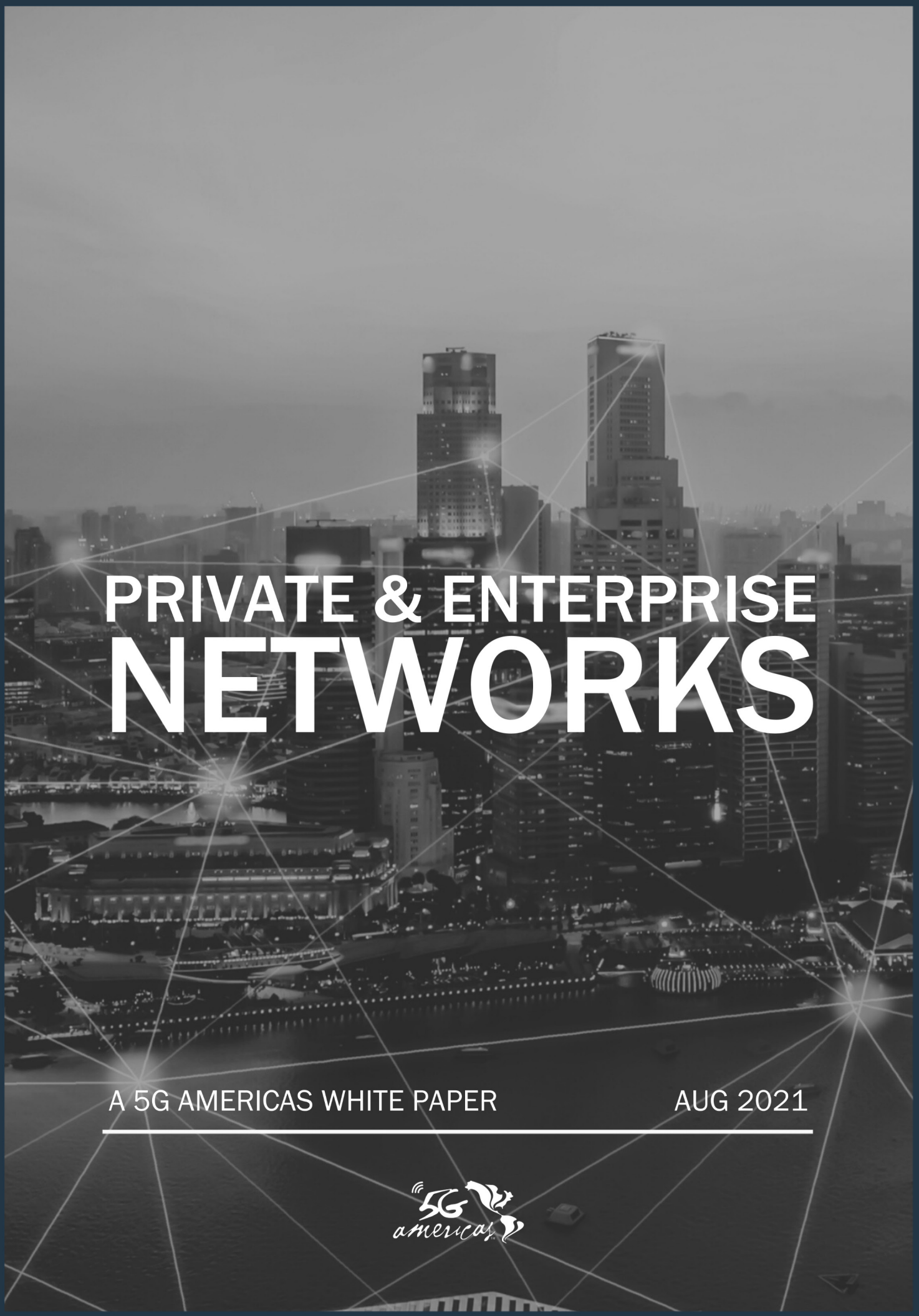


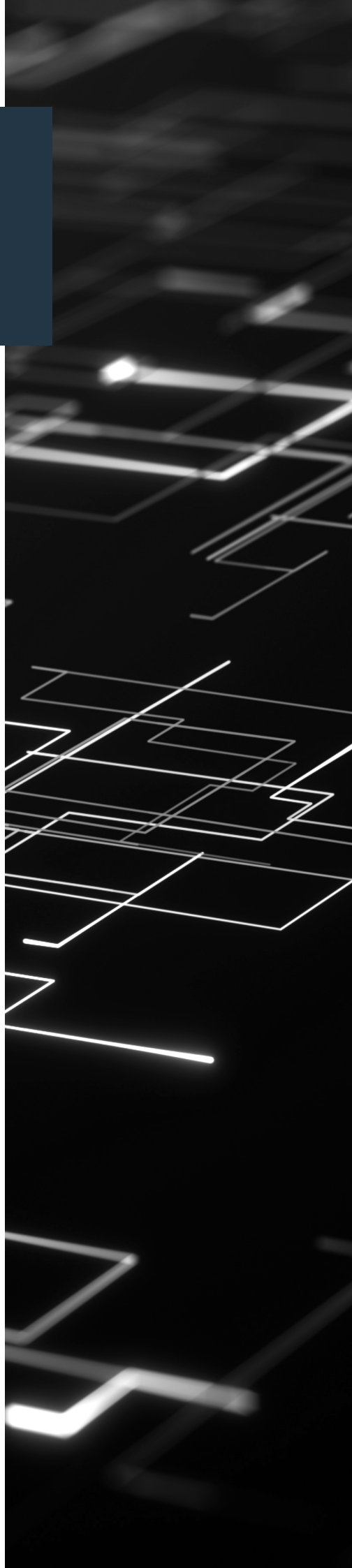
PRIVATE & ENTERPRISE NETWORKS

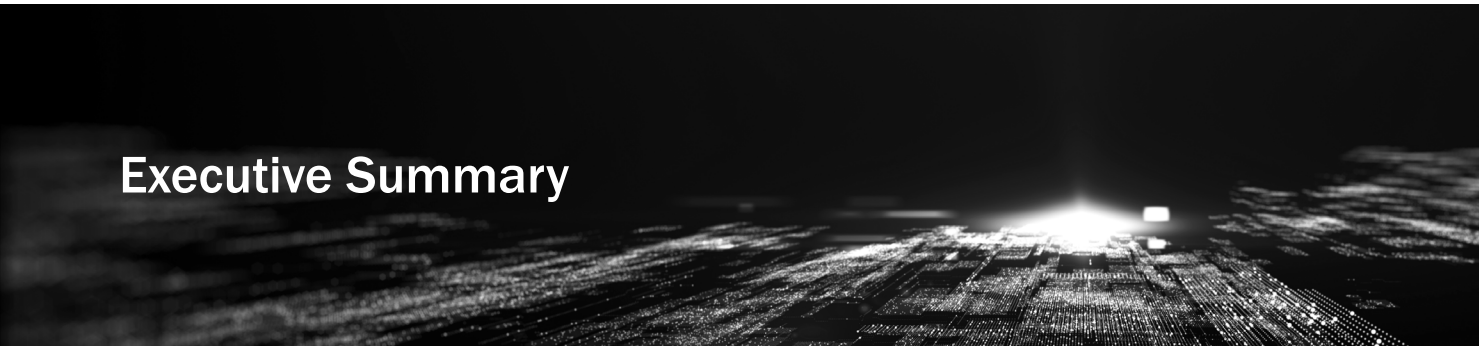
A 5G AMERICAS WHITE PAPER

AUG 2021

5G americas

Contents





Executive Summary

In today's world, enterprises are becoming increasingly distributed and autonomous. The applications and services they deliver are increasingly demanding high bandwidth, as well as reliable, deterministic communications over wide areas under different conditions and multiple networks. Enterprises and enterprise networks are increasingly demanding more spectrum, more bandwidth and lower latency. Vertical industries each present their own set of unique requirements on communications networks and no one technology or operating model will meet the needs of the enterprise. Instead, the enterprise/private network of the future can expect to be a multi-network that incorporates elements drawn from traditional enterprise models as well as from public mobile network models.

One of the greatest areas of opportunity in wireless communications is the synergistic use of cellular 3rd Generation Partnership Project (3GPP) and non-cellular (non-3GPP) technologies to expand the capabilities of enterprise and private, non-public networks (NPNs). The enhancement of cellular standards to embrace non-3GPP access and NPNs in 3GPP Releases 15 and 16, along with favorable regulatory and policy actions to open new spectrum and define new licensing models, has enabled the incorporation of cellular technologies and spectrum into the NPN. This trend has been accompanied by the development of lower cost technology to support the NPN deployment, as well as new models of operation such as Network as a Service (NaaS), bringing these solutions within reach of the enterprise or private network operator.

5G cellular network standards provide a rich set of capabilities for enabling mission critical, low-latency communications, supporting seamless mobility, and relative ease of integration with a surrounding public network. These capabilities make use of 5G technologies very attractive for cases such as industrial automation, mining, and transportation, as well as for providing extended voice coverage.

Enterprises have made enormous investments in non-3GPP networks based on Wi-Fi as the radio technology, ethernet as the transport mechanism, and very flexible management systems that enable fine grained control over identity, policy, security, segmentation, etc. These networks offer a set of capabilities that are tailored to the needs of the enterprise network operator. In general, Wi-Fi radio standards have kept up with the advances in cellular technology. Wi-Fi 6 and 5GNR offer similar performance characteristics in most dimensions, while one may outperform the other in a few areas. The enterprise or private network of the future could almost certainly be a hybrid network that combines the necessary set of elements of both traditional enterprise/Wi-Fi networks and 3GPP-standardized 5G networks.

Finding the right mix of 3GPP/5G and enterprise/Wi-Fi for a particular enterprise or private network deployment will be based on an analysis of the requirements of the intended use – one size does not fit all. This white paper explores several different go-to market business and operating models for the NPN, along with factors that will influence the ultimate model adopted. The paper presents several hybrid network architectures to support these models, examine attributes of each, and describes several solution building blocks and complete solutions to facilitate creating a hybrid NPN. The paper also outlines some geopolitical differences impacting spectrum, licensing and standardization that influence the way that NPNs may operate.

1. Introduction

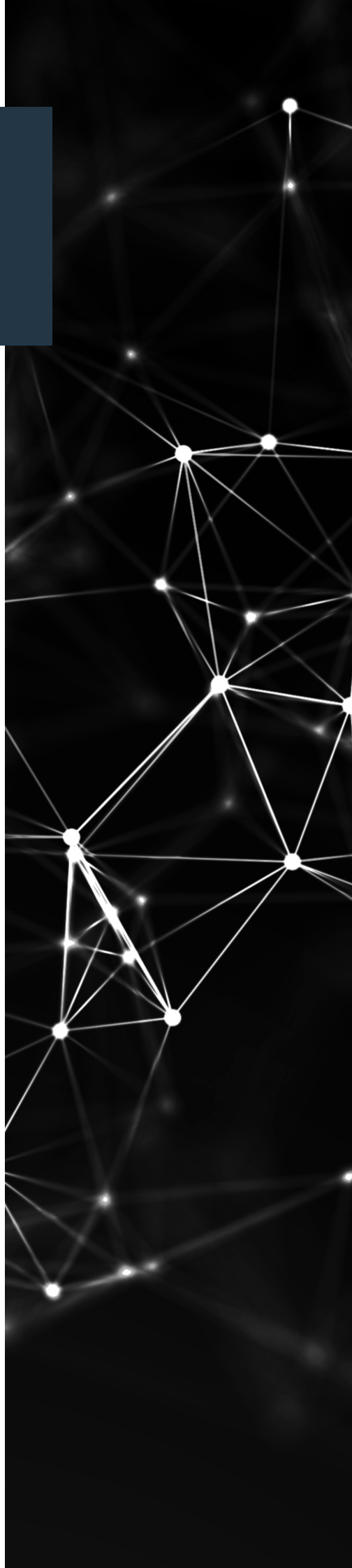
The applications and services employed and envisioned by enterprises and verticals grow ever more sophisticated and demanding. Enterprises are often widely distributed geographically and use cases range from low-latency mission critical industrial automation to coordinating communications of groups of users and devices distributed over multiple cities and states. The need for fine-grained control over characteristics like identity, policy, security, segmentation, etc., continues to grow. Maintaining a desired level of performance while preserving a consistent set of network behavior over multiple networks, multiple technologies, has become a critical need.

"5G" is the fifth-generation communication technology standard for cellular networks, initially standardized in Releases 15 and 16 of the 3rd Generation Partnership Project (3GPP). It is an end-to-end system architecture encompassing the core network, radio access network, and the new air interface, 5G New Radio (5GNR). While 3GPP initially focused primarily on public mobile network deployments, it is recognized that enterprise and private, NPNs, represent an interesting and growing opportunity that should be addressed by integrated 5G solutions. There is an expectation that 5G, along with Wi-Fi, will be the enabling technology for many vertical markets. There are some key features in the 5G system that are making it very appealing for private network deployments.

The International Telecommunication Union (ITU) has defined three standard 5G service profiles, Massive Machine to Machine-Type Communications (MMTC), Ultra-Reliable Low-Latency Communications (URLLC) and Enhanced Mobile Broadband (eMBB). These profiles are expected to meet the requirements of most industrial applications and are driving the adoption of both Wi-Fi 6 and 5G for industrial use cases. The following table characterizes these service profiles.

Fig. 1.1 Profiles of MMTC, URLLC & eMBB (Source: GSMA)

Massive Machine-Type Communications (mMTC)	Ultra-Reliable Low Latency Communications (URLLC)	Enhanced Mobile Broadband (eMBB)
• Very high device density • Extended coverage range including deep in-building • Battery life extending to multiple years • Low data rate (1 to 100 k bits-per-second) • Variable (non-critical) latency • Limited mobility (particularly with NB-IoT) • Low device cost	• Under 1 milli-second air interface latency for small data packets • Ultra-reliable communications with 99.999% or better success rate • Low to medium data rates (50 k bits-per-second to 10 M bits-per-second) • Supports high speed mobility	• Supports at least 100 M bits-per-second user rates • Peak data rate of 10 to 20 G bits-per-second • High speed mobility of 500 km/h • Up to 15 Tbps/km^2 downlink and 2 Tbps/km^2 uplink area traffic capacity



There are other industry trends which are driving 5G adoption for NPNs. The availability of dedicated or shared spectrum, roadmaps for a mature device ecosystem, and industry investments are making 5G an enterprise access option. As the manufacturing industry transitions to Industry 4.0, both 5G and Wi-Fi 6 (an IEEE 802.11ax standard) are showing the promise to meet factory automation needs.

Currently, many regulatory bodies have or are actively considering allocating spectrum for private use. In the United States there is around 150 MHz of allocated spectrum in the 3.5 GHz band, and 3.5 GHz Citizens Broadband Radio (CBRS) Service spectrum will be discussed in more detail later in this document. Similar allocations in EU and other regions, are paving the way for 5G adoption for industrial and other private networks.

Given this larger context, we can reasonably assume that 5G will enter the enterprise realm sooner or later. 5G is going to be another mainstream access technology incorporated in enterprise architectures. Furthermore, 5G will coexist with Wi-Fi 6. The growing needs of enterprise IT for a robust, secure, high-throughput and reliable connectivity service can be possibly realized with the right combination of 5G and Wi-Fi 6 access technologies, along with the right mechanisms for managing and operating the hybrid network holistically.

