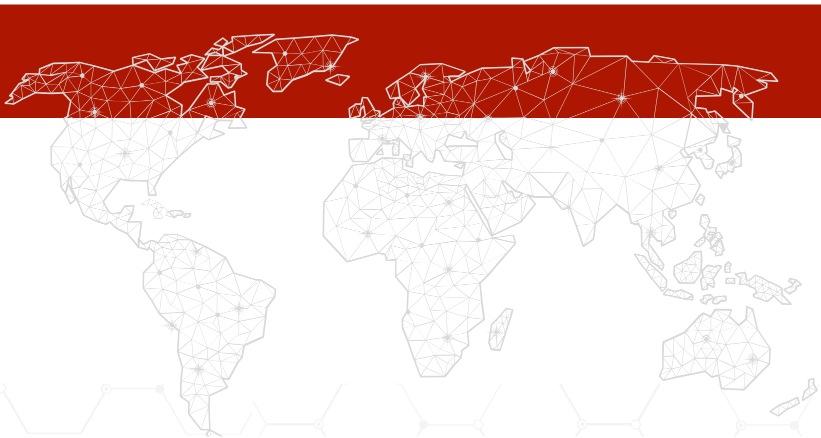
PRIVATE 5G

A NETWORK ARCHITECTURE FOR THE ENTERPRISE



ABSTRACT

This white paper aims to provide insights into private 5G networks, discussing their suitability for the enterprise market, detailing applicable architectural and operational approaches for building such networks. The white paper delves into the technical foundations of Private 5G and explores various deployment models. The aim is also to equip enterprises with the knowledge and strategies needed to harness the transformative power of Private 5G, paving the way for innovation and efficiency in their respective domains.

INTRODUCTION

Enterprises across diverse sectors, including energy, transportation, public services, and manufacturing, are increasingly recognizing the transformative potential of Private 5G networks. This cutting-edge technology represents a monumental leap forward in network capabilities, offering ultra-low latency, very high-capacity bandwidth, and robust support for massive machine communications. Industries like manufacturing, ports, mining, utility, and airports are eager to use private 5G networks to enhance their performance and reduce operating expenses.

Private 5G networks are localized networks that offer the advantages of 5G, including faster response times, higher data speeds, and operational efficiency. They can be customized to meet the specific connectivity needs of enterprises and similar organizations. They offer the advantage of a well-established ecosystem of technology suppliers, system integrators, and service providers compared to proprietary solutions. As new spectrum becomes available for 5G, enterprises and organizations can leverage private network deployments for various connectivity needs, whether general, business-critical, or mission-critical.

5G technology covers a dynamic landscape of innovation and possibilities. This paper explores the mechanics of a Service-Based Architecture, which revolutionizes the way networks are structured and services are delivered. It delves into the spectrum options available for 5G, highlighting their role in enabling faster and more reliable wireless communication. It discusses the impact of microservices and cloud-native technology, shedding light on how they enhance the agility and efficiency of 5G deployments. It will uncover the benefits of an open architecture that exposes APIs, opening new horizons for integration towards AI, automation, and evolving use cases.

The paper also addresses concepts of separation of the control and user plane, offering flexibility and scalability like never before. It also details how Quality of Service (QoS) in 5G ensures that diverse applications receive the performance they require. It explores the capabilities of the 5G NG-RAN, which enables ultra-low latency and impressive bandwidth. It examines Network slicing, revealing how it tailors network resources to meet the unique demands of various applications. Lastly, it outlines the security measures embedded in 5G, safeguarding data and communications in this era of hyper-connectivity.

UNDERSTANDING THE EXISTING ENTERPRISE LANDSCAPE

Enterprises require strong, dependable, secure, and compatible connectivity to meet their expanding demands.

Wi-Fi remains a prevalent connectivity solution, with ongoing improvements in IEEE 802.11 protocols to enhance performance. In the early stages, it is expected that both Wi-Fi and private 5G networks will coexist and complement each other.

Enterprise requirements primarily revolve around improving coverage, control, performance, reliability, flexibility, and low latency. In very large sites such as mines, factories, industrial sites, ports, airports, harbors, and resorts, there is a need for high area coverage to reach devices such as sensors, video surveillance cameras, and mobiles. There is also a great need to support devices used for mission-critical applications that require seamless mobility with ultra-reliability and low latency. Control and monitoring systems that rely on AR (Augmented Reality) and VR (Virtual Reality) require a high degree of mobility, reliability, security, and predictability.

Various industries are increasingly relying on automated devices like inventory robots and automated vehicles for tasks like inventory management and asset tracking. These devices require efficient data transmission for both sending and receiving data. To meet the demands of ultra-low latency and high reliability, which are essential for tasks like automated manufacturing and government services, 5G-based private networks are becoming crucial.

