (shown below), edge or fog computing integrated with RAN's RIC platform (ORAN) or with UPF, Multi-homed PDU Session with Uplink Classifier, session and service continuity to enable UE and application mobility are the important aspects to aid RAN for further reduction in latency and increase reliability.

4.5.2.7 QoS in URLLC services and applications

One of the key requirements for URLLC services is the stringent end-to-end QoS goals that include low latency and high reliability. The QoS differentiation within a PDU session is defined by QoS Flow ID (QFI). QFI is used as U-plane marking on N3/N9 interfaces and is unique within a PDU session. A standardized set of 5G QoS Indicators (5QIs) are defined and new "resource type", Delay Critical GBR, is also defined. A concept of "Reflective QoS" (RQoS) is defined by creating a derived QoS rule in the UE based on the received downlink traffic. The UE inspects the IP 5-tuple in the downlink packet, creates a "mirror" packet filter and associates the QoS of the downlink packet to uplink packet. RQoS is used to minimize the need for control-plane signaling (N1).

4.5.3 NR positioning

Release 16 specifies NR to provide native positioning support by introducing RAT-dependent positioning schemes. These support regulatory and commercial use cases with more stringent requirements on latency and accuracy of positioning. Location accuracy and latency of positioning schemes improve by using wide signal bandwidth in FR1 and FR2. For regulatory use cases, the following are the minimum performance requirements:

- Horizontal positioning accuracy better than 50 meters for 80% of the UEs
- Vertical positioning accuracy better than 5 meters for 80% of the UEs
- End-to-end latency less than 30 seconds
- For commercial use cases, target limits are:
- Horizontal positioning accuracy better than 3 meters (indoors) for 80% of the UEs
- Vertical positioning accuracy better than 3 meters (indoors and outdoors) for 80% of the UEs
- End-to-end latency less than 1 second

Several RAT-dependent NR positioning schemes being considered for private and NPN like network deployment as below:

- **Downlink time difference of arrival (DL-TDOA):** A new reference signal (positioning reference signal (PRS) is introduced for the UE to perform downlink reference signal time difference (DL RSTD) measurements for each base station's PRSs and sends these measurements to location server.
- **Uplink time difference of arrival (UL-TDOA):** Sounding reference signal (SRS) is enhanced to allow each base station to measure the uplink relative time of arrival (UL-RTOA) and report the measurements to the location server.
- **Downlink angle-of-departure (DL-AoD):** The UE measures the downlink reference signal receive power (DL RSRP) per beam/gNB. Measurement reports are used to determine the AoD based on UE beam location for each gNB. The location server then uses AoD to estimate the UE position.
- **Uplink angle-of-arrival (UL-AOA):** The gNB measures the angle-of-arrival based on the beam the UE is located in. Measurement reports are sent to the location server.
- **Multi-cell round trip time (RTT):** The gNB and UE perform Rx-Tx time difference measurement for the signal of each cell. The measurement

reports from the UE and gNBs are sent to the location server to determine the round-trip time of each cell and derive the UE position. Enhanced cell ID (E-CID). This is based on RRM measurements (for example DL RSRP) of each gNB at the UE. The measurement reports are sent to the location server. New LPP-a stack used for this.

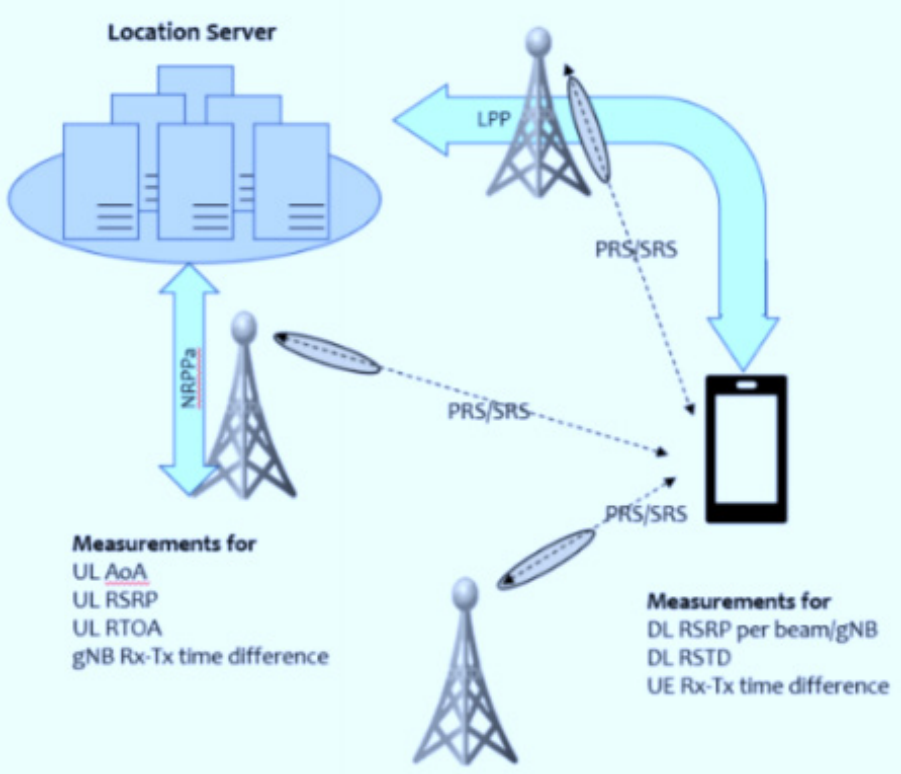


Figure *4-17* NR positioning key enablers

4.6 Time Sensitive Networking (TSN)

Support for Time Sensitive Networking (TSN) is an add-on functionality that is applicable to both public and non-public networks. In many deployment scenarios it can be assumed that an NPN will also be used to support TSN. It enables 5GS to provide time synchronization of packet delivery.

3GPP Release 16 has defined that 5G System needs to be integrated with an external network providing TSN services as a TSN bridge. Currently, only a centralized TSN model is covered.

The TSN support includes single and multiple working clock domains via single architecture where:

- gNBs provide only sync for UEs for 5G-clock (sent OTA) and RAN remains agnostic to external time domains,
- UPFs time-synced to the gNB/RAN clock,
- external clocks synced via user-plane path with time stamping in TSN translators at the edge,
- and all 3GPP user-plane nodes are synced to one common clock (3GPP 5G clock).

The entire 5G system can be considered as an 802.1AS “time-aware system”. Architecture enhancements to enable better reliability for URLLC have been suggested in four different variants:

1. Dual connectivity-based end to end redundant PDU sessions for the service associated with URLLC
2. Redundant user planes between NG-RAN and UPF (redundant N3/N9 interfaces) for same PDU session
3. Underlying transport network redundancy where UPF transmits packets utilizing two different redundant transport link and NG-RAN eliminates redundant packets and vice versa
4. URLLC QoS monitoring features were introduced to react to any performance degradation

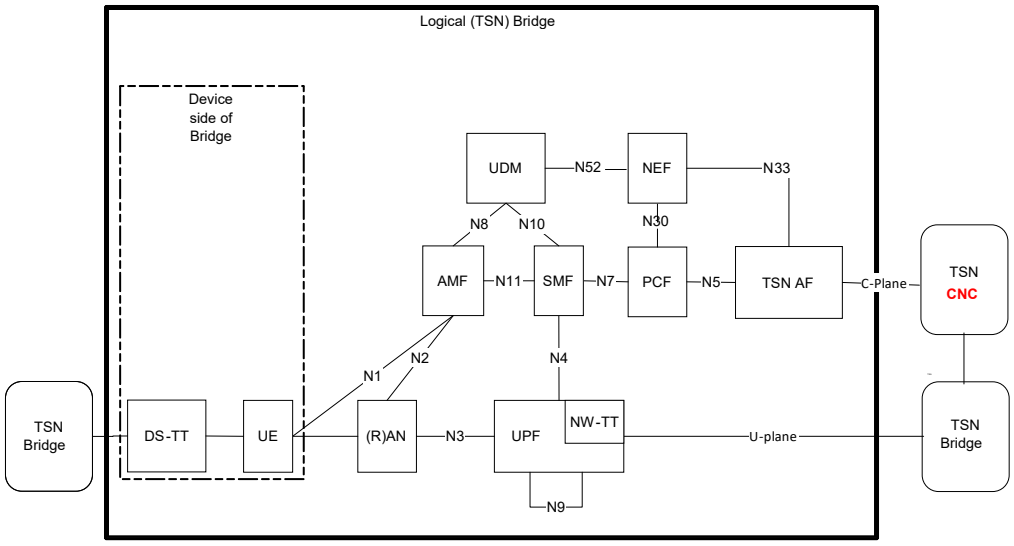


Figure *4-18* System architecture view with 5GS appearing as TSN bridge

5. CBRS: Redefining Private Networks

5 CBRS: Redefining Private Network

5.1 CBRS overview

CBRS is a shared wireless broadband use of the 3550-3700 MHz band (also referred to as 3.5 GHz Band). CBRS (also commonly known as the 'innovation band') was envisioned to support a 3-tier shared spectrum model to facilitate shared federal and non-federal use of this band using automated frequency coordinators, known as Spectrum Access Systems (SASs).

CBRS's high level view and its three tiers are covered in section 3.1.4.

Key features include:

- **Best spectrum utilization:** through spectrum sharing (SAS/ESC); always busy, always available
- **Combo public and private wireless infrastructure:** PALs for public networks, GAA for private networks. "OnGo solutions" to address both the needs of networks operators or WISP to integrate CBRS into wide-area networks
- **Alternative of macro's wide networks:** sustainable, scalable business models for location-specific connectivity and not limited to indoor solution only. No dependency on Tier 1 MNOs
- Same RF interface as LTE in the licensed spectrum or in the unlicensed 5 GHz band, the difference with CBRS lies in spectrum assignment
- Very large and mature device ecosystem already in market

5.1.1 Business players in CBRS domain

Table *5-1* "CBRS as a service" from different providers

Why MNOs should spend in CBRS?	Why WISPs (FWA) must look in CBRS?	What IIoT Industries will get from CBRS?	Neutral Host providers? Is there any advantage?
For their ultra-densification: 4G/5G indoor/outdoor	Last mile, point to multipoint: rural and sub -urban, expand to unserved and underserved	Need Private NW to maintain security and privacy	DAS-like deployment for special cases like events, mall, hotels, Small-medium business
Capacity – 5G mmWave and LAA not enough (low footprint), additional revenue in 5G FWA in NR-CBRS, MNOs lack mid band TDD spectrum	Compete with MNOs in Private LTE/NR business	New use cases: AR/VR/MCPTT/automation/self-managing NW/ smart cities	IaaS from their Het-Net deployment, piggyback with 2.4/5 GHz

5.2 Network Elements in CBRS architecture

The core principle of CBRS is dynamic spectrum access in a tiered system. For that, a real-time spectrum coordination mechanism has been created to facilitate the spectrum sharing. The spectrum coordination architecture for CBRS is based on a distributed system. At the top of the hierarchy is the FCC database which centralizes spectrum allocation. The next tier is the Spectrum Access System (SAS). The SAS is a third-party certified vendor offering SAS services. The next tier is the sensor network referred to as the Environmental

Sensing Capability (ESC). The ESC system detects and communicates the presence of a signal from an Incumbent User to an SAS to facilitate shared spectrum access. The next tier is the SAS user network which interaction with the SAS for PAL and GAA usage.

At the heart of the system is the Spectrum Access System (SAS). It is the gatekeeper that takes information from the FCC Database, other SASs, Environmental Sensing Capability (ESC), and the CBRS Broadband Service Devices (CBSD). Then it applies the FCC rules to allocate Frequency and Power resource to each of the CBSDs.

A high-level view of CBRS spectrum sharing system is given in Figure 5-1.