Many enterprises have made significant investments in IT infrastructure, such as a local area networks (LANs) and wireless local area networks (WLANs). Enterprise applications typically range from critical applications, such as for manufacturing and supporting human resources and other information systems, to providing convenient internet access and voice connectivity for guests or the public at large. A network that enables critical applications and supports information systems is often characterized by low latency and effective isolation and security. Manufacturing represents one example in the industrial sector that can comprise a range of service innovations being developed across several sectors. Retail and logistics, ports and transportation, mining, and many other types of operations are benefiting from new application and infrastructure development.

In addition, edge computing is especially adept at addressing low-latency and isolation by, respectively, establishing a physical and logical boundary onsite or close to the enterprise. A decrease in distance and in network hops can greatly reduce latency. Smart application pre-processing or co-processing at the edge can also provide latency advantages while also providing enhanced security and control all the way to the edge of the enterprise's premise, rather than only in the cloud. Edge computing can bring together IT and networking applications under a common platform. Having a common compute platform at the edge benefits enterprises with reduced latency, and also by enabling granular control and strong security.

Private cellular networks have been developed to the point that the deployment cost (CAPEX) has become more accessible to enterprises. Some OEMs have developed their equipment and ecosystem for private cellular operation to be almost as simple as plug and play and have the advantages of deterministic operation and security right out of the box. Given some of the innovations, the operational cost (OPEX) a private cellular network may approximate that of operating a fully managed Wi-Fi network with change controls, a network operations center (NOC), and security operations center (SOC). The total cost of ownership (TCO) of a private cellular network may also be on par with that of a fully managed Wi-Fi network.

Critical applications often require highly deterministic operation, whether the network is lightly used or if it is heavily loaded. A private cellular network with edge computing can be solution for critical applications that require low-latency and effective isolation and security. Another solution is to augment an existing Wi-Fi network with private cellular to deliver the most appropriate wireless network for each application, while adding capacity to the entire infrastructure.

Enterprises may often be interested in enabling cellular-like applications such as voice over 4G LTE (VoLTE) or 5G NR (VoNR), mission critical push-to-talk (MCPTT), roaming with cellular operators, or leveraging existing operations and business support systems (i.e., Business Service Systems (BSS)/OSS, billing). While there are solutions for voice over IP (VoIP) or over the top (OTT) push-to-talk (PTT) that can be implemented over Wi-Fi networks, there may be more critical requirements that cellular networks can provide, such as for built-in location tracking, or more industry-specific needs such as petrochemical, chemical manufacturing, or mining where first responders may need to be dispatched quickly.

Some enterprises may need to improve existing cellular service on their premises. For instance, multiple dwelling units (MDUs) or office buildings may benefit from offering tenants a stronger signal, greater quality, higher capacity, and more control over a public cellular operator macro-tower signal that is relatively weak onsite. An advantage of extending public cellular service on-premise is that the network can be leveraged as a private cellular network for secure in-building Internet of Things (IoT) for smart buildings. The venue or MDU property with a cellular network may increase in value, thus, attracting tenants that would pay premium fees. Also, the venue or MDU may attract additional public cellular operators, who may be open to leveraging the installed infrastructure to expand their cellular network footprint.

Private cellular networks are a solution to enable smart buildings and applications. Access to the private cellular network can be limited to building control devices such as air quality monitors, comfort, enforcing social distancing during pandemics, building energy efficiency, and physical security and safety. With sensors in

place, and reliable communication, building controls can be automated using machine learning and artificial intelligence techniques.

Like smart buildings, private cellular networks can enable smart communities. Multiple buildings are being outfitted for air quality, comfort, and energy efficiency control. Pedestrian traffic monitoring and crowd management can be established in common and outdoor spaces. If under the community's purview, a private-community cellular network can support applications such as traffic management, smart street lighting, smart parking, and emergency response and communication.

In general, enterprises that install a private cellular network increase their options and flexibility to deliver the right services to targeted customers. Enterprises can exercise more control over coverage on their property. Similarly, enterprises can benefit from having direct input regarding service quality per device or user group. To help manage costs, enterprises can start with a small network and that grows as the demand increases. Finally, enterprises can have great control over the security of the private cellular network through policy controls and network design.

When enterprises choose not to install their own private cellular network, there are available service providers such as neutral host providers, who can offer the enterprise, not only options to fulfill performance and security requirements but, a shared network at a lower cost.

Enterprise private cellular networks can also benefit from several improvements in 5G. 5G's URLLC service profile addresses several critical applications in different industries and scenarios, such as for manufacturing, automation, and autonomous equipment or vehicle operation. Also, 5G MMTC service profile targets scalable IoT deployments.

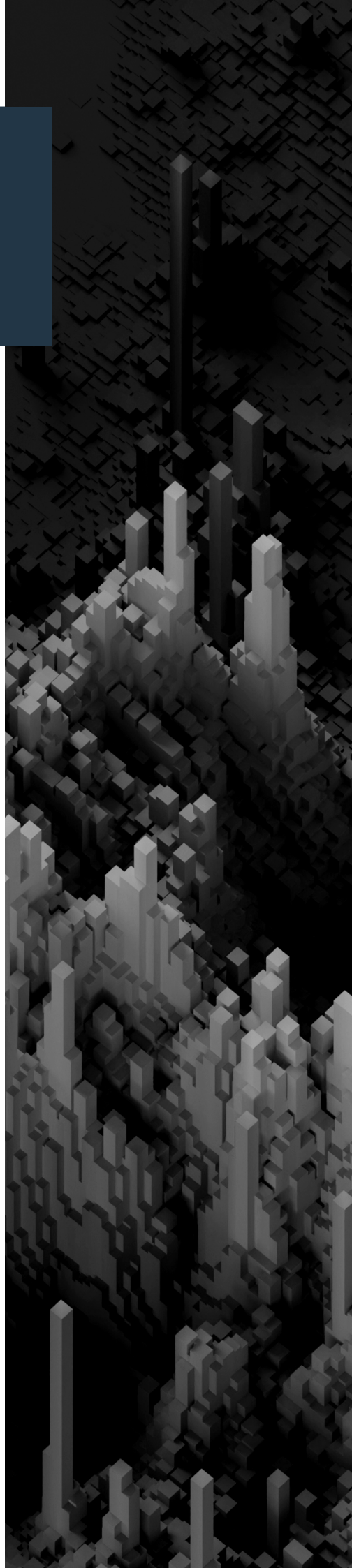
A principal feature of deploying a 5G core is the ability to leverage much of the work that has been done in software defined networking (SDN) and network functions virtualization (NFV) leading to network slicing. Conceptually, a 5G Core (5GC) with NFV infrastructure (NFVI) would enable a flexible network in which network slices can be quickly defined and deployed without having to touch any physical components of the infrastructure. Recent developments such as RESTful architectures, standardized software interfaces, and related network exposure function (NEF) facilitate more innovation. Furthermore, service providers and enterprises can leverage capabilities such as automated service provisioning to deliver the exact network to customers when they need it.

There is an industry focus on innovation and a growing ecosystem, where RAN OEMs, device OEMs, cellular network core providers, service providers, along with system integrators are bringing it all together. Also, there is an increased service innovation capability for different verticals, such as in industry, retail, and transportation.

With so many private, technological, device, and market-driven synergies, the opportunities for service providers and customers are limited only by the imagination. Public venues or smart cities or communities can manage their IoT, security and safety infrastructure while providing improved coverage for public networks. Multi-tenant office buildings or dwellings can manage their building systems while also augmenting public network coverage, increasing real estate value and potential revenues from premium fees. Hospitality can augment wireless access beyond in-building controls, security, and safety, by providing a consistent user experience across their properties.

Deploying private networks entails potentially placing edge devices at the site to provide access to enterprise resources. The requirement to integrate existing enterprise networks and applications may require interoperability development and testing to ensure proper functionality. A private cellular network may require a unique Public Land Mobile Network ID (PLMN ID) for it to be globally unique for location services and security. For example, the CBRS/OnGo Alliance has made available shared PLMNs in the United States for enterprises that require their own PLMN ID. A non-CBRS deployment may require a unique PLMN ID, of which there are few remaining available if being deployed in the United States. The choice of a PLMN may influence the architecture, connectivity, and attractiveness, to public network providers. Moreover, a public network's macro signal strength requires careful integration with an enterprise's private network if roaming is a requirement.

2. Go-to-Market and Operating Models



The NPN's go-to-business and operating model may take various forms:

- *Enterprise managed and controlled, generally where the enterprise adds 3GPP radio access technology to an already-existing NPN built on ethernet and Wi-Fi access, and choses to manage and operate the hybrid network themselves.*
- *Service provider managed and controlled, where the enterprise outsources control of the NPN to a service provider. In this model, the driver may be that the service provider wishes to expand its coverage footprint in-building, or even to offer neutral host capabilities, and will provide 5G core elements (possibly in the cloud), management, etc.*
- *Hybrid management and control, where a 5G network is added to an existing enterprise network, but where the 3GPP and non-3GPP components are managed as two separate networks. The 3GPP portion of the network in this scenario may be managed by the service provider or by the enterprise, or even by a third party. Applications and services may be split by function between the two networks, to achieve more complete separation between the two. An example would be where an enterprise migrates its factory automation to a 5G access network and keeps the rest of its traffic and applications on its existing Wi-Fi/Ethernet network.*

An enterprise or other entity contemplating the deployment of an NPN or integrating 3GPP/5G technologies into their existing network will face several decisions regarding how and by whom the network will be operated and designed. First, the NPN operator will need to decide who or what the targeted users of the network are; are they strictly internal to an organization, or will they include others? At one extreme is an entirely self-contained industrial automation deployment that is completely closed and requires no interaction with an outside network. At the other extreme is the neutral host network, which may provide services to the members of the enterprise, to customers of a service provider partner and to customers of other service providers. The degree to which the network must serve other, non-enterprise users and devices will drive many of the other decisions.

Will mobility between the private network and licensed public networks or other private networks be required, and if so, how would that be accomplished? In the case where the enterprise has an existing private network, perhaps already using Wi-Fi as the wireless access mechanism, the operator will have to decide how much integration/interaction is required between the existing network and the new 5G network.

The private network operator will need to decide which portions of the network it wishes to manage and operate, and which portions it will outsource to a service provider or third party to manage and operate. There are two prominent considerations when making this decision. Managing a 3GPP-compliant 4G or 5G network is generally regarded as being more complex than managing an enterprise network with Wi-Fi as the primary access technology. This perceived added complexity of managing a 3GPP network may be something that the enterprise IT organization would prefer not to deal with and would prefer to outsource to a service provider or third-party partner. On the other hand, many

large enterprise networks are already quite complex, operated by competent IT organizations that would be capable of managing the increased complexity, and maintaining full control over the hybrid network. That may be more important to the enterprise than avoiding some additional complexity.

A fundamental decision that the operator will face has to do with spectrum and access technologies that will need to be supported, and how those access mechanisms will be integrated into the hybrid network. If the network is to operate even partially in licensed spectrum, the NPN operator needs to determine where the spectrum will come from and using that spectrum will require partnership with the MNO license holder. The sections below deal with these issues in turn, presenting the options available, and discussing the pros and cons of each.

2.1 Managing and Operating the Private Network

Historically, enterprise and other NPNs have evolved from a different starting point and along different paths than the ones taken by public mobile wireless networks. Enterprises have made use of public mobile networks for telephony services, usually not integrated with their internal enterprise wireline telephony services, and essentially separate from them. They have made use of public mobile networks data services strictly as a transport leg, ensuring the security of their data by using encrypted VPN tunnels to render their data connections opaque across mobile networks.

The decision to integrate 3GPP radio access technology into the private network, (or to create one based on 3GPP technology from scratch) will require a different approach to operating and managing the network, perhaps with more tight cooperation with a licensed MNO.

Several options are examined in the following sections.

2.1.1 Management and operating models: Some factors to consider

When it comes to choosing a viable network infrastructure for the enterprise, there is no one size fits all solution.

The management and operating model selected will depend on the degree of autonomy and visibility into the network operation that is required as well as the degree of comfort that the NPN operator has with managing a network that is potentially more complex than a traditional, completely non-3GPP network.

Some of the factors that an NPN operator will have to consider when selecting a management and operating model are:

- *Financial models - When it comes to private networks some enterprises would choose to outsource the deployment and management of the 3GPP/5G portion of their network and adopt NaaS models that allow them to lower the capital expenditure and leverage best in class expertise for the 3GPP portion of the network.*
- *Support models - MNOs have the Operations Support Systems (OSS) that can be extended or, if necessary, instantiated for specific deployments. This is particularly true for enterprises that already take advantage of other carrier services such as broadband fiber, Enterprise VPN and others. Being able to have a holistic troubleshooting view of the network for root cause analysis and remediation has a significant advantage reducing mean time to repair and providing service continuity across the enterprise. This becomes even more critical in the case of large enterprises with complex WAN topologies. On the other hand, many existing enterprises already have a set of methods, tools and mechanisms for performing these functions in their networks and will want to integrate the new 3GPP network into their established systems.*

- *Data confidentiality and other security requirements - The ability to control which data stays local and control of devices and applications can play a significant role in the decision to adopt a private deployment model.*
- *Integration requirements - Enterprises already leverage cloud native applications (on-premise, hybrid or public cloud). Virtualized Network Functions (software-based solutions for edge) can easily integrate into existing infrastructure and can also bring cloud applications on-premise ecosystem. Combining cloud apps and tools and bringing familiar cloud applications and tools to the enterprise location increases data privacy, provides greater control and allows for low-latency.*

On the other hand, enterprises with established and complex networks (often with Wi-Fi as the primary radio access), will need to address fitting an operator led model into their existing IT practices once they decide to add 3GPP radio access to their existing network, and may opt in favor of a more autonomous operating model for the NPN to preserve the methods and mechanisms they have already developed. Some of the considerations are:

- *Policy/segmentation: What/who is permitted to connect to what/whom? Enterprise IT networks often support a broad range of options and allow a great deal of control over connectivity, priority, and access to apps and services. The NPN operator will need to evaluate how to continue to support these functions and how to integrate the new 3GPP network into its established methods.*
- *Authentication and Identity Management: Established enterprise networks already have in place mechanisms that give them a great deal of flexibility and control for authenticating devices and users on their networks. Ideally, the hybrid NPN would permit them to continue to use these mechanisms, and use them for the 3GPP access portion of their networks.*
- *Subscriber/Device management: Established enterprises have existing, well-functioning methods for managing devices, developed to suit their own individual needs, as well as for onboarding new users and devices. The new 3GPP elements of their network will generally need to either support these mechanisms or be segregated from the existing network.*
- *Control of the IT and Wi-Fi network: An existing enterprise with a well-functioning IT network and extensive Wi-Fi deployment may not want to completely outsource control to a service provider partner or third-party partner. The new 3GPP network portion will need to be integrated into existing IT processes.*
- *Control of Connectivity and Multi-Path: 3GPP has standardized methods in Releases 15 and 16 for supporting non-3GPP access in conjunction with 3GPP access, but the model supported puts control over this function into the 5G Core. Enterprises may want to preserve more control over these functions and permit more flexible multi-path and access selection architectures, even treating the 3GPP connection as just another multi-path leg in the session, as well as supporting multi-path protocols not currently considered by 3GPP.*

2.2 Enterprise Assessments and Considerations

There are three spectrum options available to the enterprise/private network operator in the United States:

- *Licensed spectrum, i.e., spectrum licensed to a public MNO*
- *Shared or lightly licensed spectrum*
- *Unlicensed spectrum*

It is also possible (and often desirable) to operate in two or more of these spectrum options, e.g., 4G or 5G, in licensed or shared spectrum along with Wi-Fi, or some other radio access technology in unlicensed spectrum. These options are described in the following sub-sections.