TECHNOLOGY

A standalone private 5G network is a network that provides access and connectivity to its private users and operates independently of a service provider. 5G offers the performance, reliability, and operational efficiency that is required for support of basic and advanced Enterprise use cases. As shown in the figure below, the key elements of the standalone Private 5G architecture are the gNB, which manages the radio resources; the AMF for access mobility functions; the SMF for session mobility functions; the UDM for user data management; the AUSF for authentication of subscribers, the UDR for user data storage, the PCF for policy control and the UPF for handling all user plane functionality (forwarding of data, voice and video).

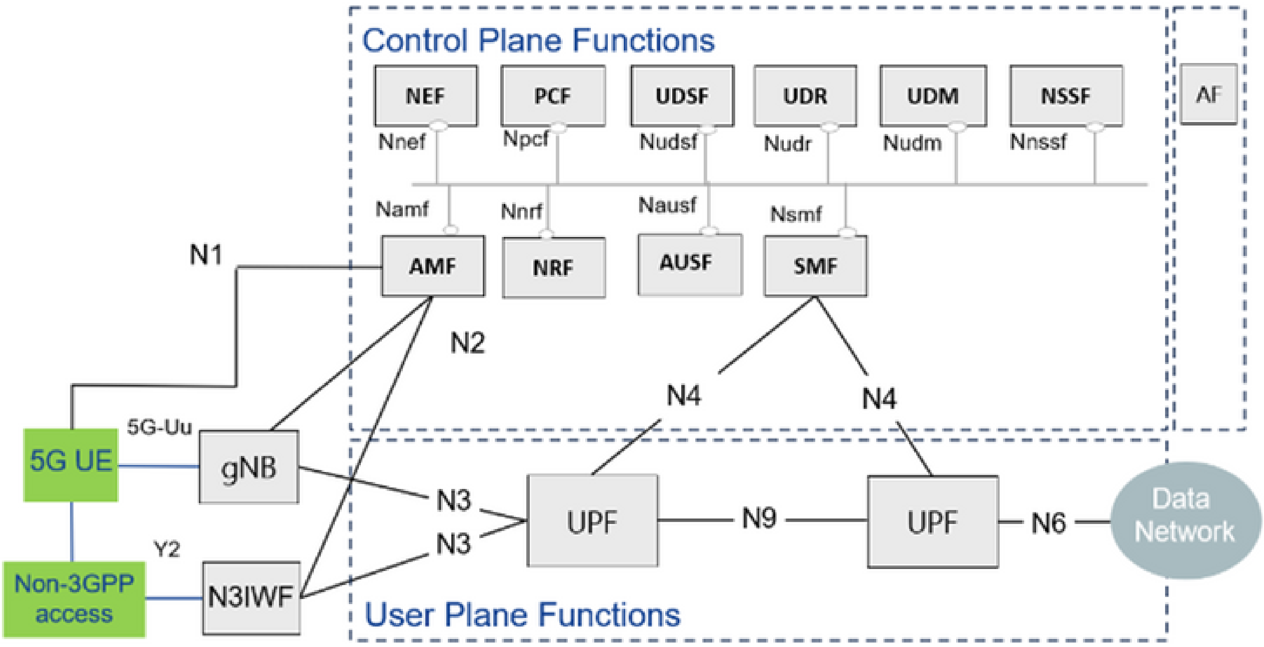


Figure 4.1 – Standalone 5G Private Architecture

The following table identifies the name of each of the network functions that are part of a typical private 5G network:

5G Function Acronym	Description
gNB	g Node B
UPF	User Plane Function
AMF	Access and Mobility Management Function
SMF	Session Management Function
NSSF	Network Slice Selection Function
NEF	Network Exposure Function
UDM	Unified Data Management
AUSF	Authentication Data Function
UDR	User Data Repository
PCF	Policy Control Function
UDSF	Unstructured Data Storage Function
NRF	Network Resource Function
N3IWF	Non 3GPP Interworking Function
AF	Application Function

Table 4.2 – Private 5G Network Functions

Service Based Architecture (SBA)

A private 5G system implements a Service Based Architecture, which offers a systematic approach to providing and receiving services. As shown in Figure 4.3 below, the architecture has a function called NRF (Network Repository Function), which coordinates the introduction and delivery of all services in the network. A core network function that has a service to offer takes the role of the service producer, and a network function that requires its services takes the role of a service producer. All service producers communicate with the NRF via REST APIs to advertise its services, and a service consumer goes through a process to discover the services available to attain the information required to communicate directly for the service. With this approach, a network function can be commissioned or decommissioned from the network without service interruptions. It is also possible to have services distributed among several network functions of the same type based on location, capabilities, redundancy, or load distribution purposes.

Figure 4.3 – SBA Operations

In the example above, a PCF is introduced into the network and goes through a service registration process to register its services and capabilities. It does so by using the HTTP PUT message to advertise its information to the NRF, and this one, in turn, sends back an ACK to confirm receipt. Now, PCF can provide its services to authorized consumers. Let's say an AMF needs the services of a PCF. It uses the service discovery process to query from the NRF available PCF services. It uses the HTTP GET message to query for a set of specific services to the NRF, which then gets back a response with the PCF information based on the requested capabilities. The AMF is now ready to consume the services of the PCF and sends a service REQUEST to the PCF using the HTTP POST message.

