altice labs

Heading to a successful private digital convergence

5G; Private networks; Convergence

White paper

Version 1.0, May 2022

Introduction

Enterprises must be efficient and agile to survive in a challenging global market. To achieve this purpose, digitalization in all the production steps and processes is unquestionable, with the integration of intelligence, automation, and computation-based tasks. Process digitalization requires distributed computation and, inherently, suitable communication channels to interconnect all the involved components. Sensors, actuators, automated guided vehicle (AGV), displays, video cameras, or computers each have their own specific connectivity capabilities, requirements, and context. Data storage and processing have also to adhere to requirements and policies, fulfilled by a scalable and continuum of computational resources, ranging from the local infrastructure to public clouds. Thus, the deployment of local, suitable communication infrastructures is of paramount relevance for the enterprise that wants to grow and succeed.

Current private networks are generally based on legacy wired or wireless (WLAN) Ethernet. More demanding production processes require specific communications, enhanced security, and reliability, like time-sensitive networks (TSN), which define mechanisms for the time-sensitive transmission of data over deterministic Ethernet networks. 5G is targeted to fulfill Industry 4.0 needs for wireless connectivity on the factory floor, guaranteeing security, minimum delay, deterministic response, and high reliability.

Private cellular networks are not new, but, as shown in **Figure 1**, from a current estimate of about one thousand private networks based on 3rd Generation Partnership Project (3GPP) specified technology, their numbers are expected to grow to 10's of thousands due to:

- Guaranteed local coverage, enabled by the availability of localized private, unlicensed/ shared spectrum and cost-efficient, cloud-based 4G/5G core deployments;
- Reduced total cost of ownership (TCO) from the elimination of wired and other connectivity (e.g., Wi-Fi);
- Growing demand for enterprise information and data security, associated with localized data processing capabilities for ultra-high-performance applications;
- Search for increased productivity solutions through automation and digitalization of enterprise processes;
- Demand for low latency and reliable services.

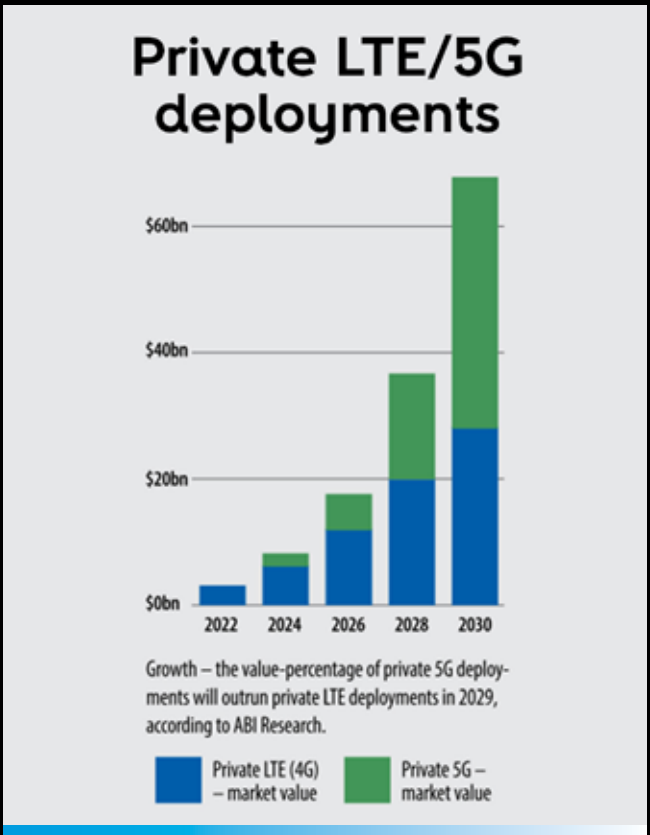

FIGURE 1 – Expected growth of private cellular networks (LTE and 5G) [4]

Polaris Market Research predicts that the global 5G private network market will grow at a CAGR of 40.9% between 2020 and 2028 [1]. ABI Research forecasts that it could be worth US$16.3 billion by 2025, in line with **Figure 2**. Nokia's CEO Pekka Lundmark recently commented that more money will be invested in private 5G networks than in public networks over the next ten years [2], significantly fostering their growth.