2.2.1 Licensed Spectrum

An NPN operator may, in partnership with a licensed public MNO, operate a private network in the partner's licensed spectrum. In this model, the NPN may operate in the same spectrum used by the MNO partner's enveloping macro network, or, less commonly, the MNO partner may dedicate some of their spectrum to the NPN. A hybrid of these two approaches is also possible if the NPN is sufficiently isolated from an RF point of view, that the NPN and the enveloping MNO macro network do not interfere with one another. Examples of this might include remote mining sites, isolated industrial deployments, or natural resource exploration and extraction.

The advantages of operating in MNO licensed spectrum may include ease of mobility in and out of the NPN and may also offer the opportunity for the MNO to extend its public coverage for its own native customers to the area covered by the NPN, subject to business agreements made between the MNO and the NPN operator. In this way, the MNO realizes enhanced in-building coverage at a fraction of the investment required to go it alone.

Disadvantages of operating in licensed spectrum may include interference between the NPN and the enveloping MNO macro network. This may require careful engineering of the NPN and may also require that the NPN be considered in the MNO's frequency planning and mobility management. There may also be some increased complexity in terms of segregating the NPN traffic and ensuring that the enterprise IT policies and SLAs are met.

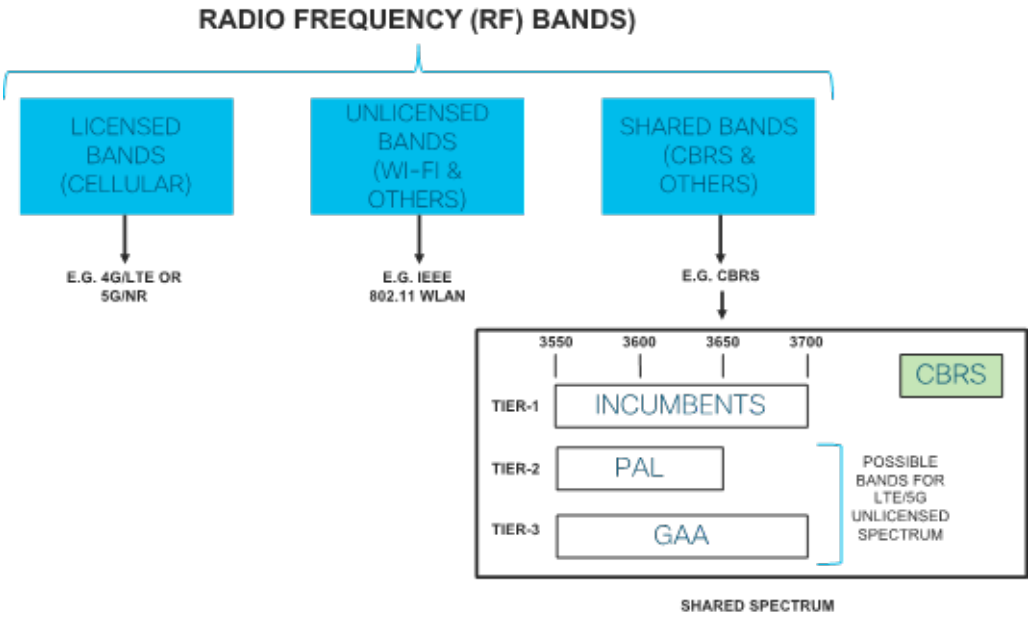
However, operating a NPN in an MNO's licensed spectrum that could still be attractive if the private network would not generate so much traffic that it would degrade the performance of the MNO's public spectrum, might be to operate in an MNO's spectrum in a spectrum sharing architecture, e.g., a Multi-Operator Core Network (MOCN) or a Multi-Operator Radio Access Network (MORAN). Moreover, the MNO partner may want to leverage the NPN as a low-cost extension of their coverage footprint into in-building and other spaces poorly covered by the MNO's macro network. More will be said about these options in a subsequent section.

2.2.2 Shared or Lightly Licensed Spectrum

To foster the adoption of small cells and spectrum sharing, the Federal Communications Commission (FCC) completed the standardization of the Citizens Broadband Radio Service (CBRS) in the USA. CBRS is a 150 MHz wide broadcast band at 3.5 GHz. (3550 MHz to 3700 MHz). Under the new rules, a wireless carrier (public or private) could use CBRS to deploy a mobile network without having to acquire a spectrum license. The FCC adopted a three-tiered spectrum authorization framework to permit flexible and orderly use of the band. The three tiers are:

- *Incumbent Access: Users in this tier include certain federal and military users (particularly US Navy radar operators), as well as historical satellite service users. Grandfathering provisions for incumbent access users are scheduled to last 5 years.*
- *Priority Access: Priority Access Licenses (PALs) are assigned via a competitive bidding process. Each PAL gives authorization to operate in a 10 MHz channel in the 3550-3650 MHz portion of the CBRS band. Authorization corresponds to a single census tract and lasts for 3 years. Many PAL licenses have been purchased by traditional MNOs and large service providers.*
- *General Authorized Access (GAA) is licensed to permit open, flexible access to the entire CBRS band. A GAA user may use any portion of the CBRS band not assigned to a higher tier (e.g., the 3650-3700 MHz band) and may also opportunistically use any unused Priority Access channel.*

Fig. 2.1 Radio Frequency Bands (Incumbent, PAL and GAA)



CBRS PAL and GAA users may be temporarily pre-empted by a higher priority (usually military) user in need of the spectrum. Apart from those instances, a PAL user will generally be assured access to the number of 10 MHz bands purchased, though the exact frequency of those bands may move from day to day. Census areas are not oversubscribed in the Priority Access band. GAA may be oversubscribed so a non-overlapping 10 MHz channel may not always be available. In the case where the GAA users are oversubscribed, they are assigned operating bands that may partially overlap other users.

CBRS bands are assigned dynamically by a Spectrum Access System (SAS), a cloud-based service which keeps track of channel assignments as well as high-priority pre-emptive users, and assigns channels according to FCC rules, for use by PAL and GAA users in their geographic areas.

Because of the restriction of authorizations to a census area (much smaller than the areas covered by a public mobile license) and the flexibility with which channels may be assigned, CBRS may potentially achieve the determinism of LTE and 5GNR scheduling at lower cost than operating in licensed spectrum. CBRS may also operate critical services and applications in an NPN in “cleaner spectrum” than is possible in the unlicensed bands, since access to the spectrum is controlled. CBRS spectrum channelization is not conducive to the use of Wi-Fi, since a 10MHz channel is insufficient to support Wi-Fi. However, CBRS spectrum may be used by itself or may be aggregated with licensed spectrum to provide LTE and/or 5GNR coverage.

It is important to note that CBRS is only available in the USA. This shared spectrum option is not currently available in the rest of North America. In Canada, for example, the 3650-3700 MHz frequency range, known as the Wireless Broadband Service (WBS) band, is currently licensed on a shared all-come, all-served basis. With a simplified licensing process and no license fees, WBS is a popular band for fixed wireless access in rural and remote areas and other services such as automatic meter reading and video surveillance. Until recently, there have been no limits on the number of WBS licenses in the same frequency range and geographic area and all licenses have equal access to the spectrum.

As a result, WBS stations often have overlapping coverage and there have been some challenges with coordination between licensees. These challenges are only expected to worsen as operators continue to expand their systems/ networks.

After a recent consultation on the 3650-4200 MHz band, Innovation Science and Economic Development (ISED) Canada has decided to displace the current WBS incumbents and designate 80 MHz of spectrum in the 3900-3980 MHz range for shared use. This provides an additional 30 MHz of spectrum for shared use, while allowing existing and new WBS operators to leverage the emerging 5G NR equipment ecosystem to increase capacity and deliver enhanced services.

As part of the ruling, WBS operations in metro areas will be displaced by March 31, 2025, and by March 31, 2027, in all rural and remote areas. In the interim, a moratorium has also been placed on new WBS station deployments in metropolitan areas.

While different shared licensing processes were proposed as part of the consultation process, including a CBRS-like system, ISED will be issuing a separate licensing framework consultation for the 3900-3980 MHz band in the future.

2.2.3 Unlicensed Spectrum

In many instances, particularly for short-range or self-contained wireless deployments, it is attractive to be able to operate without any licensing, authorization, or interaction with the FCC at all. The FCC and other jurisdictions (e.g., Canada) have designated several bands for unlicensed use. The most widely used for enterprise NPNs and consumers are the 2.4-2.5 GHz band (the 2.4GHz band), and the 5725-5.875MHz band (the 5.8 GHz band). The 6 GHz band (5925-7125 MHz) has also recently been adopted for unlicensed use by several countries in the Americas (e.g., US, Canada, Brazil, and Chile) and is under consideration by others (e.g., Mexico and Columbia). With 1.2 GHz of spectrum, the 6 GHz band effectively increases the amount of mid-band spectrum available for unlicensed use by almost a factor of five. It also enables the next generation of Wi-Fi – Wi-Fi 6E, which all promises speeds over two-and-a-half times faster than the current standard.

For the last several decades, the primary use of these bands has been for wireless local area networks (WLANS) using Wi-Fi as the dominant radio access technology, although these bands (particularly the 2.4GHz band) are also used for Bluetooth and other radio technologies. Traditionally, enterprises have operated Wi-Fi networks in unlicensed spectrum, and have built their IT infrastructure around Wi-Fi as their wireless access. It is likely that they will continue to do so because of the lower cost of Wi-Fi to deploy, maintain and scale. Moreover, enterprise IT operations are rooted in Wi-Fi, and enterprise IT organizations have designed their security, policy, authentication, authorization, etc., around their Wi-Fi networks.

Since 3GPP Release 13, there have also been efforts to introduce 3GPP radio access technologies in unlicensed spectrum with varying degrees of licensed service provider involvement. These are discussed briefly below.

2.2.3.1 Wi-Fi in Unlicensed Spectrum

The advantages of Wi-Fi in unlicensed spectrum are typically thought of as low-cost, ease of deployment, ease of management, scaling, and incumbency in existing enterprise networks, along with the ease of autonomous operation by an enterprise. Wi-Fi in its earlier incarnations used a completely unscheduled and contention-based Media Access Layer (MAC) to serve multiple users trying to gain access. Consequently, its performance was less deterministic than a tightly scheduled technology like LTE or 5GNR could deliver. However,

the current generation of Wi-Fi, 802.11ax, addresses these issues and delivers competitive, deterministic performance, hence it is very likely that Wi-Fi in unlicensed spectrum will continue to be an important component in enterprise NPNs in the future.

2.2.3.2 LTE and 5GNR in unlicensed spectrum

Since 2012, there have been efforts to introduce 3GPP radio access technologies in unlicensed spectrum. Until Release 16, these have been focused on the use of LTE, and have included:

- *LTE-Unlicensed (LTE-U), developed by the LTE-Forum in 2012, which uses an LTE control channel in an operators' licenses band, but which uses the unlicensed 5GHz band exclusively for the user plane.*
- *License Assisted Access (LAA), standardized by 3GPP initially in Release 13 (downlink only), and enhanced in Releases 14 (when uplink operation was added), and 15 (as "further enhanced LAA" or feLAA). LAA manages contention with Wi-Fi by using a protocol called "Listen Before Talk" (LBT).*
- *LTE-WLAN Aggregation (LWA), standardized by 3GPP in Release 13 and enhanced in Release 14.*
- *MulteFire, developed within the MuLTEfire Alliance as a mechanism to deploy LTE purely in unlicensed spectrum.*

Beginning in Release 16, 3GPP addresses the use of 5GNR in unlicensed spectrum globally with New Radio Unlicensed (NR-U). NR-U is an extension of LAA to support 5GNR. Two "anchored modes" are defined, where the anchor network is either a 5G network with the NR-U anchored to a 5G-CN, or is a 4G network, with the NR-U anchored to an EPC. In addition to the two anchored modes of operation, NR-U also supports a standalone mode that would operate completely in unlicensed spectrum without the need for any tethering to a licensed carrier.

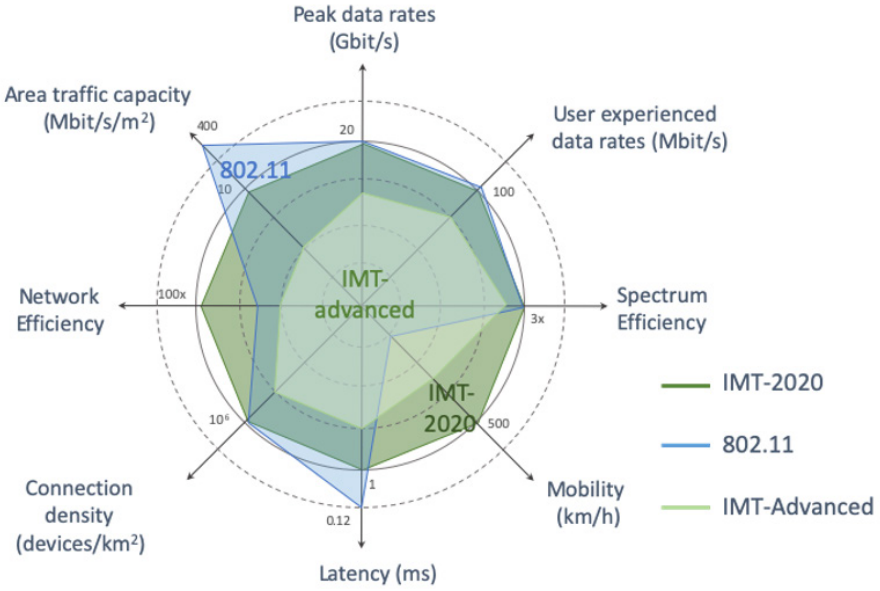
2.2.3.3 Comparing Wi-Fi and 5GNR in unlicensed spectrum

For the most part, NR-U in standalone mode is constrained by the same considerations as Wi-Fi in unlicensed spectrum, i.e., controlling interference and co-existing with other technologies (e.g., Wi-Fi), so it offers little advantage over Wi-Fi. However, when combined with licensed or shared spectrum, it could provide an improved proposition over Wi-Fi in some cases.

Figure 2.2 is a comparison of 802.11ax and both IMT-Adv and IMT-2020 (5GNR).

The two technologies offer very little difference in performance, except for mobility support – 5G and other 3GPP technologies outperform Wi-Fi in cases where seamless mobility and network efficiency are required. In deployments that do not require seamless mobility, 802.11ax may be a better choice for reasons of economics and ease of integration into existing enterprise deployments. On the other hand, Wi-Fi 6 could outperform both LTE and 5GNR in terms of latency and area traffic capacity.

Fig. 2.2 802.11ax evaluation for IMT-2020 eMBB Dense Urban test environment [1]



3. Edge and Network Architectures

3.1 Enterprise NPN Requirements

Enterprise networks built on Ethernet and Wi-Fi access (Wi-Fi) and 3GPP compliant 5G (5G) networks address some fundamental requirements differently. In some cases, the differences are complementary. In others the needs they were designed to address are not the same. 3GPP network standards have evolved to support public mobile access; enterprise networks have evolved to suit specific needs of an enterprise in a more self-contained network environment.

In some ways, the flexibility provided by the tools that have evolved to support enterprise networks give greater control to the NPN operator over things like supporting different types of identities and even multiple, context-dependent identities, very specific rules for segmentation (i.e., what can connect to what) and policy.

The enterprise NPN, whatever its architecture is and whatever its operating model is, must address the following issues:

- *Identity Management*
- *Security and Compliance*
- *Access Control*
- *Application Visibility and Control*
- *Location Management*
- *Service Assurance*

The following tables present characteristics of traditional Enterprise/Wi-Fi (called Wi-Fi for short) and 3GPP (called 5G for short) network methods.