Spectrum in 5G

5G technology introduces support for three main frequency bands: low band, mid-band, and high band. As shown in the figure below, the low-frequency band runs below 3 GHz and includes frequencies previously used by 4G LTE networks. These frequencies provide excellent coverage and penetration through buildings and other obstacles. They offer wide-area coverage and have the potential to cover vast geographic areas with fewer base stations. They provide relatively slower data rates compared to mid and high-band frequencies, although still faster than 4G LTE.

They are ideal for providing wide-area coverage, especially in rural areas or suburban regions. They are suitable for applications that prioritize coverage and connectivity over extremely high data speeds, such as IoT devices, smart meters, and rural broadband access.

The mid-frequency band runs between 3 GHz and 6 GHz. They strike a balance between coverage and capacity, offering a compromise between coverage area and data speeds, a balance between coverage and capacity, making them suitable for urban and suburban areas, providing enhanced mobile broadband, and supporting applications such as video streaming, gaming, and consumer mobile services.

The high-frequency band, also known as mmWave, runs above 24 GHz. High-band frequencies offer extremely high data speeds and low latency. However, they have limited coverage and are easily attenuated by obstacles like buildings and vegetation. They require a dense network of base stations to ensure coverage, but they provide the highest capacity and fastest data rates among the three bands. They can deliver multi-gigabit speeds, enabling applications with demanding requirements like augmented reality (AR), virtual reality (VR), and ultra-high-definition video streaming.

	Spectrum range	Bands (Example)	Coverage	Peak Data rates	Typical Usage
Cell range	Low band < GHz	• 600MHz • 700MHz	• Deep indoor • > 1 km	• ~100Mbps	• Deep indoor coverage.e.g.mMTC • Sypplementary UL eMBB coverage • Coverage Layer for eMB
	Mid-band 3-6 GHz	3.3-3.8 GHz 3.3-4.2 GHz 4.4-5.0 GHz	• Similar to LTE • ~1km	• ~1 Gbps	• 5G eMBB coverage on LTE Grid • Major first launches are in this spectrum range
Data range	High-band > 24 GHz < 52.6	• 26 GHz • 28 GHz • 39GHz	• Hot Spots • Line of Sight • ~100 m	• ~10 Gbps	• Extreme data rates for local areas, e.g. Virtual Reality in Stadiums

Figure 4.4 – 5G Spectrum Bands

Microservices and Cloud Native

Equipment vendors of 5G systems are taking advantage of the latest trends in software evolution: microservices and cloud-native technology. Software has evolved from a monolithic to a microservices architecture, and 5G vendors are implementing them in their products. This makes private 5G networks more flexible to operate, with a greater degree of reliability.
Let's look at the AMF and UDSF network functions, for instance. AMF manages the mobility aspect of the UE, and UDSF stores stateful information from other elements. A vendor AMF may have a group of microservices dedicated to different sub-functions.

These sub-functions may be:

- Load Balancing to handle traffic from/to the network. (stateless)
- Service Logic to process the session service requests (stateless)
- OAM for configuration, fault, and performance management (stateless)

The session stateful information that the AMF needs to keep track of, such as the UE context information, on the other hand, can be serviced by the UDSF.

This implementation provides a higher level of performance over monolithic-based software network environments. Greater performance is achieved thanks to the separation of stateless and stateful functions, which dedicate processing power to very specific roles. The microservices dedicated to load balancing, service logic, and OAM handle stateless information. The UDSF handles the storage of the stateful information (UE context) and off-loads that processing from the AMF.

The microservices network environment also benefits from greater redundancy because these microservices are highly distributed with no single points of failure.

Furthermore, the implementation of cloud-native technologies such as Kubernetes and Container run time provides the perfect environment to deploy, orchestrate, and manage these microservices. The cloud-native environment is always aware of the current and available CPU, memory, and storage resources. It also understands the network requirements of microservices. As such, it can make correct decisions to deploy and adapt if the level of processing, storage, and redundancy changes.

Open Architecture

A private 5G network also features an open architecture, where standard REST APIs can be exposed to 3rd party systems, allowing them to get visibility into the private 5G environment, perform analysis of the data and events, and potentially inject appropriate actions into the network. Security and coordination of the communication between a 3rd party entity and the private 5G network is managed by the NEF (Network Exposure Function). It is also possible to integrate systems that can provide automation and AI interaction in support of evolving use cases.

This openness will keep 5G relevant for years to come. Future-proof technology protects the Enterprise's investment by deploying the infrastructure today and gradually implementing new capabilities through integration with other systems. Examples include AI (Artificial Intelligence), automation, and analytics, which can potentially turn into future revenue use cases.