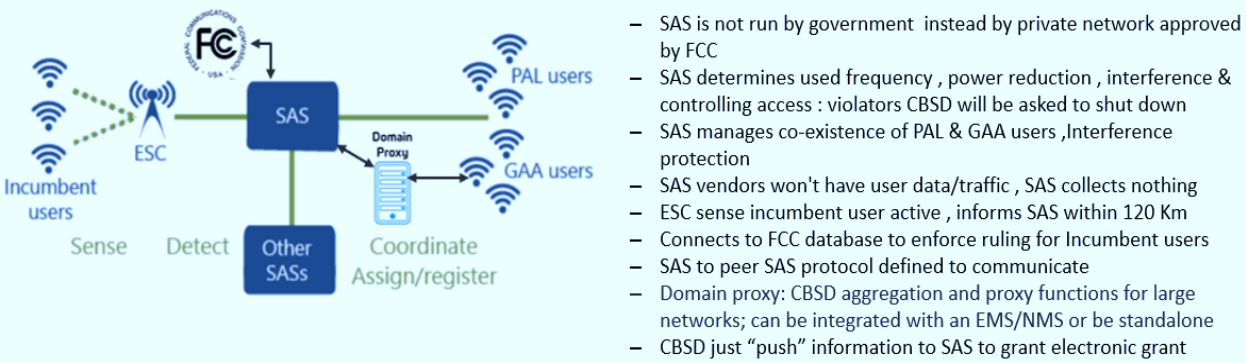


Figure *5-1* CBRS network elements with roles and responsibilities

5.3 CBRS Requirements

The following section reflects the requirements on Citizens Broadband Radio Service Device (CBSD), End User Device (EUD), Priority Access License (PAL), and General Authorized Access (GAA) to specify the necessary operation and standards interfaces to effect a properly functioning spectrum sharing environment in the 3550-3700 MHz band.

We strongly encourage the reader to visit following link for further detail on all requirements:
Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band: Document WINNF-TS-0112, Version V1.9.1, 11 March 2020.

Table *5-2* CBSD ruling – PAL vs GAA and Cat A vs Cat B

CBRS Equipment	EIRP dBm/10 MHz
End User Device	23
CAT A CBSD	30
CAT B CBSD	47

Device limitation	Can operate after successful decoding of SIB1 from CBSD
Cat A limitations	6m. Antenna Height @ outdoor ,
Cat B limitations	CPI installed , Outdoor only and must meet SAS/ESC guidelines

PAL – 70 MHz to 100 MHz (3550 MHz to 3650 MHz)
- Auction, bid, secure & win block of 10 MHz , lower 100 MHz range , managed /protected by SAS from GAA users
- RRU will cover all 100 MHz but winner won't know which 10 MHz : its floating spectrum in real
- One winner can acquire maximum of 40 MHz in one market
- No PAL in upper 50 MHz
- CBSD will report location, power , azimuth , beam tilt/width

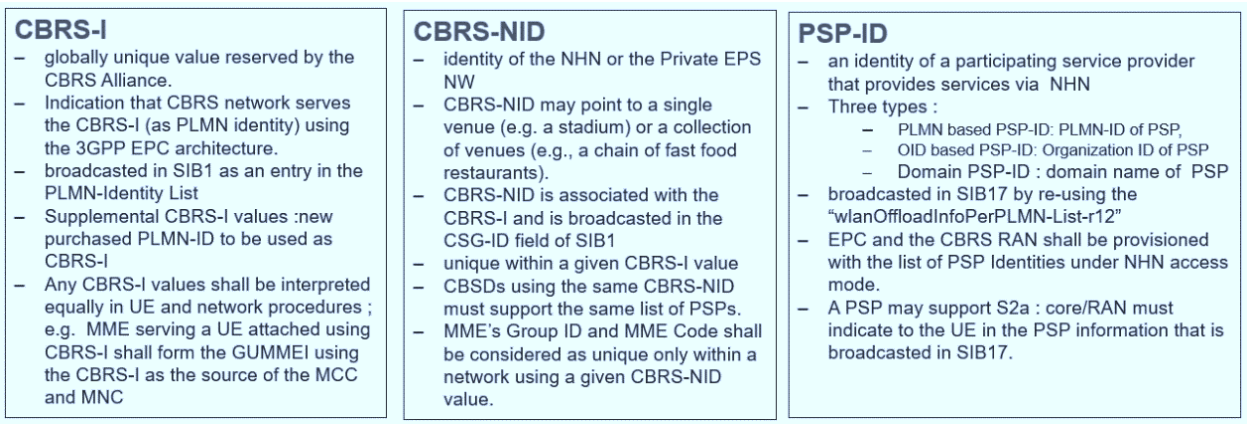
GAA – 80 to 150 MHz (3550 MHz to 3700 MHz)
- No auction , "it's a gift" to anyone who buy CBRS compatible equipment and talk to SAS , will get spectrum
- RRU can cover up to full 150 MHz spectrum but can never be guaranteed of free spectrum at give time and location.
- Will never get anything from tier 2 (PAL) if being used
- Upper 50 MHz protected for GAA, 80 MHz is minimum for GAA
- CBSD will report location & power level

5.4 CBRS identifiers

A normal LTE operator uses the unique PLMN-ID in the System Information Block 1 (SIB1) over the LTE channel to allow devices to distinguish the home network, initial access and camping information. To continue the similar procedure, the CBRS Alliance has decided to use the 3GPP Closed Subscriber Group (CSG-ID) to uniquely identify the network of a shared CBRS home network ID. The CBRS Alliance decided to assign each CBRS operator a unique CSG-ID (CSG Identifier) called the CBRS-NID (CBRS Network Identifier).

CBRS forum has defined three new network identifiers (TAI/ECGI/GUMMEI/IMSI – updated with shared home network ID (SHNI) and 5-digit long user identity number (UIN) excluded (refer CBRSA-TS-1002):

Table *5-3* CBSD Network identifier



IMSI Provisioning:

- Used in the Attach Request; indicates the preferred Access Mode for a UE
- IMSI MUST be comprised of a CBRS-I value and 9 zeros is used to indicates preference for NHN Access Mode. Any other IMSI indicates the UE's preference for 3GPP Access Mode.

5.5 CBRS network architecture

The CBSDs are fixed base stations (BS), or networks of such, and can only operate under the authority and management of a centralized SAS. Both the PAL and the GAA users are obligated to use only the certified FCC approved CBSDs, which must register with the SAS with information required by the rules, for example, operator ID, device identification and parameters, and location information. In a typical MNO deployment scenario, the CBSD network is a managed network comprising of the Domain Proxy (DP).

The CBSDs are like LTE and NR base stations but difference is that these base stations can only operate under the SAS authority. Both PAL and GAA users are supposed to be compliant WinnForum technical specifications and must be tested in approved lab for OnGo certification. After successful completion in OnGo certified lab, such CBSD gets FCC approved ID and serial number which is also saved in FCC database. Such approved CBSD will also get registered with SAS with information required by the rules, for example, operator ID, device identification and parameters, and location information and more. In a large commercial deployment, it is advisable that all CBSD devices should be managed by new network element, the "Domain Proxy (DP)" along with the element management system (EMS) or network management System (NMS) functionality.

The DP may be a bidirectional information routing engine or a more intelligent mediation function enabling flexible self-control and interference optimizations in such a network. In addition, DP enables combining, for example, the small cells of a shopping mall or sports venue to a virtual BS entity, or provides a translational capability to interface legacy radio equipment with a SAS. An element management system (EMS) is a required component for provisioning and configuring CBSDs, like conventional LTE systems. Network management system is an optional but preferred approach for large deployment of CBSD (for example MNO) to centralize communication to the SAS network while also offloading and simplifying the individual CBSDs.

SAS main role is to control the interference environment and enforces protection criteria and exclusion zones to protect higher priority users, and dynamically determines and enforces CBSDs maximum power levels in space and time. The FCC requires all SASs to have consistent models for interference calculations. In addition to above, SAS also takes care of registration, authentication and identification of user information and SAS-SAS message exchange.

In order to meet the mission critical requirements of the DoD Incumbent Access, the FCC adopted rules to require Environmental Sensing Capabilities (ESC) in and adjacent to the CBRS band to detect incumbent radar activity in coastal areas and near inland military bases. Once Incumbent access activity is detected, the ESC communicates that information to a SAS for processing, and if needed, a SAS orders commercial user to vacate an interfering channel within 300 seconds in frequency, location, or time.

As per the CBRSA-TS-1002 V1.0.0 (Rev 13.0 moving to V2.0.0), multiple deployment models have been defined based on network infrastructure as below:

- Public Network (RAN + Core) operating in 3GPP PLMN Access Mode (PLMN)
- Private Network (RAN + Core) operating in 3GPP Private CBRS-I (CBRS-ID as PLMN ID) Access Mode
- CBRSA NHN (RAN + Core) operating in NHN Access Mode with CBRS-NID ONLY.
- Private CBRS network (RAN + Core) operating in NHN Access Mode with PSP-ID along with optionally with a USIM based subscription or a certificate-based subscription associated with PSP-ID
- CBRS Network operating in 3GPP-based Access Mode to serve CBRS devices equipped with non-USIM based subscription

Different architecture models can be summarized as below where end to end enhancement are dictated along with USIM based credentials:

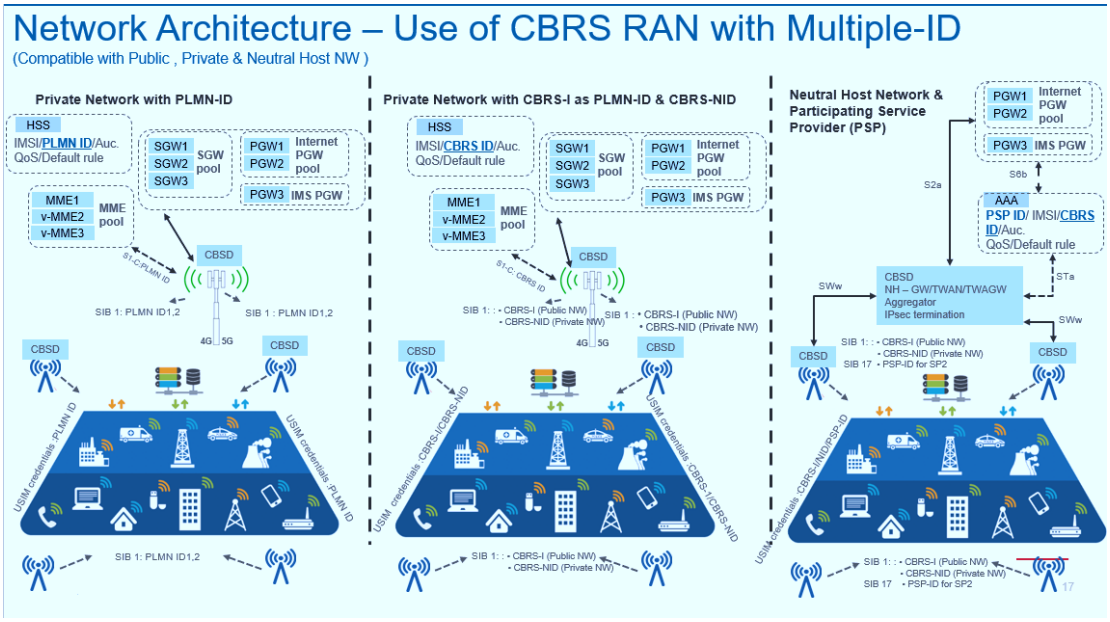


Figure *5-3* CBSD end to end deployment models

The architecture enables the CBRS NHN to operate as a trusted non-3GPP Access Network and/or untrusted non-3GPP Access Network for UEs associated with PSPs. In trusted mode, a CBRSA NHN uses the STa-N interface for UE authentication and enables one or more simultaneous home routed PDN connections between the UE and the PSP's PDN-GW using the S2a interface. If the subscriber's home operator allows, the CBRSA NHN may provide additional PDN connections for local breakout of data traffic. Legal Intercept is not specified for local breakout.

In untrusted mode, a CBRSA NHN uses the SWa-N interface for UE authentication. In this mode, all PDN connections use local breakout of data traffic. Legal Intercept is not specified in the untrusted case. In untrusted mode, a UE with a USIM based subscription can establish a secure IPsec tunnel (for example, SWu in 3GPP TS 23.402) with its service provider's ePDG using the subscription and receive the service provider's services via the SWu interface.

We recommend visiting CBRSA-TS-1002 V1.0.0 (Rev 13.0 moving to V2.0.0) for further detail on Network Architecture for "Neutral Host Network and PSP" as well as "Private Network using Neutral Host Network".