However, the widespread adoption of private 5G networks will only become a reality when their operational costs become small, and a seamless interworking between 5G access and other industry technologies, like wired Ethernet or Wi-Fi, is achieved [3]. Taking advantage of a 5G network and its associated services via a non-3GPP access opens the opportunity for new value-added services to be extended to a larger group of devices and use cases. Altice Labs is working on the development of wireline-wireless integrated connectivity and computing solutions for private industrial domains, to guarantee the best possible continuous connectivity for all scenarios. This article extends the concept to all technologies while keeping common control and management, bringing fixed-mobile convergenc to the private domain.

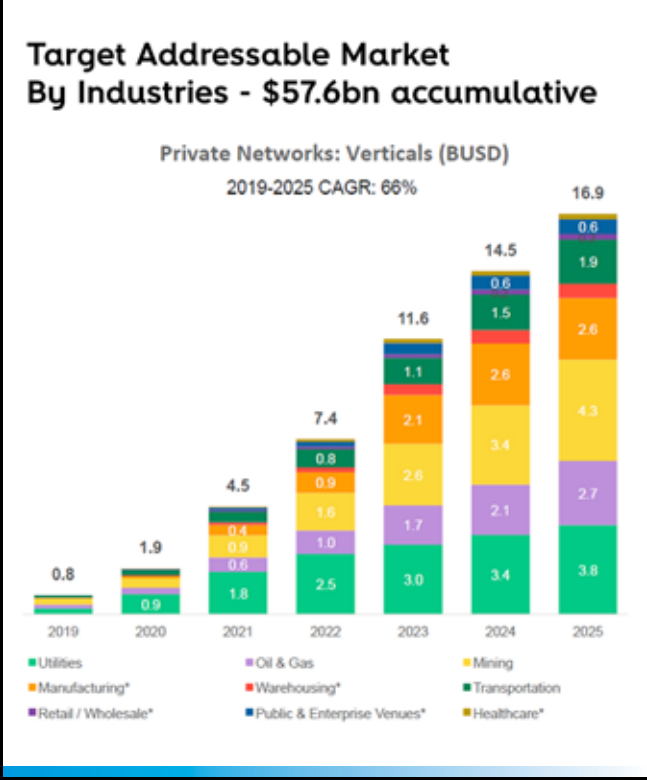

FIGURE 2 – Expected evolution of the private market value by vertical [6]

Private 5G networks

In the technical specification related with service requirements for the 5G system [5], 3GPP describes non-public networks (NPN), 3GPP's terminology for private networks, as being "*intended for the sole use of a private entity such as an enterprise, and may be deployed in a variety of configurations, utilizing both virtual and physical elements. Specifically, they may be deployed as completely standalone networks, they may be hosted by a public land mobile network (PLMN), or they may be offered as a slice of a PLMN*". That way, a 5G NPN consists in the usage of a 5G system for private use, being deployed as:

- a standalone NPN (SNPN): operated by an NPN operator and not relying on network functions provided by a PLMN, or
- a public network-integrated NPN (PNI-NPN): a non-public network deployed with the support of a PLMN.

As any 5G system, 5G NPN are composed of user equipments (UE) - terminals or end-systems -, 5G accesses - consisting of next-generation NodeB (gNB) units connecting UE via a 5G new radio (5G-NR) wireless interface -, and a 5G core (5GC). Hence, SNPN and PNI-NPN use the same underlying network solutions, including hardware and software, the same encoding schemes, and the same type of spectrum as public 5G networks. However, they differ in their usage. While a public 5G network is intended for public usage, with tens of millions of subscribers on a given nationwide network, typically supporting best-effort applications, a private 5G network is dedicated to a single enterprise or organization. Often, they are confined to a single location, which can be as small as a building or as large as a sea or airport, supporting more demanding applications (e.g., remote control of a machine). This impacts, for instance, dimensioning and redundancy of the different control and data plane entities, the adopted security and authentication mechanisms, and the distribution of the available bandwidth in the up and downlink directions. Besides the two extreme SNPN and PNI-NPN scenarios, other intermediate solutions are possible, for instance, via radio access network (RAN) sharing between the operator and private entities, as is the case of a multi-operator core network (MOCN).