Control and User Plane Separation

Another major capability offered by 5G technology is the separation of control and user plane (CUPS). As illustrated in Figure 4.1, the architecture for 5G is broken down into control functions and user plane functions. This separation allows the orchestrator of the cloud environment to make resource changes in the user plane element without impacting the control elements. For example, let's assume a private 5G network has been integrated with an automation system that is monitoring traffic capacity on the UPF and is also getting traffic utilization data from the network. When it detects the need for more resources, the system can notify the orchestrator to scale up the media resources on the UPF without impacting the control plane.

The separation of control and user plane entities in the environment makes possible the granular adaptation of resources in the network when planned or unexpected changes occur. It also allows for more flexible deployment options. Network functions that handle the user plane can be placed at the edge of the network closer to the users to reduce latency, while control functions can be more centralized.

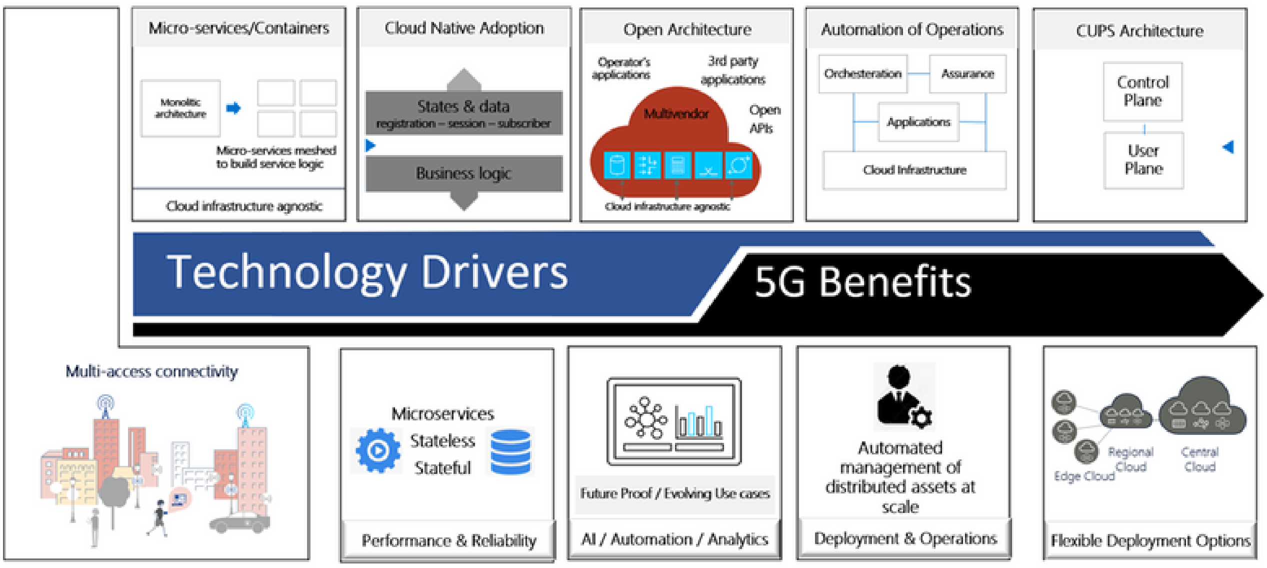


Figure 4.5 – 5G Drivers and Benefits

5G QoS Implementation

One of the most valuable tools that 5G offers is the ability to define QoS policy in the Policy Control Function to offer differentiated service treatment to the traffic.

QoS is one of the aspects that 5G is second to none. The implementation is so granular that it can provide differentiated treatment to all the IP flows from a single user. Unlike 4G, which required the establishment of dedicated bearers for each traffic type per user, the 5G implementation only requires a single session (called the PDU session) to carry multiple IP flows, which can be assigned to a particular service class and treated accordingly. This is well represented in Figure 4.6.

5G has defined several 5G QoS ID values to characterize the different SLAs for each traffic type. Parameters include the resource type, priority level, packet delay budget, maximum data burst volume, and default averaging window. Once a UE has established a PDU session, it will be able to forward traffic in the form of IP flows.