5.6 CBRS new UE profile

The CBRS Alliance defined new CBRS-Profiles where each profile points to certain network compatibility as well as functional supports. A single UE may and may not support multiple profiles in certain cases though. CBRS core and policy network elements are responsible for policy and rule enforcement based on profile as in LTE. One such policy can be mapping of access mode to the relevant CBRS-Profile and a subscription. The following table provide a high-level summary of UEs supporting various CBRS-Profiles.

Table *5-4* UE Types and required network Configuration

CBRS-Type I UE
- A normal LTE UE supporting 3GPP procedures with CBRS band support
- UE cannot attach to NHN and does not support NHN procedures.
- Two radio states:
  - RRC idle
  - RRC connected
	CBRS-Type I-A UE
	- A normal LTE UE supporting 3GPP-based Access Mode (non-EPS-AKA)
	- UE cannot attach to NHN and does not support NHN procedures.
	- Two radio states:
	  - RRC idle
	  - RRC connected
		CBRS-Type II UE
		- UE supports NHN selection procedures, mobility session, security procedures, and RAN identifiers
		- Has a single LTE transmit radio and a dual EMM context
		- Can be EMM Registered on a single access network at a time
		- All PDN connections over 3GPP are assigned to the same access NW (for example, all on an SP NW or all on an NHN)
		- Four radio states:
		  - SP RAN RRC idle
		  - SP RAN RRC connected
		  - NH RAN RRC idle
		  - NH RAN RRC connected
			CBRS-Type III UE
			- A single LTE transmit radio, dual EMM contexts, can listen for paging on both contexts
			- Search and identify target cells on the non-serving NHN or SP NW
			- Can be EMM Registered on two access networks simultaneously
			- A single transmit radio, it can send/receive data only on one access network at a time
			- PDN connections over 3GPP access can be assigned to different access NWs (for example, Internet on the NHN and VoLTE on the MNO
			- Four radio states:
			  - SP RAN RRC idle
			  - NHN RRC idle
			  - SP NW RRC idle, NHN RRC connected
			  - SP RAN RRC connected, NHN RRC idle
			  - Not idle on SP NW, NH RRC connected
				CBRS-Type IV UE
				- Has dual LTE transmit radios, dual EMM contexts, and dual ESM contexts
				- User plane data can flow over both ESM contexts simultaneously, at the granularity of PDN connections
				- Radio states to be determined:
				  - One state is dual uplink/downlink radio chains and a full LTE state machine for both access networks
					CBRS-Type V UE
					- A normal LTE UE supporting 3GPP procedures with CBRS band support
					- UE cannot attach to NHN and does not support NHN procedures.
					- Mutually exclusive radio states:
					  - SP NW RRC idle
					  - SP NW RRC connected, all PDN services from SP NW
					  - CBRS access NW [SP/NHN/Private] RRC idle
					  - CBRS access NW [SP/NHN/Private] RRC connected

The CBRS Alliance has added CBRS-Type I UE and CBRS-Type V UE configurations to extend to 5G use cases.

6. Confidentiality & Security

6 Confidentiality and Security

6.1 Introduction

Integrity, confidentiality, and privacy are primary requirements for the 5G System (5GS) and 5G New Radio (5G-NR). These systems were architected to be networked along particular interfaces to provide options for scalability, solution OPEX and flexibility for life-cycle management. 3GPP has defined specific methods for each of these interfaces to provide confidentiality and security.

3GPP also provides the options to not provide integrity, confidentiality, and privacy on these interfaces as the standard is to be deployed around many use cases all over the world. In some jurisdictions of the world the security simply cannot be used by law. There are other cases where physical security is in place on these networked interfaces.

As you read 3GPP standards and papers on 5G security you will find instances of these options and perceived threats. If you delve deeper you will also find additional standards published by localized standards bodies such as ATIS, NIST, ETSI as well as other government and enterprise requirements that close such gaps. In a fully Non-Public Private Network situation it is up to each deployment to determine if security is enabled on interfaces as part of the solution. However, the scope of this section will suggest cases where full and partial security methods are deemed necessary on the interfaces.

Finally, the components that make up the private network including public components as well as the applications leveraging the solution. These applications need to be secured from an infrastructure environment perspective (for example secure boot, port lockdown, signed software, zero-trust, and more). A more in-depth 5G America's paper on 5G security, "Security Considerations for the 5G Era" deals with these topics and security of slice management. We recommend this paper as well.

We structure this section beginning with key enterprise considerations critical to private networks. Second, we discuss key technologies and parameters that have security and privacy implications that are passed on interfaces and recommend secure options provided by the 3GPP standards. The third section discusses air interface security as it is common to all deployments defined in sections above. Lastly, we provide sections on the security of key network demarcation interfaces relevant to the deployment possibilities discussed in previous chapters.

A diligent enterprise customer will likely be presented a number of possible solutions from different parties each with their pros and cons. This section should provide the enterprise with an understanding of the security of each demarcation point for each solution presented. An independent, wholly-owned and managed private network may also have the same demarcation points if components are separated between sites. When options for security are possible at each demarcation point the flexibility of the options allowed by standards are discussed.

6.2 Enterprise Considerations

Security and privacy are paramount from an enterprise and from an operator perspective. As networks evolve and converge as in 3GPP Release 16, the multi-access capability enables device applications to always be seamlessly connected. The multi-access network must have security on all types, licensed, unlicensed, shared, and start with a root of trust. In essence, zero trust is required. Depending on if the installation of a private network is greenfield or brownfield there are different considerations. If the installation is a greenfield and there are not any legacy networks to consider, a private 5G Network could enable the control of the multi-access from one controller. Thereby the security, AAA, privacy could be a framework that cuts across the different types of spectrum and access types, devices and the applications. If there are legacy networks to interface with, the legacy controller will need policies, traffic routing, and more, to interface with the private network,

if so desired by the enterprise. It is an important factor that needs to be considered when designing for a 5G private network.

The devices and applications must be securely on-boarded, and communication between applications needed security as the applications could be from different enterprise vendors.

Beyond the basic infrastructure, the enterprise typically will have concerns with location of the devices, on or off facilities and secure use, the reach of the private network (spectrums) to ensure privacy, the data security and enabling secure data transactions in low latency, and total control of the enterprise data. The enterprise typically is deploying a multi-access solution and therefore no matter what spectrum, a secure frictionless use of the networks is required. Another potential concern would be connecting to a public network, and the controlling and securing of data traffic to and from the public network.

6.3 Mitigation and Securing Data for Private Networks.

Release 16 enables an infrastructure that covers from the user equipment (UE) or end device to the core for a single multi-access system. The edge applications, break out, zero trust and root of trust for the applications themselves will need considerations. Additional caution is required in considering the legacy equipment and network when building a private secure network.

The interfaces to legacy environments are likely to be wired or based upon Wi-Fi. The key network element that will interface to these environments is the UPF. The UPF can be firewalled and IDS protected to alleviate other concerns.

In the case that applications are designed to use Ethernet interfaces the 5G System allows for native LAN service. UE adaptors should be available perform these transitions from either wireline or other wireless technologies.

6.4 Technologies for secure private networks

This section provides are short overview of key technologies leveraged to implement SNPN and PNI-NPNs. For additional details please refer to the companion paper 5G America's paper on 5G security, "Security Considerations for the 5G Era". It provides additional explanations of each technology applied to use cases. 3GPP 33.501 has even more technical details on algorithms and network flow details.

Table *6-1* Key enabler for secured Private network

Technology	Discussion
Secure Infrastructure (Zero Trust)	A key part of 5G is the emphasis put on hardening and zero trust aspects of the network elements. This includes secure boot signed software, ongoing security audits of new software and mutual authentication and integrity of communicating identities. This topic is beyond the scope of this paper but is already covered the companion paper 5G America's paper on 5G security, "Security Considerations for the 5G Era".
Network Public Private Key Pair	At the heart of 5G Systems and major development of security over LTE is the introduction of managed network public private key pairs. The UEs that are to access that network are provisioned with the public keys as part of the activation or fulfillment process. The ECC public key can be updated via OTA or other PKI Management Procedure. The UEs use this public key as input for key agreement and encrypt information when they attach to the network to ensure privacy. This pair is also important to prevent the UEs from erroneously connecting to nefarious networks broadcasting a cloned PLMN and/or NID. The management of these network credentials and lifetime management with the MEs needs to be worked out as part of any NPN deployment with your vendor or provider.
SUPI	The SUPI is defined as Subscriber User Public Identity. It is the unencrypted identifier set that identifies the user and the network they belong to. 3GPP has defined that it can take several forms IMSI (with MNC and MCC) and NAIs (user@realm). Either IMSIs or NAIs can be used for NPN credentials. If IMSI are used EAP-AKA' can be leveraged with associated credentials (for example A-KEY) for authenticating the mobile. If NAI is used then ECC certificates for the MEs are leveraged and EAP-TLS can be leveraged for authentication.
SUCI	3GPP has defined a method to protect the identity of devices called Subscription Permanent Identifier (SUPI). An Elliptic Curve Integrated Encryption Scheme (ECIES) – based privacy-preserving identifier containing the concealed SUPI is used for transmission. This concealed SUPI is known as SUCI (Subscription Concealed Identifier) The ME generates the SUCI using the following method. • The ME has been preconfigured with the network's public key. • It generates an ephemeral key pair using the network's public key as input. • The ME then generates a shared key by using the ephemeral pair and the network's public key. • This shared key then encrypts the user portion of the IMSI or NAI generating the SUCI. • The ME passes its ephemeral public key as part of the SUCI. • The network uses the network's private key and the ME's ephemeral public key to decrypt the SUCI back to SUPI form. Appendix C section C.3 of 3GPP 33.501 describes the Elliptic Curve Integrated Encryption Scheme (ECIES) used for SUCI protection.

Multiple Authentication Methods and Credentials	There are 3 methods for authenticating subscribers for NPN solutions: 1. **IMSI SUPI – based EAP-AKA:** using A-KEY as credential 2. **NAI SUPI – based EAP-TLS:** using ECC ME certificate as credential 3. **NSSSA – based EAP-TLS:** PNI-NPN also allows for a separate Network Slice-Specific Authentication and Authorization in addition to the operator authentication allowing the enterprise to enforce a 2nd factor of authentication to their network. Any EAP-TLS authentication scheme can be supported between the ME and Enterprise. This is transparent to the network provider. Please refer to Appendices A-C of 3GPP 33.501 for additional details.
PLMN and NID Network Identifiers	Mobile operators are allocated Public Land Mobile Network PLMN IDs. These identifiers are somewhat rare and allocation always takes from a global pool managed by the GSMA. For SNPN 3GPP and GSMA have allocated some re-usable values that all SNPNs could share. 3GPP has also identified a Network Identifier (NID) that can be used to further distinguish NPN instances providing additional scale. Each PLMN can define their own NIDs. The combination of PLMN, NIDs and in some cases and S-NSSAI identifies the NPN. In the case of SNPN the enterprise allocates and defines the NID. In the case of PNI-SPN the operator and enterprise agree on the NID allocation and definition. These identifiers are transmitted in the clear by the GeNBs themselves. Obfuscation of the NID is a choice but this may affect user friendliness.
Slicing	A Network Slice is a logical network that provides specific network capabilities and characteristics. Slices can be deployed within an SNPN to fulfill network services for different MEs of the SNPN when locally connected. Traffic separation is one example. In a PNI-NPN environment slices can be defined to remotely connect MEs to the NPN as well as fulfillment of network services to the NPN when locally connected or abroad. Multiple slices can be leveraged for the same PNI-NPN.
S-NSSAIs	The S-NSSAI essentially identifies a slice template, type and properties of the slice in terms of 5G System resources, QoS, Association private networks, etc. An S-NSSAI can also identify a PNI-NPN. S-NSSAIs should be closely guarded and not sent in clear if possible, to prevent them from identifying organization affiliation of a subscriber.
NSSAIs	The Network Slice Assistance Information is the list of Single Slice Assistance Identifiers (S-NSSAIs) that an ME is subscribed to. The ME can be configured to send this in the clear or protected by NAS encryption. It is recommended MEs are configured to send this protected by NAS encryption or have the network simply look up the provisioned NSSAI list without the mobile ever sending it.