Table 3.1 Identity Management

Wi-Fi	5G
IT admin securely manages inventory of user credentials, device identitiesand workload/application identities	User credentials (high entropy key) defined in SIM and AuC
Integration with different systems of authoritative record, e.g., HR, email, inventor etc.	SIM lifecycle management for corporate devices augmented with more complex eSIM lifecycle management for things
Perform lifecycle management of digital identities	Managing device identities on public and private networks

Table 3.2 Enterprise Security and Compliance

Wi-Fi	5G
Configuration and compliance management delivers integrated monitoring and reporting	Compliance focused on spectrum
Best practice and configuration guidelines and image management	Slice management for handling sovereignty and isolation requirements
Measurements against regulatory compliance	
Ongoing consultation around liability when using private Wi-Fi networks	

Table 3.3 Enterprise Access Control

Wi-Fi	5G
Shift from single factor to context-aware multi-factor (location, endpoint type, device posture, time, on-net/off-net…)	Primary SIM based authentication enhanced with secondary enterprise authentication
Role-based and context-based policy enforcement	PDN/APN based policy control

Table 3.4 Enterprise Application Visibility and Control

Wi-Fi	5G
Network based application recognition with heuristic algorithms to detect encrypted traffic	Flow Based Charging for network usage for service data flows, including charging control and online credit control
DNS as Authoritative Source (DNS-AS) for subsequent flow policy	Policy control for session management and service data flows (e.g., gating control, QoS control, etc.)
Integrated QoS Policy Control	
IPFIX (RFC7011) based instrumentation of application usage and performance	

Table 3.5 Location Management

Wi-Fi	5G
Inventory systems integrate with imported maps and floor configuration	Location Management Function uses RAN and UE measurements to compute position of UE
Angle-of-arrival, path loss and multi-AP triangulation used to enhance accuracy to ~ +/- 1m	Angle-of-departure/arrival, path loss and multi-cell RTT triangulation used to enhance accuracy
Integrated beacons for enhanced location aware use cases	Indoor open office accuracy < 1m

Table 3.6 Service Assurance

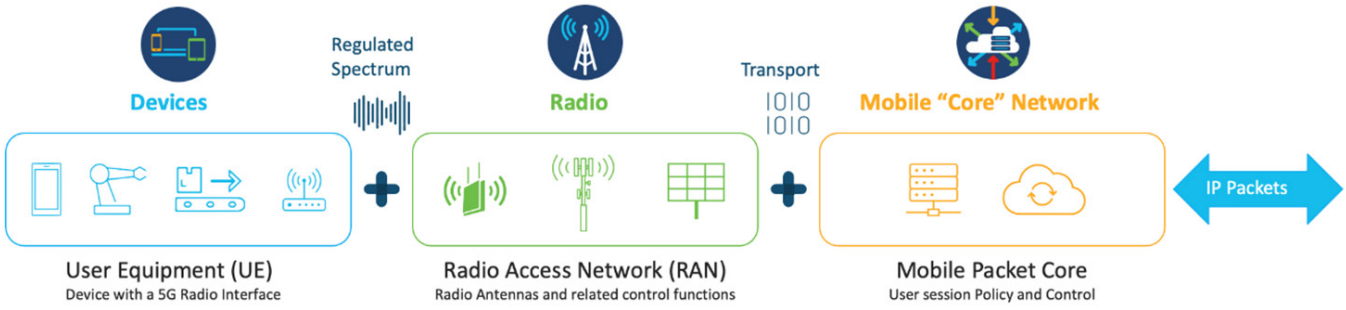
Wi-Fi	5G
Self-build campus network responsibilities accommodate extreme production critical requirements (e.g., line outage cost of $20k/minute)	Slicing foundation for simultaneously supporting different assurance offers
Intent base networking with (Artificial Intelligence) AI based issue detection and root cause analysis	Network Data Analytics Function (NDAF) defined network level data analytics
Wi-Fi 7 Multi-AP and Multi-Link capabilities targeted at increased reliability and determinism	Dual Active Protocol Stack delivering enhanced reliability

3.2 The 5G Network Architecture

By definition, a 5G Private or Enterprise network must incorporate a 5G network, i.e., a 3GPP compliant network that can grant access to 5G devices, connect them appropriately, and can perform the functions outlined in the previous section.

The 5G network comprises three main elements, as shown in Figure 3.1.

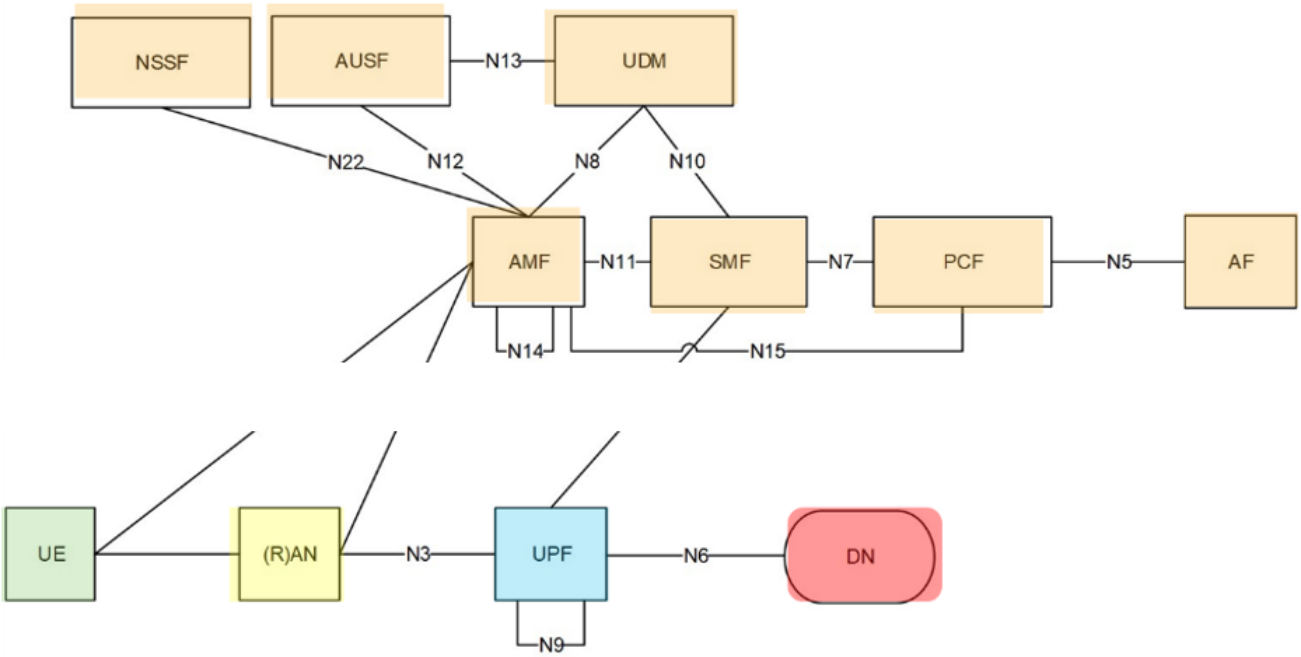
Figure 3.1 High level view of 5G Network



The 5G portion of the NPN includes:

- *Devices/user equipment (UE) that are capable of connecting to the NPN,*
- *A radio access network (RAN) over which the devices connect to the network, and*
- *A core network that performs access control, session management, and various other functions described below.*

3GPP has defined many network functions (NFs) that can be included in a 5G Core network. Figure 3.2 shows a reduced set of functions.



The UE is shown in green. The user plane is shown in blue. The core functions are shown in gold. Finally, the external network, i.e., the internet or other data network is shown in red. Brief descriptions of the NFs are shown below:

- *Access and Mobility Management Function (AMF) which provides access specific functions including access authentication and authorization along with registration, connection, reachability, and mobility management functions*
- *Authentication Server Function supports authentication for 3GPP access and untrusted non-3GPP access*
- *Data Network (DN) refers to internet or private network access along with any 3rd party services*
- *NEF supports the exposure of capabilities and events to other NFs enabling secure exposure to 3rd party application functions*
- *NEF stores/retrieves information as structured data using a standardized interface (Nudr) to the Unified Data Repository (UDR)*
- *Network Repository Function (NRF) supports service discovery and provides the discovered network function instances to the calling network function instance*
- *Network Slice Selection Function (NSSF) selects the set of Network Slice instances serving the UE*
- *Policy Control Function (PCF) supports a unified policy framework to govern network behavior; providing policy rules to Control Plane function(s) while accessing subscription information relevant for policy decisions in a Unified Data Repository (UDR)*
- *Session Management Function (SMF) provides session management including session establishment, modify and release, IP address allocation and management, selection and control of the user plane function (UPF), and charging data collection*

- *Unified Data Management (UDM) provides subscription management functions including generation of 3GPP AKA Authentication Credentials, user identification handling and access authorization based on subscription data*
- *UPF provides user packet routing and forwarding as well as packet inspection, downlink buffering, gating, redirection, traffic steering, legal intercept and QoS marking*
- *Application Function which may interact with the 5GC for application services that may include influences on traffic routing, accessing the NEF and interacting with the Policy framework for policy control*
- *UE*
- *(Radio) Access Network ((R)AN)*

In addition to the UE, RAN and 5G Core, a network deployment also needs to provide entities that manage the network, onboard subscribers, manage SIMs, define and propagate policy to the network, define network slices (if used), etc. There is a management layer above the 5G Core consisting of OSS and BSS that perform these management functions. 3GPP does not define standards for these systems; however, the interfaces by which the interact with the 5G Core are defined in the architecture above.

3.3 Traditional (non-3GPP) Enterprise Network Architecture

A typical Enterprise network is shown schematically in Figure 3.3

The access layer consists of Wi-Fi access points and access switches, controlled by a Wireless LAN controller located in the core. The core also contains the transport switching fabric and interfaces to (potentially) a Wide Area Network and the Internet.

The Wireless LAN controller serves essentially the same purposes as the AMF and the SMF in the 5G network, i.e., access and session management.

The intelligence of the network resides in the Enterprise Domain Controller in the data center, in the server farm. The Enterprise Domain Controller is responsible for:

- *DNS (which, as was explained in section 3.1, also performs policy definition and propagation)*
- *Authentication, Authorization and Accounting (AAA)*
- *Identity management, including multiple identities and context-dependent identities and profiles, as described in section 3.1*
- *Location management*
- *Service assurance and performance monitoring*
- *Onboarding, device and user management, provisioning, lifecycle management, etc.*
- *Access selection and multi-path policy and proxy(ies)*
- *Content and application servers*

In addition to these functions, the server farm in the data center also contains the administration and management systems analogous to the OSSs and BSSs in the 5G network that permit the network operator to interface with the Enterprise Domain Controller to manage the network.

In the case of both 3GPP/5G and Enterprise/Wi-Fi networks, the various parts of the network can be distributed, and can be implemented as cloud-based services by the enterprise IT organization, by an MNO partner, or by a third party cloud provider.

3.4 Enterprise and Private Network Models

There are three fundamental models for the enterprise NPN:

- *5G integrated into enterprise Wi-Fi network, managed by the enterprise using enterprise IT methods*
- *Enterprise Wi-Fi network integrated into a 3GPP 5G framework and managed as an extension of the 3GPP network*
- *Enterprise Wi-Fi and 5G networks operated and managed separately*

In all these models, the various parts of the network can be distributed, and can be implemented as cloud-based services by the enterprise IT organization, by an MNO partner or by a third party cloud provider. An enterprise NPN may not be constrained to fit into just one of the models listed above but may combine elements of two or more.

3.4.1 5G Integrated into Enterprise Wi-Fi Network, and Managed by the Enterprise Using Enterprise IT Methods

Figure 3.4 Shows a schematic view of a 5G network integrated into an enterprise/Wi-Fi network, and managed by the enterprise.

This model requires a set of translation functions that permit the enterprise management interfaces to speak to the control plane of the 5G Core. Some capabilities that are typical for enterprise IT may not be natively supported by the 5G Core in the same way that they are supported in the enterprise/Wi-Fi network (see section 3.1). However, by bringing all the control up to the enterprise data center server farm, the 3GPP/5G portion of the network can be managed as a transport leg. The following are some key points:

Fig. 3.3 Enterprise Network Schematic

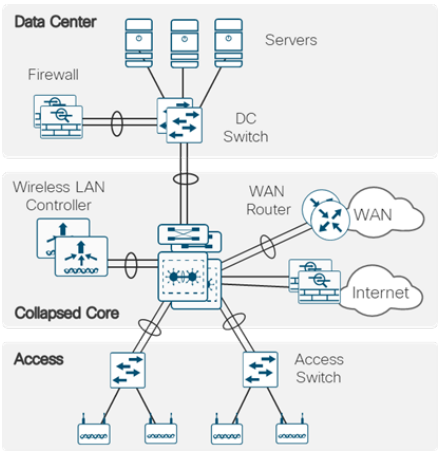
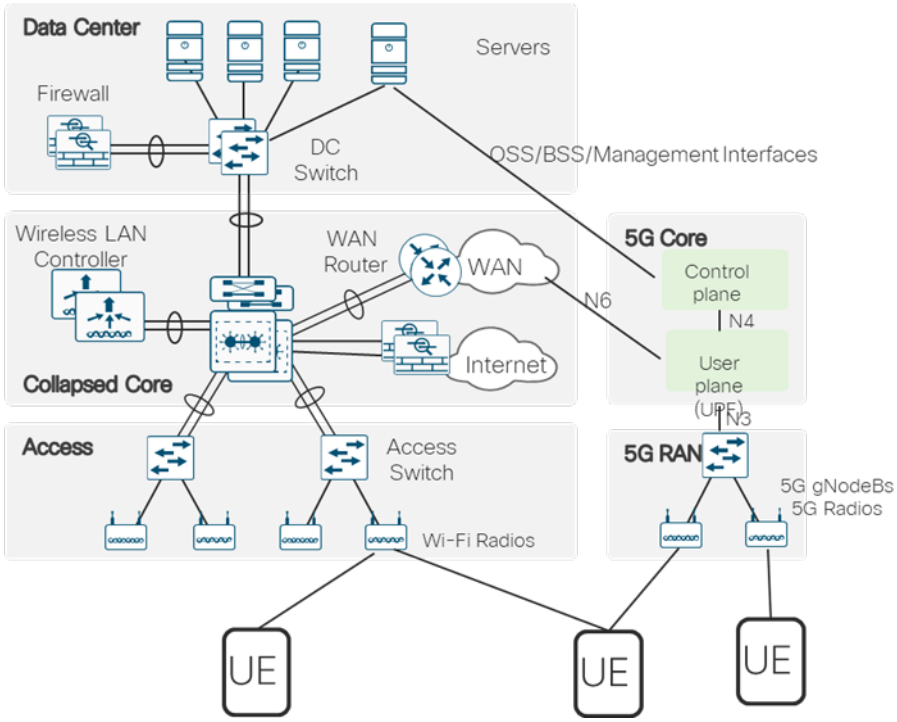


Fig. 3.4: Hybrid NPN with 5G Core and RAN integrated into the Enterprise/Wi-Fi network and managed by the enterprise



- *Minimal change to enterprise operating procedures/methods*
- *Enterprise has full control over identity (including multi and context-dependent identity), onboarding, authorization, etc.*
- *Because the 3GPP/5G user plane interfaces to the enterprise network via the N6 interface and has no other connection to the internet or the outside world, enterprise has full control over policy and segmentation*
- *Authentication is performed by the enterprise AAA using mechanisms defined in 3GPP Release 16*
- *Enterprise has full control over access selection and multi-path*

Issues:

- *Spectrum: Unless using CBRS GAA or unlicensed spectrum for the 3GPP/5G access, this model still requires coordination with an MNO partner*
- *PLMN ID management: Mechanisms for addressing this have been developed by the CBRS alliance for CBRS deployments. In unlicensed spectrum, 3GPP has addressed PLMN ID management in Release 16, whereby the NPN uses country code 999 and self-asserted MNC.*

3.4.2 Enterprise Wi-Fi Network Integrated into a 3GPP/5G Framework and Managed As an Extension of the 3GPP Network

The UE must first acquire the Enterprise/Wi-Fi Network by authenticating with it in the usual way. Once a connection to the Wi-Fi network has been established, the UE tunnels through the Wi-Fi network to create a connection to the Non-3GPP Interworking Function (N3IWF), which upon authentication with the 3GPP/5G network, establishes N2 interfaces to the AMF. At that point, the Wi-Fi (or other non-3GPP) UE appears to the network as a Wi-Fi UE.