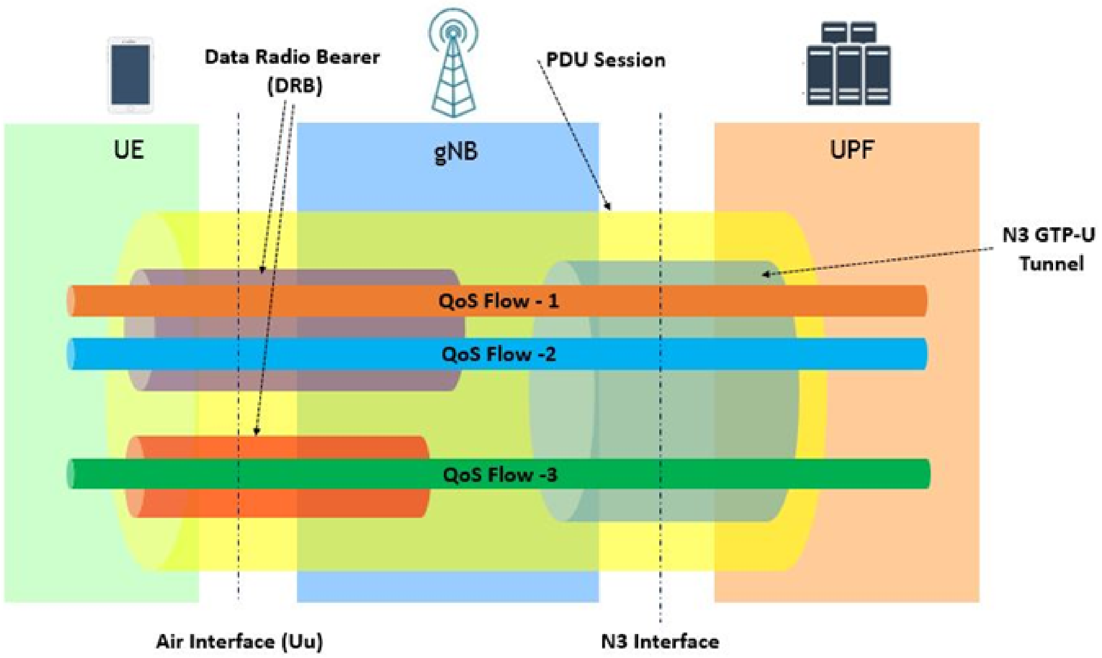


Figure 4.6 – 5G QoS

The QoS framework for 5G is more flexible and efficient than previous generations of 3GPP cellular networks because it requires less signaling and can treat traffic at the IP flow level. 5G provides a perfect environment to define policies and enforce them, guaranteeing the service level agreement committed for each traffic class.

5G NG-RAN Capabilities

To meet the extreme requirements for very high throughput, ultra-reliable low latency communications (URLLC), and massive machine communications (mMTC), the 5G NG-RAN has improved its spectrum efficiency.

With advanced technologies such as massive MIMO (Multiple Input Multiple Output), which enables the transmission of multiple data signals at the same time over the same radio channel, and beamforming, a 5G network can offer speeds up to 20Gbps in the downlink with mm-Wave frequency bands and a latency of 1 msec.

The NG-RAN also introduces support for unified access. NAS signaling is common for both 3GPP and non-3GPP access networks. This allows an enterprise to support the coexistence of several access technologies while using a consistent approach for signaling and authentication.

Network Slicing

5G provides the Enterprise with the ability to logically partition the 5G network into slices. In Figure 4.7, two slices have been defined with a dedicated AMF, SMF, and UPF. UE1 has been assigned to slice #1 and UE2 to slice #2.