Network Slice Instances	A Network Slice instance is a set of network function instances and the required resources (for example compute, storage and networking resources) which form a deployed network slice. In a PNI-NPN solution an S-NSSAI can identify an NPN that ME are connected to. Slices are a method to implement PNI-NPN. The 5GS uses this S-NSSAI information to allocate and assign Network Slice Identifier ID (NSI ID) for each instance of a slice to fulfill the services associated with it in real time. NSI IDs can sometimes take on a subnet like form with for example the high order bits defining RAN characteristic, middle order bits assigning core/application characteristics and low order bits identifying customer or network organization. It is up to each operator on how to define and interpret the IDs internally. An SNPN can also implement slices as well but this takes on considerable overhead. To see this point refer to a recent GSMA generic template for slices Generic Network Slice Template Version 3.0 22 May ... – GSMA. The solution vendor or provider will likely have a set of templates for slices that meet your needs.
DNN	Data Network Name is an identifier which can steer each of the ME's bearers to a particular network. Examples are the Internet, Enterprise Private Network MPLS VPN, etc..
CAG	Closed Access Groups are access control lists for cells that MEs have access to. The MEs are configured with the CAG Identifiers and are programed to try to attach to cells that allow the CAG. The GeNBs broadcast the CAG identifiers as part of this SIB broadcasts. The actual lists of users that are allowed on the CAG must be shared between the operator and the enterprise customer in a PNI-NPN scenario. Updating the list needs to be secure and timely. The 5GC enforces the access control. An SNPN could also provision CAGs to restrict users to particular cells within their network.
TAI	Tracking Area Identifiers are assigned by the operator in a PNI-NPN situation or can be assigned by an SNPN. The TAI is representation of a high granularity location area and are also used for paging. A single cell can be a tracking area or many cells can be defined in a tracking area. This function can be leveraged to implement geo-fenced PNI-NPN applications. For instance, only allow certain users' access to a CAG or PNI-NPN if they are in a list of TAIs. Updating the information needs to be secure and timely.

ABBA	Finally 5G has also defined the ABBA (Anti-Bidding-down Between Architectures) parameter. This parameter allows the 5G system to enforce that a UE cannot access the network using older mechanisms that have had vulnerabilities associated with them. Think of this as an enveloping security version of a system. The network tells the MEs this version when the ME attempts to attach. The ABBA is used as input to and is therefore protected by the authentication algorithms.

6.5 Security of the Air Interface NAS, Access, and User Planes

The security of the air interface is common to all deployment scenarios.

The Non-Access Stratum (NAS) and Access Stratum are of primary concern from a privacy standpoint.

The PLMN, NID, TAI and CAG are broadcasted in the clear by the NG-RAN systems. The NID and CAG could be leveraged to identify locations of an organization by scanners given they know these values. Obfuscated assignment of these values may help but would inhibit user friendliness in some use cases.

When an ME is first activated SUPI can be passed in the clear as part of fulfillment and activation but after that the mobile will encrypt SUPI in SUCI form. The first access procedure establishes security associations for integrity and encryption. After this first activation user privacy is protected by encryption of user portion of the SUPI in the form of the SUCI. If the ME was manually provisioned with the public key the first SUPI registration can be avoided entirely.

3GPP NAS options are provided to protect all other network parameters. For privacy reasons the NID, DNN and NSSAI should only be sent by the UE after NAS is encrypted.

Both control and user plane functions can be activation user privacy is protected by encryption of user portion of the SUPI in the form of the SUCI. If the ME was manually provisioned with the public key the first SUPI registration can be avoided encrypted, and integrity can be protected over the air. User plane is paramount to be protected. Non-NAS control plane typically does not have any user privacy information to protect but is usually protected as well to prevent Man-in-the-Middle (MiTM) and Denial of Service (DOS) attacks. Please refer to Chapter 6 of 33.501 for additional details.

6.6 SNPN Core and RAN all at one Site Use Case

The simplest use case is that all the equipment for an SNPN is at one site. The security policy for each network interface is entirely up to the enterprise for the applications they want to support. As the wired interfaces to each of components are likely switched there is a degree of risk mitigation by default.
3GPP 33.501 should be inspected to determine the needs of the enterprise at the site and security enabled as seen fit for the applications and users running on the network.
Minimally, we recommend that the air interface for control, NAS and user plane are protected to match a switched wired environment level of risk. If the SNPN is distributed with backhaul (For example, Cloud 5G Core and RAN at sites) then the options presented in 33.501 should be considered for each interface. The next sections elaborate more on these options as well.

6.7 Network Demarcation Security Use Cases

The table below describe network demarcation examples when multiple sites are involved in a deployment of an SNPN or PNI-NPN.

Table *6-2* Network demarcation use cases in a SNPN or PNI-NPN deployment

Use Case	Demarcation Interfaces	Protection Method

5GC networked to RAN Sites
SNPN (cloud core)
PNI-NPN (Core in provider – RAN at enterprise)
	N1, N2, N3
	OA&M (CWMP or Netconf)
		• If BH provided by Provider or Enterprise's Private Network (For example MPLS/VLAN)
		  ○ NDS IPSEC or MACSEC recommended but optional.
		• If Internet BH or 3rd party non-core then NDS IPSEC with tunneling.
		  ○ May need multiple tunnels (OA&M and Signaling/Traffic).
		  ○ SeGW may be needed at Core Sites.
		  ○ Netconf can run on ssh or TLS and CWMP can run on TLS as well.

MOCN	Multiple Core N1, N2, N3 OA&M (CWMP or Netconf)	• Multiple Instances of Core Connectivity – Same as above but multiple instances to each RAN. • SeGW may be needed at Core Sites.

Mid-Haul Demarcation (RAN Split 6)	F1
	OA&M Netconf
		• If BH provided by PP-VPN (For example MPLS/VLAN metro) then no tunneling may be needed.
		• NDS IPSEC is an option.
		  ○ Refer to Front-haul and Mid-haul considerations section.
		• If Internet BH or 3rd party non-core then NDS IPSEC tunneling.
		  ○ May need multiple tunnels (OA&M and Traffic).
		  ○ SeGW may be needed at Core Sites for topology hiding.
		• Netconf over ssh is an option
		• Netconf can also run on TLS or DTLS.
		• DTLS can be used on F1-AP interface. This is typically used to provide additional protection to the F1 control information to a virtual environment networked within a private network when an NDS SeGW is leveraged over a public interface.

Front-Haul Demarcation ORAN or eCPRI (RAN Split 7.2 or 8)	ORAN, eCPRI, Netconf	• Latency and timing constraints limit front-haul options for URLLC solutions to newer transport solutions, networked fiber or direct fiber. • The distance between RRH and AU/DU is limited. (for example 10-20km) depending on features enabled. • MACSEC or IPSEC can be applied but any induced delay will decrease distance limit when trying to achieve URLLC requirements. • Netconf over ssh is an option • Netconf can also run on TLS or DTLS.
Distributed Core (Only UPF local)	N4 PDCF	• Use same protection choice as above case chosen.
Distributed Core (AMF, SMF, UPF local)	SBI	• SBI interfaces require use of TLS with mutual authentication.

6.8 URLLC Considerations and Security

When components of a 5G System are separated, you are working against the speed of light in networked situation. Light travels through 1 mile of fiber every 0.82 us. A separation of 100 miles would then be 0.82 ms of latency (Core to RAN) can achieve < 1ms latency. The air interface uses up about 0.5ms.

If the transport between the elements applies encryption, then you can expect a 1-3us latency impact at each endpoint total 2-6us end to end. Note that though this may vary depending on solution. Measurement should be done via testing under load to determine actual latency impact. Based upon this latency impact, the transport distance may have to be reduced between elements to achieve the URLLC goals when IPSEC or MACSEC is used.

6.9 Front Haul and Mid Haul Security Debate.

Performing extra security on Front Haul and Mid-haul interfaces have been debated quite a bit in the past with pros and cons for each. The 3GPP standards recommend that encryption and integrity protection be enabled on both the front-haul (for example eCPRI/oRAN) interfaces as well as the mid-haul interfaces but still leave options to not use them as well. Many argue that if UE security is enabled over the air, the corresponding network endpoints lie upstream from these distributed RAN NEs and therefore the security is redundant. Others argue that some NE (Network Element) to NE control information is not protected and require additional protected to prevent DoS and reduce the attack surface for MiTM and rogue NEs.

One the primary tenants of the 5G system is that of zero trust which translates to every node in the system performing mutual authentication over every interface along with integrity and confidentially. Note this could be vNFs running on the same physical platform too.

Another tenant of 5G is that security is there from day 1 and not bolted on. The following figure shows the distributed RAN transport discussion points from a high level.

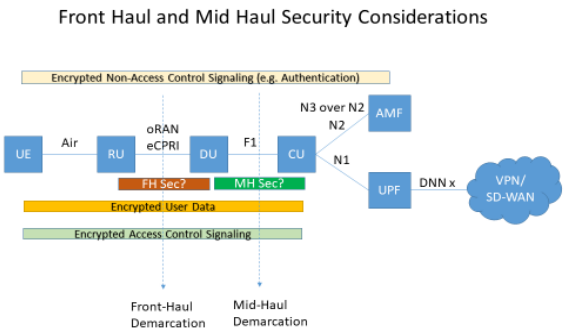


Figure *6-1* : Network Architecture depicting the front haul and mid haul security considerations

In the figure above we see that Encrypted and Integrity protected:

- NAS signaling is terminated on the UE and the AMF
- Access Stratum Signaling is terminated on the UE and the CU.
- User plane is terminated on the UE and CU

Front-haul Security is included as an option in the standards (FH Sec) which is terminated between the RU and DU and Mid-haul Security which is terminated between the DU and the CU. IPSEC or MACSEC are generally options for these interfaces.

Proponents of the need for FH and MH Security make the following points:

- Mutual Authentication is done between these endpoints preventing rogue network elements from connecting unbeknownst to the other network elements. The concern is that of consuming resources on the other network element or causing issues over the air or between peer network elements located at the same network tier.
- Integrity Protection is done between these endpoints. A man-in-the middle cannot forge and inject valid packets between the two entities which can cause denial of service by exhausting resources.

- Confidentiality Protected is done between the endpoints such that an observer on the link cannot see the control messages in order to mount an appropriate man-in-the-middle DoS attack.
- The threats these protections mitigate against are selective denial of service which is more difficult to analyze than simply a cut fiber (support costs could be impacted).
- It better prevents against multi-vector attacks.
- It adheres to the 5G tenant of zero-trust and security built-in.

Opponents of the need for FH and MH Security make these points:

- If these nodes are located on private transport and transport authentication is enforced then the threat is very low.
- The impact shown by proponents of additional IPSEC above is denial of service. The same thing can be accomplished by simply damaging the transport facility (for example cut the fiber).
- Doing this FH-SEC and MH-SEC significantly increases the complexity of the solution. Even with hardware acceleration, capacity is reduced by performing these duplicated functions.
- The signaling and user data between the UE and CU are already protected. This is duplicate security. These nodes only relay the already encrypted information and RRC signaling. They are providing no true benefit.
- There is an impact on latency, which may affect URRLC.
- Other less complex options are available for integrity and mutual authentication or full protection of the control signaling. Do we really need to encrypt twice?
- IPSEC also affects the MTU over the transport affecting the link efficiency and complexity.

There are many additional facets and details of this debate. One can certainly conclude though that FH-SEC and MH-SEC vs. increased latency and additional complexity are a choice to consider when using these demarcation points.

6.10 Shared and Lightly Licensed Spectrum Security

Shared spectrum blocks of RF are becoming more common. CBRS is one such allocation. Shared spectrum solutions typically require that the RAN check with and perform license checking for certain locations with an authorized authority (for example a SAS for CBRS). These protocols typically leverage TLS with mutual authentication of both parties. Most SAS providers have recommended PKI management providers to manage the certificates. These interface transactions typically use the Internet. Unlicensed spectrum deployments are unencumbered with the SAS function.