This functionality was limited in Release 15 but was expanded in Release 16 to be much more flexible. Release 16 introduced the Access Traffic Steering, Switch and Split (ATSSS), shown in Figure 3.6.

Fig. 3.5: Integration of non-3GPP access into a 3GPP/5G network.
Source: 3GPP TR.501 (Release 15)

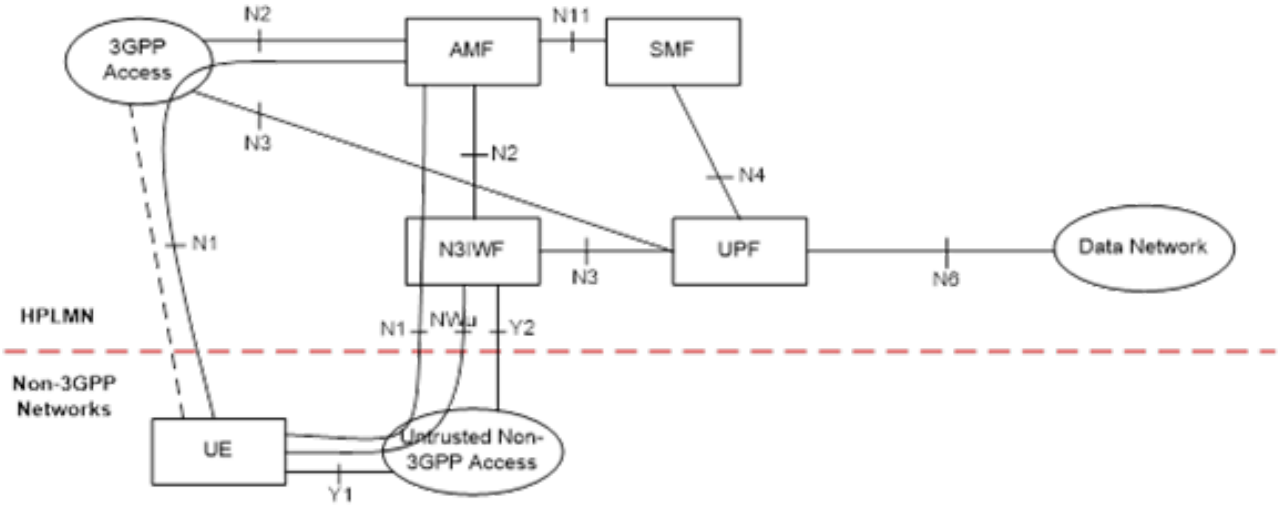


Fig. 3.6: 3GPP Release 16 Access Traffic Steering,Switch and Split (ATSSS) [2]

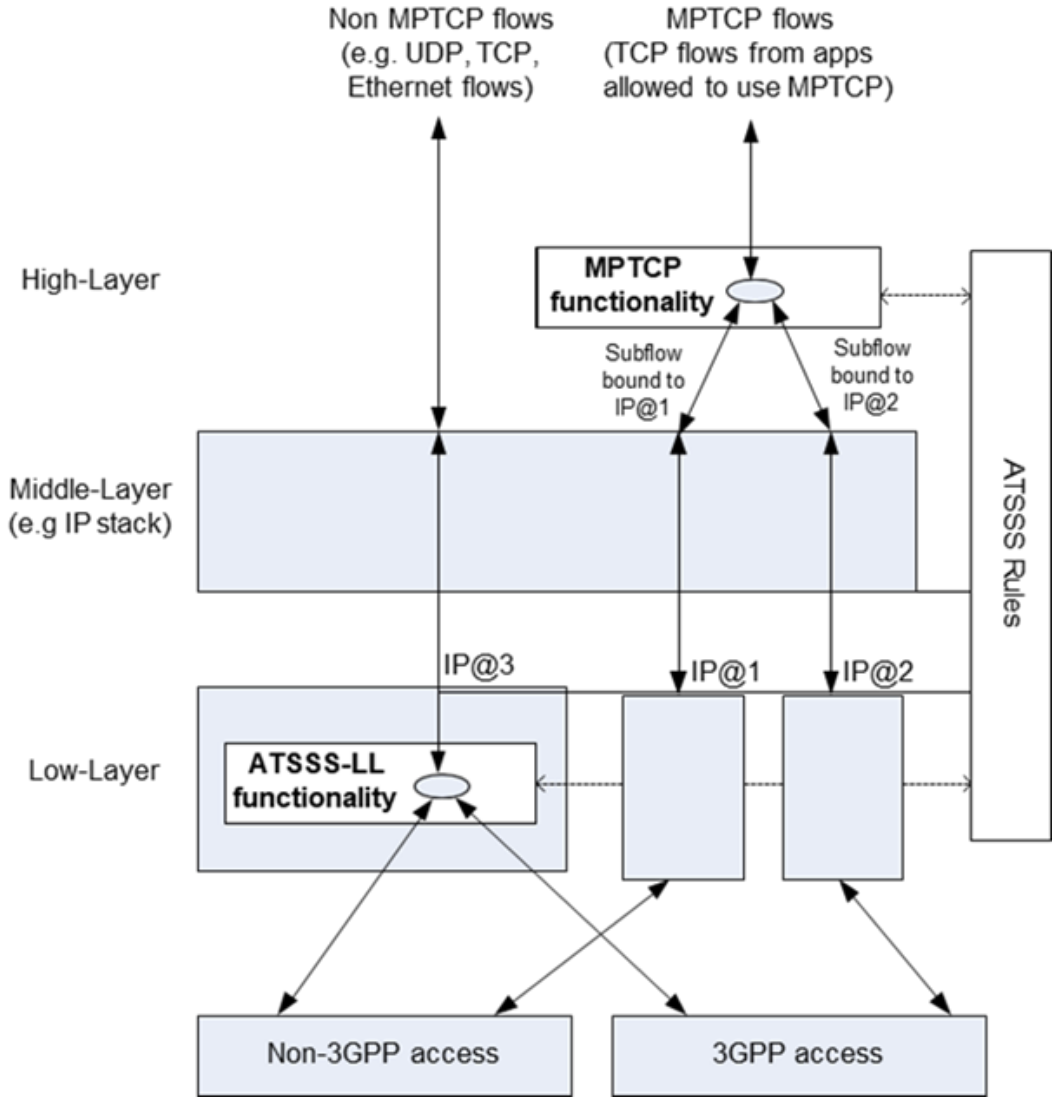


Figure 3.6 shows a possible architecture for integration of an Enterprise/Wi-Fi access network into a 3GPP/5G framework. The enterprise data center's functions are reduced in this model, but it is still necessary for a device to acquire the Wi-Fi network prior to establishing the interfaces required to access the 3GPP/5G network. Once acquired, in this figure, the only path to the internet is via the 3GPP/5G Core.

This is an extreme view. In practice, it is likely that enterprise native ethernet traffic and possibly some Wi-Fi traffic would be permitted to access the internet and/or internal enterprise applications directly, as shown in Figure 3.4

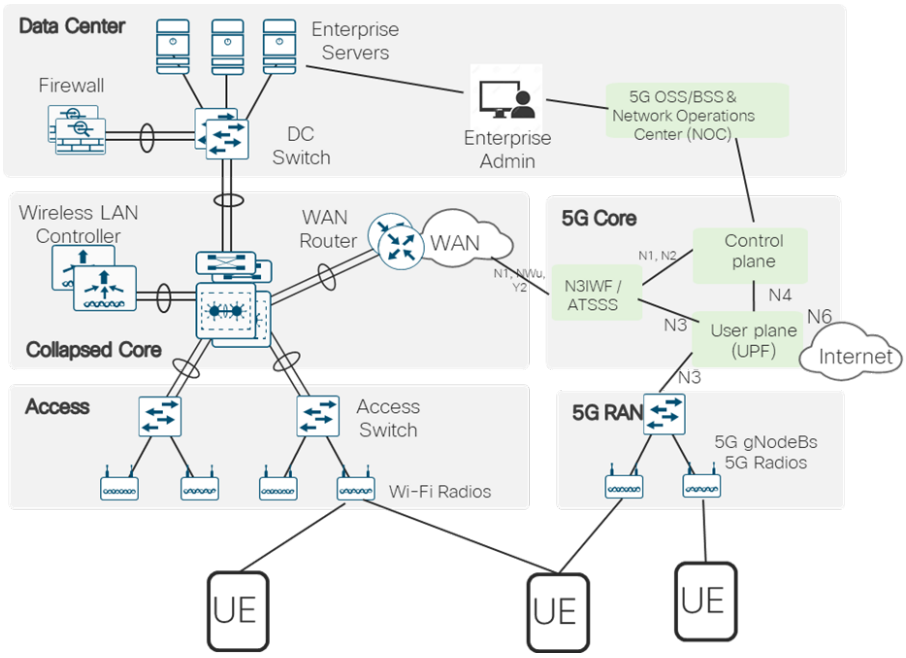
The following are some key features:

- *This model lends itself well to a partnership between the enterprise and an MNO or third party. For example, the 3GPP/5G Core as well as the management layer may be hosted by an MNO or third party and provided as a service to the NPN operator. If the 5G portion of the network operates in licensed spectrum, the NPN operator and the MNO spectrum-owner may agree to implement a spectrum sharing arrangement such as MOCN or MORAN, whereby the MNO gains the benefit of extending its coverage. The MNO or 3rd part might also take on functions such as SIM management, provisioning, onboarding, etc.*
- *Initial authentication for the purpose of network acquisition (on Wi-Fi) is done via AAA. After network acquisition, 3GPP methods are used. Just as in the network of the previous section, the features in 3GPP Releases 15 and 16 permitting authentication via non-3GPP methods could also be used.*

Issues to consider:

- *This model does not provide the enterprise IT organization the same level of control over identity management, policy, segmentation and the other characteristics of an Enterprise/Wi-Fi network described in section 3.1.*
- *While 3GPP Release 16 greatly enhanced the access selection and multi-path capabilities of the 3GPP network relative to Release 15, they are still not as flexible or application aware as an option whereby the multi-path proxy and control is performed by the enterprise in direct cooperation with the enterprise applications.*

Fig. 3.7: Enterprise/Wi-Fi network integrated into a 3GPP/5G framework



3.4.3 Enterprise Wi-Fi and 5G Networks Operated and Managed Separately

In some cases, it might be desirable to not integrate the existing enterprise network with the 5G network at all, but instead to operate the two networks side by side, as non-interacting networks. Figure 3.8 shows an example of extreme segregation of the two networks.

Some examples of use cases in which this could be desirable are:

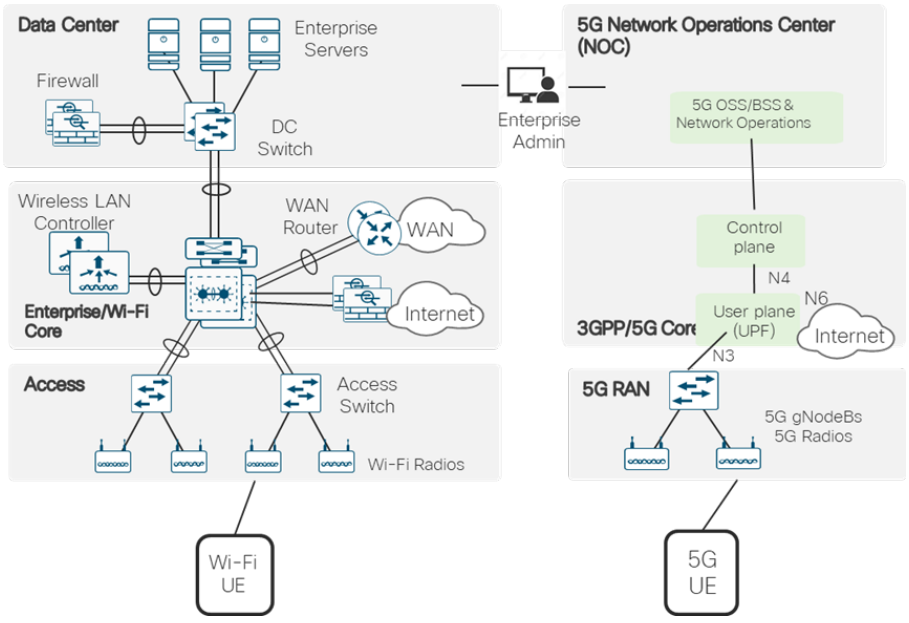
- *The two networks can be segregated by function and serve distinct sets of identities and/or devices. For example, in an industrial automation deployment, it might be desirable to use the 5G network strictly for mission critical machine control and monitoring, with dedicated devices that connect only to the 5G network.*
- *The 5G network is deployed in a spectrum sharing arrangement such as MOCN or MORAN, providing coverage extension to an MNO partner, or even to provide neutral host services for 5G devices and users. 5G Neutral Host options are explored in depth in "Neutral Host Solutions for 5G Multi-Operator Deployments in Managed Spaces" [3].*

3.4.4 Distributed/Cloud Enterprise 5G Deployment

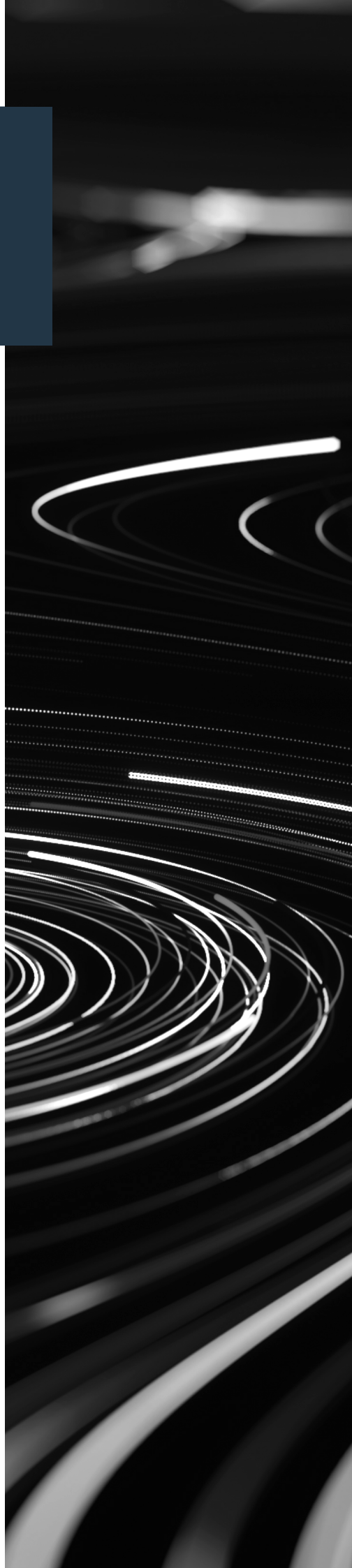
Particularly when partnering with a MNO or third party, the enterprise may want to deploy the 5G NPN in a distributed fashion, potentially taking advantage of cloud implementations of the core, the management layer, and even the RAN. Figure 3.9 shows a distributed cloud implementation of the enterprise 5G NPN, where the RAN, the dedicated enterprise UPF and critical core functions such as enterprise DNS, session management (SMF), access and mobility management (AMF) are located on the enterprise premises. The local core also has access to the enterprise servers, including those supporting Mobile Edge Compute (MEC) functions.