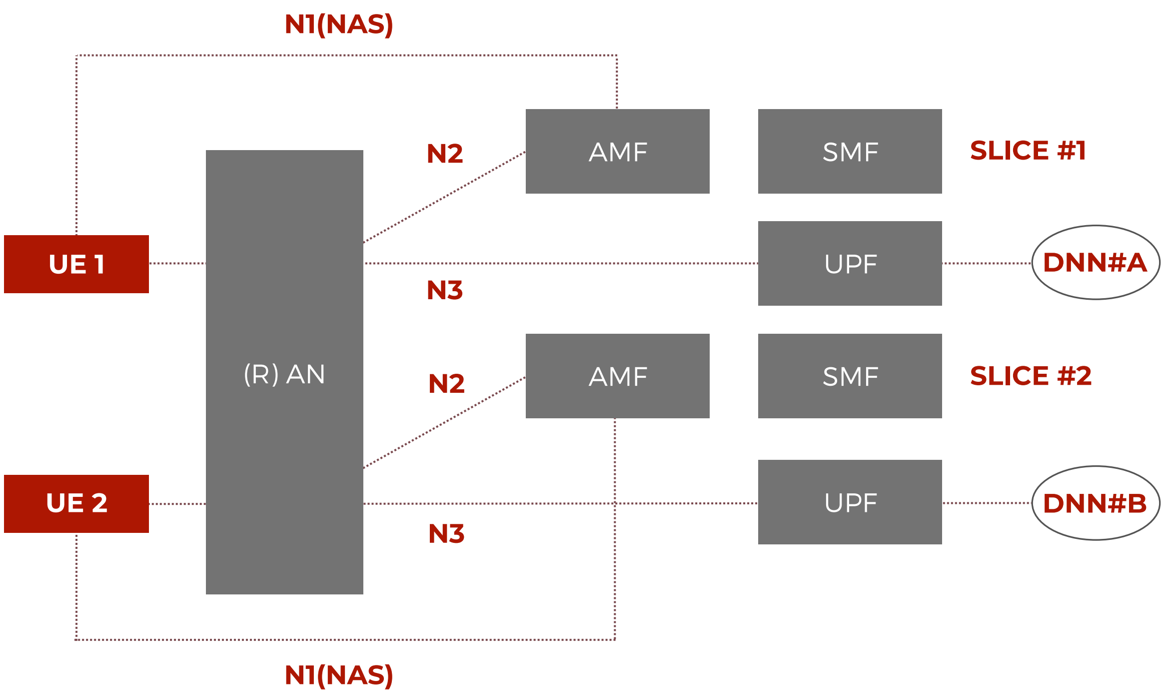


Figure 4.7 – Network Slicing

An Enterprise can configure multiple slices to isolate and prioritize traffic from its business domains. It could dedicate one strictly for employee mobile services, another for business applications, another for critical business applications, and another for mission-critical applications. Each domain can have a differentiated QoS treatment.

Similarly, a Service Provider that implements 5G can offer a hosted private 5G network to an Enterprise using network slicing.

Security

The 5G security framework is built on several key principles that ensure the safety and integrity of data and communications. One crucial aspect is end-to-end encryption, which safeguards information as it travels between devices and network infrastructure. This encryption makes it exceedingly difficult for unauthorized parties to intercept or manipulate data.

Additionally, 5G incorporates robust authentication mechanisms, requiring devices to verify their identities before accessing the network, reducing the risk of unauthorized access. Furthermore, the architecture includes strict access control and authorization protocols, granting specific permissions only to authorized users and devices.

To counter emerging threats, 5G networks can leverage advanced security technologies like artificial intelligence and machine learning, allowing for real-time threat detection and response.

5G's secured architecture prioritizes encryption, authentication, access control, and cutting-edge technologies to fortify the network against potential security breaches.

DEPLOYMENT

3GPP Rel16 has defined different models for the deployment of private 5G networks. This section will address them and provide considerations for operating and managing the network.

Deployment Models per 3GPP

As defined in 3GPP Rel 16 specifications, a private 5G network (also known as a Non-Public Network or NPN) can be deployed as either a fully standalone system that requires no Service Provider support, or it may be deployed with the support of a Service Provider. This second approach is called Public Network Integrated NPN or PNI-NPN.

SNPN Deployment

As illustrated in Figure 5.1, the 5G private network is deployed as a standalone independent network. All network functions are located within the enterprise environment, isolated from the Service Provider. Optionally, communication between the Enterprise and the service provider can be implemented via a firewall and serves as the demarcation point. This connection can be used for accessing public services. The Enterprise has the responsibility for operating its private network and for the configuration of the service attributes. Alternatively, enterprise devices can subscribe directly to the Service Provider network to access its services with a dual subscription. Optionally, a connection can be leveraged to access enterprise services via the Service Provider network.

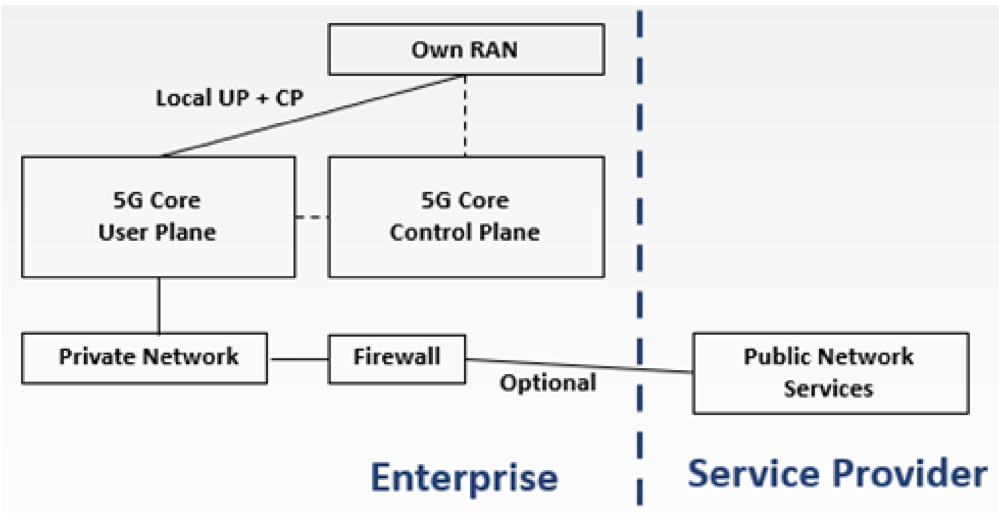


Figure 5.1 – SNPN Deployment

PNI-NPN Deployment

A PNI-NPN deployment is a private 5G network that leverages services from a Service Provider. Different implementation combinations may be provided. Here is a description of the three options:

RAN Sharing Only Scenario: As illustrated in Figure 5.2, the Enterprise and the service provider network share part of the radio access network, while other network functions remain segregated in the enterprise premises. All data flows related to the private network stays within the Enterprise, and the public network traffic portion is transferred to the service provider network.