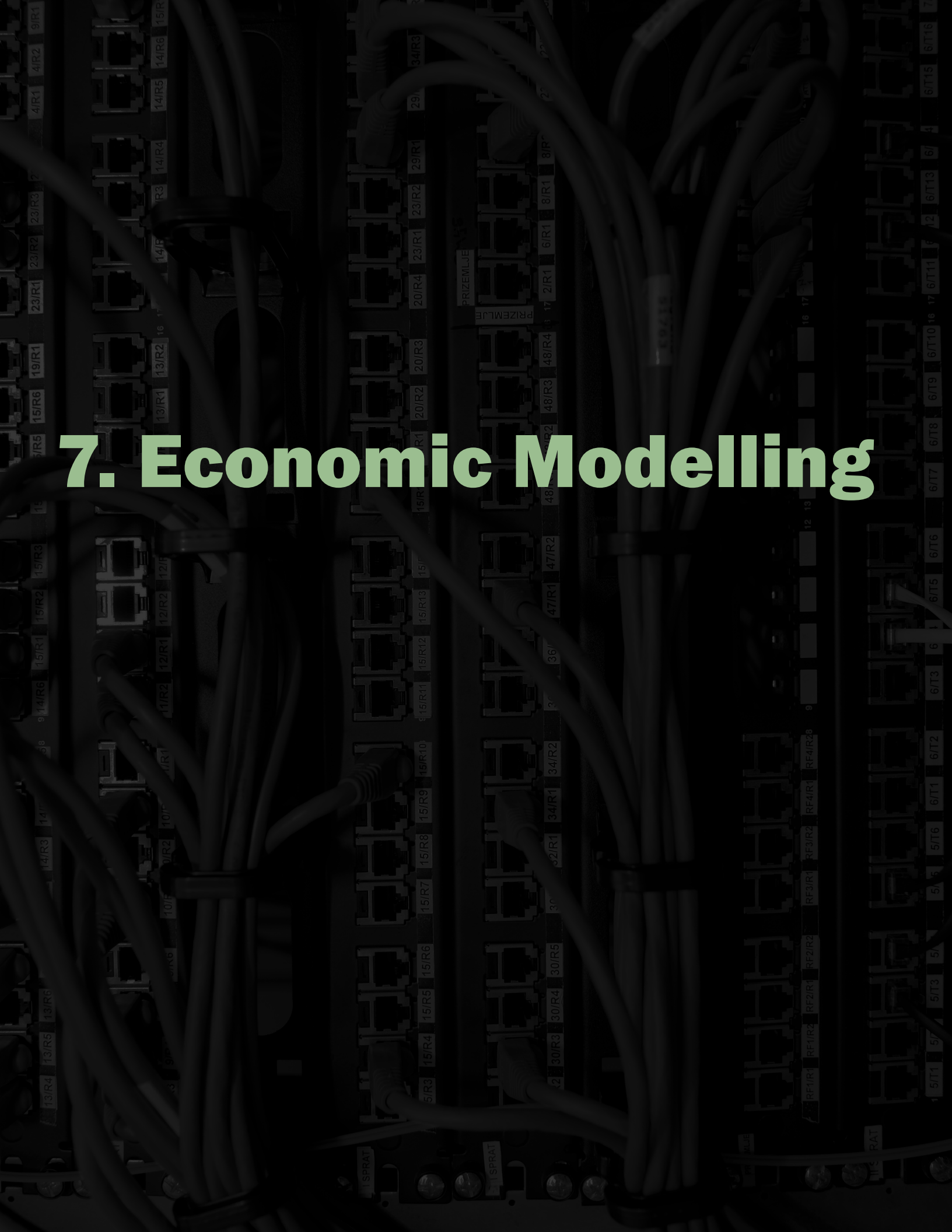
6.11 LTE-based CBRS and Multi-fire Technologies and Migration to 5G

Both CBRS and Multefire enhanced the EPC and LTE systems to support many aspects of private networks. They both allowed the broadcast of an equivalent of the 5G NID information over the air to identify the network. The CSG Name in the SIB1 is overloaded for this purpose in CBRS. When you move to a 5G system, the fields are built into the standards instead of having to overlaying.

These systems also have the threat that someone walking by could identify the enterprise; again, obfuscation of these names might help, but deter user friendliness.

CBRS and Multefire also support EAP-TLS NAS authentication, which can hide the identity of the subscriber. The user initially uses anonymous as the user at initial EAP contact, then waits for a secured channel to transmit the user id from a certificate Subject field. In a 5G System, the PLMNs public key handles this protection.

Migration from LTE CBRS to 5GS CBRS or LTE Multefire to 5G-U may involve some minor backend changes due to the differences but in many cases, they are completely compatible. For instance, even though 5G uses the public key to protect the user-id, the same EAP-TLS certificate mechanism could still be employed without changes providing double protection. If attachment latency for new devices are an issue you can always optimize their attachment leaving the legacy UEs doing it the old way.



7. Economic Modelling

7 Economic Modeling

7.1 Overview

Private Networks provide several niche opportunities to evaluate the economic value concerning different business model options. The key differentiator is the flexibility of ownership within the value chain. Infrastructure vendors, service providers, enterprises, and anyone else in the value chain may decide to pursue Private Networks for their benefit or serve others.

The decision to invest for their benefit is not likely to be dependent on external factors but the innate understanding of different value drivers and how it compares against existing or alternative solutions. The use case section listed the overarching value drivers such as Privacy, Security, Control, and Performance.

7.2 Different Business Perspectives

7.2.1 Enterprise Perspective

Current day enterprise faces an increased number of challenges while pursuing their digital transformation journey. The convergence of OT and IT worlds is vital for a successful digital transformation journey, and network infrastructure acts as the fabric stitching everything together, thus plays a crucial role in this convergence. However, the requirements for OT and IT, are in a highly dynamic and ever-evolving state; the flexibility, futureproofing, and control mechanics of the Network fabric should respond to this reality. Private Networks offer such flexibility and control as well as performance, security, and privacy, all of which are key features.

One way to quantify each of these characteristics is to evaluate current capabilities or lack thereof, the negative impact of rising challenges, and how Private Networks may solve some of these challenges. The elimination of a particularly negative impact will be the direct benefit of deploying Private Networks such as using wirelessly connected robotic arms with real-time capability in manufacturing plants. Wireless connectivity may improve the downtime during retooling also provide a more accurate predictive maintenance to reduce downtime related to malfunctions and decrease the number of incidents provided by the accuracy of the increased number of sensors connected wirelessly. New value creation opportunities may augment the benefits, such as being able to run workloads closer to where they are needed and eliminate some restrictive backhaul or latency expectations.

7.2.2 Service Provider Perspective:

The consumer market is saturated; service providers are discovering new revenue opportunities within enterprise space. Connectivity revenue from enterprise accounts appears to be the direct expectation of deploying Private Network solutions, but there are also other opportunities such as managed services, premium SLA services, macro network offload, new IoT business opportunities. However, the cost of each of these additional services needs to be measured carefully. Typical investment plans may provide accurate estimates on working conditions, but the key is to figure out the economics of when things are not working properly. The expectations are high, and the decentralized nature of these networks is a significant challenge to predict worst-case scenarios before deploying the solution. Network automation such as self-healing networks, predictive maintenance, or more accurate incident management may alleviate some of the challenges. However, there will still be a percentage of incidents requiring traditional break-fix or managed service solutions, which is not necessarily inexpensive to provide.

7.2.3 Infrastructure Vendor Perspective

In addition to the traditional vendor and provider partnership opportunity, there is also a direct to market opportunity due to the availability of more shared and unlicensed spectrum available for Private Networks. Lower entry barriers will allow vendors to tap into new revenue sources and enhance their traditional revenue structure with recurring contracts like a service provider. However, the cost of providing such solutions and services will require establishing a new operational workforce and capabilities, which is a significant investment and ongoing capital commitment. Automation of the network management may relieve some

of these complexities, but not all. Therefore, it is essential to have an accurate risk/benefit analysis before making such a commitment.

7.2.4 New Player Perspective

New players such as tower companies or real estate companies may consider private networks a niche opportunity, among others, to tap into new markets as barriers to entry are slightly lowered with additional shared and unlicensed spectrum opportunity. These players may have significant operational cost synergies due to assets they currently own or decide to hold in the future. Their core expertise and capital structure are more suitable to keep facilities-related costs while providing an operational base to run these networks.

7.2.5 Funding / Operational Models

Ease of Use is a primary component of adoption by the enterprise. It is crucial to consider how easy the solution is installed and managed by the enterprise. IT has an impact on adoption and, ultimately, the Total Cost of Ownership (TCO). TCO is always at the forefront with IT departments. The operational models need to include legacy infrastructure or path to encompass legacy. The workloads need to be consolidated to easily maintain, see the big picture, and reduce disparate servers. Finally, how the enterprises are leveraging the cloud as part of the overall operations, data control, and cost.

Besides, the ownership structure and the roles and responsibilities are flexible mostly because the ecosystem is not yet consolidated on any dominant business model structure. The needs and capabilities are highly diverse therefore there is a possibility of standalone funding as well as hybrid funding opportunity as illustrated below:

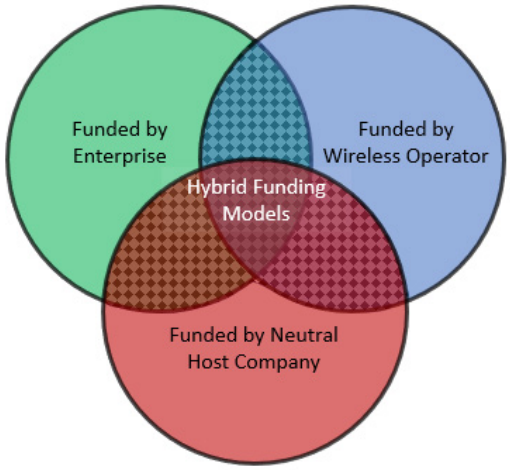


Figure *7-1* Different Funding Models for Private Networks

7.3 Examples of Value Drivers

One example is the manufacturing industry. All the overarching themes listed above will indeed add value; however, the real value proposition is addressing challenges like reducing downtime (for example, factory retooling, or incident related downtime) and other associated costs. Deploying intelligent solutions that require higher network SLAs (provided by Private Networks) for a more real-time control to decrease the number of incidents and subsequent impacts and financial damages may be one way to measure value. Another example could be to deploy intelligent solutions to improve further the quality control metrics, which will save time, money, and increase customer satisfaction. For some of these value levers, features like flexibility, mobility, or low latency and jitter will be vital; for others having a robust and reliable network infrastructure that can run intelligent solutions on-premises will be essential.

7.4 Identifying Common Synergies

Each player in the value chain will be likely to evaluate "one takes all" type of approach for competitive advantage. However, the lack of end-to-end solution capability in today's ecosystem indicates significant investment requirements, which may be a challenge in current market conditions. On the other hand, there may be

an opportunity to identify potential synergies and overlaps between different players to pursue scalable business models in the early days of Private Networks as depicted below in Figure 7-2:

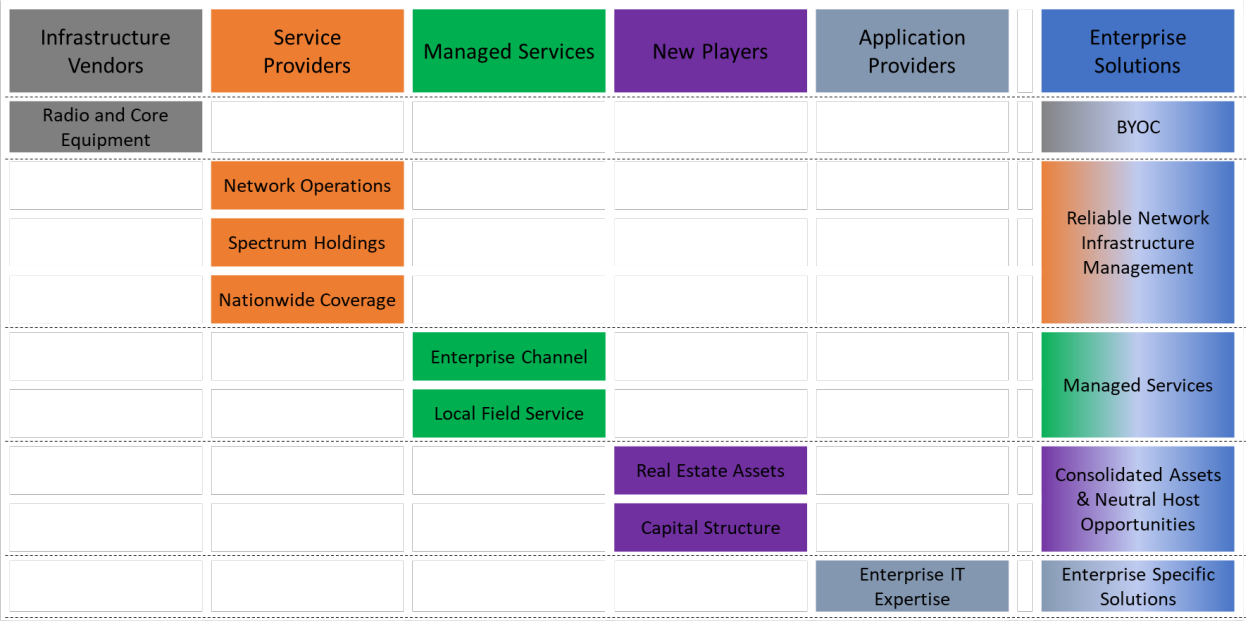
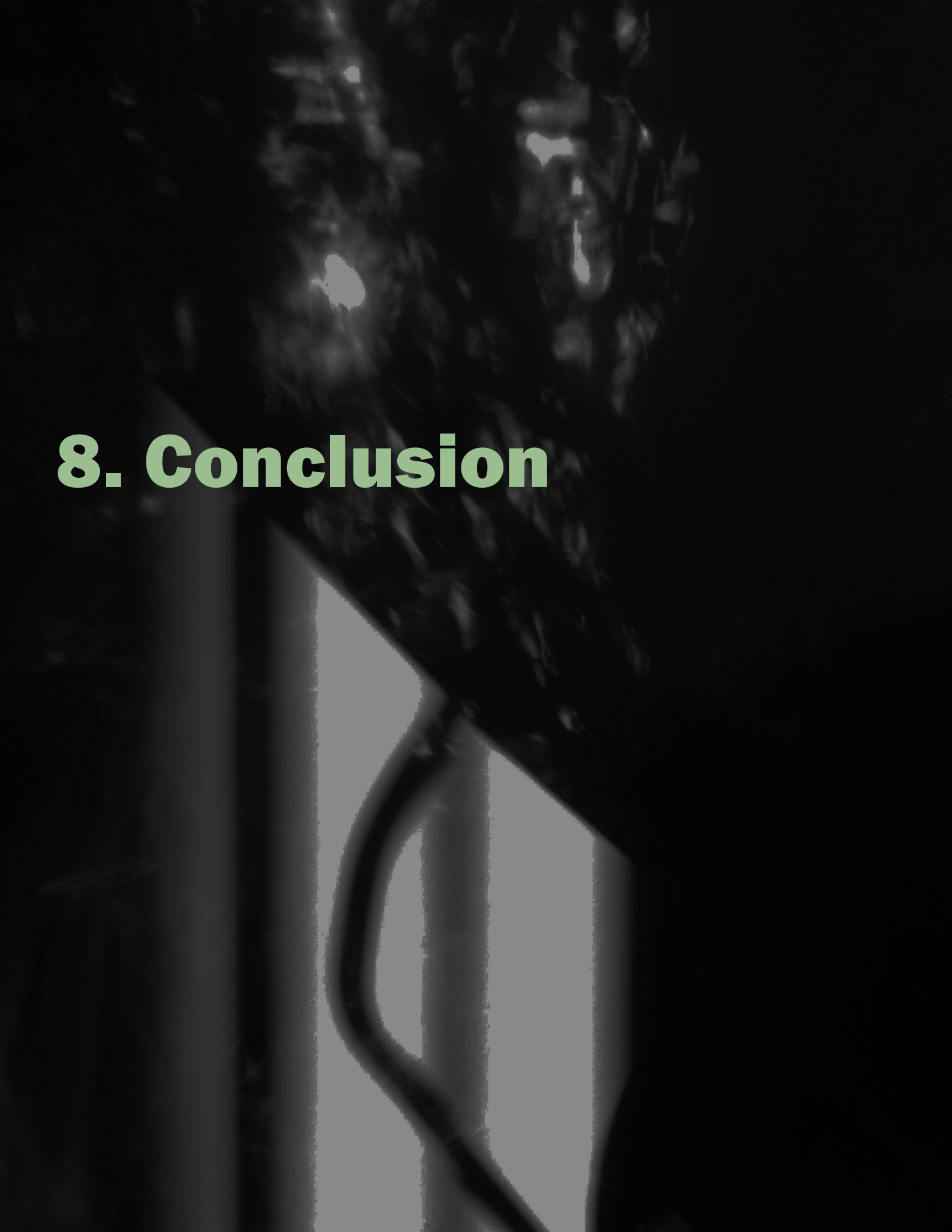


Figure 7-2 Summary of Different Player Capabilities and Potential Enterprise Solutions.

In an increasingly digital world where virtual solutions are increasingly containerized and stackable it may also be possible to containerize the physical components of each potential offering to mix and match a variety of solution stacks to different enterprise needs.

It may be valuable to provide that customized approach as each enterprise will likely have unique requirements and needs, so the "one-size-fit-all" type of solutions may be too difficult to implement. On the other hand, this level of customization will require a significant level of collaboration, testing, and standardization of each solution stack to provide an end to end capability. It will be very challenging to achieve such mature cooperation without strong commitment and partnerships among industry players.



8. Conclusion

8 Conclusions

Private Networks have become one of the telecom industry's highest growth sector with analysts estimating it to be an $60 billion industry in the next five years. Global enterprise organizations, utilities and mining industries, airports, ports, sport facilities, campuses and more are already adopting this technology. The confluence of new capabilities introduced in 5G, as well the increased availability of both licensed, unlicensed and shared spectrum is fueling this growth. As a result of this convergence, private networks can be delivered by either a third-party network provider, a traditional cellular operator, or the enterprise customer itself.

Past attempts of implementing private networks were fragmented, made up of disparate proprietary networks, and lacking in performance, reliability and security. 5G brings a significant increase in throughput, millisecond latencies, massive device connectivity, enhanced security and deterministic, reliable performance rivaling the capabilities of wired networks.

The service-based architecture of the 5G enables new applications and business models to be implemented more easily and faster. Network slicing is a new capability of 5G infrastructures that provides a high degree of deployment flexibility and efficient resource utilization when deploying diverse network services and applications. The combination of 5G and edge computing brings an unprecedented potential access to enterprise infrastructure. 5G is continuing to evolve in subsequent 3GPP standard releases that will continue to enable and expand the private network use cases and capabilities.

Appendix

Appendix A

5G RAN Sharing Architecture: NPN network with network sharing architecture

3GPP TS 23.501 specifies a network sharing architecture allowing multiple participating operators to share resources of a single radio access network.Release-16 specifications support only the so-called 5G Multi-Operator Core Network (5G MOCN) network sharing architecture, in which only the RAN is shared in 5G System.

5G MOCN supports all the following combinations of NG-RAN sharing involving non-public networks:

- NG-RAN is shared by multiple SNPNs (each identified by PLMN ID and NID);
- NG-RAN is shared by one or multiple SNPNs and one or multiple PLMNs;
- NG-RAN is shared by one or more PNI-NPNs (with CAG) and one or more SNPNs; and
- NG-RAN is shared by one or multiple PLMNs and one or multiple PNI-NPNs (with CAG).

5G RAN Sharing shall follow 4G, which includes MORAN and MOCN features.

MOCN in unlicensed bands like LAA, CBRS, C-band are the most probable options.

Two approaches have been proposed for RAN infrastructure Sharing:

- Multi-Operator Radio Access Network (MORAN)
- Multi-Operator Core Network (MOCN)

Multi-Operator Radio Access Network (MORAN) standard proposed an architecture where the eNBs/gNBs are shared, while the core network is different for each network provider. The MORAN standard also proposed the sharing of the Radio Access Network (RAN), using dedicated radio frequencies assigned to each service provider. In this approach, they can independently control cell level e.g. each operator can decide his own optimization parameters, Transmit Power to control the cell range and interference. There is no specific requirement on UE for such topology.

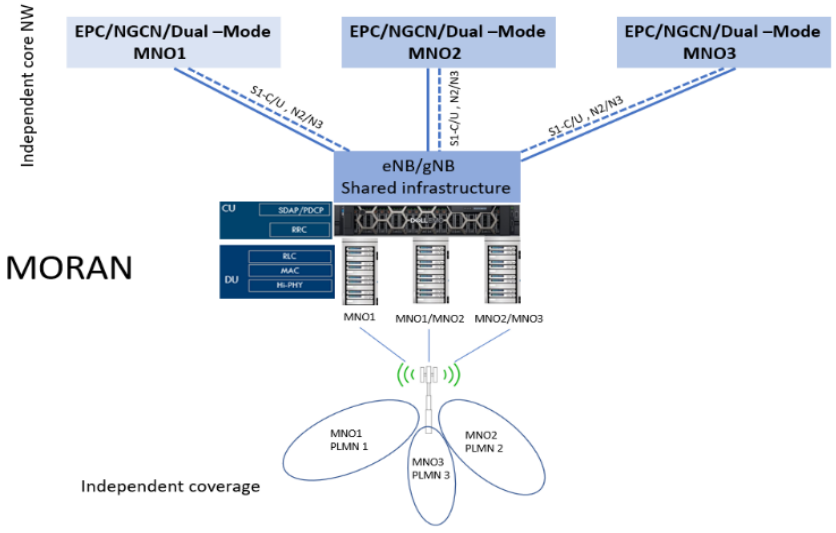


Figure A-1: MORAN Architecture

Multi-Operator Core Network (MOCN) standard allows the sharing of the same architectural elements as MORAN i.e. eNBs/gNBs. However, in MOCN, the operators also share frequencies. This prevents the operators independently from being able to control their networks at the cell level.

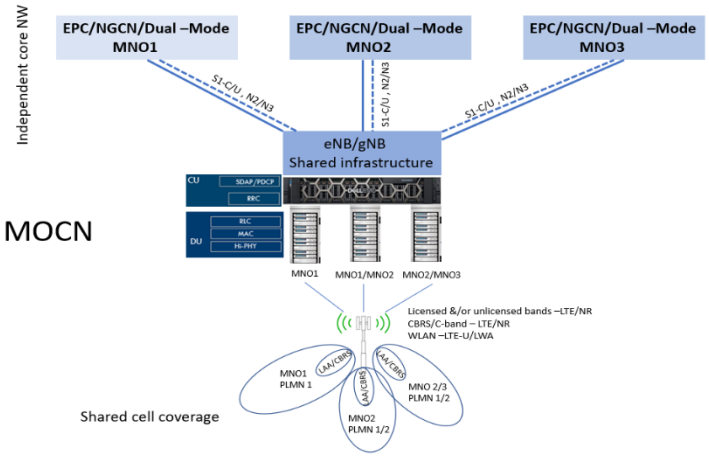


Figure A-2: MOCN Architecture

In NAR market, MNOs have preferred licensed bands for the initial deployment for 5G in Non-Standalone Architecture (5G NSA) option 3x (EN-DC), following 4 options for RAN sharing:

- Both LTE eNB & NR gNB with MORAN
- Both LTE eNB & NR gNB with MOCN
- LTE eNB as MORAN & NR gNB with MOCN
- LTE eNB as MOCN & NR gNB with MORAN

Case 1: Both LTE eNB & NR gNB with MORAN

In this network architecture both 4G LTE eNB and 5g gNB is configured to support MORAN. There are two Independent Core network connected eNB and gNB. eNB does support both control plane as well as user plane where as gNB support the data plane. Both eNB and gNB is shared by both MNO.
At cell level, both operators have independent spectrum for eNB (f1, f2) and gNB (F1, F2).