This architecture is ideally suited to high availability, low-latency, mission critical applications such as industrial automation. There are many possible variations of this general idea, each suited to a particular enterprise NPN application.

Figure 3.8: Enterprise/Wi-Fi and 3GPP/5G deployed as non-interacting networks



4. Reference Designs and Solutions Accelerating Adoption of Private Enterprise Network Deployment



Open, Common Models for Efficient, Mass-Market and Scalable 5G Infrastructure

The public sector (e.g., US Federal Government), commercial IT enterprises, private network operators, industrial automation sector (Operational Technology) and other enterprises may require assistance in baselining their 5G plans on common MNO and vendor models. Without a baseline, these entities will have to piece together on their own what a 5G network comprises, potentially causing confusion, fragmentation, and divergence from other 5G network deployments. Several open industry initiatives are developing these common models to baseline these 5G network architectures and implementations for efficient, mass-market, and scalable infrastructure.

Open 5G Standards

The 3GPP sets specifications for 5G services, scalable architectures, and protocols spanning mobile devices, radio access networks, core networks, and edge networks [4]. Most 5G MNO and vendor models strive to follow 3GPP specifications to maintain a consistent set of services and features for mobile communications worldwide.

Open 5G Cloud Models

5G mobile networks need a cloud infrastructure to operate their 5G network functions s. The Linux Foundation Anuket Project brings together reference cloud infrastructure models and architectures with conformance programs and tools to deliver mobile network services faster, more reliably, and securely [5]. Anuket works with the GSMA to develop a reference model for cloud infrastructures comprising workload requirements (e.g., 5G core network functions), infrastructure capabilities (e.g., compute power), infrastructure operations, and lifecycle management, to name just a few aspects of the reference model [6]. Anuket bases its references architectures and implementations on OpenStack for virtualized network functions (VNFs) and Kubernetes for containerized network functions (CNFs) [7].

Open 5G Cloud Infrastructure

To accelerate adoption, industry has progressed in the deployment and management of 5G cloud infrastructure through Airship: Airship is a purpose built, high performance network cloud infrastructure that integrates about 14 different CNCF projects to automatically deploy, manage and seamlessly upgrade VNFs and CNFs [4]. Airship enables faster deployments, much greater scale, and ensures 100% consistency that the network is operating as expected and secured as needed. Airship is a certified Kubernetes distribution under the CNCF conformance program [8].

Open Source development for 5G End-to-End Networks

Realizing an open source 5G network is more than building 5G core network functions and cloud infrastructure, it is also “orchestrating, managing, and automating across the networking stack” [9]. The Linux Foundation Networking Project is bringing together 5G and open source in the form of the 5G Super Blueprint [10] to help developers to create the networking stack and end-to-end 5G networks. Components for the 5G Super Blueprint include ONAP for Enterprise Business [11] for orchestration, Magma [12] for 5G core network functions, and Anuket for infrastructure management.

Figure 4. Anuket Scope (Source: Anuket Reference Model)

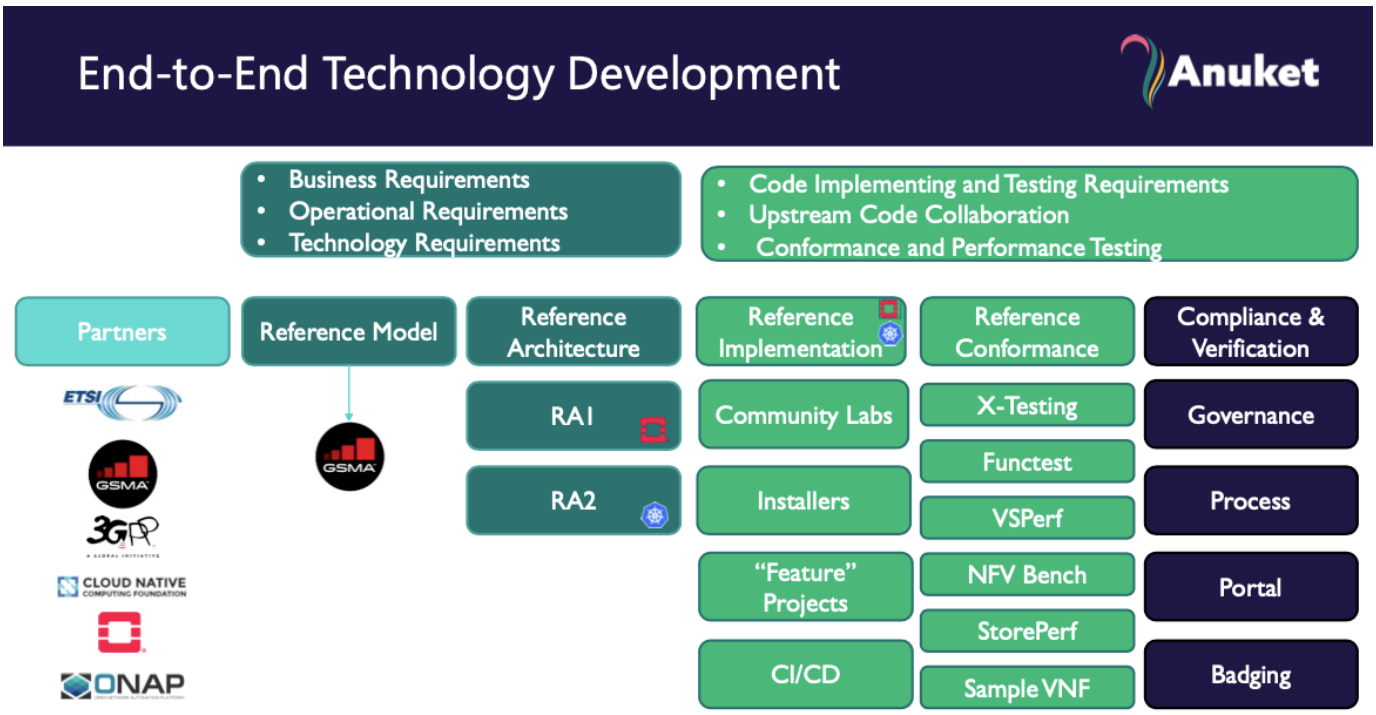
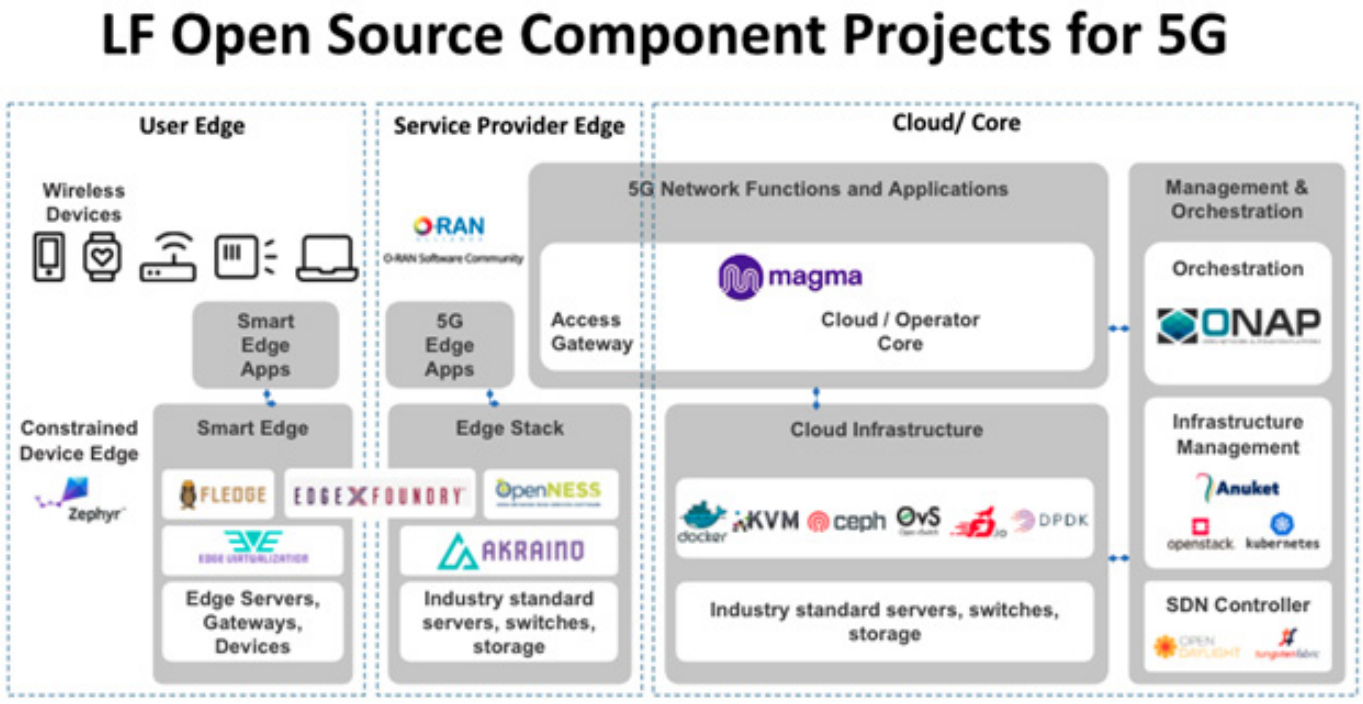


Figure 4.1. Linux Foundation Networking – 5G Super Blueprint [10]



Reference solutions (HW and SW stack) for On-Premise deployment

Carrier-class wireless connectivity using managed or licensed spectrum must be easily deployable and simply operated on an ongoing basis. Private wireless, encompassing leased, licensed and CBRS spectrum, provides the comprehensive consistency and control that mission critical applications require.

In a complex landscape of technologies and multiple vendors it is not enough to provide hardware and let customers manage deployments with the choice of software. For robust deployments that can scale and handle the complex needs while meeting time to market it is important to have a scalability of the hardware and a unified software platform that can scale along with the performance needs. The reference design should have the basic building blocks of hardware management and scale out orchestration capabilities in its core. The need for frictionless connectivity, telemetry and AI based software defined network management cannot be overemphasized.

Zero Trust Security Model

The software of any contemplated solution must ensure that remotely deployed edge compute comprehensively protects the increase in "attack surface". Leveraging asymmetric cryptography and strict mutual authentication for control interfaces is a critical requirement. In addition, policy-driven operation combined with centrally controlled permissions ensure that only legitimate traffic flows between applications and devices.

A converged solution that brings these requirements together in a cohesive manner, with security at the center of it, should be able to provide benefits of a secured operational environment with high performance compute and storage. It should be easy to deploy and use while providing faster responses and lower latencies for the demanding applications of next generation.

It is important for a reference solution to have the following features for faster TTM of a robust deployment:

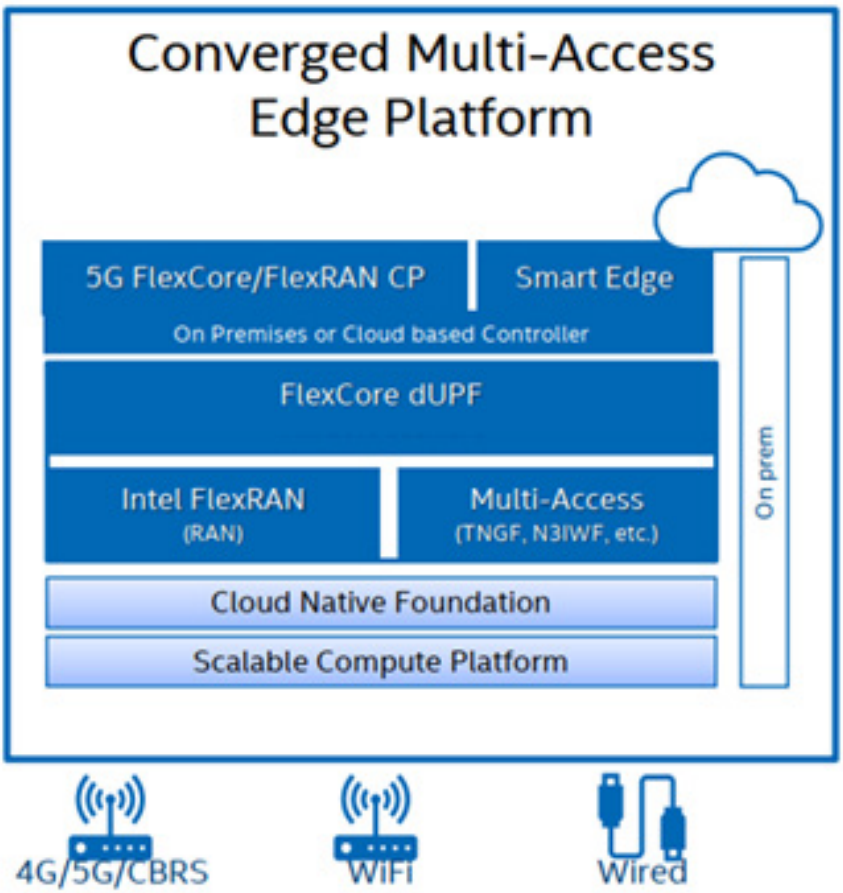
- *Cloud native RAN network proven in Telco environments*
- *Provide multi-access 5G, Wi-Fi, Time Sensitive Networking, & wired*
- *Enable improved security, unified network policy*
- *Integrated Smart Edge MEC and controller*
- *Optimized footprint for enterprise deployment*

Figure 4.2 is an example of components of a converged Multi-Access Edge platform from Intel.

Of course, other perspectives for potential reference architectures exist. Another view of a reference architecture needed to enable faster TTM is a cohesive stack all the way from hardware to the application. As in the example below, it is important to not only have the range of hardware from FPGA to general purpose compute but also important to have specialized accelerators required for various verticals the private wireless deployments are targeting. The range of compute capabilities also needs to be able to scale from low power, low-cost, low compute to high performance and high availability compute. The need for scalable architecture drives requirements for the hypervisor to be cloud native and highly performant.

Additionally, orchestration needs for on-prem deployment are not like that of a data center. In many cases customers deploying these solutions already know where the workload needs to run. The underlying devices also have much broader capabilities, unlike in a datacenter where deployment is more homogeneous. A set of VNF's or CNF's, along with middleware and toolkit to program and manage the deployment, is essential for the success of a reference stack. The significance of scalable compute and cohesive hardware and software toolkit is immeasurable when it comes to deploying complex networks.

Fig. 4.2. Converged Multi-Access Edge Platform



In another practical deployment scenario shown below, an Enterprise on-premises MEC node is controlled by a controller hosted in Public, Private or Telco edge. We can see the elements of hardware and software come together. Multiple opportunities can exist when collaborations with vendors occurs. For instance, where one entity brings its specialization of platforms and cloud deployments to provide the platform for on-premises MEC and cloud solution for hosting MEC controller, an easy fit may occur with another entity's edge controller that manages the smart edge MEC devices.