The private network gets its own dedicated NPN ID, but there is a RAN sharing agreement with the service provider. It is possible to have an optional connection between the Enterprise and the service provider via a firewall, and it is also possible to configure additional base stations that are only accessible to enterprise users and devices.

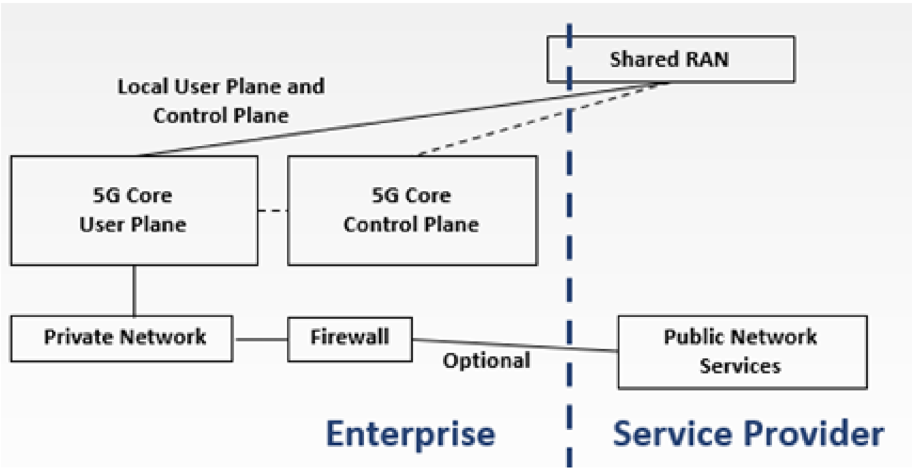
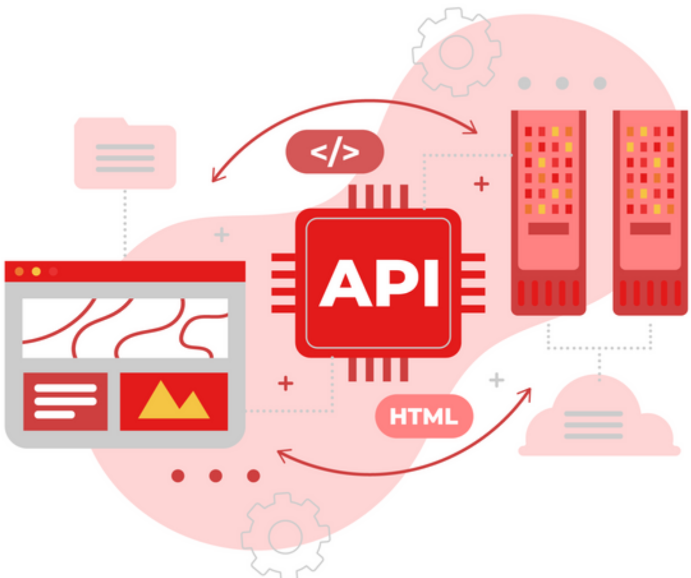


Figure 2 – RAN Sharing Only



RAN Sharing and Control Plane Hosted: As illustrated in Figure 5.3, the Enterprise and the service provider network share the radio access network for the defined premises, and network control tasks are always performed in the service provider network. Nevertheless, all private network traffic flows remain local within the Enterprise, while the service provider network traffic portion is transferred to the service provider network.

This can be implemented by means of network slicing at the service provider network. Isolation of the public and the private networks is achieved by employing different network slice identifiers. Another approach is to use the 3GPP-defined feature called access point name (APN), which identifies where to route traffic, allowing differentiation between traffic portions.

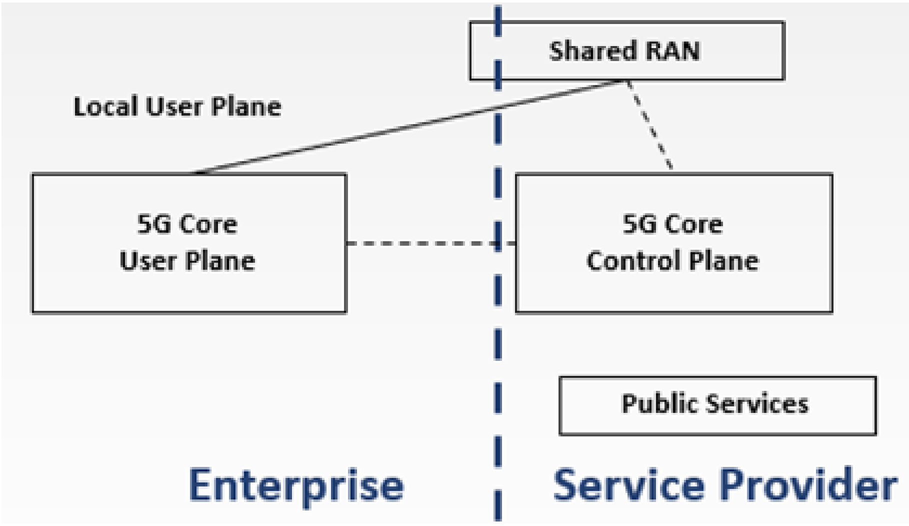


Figure 5.3 – RAN Sharing and Control Hosted

Fully Hosted Model: As illustrated in Figure 5.4, both the public network traffic portion and the private network traffic portion are external to the Enterprise's physical premises but treated as if they were parts of completely different networks. This scenario can be implemented by means of network slicing or APN (Access Point Name) functionality.