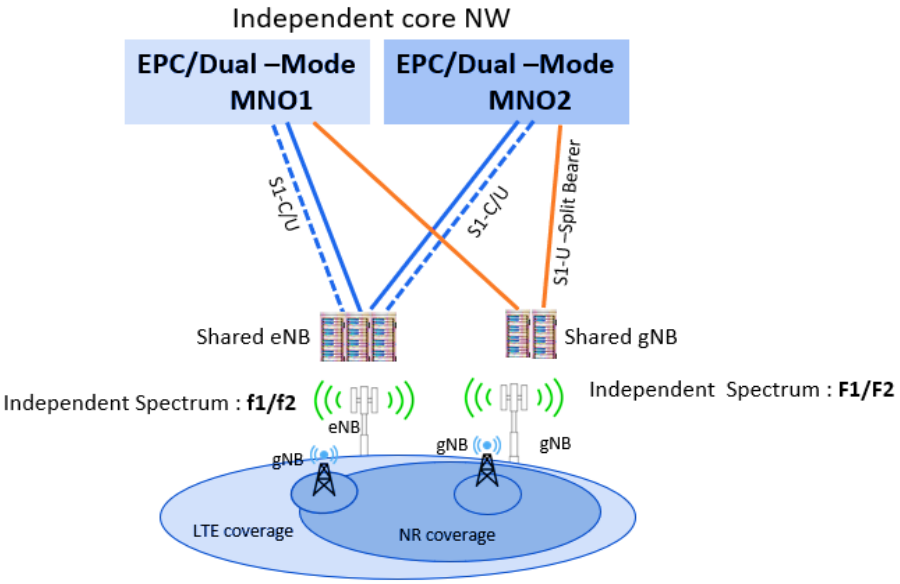


Figure A-3: MOCN Configuration Case 1

Case 2: Both LTE eNB & NR gNB with MOCN

In this network architecture both 4G LTE eNB and 5g gNB is configured to support MOCN. There are two Independent Core network connected eNB and gNB. eNB does support both control plane as well as user plane where as gNB support the data plane. Both eNB and gNB is shared by both MNO. At cell level, both operators share spectrum for eNB (f1) and gNB (F1).

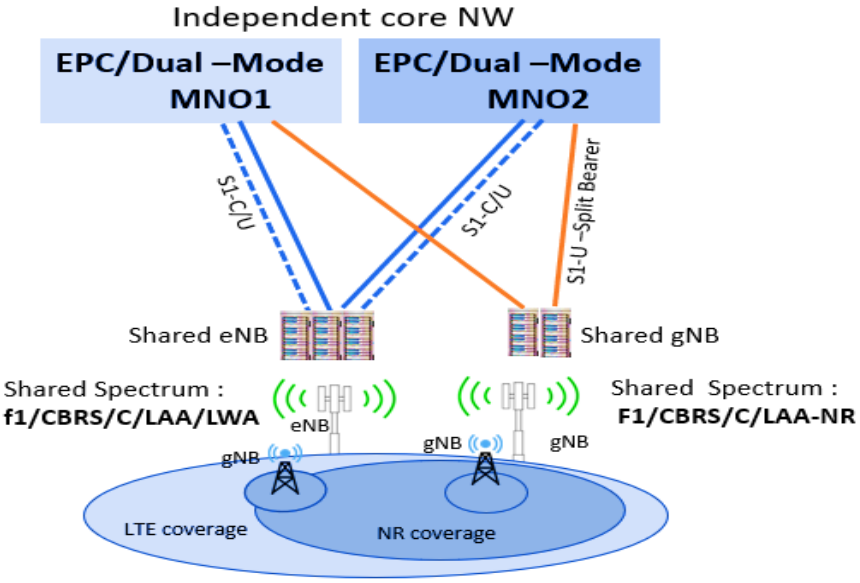


Figure A-4: MOCN Configuration Case 2

Case 3: LTE eNB in MORAN & NR gNB with MOCN OR LTE eNB as MOCN & NR gNB with MORAN

In this network architecture LTE eNB is configured to MORAN and 5g gNB is configured to support MOCN. There are two Independent Core network connected eNB and gNB. eNB does support both control plane as well as user plane where as gNB support the data plane. Both eNB and gNB is shared by both MNO. At cell level both operators have independent spectrum for eNB (f1, f2) & shared spectrum for gNB (F1). Though it will increase network complexity where two RAN nodes in different mode of operation – one in MORAN and other in MOCN. CBRS-NR, C-Band NR are most potential candidate.

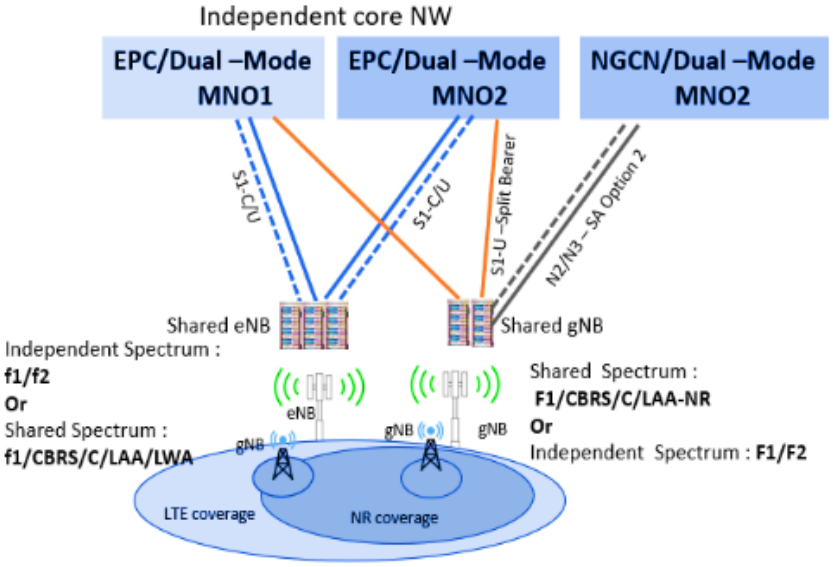


Figure A-5: MOCN Configuration Case 3

5G Non-Stand-alone based NPN

A non-stand-alone (NSA) deployment requires 4G and 5G radio coverage. Both 4G and 5G (preferred to have an overlapping RF footprint) could run on private bands or unlicensed bands (with interference mitigation mechanism). An NSA implementation refers to coverage & capacity centric deployment with traffic handling priority for private network.

The 5G Non-stand-alone (NSA) is based on the network evolution option 3 (or 3x) where 5G NR is working as data only leg & LTE handles control plane with data. Core perspective, legacy EPC will still exist.
The illustration below again shows two scenarios of private network (left side) and a private network sharing the SDM and PLMN-ID of the macro network (right).

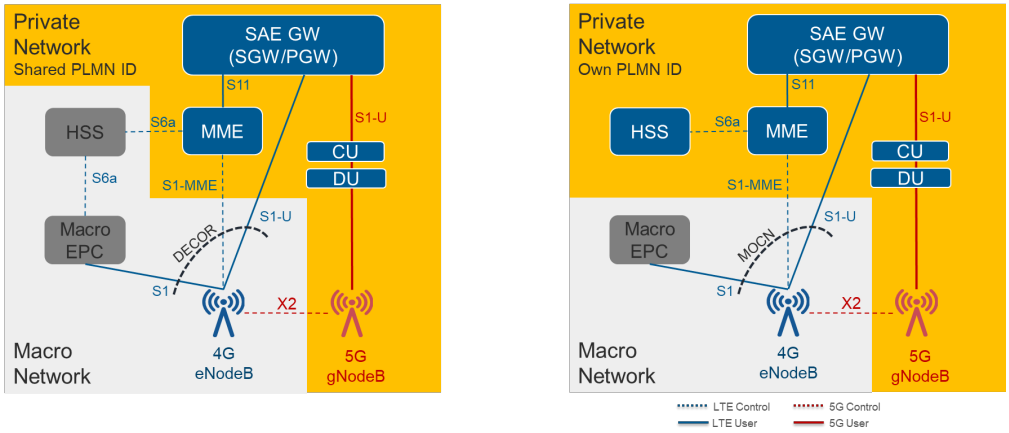


Figure A-6 – NPN in 5G NSA.

The illustration above indicates that the 5G split architecture of the private network implementing ORAN architecture where the radio units (RRU) is separated to the virtual RAN units the vBBU consisting of Distributed Unit (DU) and Central Unit (CU).

NPN Roaming Considerations

A private network with private radio units may integrate to other networks using LTE and/or NR roaming standards for authentication and home routing.

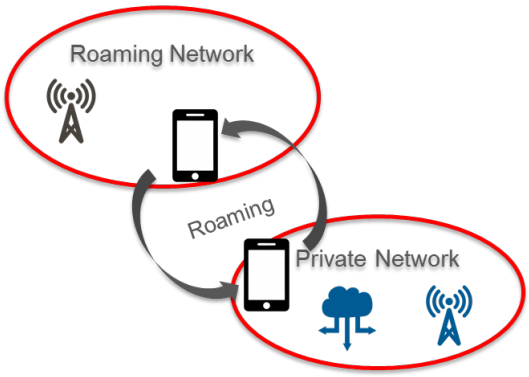


Figure A-7: Subscriber roaming to and from a private network

If the private network runs on the same PLMN-ID as the host MNO Macro network, the visited roaming network will connect towards the macro network for authentication and LTE/NR attachment as illustrated below:

- For the LTE/NR authentication, the macros network routes the authentication requests
- To the private network HSS/UDR/UDM based on the IMSI ranges/NID/CAG-ID or combination of any
- To the macro networks HSS/UDR/UDM in case the SDM is centrally used also for private networks

Private Network Management

The Network Management functions can be part of the private network (left) or centrally located to serve multiple private networks (right).

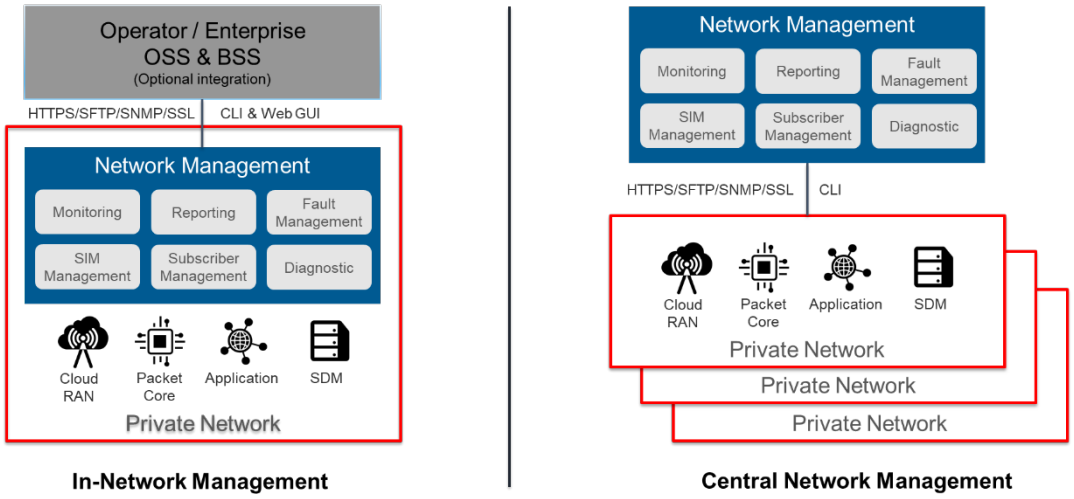


Figure A-8 - Network Management Overview

SIM and eSIM Management as well as Subscriber Management are optional management components depending the requirements on the dynamic of devices/users accessing the private network.
Monitoring, Reporting, Fault Management and Diagnostics are standard functions required for every private network. That is provided by the Central Network Management System on VNF or CNF platform.
Optionally, such solution can support North-Bound interfaces towards an existing network management solution if exists like in commercial MNO.
A network management system (either in-network or central) must support:

- Netconf/YANG or any compatible Model for Configuration Management of
- REST API for Health check queries (via GET over HTTPs)
- Zero touch rolling upgrades and downgrades, Zero touch instantiation and life cycle management
- Controller APIs (Audits, configuration etc.,) via Netconf or other
- VES for streaming life cycle EVENTs and KPIs to DCAE or other

Subscriber and SIM Management

As part of the NPN subscriber data management (SDM), solution is included in the form of the HSS or UDM/ UDR for 4G / 5G networks. For private networks working in conjunction with a macro network, SIM and subscriber management is typically integrated to the MNO's provisioning systems using REST or SOAP or compatible APIs. This Subscriber/SIM information need to be provisioned with two options:

- A lightweight option supporting physical SIM cards only: a package of SIM cards in combination with NPN delivery & pre-provision the SDM databases accordingly.
- eSIM & Subscriber Management Solution: NPN will interwork with an externally hosted subscriber management solution connected to an SM-DP+ server to provision eSIM to the private network & UE.