To make the solution easy to deploy and use it is important to provide additional software components like RAN and Core Network components and SDK for easy programming and deployment of application software. It is important to note the success of the solution depends a lot on the ecosystem software components, like Kubernetes, which help leverage datacenter learnings and allow reuse of software between cloud and edge. This reference architecture is integrated with hardware technologies, foundational software, and software ingredients such as OpenNESS, OpenVINO, FlexRAN, and other components from ecosystem partners. The Internet of Things (IoT) will be empowered by the potential of 5G and will demand wireless compute capabilities for smart devices at the edge.

Fig. 4.3. Hardware to Application Cohesive Stack

Open Source initiatives

The last decade has been transformational for open source. Companies have learned that embracing open source can open tremendous value and create new opportunities like never before. Open source has maximized the impact of enabling and speeding up adoption of these new technologies from cloud to edge. While hardware enhancements have been great, Open Source initiatives like Kubernetes and Open Networking Foundation, have opened the doorway to new possibilities with Industry 4.0 and smart cities.

Figure 4.5 is a summary of the Open Source initiatives around Open Networking Forum (ONF) that are working on projects that help with private enterprise RAN technologies and companies associated with them.

Fig 4.4. MEC Controllers – On-premise and Hosted

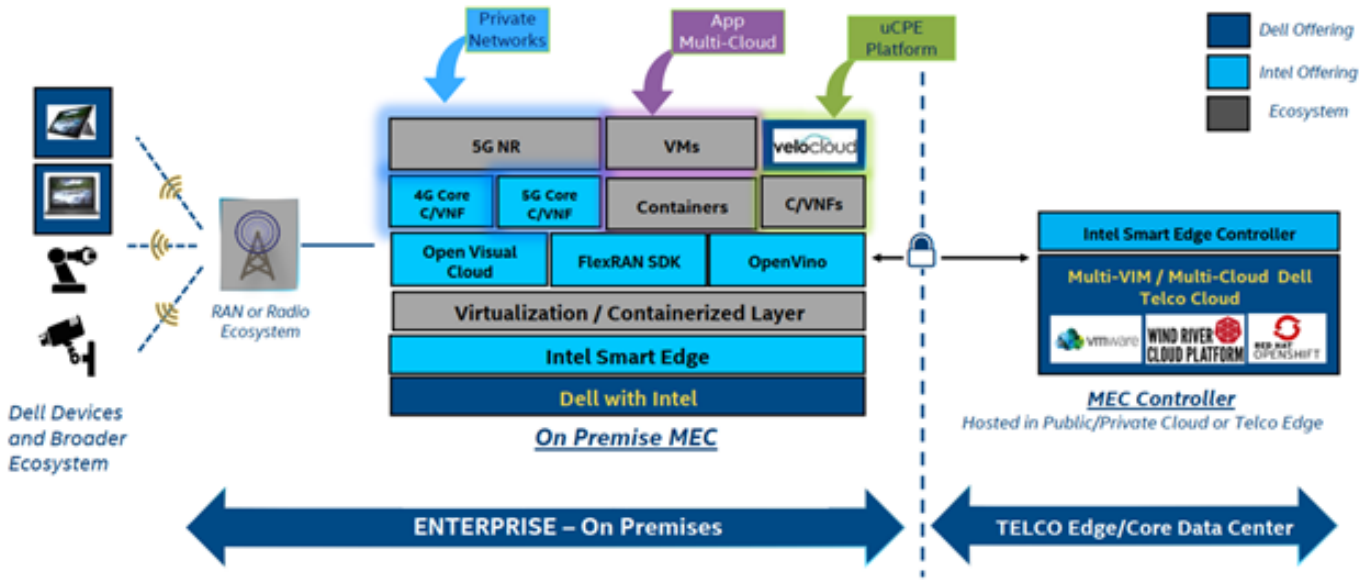
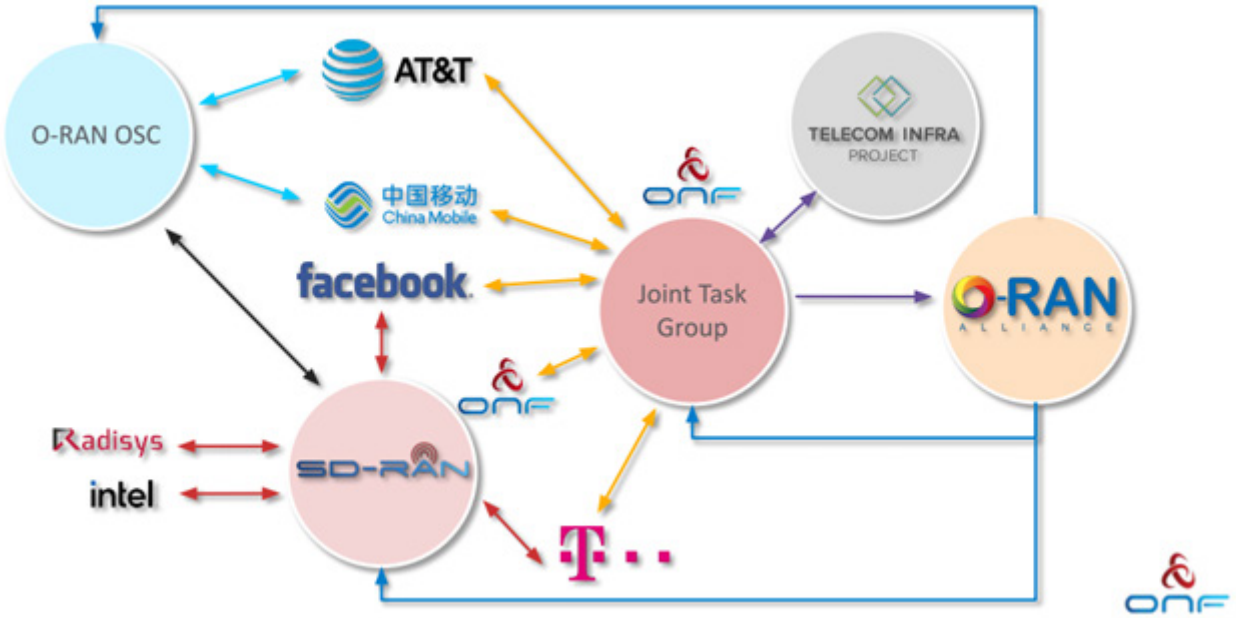


Fig 4.5. Open Source Initiatives and Private RAN Technologies

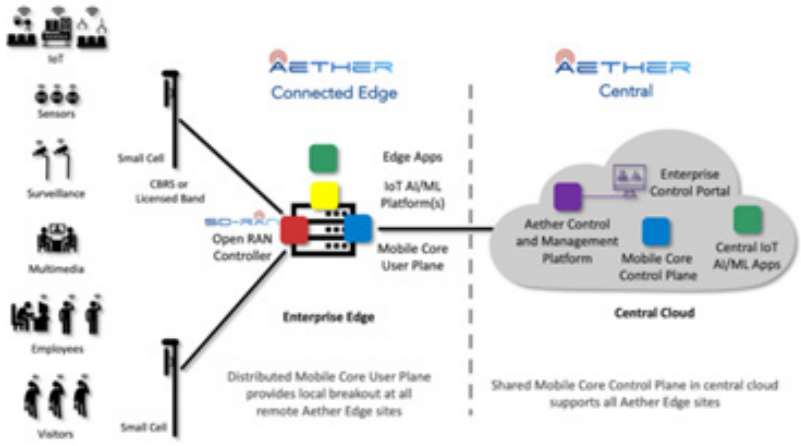


Aether

ONF's Aether is an open source enterprise software platform for leveraging private cellular connectivity and multi-access edge compute (MEC) for mission critical applications and operational use cases. Aether is a fully open source platform for private, secure, software defined enterprise LTE/5G connected cloud native edge, designed to be cost-effectively delivered as a service.

Aether uses and builds upon production-tested open source components from ONF like ONOS®, Trellis™ and CORD®, and other general purpose mainstream projects (e.g., Kubernetes, Rancher, etc.). It runs on open-specification commodity compute and networking hardware and connects with 3GPP compliant small cells for cellular access. Architecturally, it leverages state-of-the-art cloud, software defined and micro-services principles. Aether integrates with and offers onboarding and lifecycle management of commercial operational platforms for video stream analytics, IoT and AI/ML, as well as custom enterprise edge applications.

Fig 4.6. Open Source Enterprise Software Platform



Physical deployment of the distributed Aether platform

5. Geopolitical Considerations

In general, commercial sector and government have access to the same spectrum as a resource. However, government entities may have access to additional military, or other government bands, depending on the function. In the US, government-run and critical infrastructure IT departments usually comply with US Department of Homeland Security mandates, as well as departmental regulations and policies specific to their industry. These regulations and policies may affect the decisions stakeholders make to primarily, obtain spectrum, then to build the network.

In review, whether commercial or government IT departments, network designers may need to license or subscribe to obtain globally unique network identifiers (e.g., PLMNs, ECGIs, et al.) if the private network inter-operates with mobile operators. IT departments can either work with a service provider that already possess a PLMN ID, usually tied with core services, or can self-perform and obtain a shared PLMN ID such as those offered by the OnGo Alliance for the CBRS band. IT departments also should account for SIM management (i.e., IMSIs, IMEIs, APNs, etc.) and policy enforcement regardless of the source of network identifiers.

In the US, IT departments may choose to invest in bidding for spectrum with the FCC to obtain capacity for a long term. Otherwise, opportunities may arise, such as subleasing (or sublicensing) CBRS spectrum from the PAL-holder over a section of a county.

If voice, such as VoLTE or VoNR is integrated into the private wireless network, it may be required to follow e911, lawful intercept, and other emergency mode information sharing laws and regulations.

In the United States, the FCC has been making additional spectrum available for 5G services, updating regulations to speed up their processes and foster rapid innovation, and partnering with industry experts for the development and deployment of open radio access networks [13].

Some of the recent developments provided by the FCC that promote 5G-use are:

- *5G-specific spectrum in high-band has been auctioned in 28 GHz, 24 GHz, 37 GHz, 39 GHz, and 47 GHz, for a total of 5 GHz. More work is being done to free up to 2.75 GHz for 5G-use, including 26 and 42 GHz bands and others.*
- *Mid-band spectrum for 5G use, is well suited for striking a balance between coverage and capacity, and 600 MHz of spectrum is being made available in the 2.5 GHz, 3.5 GHz (CBRS), 3.7 - 4.2 GHz (C-band) bands.*
- *Low-band spectrum is also being utilized for 5G use, such as the 600 MHz, 800 MHz, and 900 MHz bands.*
- *Unlicensed spectrum is being made available to support 5G use. Though specific to Wi-Fi for now, the 5.9 GHz, 6 GHz, and 95 GHz bands will enable further integration to support 5G services (i.e., 5G NR-U). Except for one case, 5G-use in unlicensed bands is defined (by the 3GPP) for capacity augmentation, requiring an operator to have a licensed anchor band.*

As of this writing, next generation (so called “6G”) cellular bands are viewed as those above 95 GHz up to 3 THz [14]. Much of the spectrum being allocated for 6G was previously thought to be unusable; however, much research and innovation is being performed, such as high-resolution imagery and different types of sensing.

Spectrum for private cellular is critical for 5G deployment and interoperability [15], and is being harmonized on a global scale. As an example, the Dynamic Spectrum Alliance (DSA) currently promotes unlicensed access to the 6 GHz band predominantly in the Americas, for more mid-band shared spectrum, CBRS, TVWS, and innovation in the mmWaves [16]. According to a GSMA report [17], 5G needs significant new harmonized mobile spectrum as:

- *80-100 MHz of contiguous channels per operator in the mid-bands and 800 MHz in the mmWave bands; and*
- *plans for additional allocation as needed, including more in the ranges of 3.3-4.2 GHz, 6 GHz, and 40 GHz.*

Though some models in the UK and Germany have been developed for licensed spectrum sharing, sublicensing, or subleasing, for private use, more work needs to be done to develop a framework to allocate and harmonize (with licensed) spectrum for 5G private use.

Spectrum is a critical and scarce resource for 5G communications. It is a requirement for future advanced services and solutions from various entities throughout the wireless and technology ecosystem. In the shared spectrum model, once incumbents such as the military (as in the CBRS band) are protected, coexistence and interference mechanisms may be required for coordination among private and/or commercial service providers. Shared spectrum should also be reliable to service providers and to users. Internet and telecom service providers, and innovators who want their devices and services made available in global markets, stand to benefit from spectrum availability and coordination.

National organizations in the United States, such as the FCC, NTIA, CTIA, OnGo Alliance, and international organizations like the ITU, 3GPP, IEEE, ETSI, and GSMA, help to promote many of the functionality and interoperability needed for 5G development and deployment. At a national level, infrastructure requires government cooperation with the private sector. This can include the FCC, the Wireless Innovation Forum (WInnForum), NTIA, and even the Department of Defense (DoD). State and local governments can further help by streamlining permitting to bring 5G innovations more quickly to market. National, international organizations and industry can help 5G progress by developing standards and testing where it is needed for interoperability and security. The ideal outcome is for everyone to cooperate and develop a competitive and pluralistic supply chain globally.

In addition to security concerns posed by certain governments and companies, there are also recent examples of the drive to a more varied and competitive global market by overcoming challenges brought about by subsidized and predatory pricing [18]. Equipment from some equipment providers have become a particular area of focus for 5G supply chain integrity for many stakeholders [15].

For instance, in the United States, the White House, Department of Commerce, FCC, and Congress have created a new regulatory regime to review certain international transactions, which has led to the creation of the Commerce Department’s Entity List for evaluating supplier security. The FCC has cooperated by restricting Universal Service funds from going to manufacturers on the Entity List. The Department of Homeland Security (DHS) worked on a 5G security risk assessment, led by the National Risk Management Center (NRMC) in the Cybersecurity and Infrastructure Security Agency, The DoD and Defense

Innovation Board reviewed the 5G ecosystem for risks and opportunities, while National Institute for Standards and Technology (NIST) looked at supply chain risk management in its Cybersecurity Framework. Finally, several legislative proposals coordinated with the efforts of the different government agencies.

The bans may have potentially provided an opportunity for the US to strengthen cooperative policies with Japan, Australia, Korea, and the EU to use foreign assistance, co-financing, and export support. The bans brought attention to the US government to promote and develop a broad supply chain. The United States' policies have seemingly shifted to rules favoring certain western based equipment suppliers for 5G equipment potentially bringing about more opportunities for innovation.