In this scenario, enterprise subscribers are, by definition, also service provider subscribers. Since all data is routed via the service provider network, access to public network services and the ability to roam can be implemented easily in accordance with the agreement between Enterprise and the service provider.

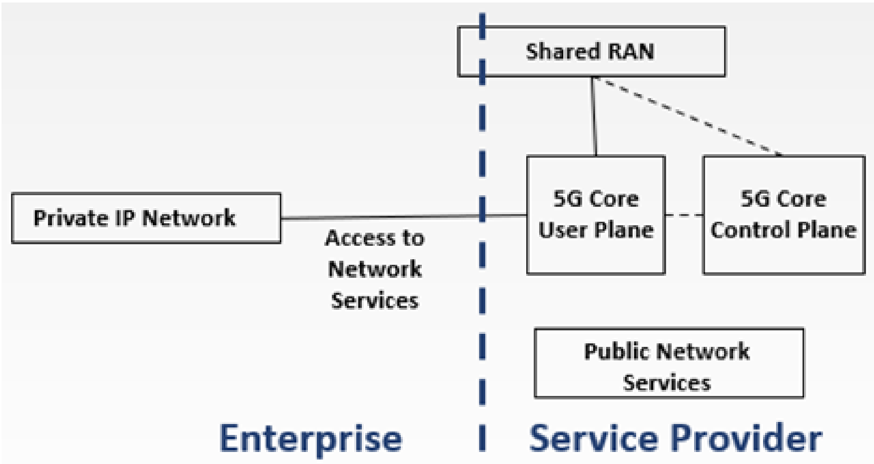


Figure 5.4 – Fully Hosted

In all deployment models, operations and management is a key aspect to consider. Enterprises managing the fully standalone private 5G network have local access to their network functions and can strive for the implementation of a unified management system with the flexibility to manage the Network Functions life cycle via a cloud orchestrator system and the FCAP aspects (Fault Configuration and Accounting Performance) via an Element Management System, which is typically provided with the purchased vendor product.

For the deployment models that involve the service provider, access to the network functions can be achieved via APIs. The level of management and control will be dictated by the service provider.

In essence, the deployment approach of enterprises significantly impacts how they operate and manage network functions and access critical network and service data, particularly when the 5G private network coexists with the service provider on the same infrastructure.

Selecting the appropriate deployment model will depend on factors such as how much control over the equipment and operations is desired, the level of expertise available, the network footprint, and the business model.

CONCLUSION

Private 5G networks are a transformative benefit for enterprises across various sectors. They bring forth the unmatched attributes of 5G technology, such as exceptional speed, capacity, reliability, and operational efficiency, all within localized settings designed to meet the unique demands of each Enterprise.

The inclusion of cloud-native technologies presents an optimal platform for deploying, orchestrating, and managing the private 5G environment. With a native awareness of available CPU, memory, storage resources, and network demands, this infrastructure can autonomously make informed decisions, adapt to fluctuating conditions, and maximize resource utilization, ushering in a new era of operational agility.

The open architecture of 5G ensures enduring relevance by allowing the gradual integration of emerging capabilities such as AI, automation, and analytics, thereby safeguarding the Enterprise's investment while paving the way for potential revenue diversification

ABOUT COMMDEX

For over 20 years, Commdex has been providing a broad, rich portfolio of proven network solutions to Government and Enterprise customers for the deployment of telecom networks, facilities, and supporting systems. Commdex specializes in designing and implementing missioncritical voice and data networks over 5G, microwave, land mobile radio, DAS, SATCOM, and other technologies. Its solutions, services, and methodologies have been tested and proven in hundreds of customer environments nationwide. With its ability to design 5G Solutions coverage and our experience in regional and statewide systems, Commdex has not only the technical expertise to build the systems but also the management expertise to aid in the integration and operation.

Based on its years of experience in implementing large, complex systems, Commdex has perfected an integrated approach that maximizes the capability of any solution that a customer may require while minimizing the associated risks, schedule, and cost. This iComm360o approach ensures that the project is delivered with proven expertise through the capability of a proven integrator that understands the entire life cycle of Communications projects. This experience gives it the ability to confidently and quickly implement the 5G network. For more information, visit Commdex at http://www.commdex.com.