Acronyms

3GPP	3rd Generation Partnership Project
A1	O-RAN interface
AAS	Advanced Antenna Systems
AI	Artificial Intelligence
ANR	Automatic Neighbor Relation
ARIB	The Association of Radio Industries and Businesses, Japan
ARM	processors from ARM Holdings
ASIC	Application Specific Integrated Circuit
ATIS	The Alliance for Telecommunications Industry Solutions, USA
BF	Beamforming
CAM	Cooperative Awareness Messages
CCO	Coverage and Capacity Optimization
CCSA	China Communications Standards Association
CNF	Container Network Function(s)
COTS	Commercial Off-the-Shelf, also Common Off-the-Shelf
CP	Control Plane
CPRI	Common Public Radio Interface
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CU	Centralized Unit
CU-CP	Centralized Unit-Control Plane
CU-UP	Centralized Unit-User Plane
DARPA	Defense Advanced Research Projects Agency
DL	Downlink
DOCSIS	Data Over Cable Service Interface Specification
DPDK	Data Plane Development Kit
DSP	Digital Signal Processor
DU	Distributed Unit
E1	O-RAN interface: Connection Control Interface between PPF and RCF
E2E	End to End
eASIC	Fabless semiconductor company acquired by Intel in 2018
eCPRI	enhanced Common Public Radio Interface
eMBB	Enhanced Mobile Broadband
EMS	Element Management System in LTE
eNA	Enablers for Network Automation
eNB	see eNodeB
EN-DC	eNB to NR Dual Connectivity
eNodeB	4G LTE Base Station
ETSI	The European Telecommunications Standards Institute
F1	Baseband interface between CU and DU

F1-C	Baseband control-plane interface
F1-U	Baseband user-plane interface
FAPI	Functional Application Platform Interface
FCAPS	Fault-management, Accounting, Performance and Security
FD.IO	Fast Data - Input/Ouput project
FPGA	Field-programmable Gate Array
FRAND	Fair, reasonable and non-discriminatory licensing
GDPR	General Data Protection Regulation
gNB	5G NR Base Station
GPPP	General Purpose Processing Platforms
GPU	Graphics Processing Unit
HLS	Higher Layer Split
HVAC	Heating, Ventilation and Air Conditioning
ICIC	Inter-Cell Interference Coordination
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
ITU-T	The Study Groups of ITU's Telecommunication Standardization Sector
JSON/REST	JavaScript Object Notation representational state transfer
KPI	Key Performance Indicator
L1	see PHY
L2	Layer 2 of protocol stack - see MAC
L3	Radio Signaling Layer
Layer 1	see PHY
LCM	Life Cycle Management
LDPC	Low Density Parity Check
LLS	Low Layer Split
LTE	Long Term Evolution (4G)
MAC	Medium Access Control (3GPP NR protocol stack)
MANO	Management and Orchestration
MEC	Mobile Edge Computing
MIMO	Multiple In, Multiple Out
ML	Machine Learning
M-MIMO	massive MIMO
mMTC	massive machine-type-communications
MNO	Mobile Network Operator
M-Plane	Open Fronthaul Management Plane
MRO	Mobility Robustness Optimization

multiRAT	multiple RATs
near-RT	near Real-Time
near-RT RIC	near Real-Time RIC
NEBS	Network Equipment Building System
NETCONF	Network Configuration Protocol
nFAPI	networked FAPI
NFV	Network Function Virtualization
NFVI	NFV Infrastructure
NIC	Network Interface Card
NMS	Network Management System
non-RT RIC	non-Real-Time RIC
NR	5G New Radio, i.e. 5G radio access technology
nRT	near Real-Time
nRT RIC	near real-time RIC
NRT RIC	non real-time RIC
NSA	Non-Stand Alone
O&M	See OAM
O1	O-RAN interface
O2	O-RAN interface
OAI	Open Air Interface
OAM	Operations, Administration and Maintenance
OCP	Open Compute Project
O-CU	open CU
ODP	Open Data Plane project
O-DU	open DU, the virtualization of the RPF
ONAP	Open Networking Automation Platform
OPS-5G	Open, Programmable, Secure 5G
O-RU	O-RAN Radio, Open RAN Remote Unit
OS	operating system, e.g. Cloud OS
OSC	O-RAN Software Community
OTIC	O-RAN Testing and Integration Centers
PCI	Physical Cell Identity
PDCP	Packet Data Convergence Protocol (3GPP NR protocol stack)
PHY	Physical Layer (3GPP NR protocol stack)
PNF	Physical Network Function(s)
POC	Proof of Concept
PON	Passive Optical Network
PPF	Packet Processing Function
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network

RAT	Radio Access Technology
RCF	Radio Control Function
RIA	TIP Radio Intelligence and Automation workstream
RIC	Radio Intelligent Controller
RLC	Radio Link Control (3GPP NR protocol stack)
RPC	Remote Procedure Call
RPF	Radio Processing Function
RRC	Radio Resource Control (3GPP NR protocol stack)
RRH	Remove Radio Head
RRM	Radio Resource Management
RRU	Remote Radio Unit
RT	Real Time
RTL	register-transfer levels
RT-RIC	Real-Time RIC
RU	Remote Unit
Rx	Receive
SCF	Small Cell Forum
SDAP	Service Data Adaption Protocol (3GPP NR protocol stack)
SDN	Software Defined Network
SDO	standards development organization
SLA	Service Level Agreement
SON	Self-Optimizing Network
SR-IOV	Single Root Input/Output Virtualization
TCO	Total Cost of Ownership
TIFG	Testing Integration Focus Group
TIP	Telecom Infra Project
TSDSI	Telecommunications Standards Development Society, India
TTA	Telecommunications Technology Association, Korea
TTC	Telecommunication Technology Committee, Japan
TTI	Transmission Time Interval
Tx	Transmit
UAV	Unmanned Aerial Vehicle
UE	User Equipment
UL	Uplink
UP	User Plane
URLLC	Ultra-Reliable Low-Latency Communication
V2X	Communication between vehicles and other devices, Vehicle to Anything
vCU-CP	Virtuazlized CU-CP
vCU-UP	Virtualized CU-UP
vDU	Virtualized DU
VES	VNF Event Stream
VM	Virtual Machine

VNF	Virtual Network Function(s)
VoLTE	Voice Over NR
VoNR	Voice Over LTE
VPP	Vector Packet Procession (see FD.IO)
VR	Virtual Reality
vRAN	Virtualized RAN
WG	Working Group
x86	Intel processor family
xApps	Third party applications hosted by O-RAN
xWDM	wavelength-division multiplexing technology
YANG	Yet Another Next Generation

References

[1] J. Clayton, "Crafting a Powerful Executive Summary," Harvard Business School, 8 Sept. 2003. [Online]. Available: https://hbswk.hbs.edu/archive/crafting-a-powerful-executive-summary. [Accessed 13 Feb. 2020].

[2] 3GPP, "Study on New Radio Access Technology: Radio Access Architectures and Interfaces. 3GPP Technical Specification," 3GPP, 2018.

[3] 3GPP, "TR 38.801, Technical Specifications Group Radio Access Network: Study on new radio access technology: Radio access architecture and interfaces," 3GPP, 2017.

[4] 3GPP, "TS 38.401, NG-RAN Architecture description," 3GPP, 2019.

[5] ITU-T, "Technical Report GSTR-TN5G - Transport network support of IMT-2020/5G," ITU-T, 2018.

[6] ITU-T, "Technical Report GSTR-TN5G, Transport network support of IMT-2020/5G," 2018.

[7] CPRI, "eCPRI Specification V2.0, "Common Public Radio Interface: eCPRI Interface Specification"," CPRI, 2019.

[8] G. Macri, "Deploying-5G-Will-Cost-at-Least-130-Billion-in-Fiber-Study-Says," 10 July 2017. [Online]. Available: https://www.govtech.com/network/Deploying-5G-Will-Cost-at-Least-130-Billion-in-Fiber-Study-Says.html.

[9] 3GPP, "RP-193251, Enhancements of Integrated Access and Backhaul," Dec 9 - 12, 2019.

[10] 3GPP, "Study on integrated access backhaul," 3GPP, 2019.

[11] 3GPP, "R1-1812199, System Performance Evaluation in Multi-Hop IAB network," Nov 2018.

[12] S.-Y. R. Li, R. W. Yeung and N. Cai, "Linear Network Coding," IEEE Transactions on Information Theory, vol. 49, no. 2, pp. 371-381, 2003.

[13] O. Orhan, H. Nikopour, J. Nam, N. Naderializadeh and S. Talwar, "A Power Efficient Fully Digital Beamforming Architecture for mmWave Communications," in 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, 2019.

[14] CableLabs, "Data-Over-Cable Service Interface Specifications - DOCSIS 1.0," CableLabs, 1997.

[15] CableLabs, "Low Latency Mobile Xhaul over DOCSIS Technology," CableLabs, 2019.

[16] CableLabs, "Low Latency Mobile Xhaul over DOCSIS Technology, CM-SP-LLX-I01-190628," CableLabs, Boulder, CO, 2019.

[17] J. Andreoli-Fang and J. T. Chapman, "Mobile-aware scheduling for low latency backhaul over DOCSIS," in Proc. of IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Montreal, 2017.

[18] J. Andreoli-Fang and J. T. Chapman, "Latency reduction for mobile backhaul over DOCSIS through pipelining," in Proc. of IEEE Globecom, Singapore, 2017.

[19] J. T. Chapman, J. Andreoli-Fang, M. Chavin, E. C. Reyes, L. Zheng, D. Liu, J. Padden and A. Bernstein, "Low latency techniques for mobile backhaul over DOCSIS," in Proc. of IEEE Wireless Communication and Networking Conference (WCNC), Barcelona, 2018.

[20] CableLabs, "Synchronization Techniques for DOCSIS Technology Specification, Version I01," CableLabs, Boulder, 2020.

[21] CableLabs, "Low Latency Mobile Xhaul over DOCSIS Technology," CableLabs, Louisville, 2019.

[22] Bell Labs, "Quantifying the cost benefits of FTTH for 5G transport," Bell Labs, 16 April 2020. [Online]. Available: https://www.nokia.com/blog/quantifying-cost-benefits-ftth-5g-transport/. [Accessed 20 May 2020].

[23] 3GPP, "Study on scenarios and requirements for next generation access technologies," 3GPP, 2018.

[24] IEEE, "IEEE P1914.1, IEEE Draft Standard for Packet-based Fronthaul Transport Networks," IEEE, 2019.

[25] ITU-T, "G.8273.2: Timing characteristics of telecom boundary clocks and telecom slave clocks," ITU-T, 2019.
[26] IEEE, "1914.3-2018 IEEE Standard for Radio over Ethernet Encapsulations and Mappings," IEEE, 2018.
[27] IEEE, "IEEE 802.1CM - Time-Sensitive Networking for Fronthaul," IEEE, 2018.
[28] ABIresearch, "Mobile backhaul options -Spectrum analysis and recommendations," GSMA, 2018.
[29] C. W. M. E. Jim Zou, "Optical fronthauling for 5G mobile: A perspective of passive metro WDM technology," in 2017 Optical Fiber Communication Conference and Exhibition (OFC), Los Angeles, CA, USA, 2017.
[30] Commscope, "How WDM Helps With 5G Deployment," Commscope, 17 07 2017. [Online]. Available: https://www.commscope.com/blog/2017/how-wdm-helps-with-5g-deployment/. [Accessed 25 05 2020].
[31] NGOF, "5G-Oriented OTN Technology," NGOF, 2018.
[32] CableLabs, "P2PCO-SP-ARCH-I02-190311 - P2P Coherent Optics Architecture Specification," CableLabs, Louisville, CO, 2019.
[33] ITU-R, "Recommendation M.2083-0, IMT Vision - Framework and overall objectives of the future development of IMT for 2020 and beyond," ITU-R, 2015.
[34] Ericsson, "Ericsson," June 2020. [Online]. Available: https://www.ericsson.com/49da93/assets/local/mobility-report/documents/2020/june2020-ericsson-mobility-report.pdf. [Accessed 29 June 2020].

Acknowledgments

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 AT&T, Cable and Wireless, Ciena, Cisco, CommScope, Crown Castle, Ericsson, Intel, Mavenir, Nokia, Qualcomm Incorporated, Samsung, Shaw Communications Inc., T-Mobile USA, Inc., Telefónica and WOM.

5G Americas would like to recognize the significant project leadership and important contributions of group leaders of Intel and Matt Melester of CommScope, along with many representatives from member companies on 5G Americas' Board of Governors who participated in the development of this white paper.