The following non-exhaustive list identifies alliances, standards, advocacy, and government entities that cooperate in the development of 5G:

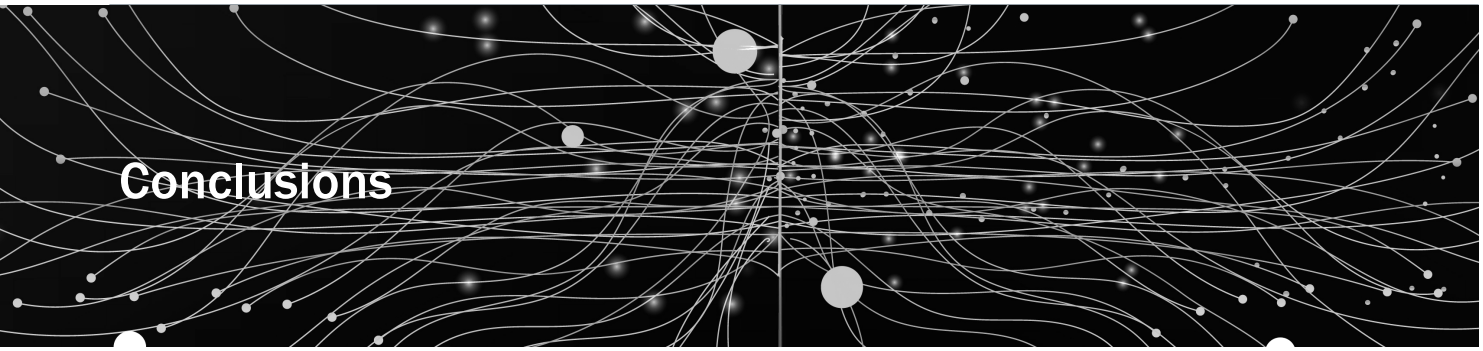
- *3GPP - The 3rd Generation Partnership Project (3GPP) unites [Seven] telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as "Organizational Partners" and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies. The project covers cellular telecommunications technologies, including radio access, core network and service capabilities, which provide a complete system description for mobile telecommunications. The 3GPP specifications also provide hooks for non-radio access to the core network, and for interworking with non-3GPP networks. [https://www.3gpp.org]*
- *5G Americas - Facilitates and advocates for the advancement and transformation of LTE, 5G and beyond throughout the Americas. [https://www.5gamericas.org]*
- *Cellular Telecommunications Industry Association (CTIA) - Represents the US wireless communications industry. From carriers and equipment manufacturers to mobile app developers and content creators, we bring together a dynamic group of companies that enable consumers to lead a 21st Century connected life. [https://www.ctia.org]*
- *Dynamic Spectrum Alliance (DSA) - promoting unlicensed access to the 6 GHz band, more mid-band shared spectrum, CBRS, TV whitespace, innovation in the mmWaves and more. [http://dynamicspectrumalliance.org]*
- *ETSI - ETSI provides members with an open, inclusive and collaborative environment. This environment supports the timely development, ratification and testing of globally applicable standards for ICT-enabled systems, applications and services. [https://www.etsi.org]*
- *Global Mobile Suppliers Association (GSA) - A not-for-profit industry organization representing companies across the worldwide mobile ecosystem who are engaged in the supply of infrastructure, semiconductors, test equipment, devices, applications and mobile support services. [https://gsacom.com]*
- *GSM Association (GSMA)- The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors*
- *Institute of Electrical and Electronic Engineers (IEEE) - A leading developer of industry standards in a broad range of technologies that drive the functionality, capabilities, and interoperability of a wide range of products and services, transforming how people live, work, and communicate. [https://www.ieee.org]*
- *International Telecommunication Union (ITU) -- A specialized United Nations agency for information and telecommunications technologies*

(ICTs). The ITU has three sectors (a) radiocommunications, (b) standards, and (c) development, who work together as study groups to establish technical standards or guidelines (Recommendations). [https://www.itu.int/en/about]

- *Internet Engineering Task Force (IETF) - The mission of the IETF is to make the internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet*
- *Linux Foundation (LF) Networking Project - Software and projects providing platforms and building blocks for Network Infrastructure and Services across Service Providers, Cloud Providers, Enterprises, Vendors, and System Integrators that enable rapid interoperability, deployment, and adoption. [https://www.lfnetworking.org]*
- *MulteFire Alliance - Supports the common interests of its members, developers, and users in the application of LTE and next-gen mobile cellular technology in configurations that use only unlicensed radio spectrum. MulteFire is expected to provide mutual value across the ecosystem – acting as a neutral host to service multiple entities – or provide dedicated broadband service at enterprises, venues, or for clusters of residences. MulteFire aims to extend the benefits of LTE to unlicensed spectrum with a simple, secure, and seamless network architecture, offering service providers of all stripes – big and small – a new connectivity option. [https://www.multefire.org]*
- *National Telecommunications and Information Administration (NTIA) - Fifth-generation wireless technologies are essential to the future prosperity and security of the United States, but malicious actors seeking to exploit these technologies pose significant risks and vulnerabilities. NTIA is engaged in a few efforts to help ensure that 5G networks and the broader telecommunications supply chain are secure. [https://www.ntia.doc.gov/category/secure-5g]*
- *O-RAN Alliance - to reshape the RAN industry towards more intelligent, open, virtualized and fully interoperable mobile networks. The new O-RAN standards will enable a more competitive and vibrant RAN supplier ecosystem with faster innovation to improve user experience. O-RAN based mobile networks will at the same time improve the efficiency or RAN deployments as well as operations by the mobile operators. [https://www.o-ran.org]*
- *OnGo Alliance – An industry forum created to champion 3GPP based RANs in shared spectrum bands. [https://ongoalliance.org]*
- *Open Edge Computing Initiative – a collective effort by multiple companies, driving the business opportunities and technologies surrounding edge computing. [https://www.openedgecomputing.org]*
- *Open Network Automation Platform (ONAP) – A comprehensive platform for orchestration, management, and automation of network and edge computing services for network operators, cloud providers, and enterprises. Real-time, policy-driven orchestration and automation of physical and virtual network functions enables rapid automation of new services and complete lifecycle management critical for 5G and next generation networks. [https://www.onap.org]*
- *Open Networking Forum (ONF)NF - A non-profit operator led consortium driving transformation of network infrastructure and carrier business models through applied research, development, advocacy, and education. [https://opennetworking.org]*
- *Open RAN – An intelligent RAN integrated on general purpose platforms with open interface between software defined functions. The ecosystem enables enormous flexibility and interoperability with a complete openness to multi-vendor deployments. The architecture is designed for building*

virtualized RAN with AI powered control, which is the key to tame the 5G complexity. [https://open-ran.org]

- *Open RAN Policy Coalition - The Open RAN Policy Coalition is a group of companies formed to promote policies that will advance the adoption of open and interoperable solutions in the RAN to create innovation, spur competition and expand the supply chain for advanced wireless technologies including 5G. [https://www.openranpolicy.org]*
- *Small Cell Forum - A global membership organization committed to supporting agile, low-cost mobile infrastructure through small cells. Our mission is to make mobile cellular connectivity an accessible resource for organizations of all sizes, and to support digital transformation of industry, enterprise and communities. [https://www.smallcellforum.org]*
- *Telecom Infra Project (TIP) - A global community of companies and organizations working together to accelerate the development and deployment of open, disaggregated, and standards-based technology solutions that deliver the high quality connectivity that the world needs – now and in the decades to come. [https://telecominfraproject.com]*
- *Wireless Innovation Forum (WInnForum) - An international group of equipment vendors, subsystem vendors, software developers, technology developers, communication service providers, research and engineering organizations, academic institutions, government users, regulators and other interested parties who share the common business interests of advancing technologies supporting the innovative utilization of spectrum and the development of wireless communications systems, including essential or critical communications systems. [https://www.wirelessinnovation.org/about_the_forum]*



Conclusions

Enterprises and verticals have become increasingly distributed geographically, and more demanding in terms of their wireless communications needs. The modern enterprise may span many cities, states/provinces, countries, coordinate multiple centers of operation, and will require dependable, predictable communications services between those centers. As the services and applications implemented by enterprises become more demanding, enterprise networks require more spectrum, more bandwidth, more fine-grained control, and more dynamic flexibility for solutions than ever before.

It is expected that the enterprise and public networks of the future will combine traditional enterprise Wi-Fi radio access along with 5G and will incorporate both 3GPP/cellular and traditional enterprise network operating and management models to satisfy the intended use. Intended uses may range from mission critical, ultra-low-latency applications like industrial automation or remote surgery or may extend indoor coverage for an MNO partner or provide neutral host services, while at the same time providing voice services, increased bandwidth, and seamless roaming to a public network for members of the enterprise.

The hybrid network must provide the necessary flexibility and control to satisfy the requirements of the enterprise/private network operator: identity management, authentication, onboarding, authorization, policy definition and enforcement, access selection and multi-path, security, determinism, etc. It must be cost-effective. In many cases, it must be integrated into an already-functioning enterprise IT operation, without sacrificing capabilities that have become necessary to the enterprise operations.

We have examined several operating models for the hybrid network, the factors that will affect critical decisions regarding the model chosen and have presented the architectures to support them. Some of the factors influencing the decision are:

- *Who are the intended users of the 5G network? Internal only? Guests? Machines? People?*
- *In what spectrum will it operate? If licensed, how will a partnership with a MNO be structured and managed?*
- *Is it self-contained or does it need to interact with external, public networks?*
- *How much control does the enterprise need to maintain over the behavior and performance of the 5G network?*
- *Is the enterprise willing to take on the additional complexity of managing a 5G network along with its existing network?*

The operating models fit into three broad categories, with a fair amount of overlap and blurring of boundaries among them:

- *The Enterprise-Supported model, in which the enterprise integrates 5G elements, but manages them using the same set of methods that are employed to manage their non-3GPP network. This model permits the enterprise to maintain full control over the behavior of the network, and to maintain the set of capabilities that they have developed to meet their needs.*
- *The Operator-Supported model, in which part or all the management and operation of the hybrid network is outsourced to an MNO or third party partner. In this model, both 3GPP and non-3GPP access may be managed using principles developed for cellular networks by 3GPP.*
- *The Non-Interacting model, where 3GPP and non-3GPP networks are operated with minimal interaction between them. The 5G portion of the network may be fully or partially operated and managed by an MNO or third party partner.*

No single network model is expected to meet the needs of all enterprise and private networks. The paper has described the operating models and architectures to support three categories of networks and outlined the factors that might drive the decision regarding which model to adopt, as well as describing a set of tools and building blocks that can facilitate implementing and running a non-public network. The technology to support building customized networks from common building blocks is advancing rapidly, as are alternative models for managing and operating them. The network of the future will be a multi-network, taking advantage of both cellular and non-3GPP technologies to deliver an experience that is access agnostic and tailored to the specific intended use.

Acronyms

3GPP: 3rd Generation Partnership Project

3GPP AKA: 3GPP Authentication Credentials

5G-CN: 5G Core Network

5GNR: 5th Generation New Radio

A1: O-RAN interface

AAS: Advanced Antenna Systems

AI: Artificial Intelligence

AMF: Access and Mobility Management Function

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

BSS: Business Service Systems

CAM: Cooperative Awareness Messages

CAPEX: Capital Expenditure

CBRS: Citizens Band Radio Service

CCO: Coverage and Capacity Optimization

CCSA: China Communications Standards Association

CN: Core Network

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

DN: Data Network

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

ECGI: European Corporate Governance Institute

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

FCC: Federal Communications Commission

FD.IO: Fast Data - Input/Ouput project

feLAA: Further enhanced License Assisted Access

FPGA: Field-programmable Gate Array

FRAND: Fair, reasonable and non-discriminatory licensing

GAA: General Authorized Access

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

ISED: Innovation Science and Economic Development

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

LAA: License Assisted Access

LAN: Local Area Network

Layer 1: see PHY

LBT: Listen-before-talk

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)

MAC: Media Access Layer

MANO: Management and Orchestration

MCPTT: Mission critical push-to-talk

MDU: Multiple Dwelling Units

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

MOCN: Multi-Operator Core Network

MORAN: Multi-Operator Radio Access Network

M-Plane: Open Fronthaul Management Plane

MRO: Mobility Robustness Optimization

multiRAT: multiple RATs

NaaS: Network as a Service

NDAF: Network Data Analytics Function

near-RT: near Real-Time

near-RT RIC: near Real-Time RIC

NEBS: Network Equipment Building System

NEF: Network Exposure Function

NETCONF: Network Configuration Protocol

NF: Network Function

nFAPI: networked FAPI

NFV: Network Function Virtualization

NFVI: NFV Infrastructure

NIC: Network Interface Card

NMS: Network Management System

NOC: Network Operations Center

NPN: Non-Public Network

non-RT RIC: non-Real-Time RIC

NR: 5G New Radio, i.e., 5G radio access technology

NRMC: National Risk Management Center

nRT: near Real-Time

nRT RIC: near real-time RIC

NRT RIC: non-real-time RIC

NR-U: New Radio Unlicensed

NSA: Non-Stand Alone

NSSF: Network Slice Selection Function

NUDR: Network Unified Data Repository

O&M: See OAM

O1: O-RAN interface

O2: O-RAN interface

OAI: Open Air Interface

OAM: Operations, Administration and Maintenance

OEM: Original Equipment Manufacturer

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

ONF: Open Networking Forum

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

OSS: Operations Support Systems

OTIC: O-RAN Testing and Integration Centers

OTT: Over the top

PAL: Priority Access Licenses

PCF: Policy Control Function

PCI: Physical Cell Identity

PDCP: Packet Data Convergence Protocol (3GPP NR protocol stack)

PHY: Physical Layer (3GPP NR protocol stack)

PLMN: Public Land Mobile Network

PLMN ID: Public Land Mobile Network Identification

PNF: Physical Network Function(s)

POC: Proof of Concept

PON: Passive Optical Network

PPF: Packet Processing Function

PTT: Push-to-talk

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

SAS: Spectrum Access System

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

SMF: Session Management Function

SOC: Security Operations Center

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

TTM: Time Transfer Modem

Tx: Transmit

UAV: Unmanned Aerial Vehicle

uCPE: Universal Customer Premise Equipment

UDM: User Data Management

UDR: Unified Data Repository

UE: User Equipment

UL: Uplink

UP: User Plane

UPF: User Plane Function

URLLC: Ultra-Reliable Low-Latency Communication

V2X: Communication between vehicles and other devices, Vehicle to Anything

vCU-CP: Virtualized 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 LTE

VoNR: Voice Over NR (New Radio)

VPN: Virtual Private Network

VPP: Vector Packet Procession (see FD.IO)

vRAN: Virtualized RAN

WBS: Wireless Broadband Service

WInnForum: Wireless innovation Forum

WLAN: Wireless Local Area Network

References

[1] "IEEE 802.11-19/12983r0," [Online]. Available: https://mentor.ieee.org/802.11/dcn/19/11-19-1283-00-AANI-802-11ax-for-imt-2020-embb-dense-urban-test-environment.pptx.

[2] "3GPP TR23.501," [Online].

[3] "Neutral Host Solutions for 5G Multi-Operator Deployments in Managed Spaces," Alliance for Telecommunications Solutions (ATIS), 2019.

[4] [Online]. Available: https://www.3gpp.org/.

[5] [Online]. Available: https://anuket.io/.

[6] [Online]. Available: https://www.gsma.com/newsroom/resources/ng-126-cloud-infrastructure-reference-model-v1-0/.

[7] [Online]. Available: https://cntt.readthedocs.io/en/stable-elbrus/ref_arch/README.html.

[8] [Online]. Available: https://www.cncf.io/certification/software-conformance/.

[9] [Online]. Available: https://www.onap.org/software#:~:text=An%20ONAP%20 enterprise%20task%20force%20has%20been%20established,orchestrate%2C%20manage%2C%20and%20automate%20across%20the%20networking%20stack.

[10] [Online]. Available: https://www.lfnetworking.org/5g-super-blueprint/.

[11] [Online]. Available: https://wiki.onap.org/display/DW/TSC+Task+Force%3A+ONAP+for+Enterprise+Business.

[12] [Online]. Available: https://www.magmacore.org/.

[13] [Online]. Available: https://www.fcc.gov/5G.

[14] [Online]. Available: https://www.miwv.com/what-is-6g.

[15] [Online]. Available: https://www.wiley.law/media/handbook/550_2021-Wiley-5G-Roadmap.pdf.

[16] [Online]. Available: http://dynamicspectrumalliance.org.

[17] [Online]. Available: https://www.gsma.com/spectrum/wp-content/uploads/2021/04/5G-Spectrum-Positions.pdf.

[18] [Online]. Available: https://www.commerce.senate.gov/services/files/563D903B-FEF0-4A1C-9202-A7DC1CCEFC6F.

Acknowledgments

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

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

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