In a phased approach, a private entity may start by a PNI-NPN for the initial, less demanding use cases and progress towards an SNPN, as the technology matures, gets cheaper and a higher level of digitalization is achieved, leading to more demanding use cases, requiring dedicated 5G support (as shown in **Figure 3**).

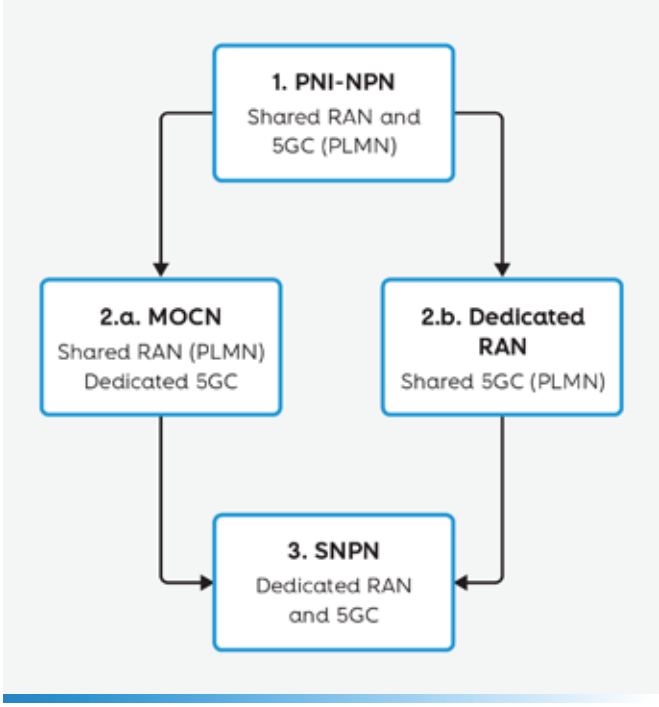

Figure 3 – Possible NPN deployment evolution for a single enterprise

For each of the identified deployment options, we have the following:

1. PNI-NPN

- The NPN is established on top of the PLMN via slicing, a differentiating feature of 5G;
- Private 5G data is delivered at the operator domain. Via an existing or new connection, most likely protected by a virtual private network (VPN), the traffic will be exchanged with the private domain;
- The operator may deploy dedicated regional 5GC to address the B2B market, independent from public, B2C services. Still and to a large extent, common core and RAN configurations are shared between different business customers.

2.a. MOCN

- To benefit from specific configurations and UE provisioning, business customers may deploy their own 5GC at their premises but share a common 5G access;
- This 5GC may already be used to control/manage other accesses;
- Common RAN configurations will be shared amongst customers, and traffic is delivered at a common point, even if securely isolated from others;
- Considering the availability of open source 5GC implementations, this may represent a CAPEX suitable to start with for most enterprises.

2.b. Dedicated RAN

- A dedicated RAN and user plane function (UPF) is locally deployed, guaranteeing the date plane is restricted to the enterprise premises, which can be configured according to specific customer needs;
- A shared 5GC exists at the operator domain, which shall be multi-tenant;
- Having local and possibly shared core UPF units, convergence, traffic steering, and multi-connectivity is likely to be possible;
- It requires spectrum (dedicated, sub-leased from the operator, shared, or unlicensed) to be dedicated for this private usage.

3. SNPN

- A complete 5G system is deployed at the enterprise with dedicated RAN and other access components (convergence);
- Like the previous one, it requires a dedicated 5G spectrum;
- It provides maximum control over the data and control planes but shall also be the more expensive solution in CAPEX and OPEX.

Starting with the PNI-NPN model may be impossible since just a few operators have deployed 5G in standalone mode. Most operators are focusing their current investments in non-standalone mode, by upgrading their evolved packet core (EPC) nodes and adding 5G radios on selected cell sites to address the consumer market with more bandwidth. Regarding MOCN, the required RAN sharing implies customers are in the same coverage area, and cell locations will most likely be outdoors.

Altice Labs is working on solutions where the radio access (5G-NR) is always deployed at the private domain as dedicated access. **Figure 4** illustrates three possible configurations, with the first corresponding to the SNPN scenario described above, with middle and right ones as variations of the dedicated RAN scenario. Here, the focus is on the location of the control entities and edge computing platforms.

The first deployment enables maximum security with minimum delays. Still, via its external access, workloads can be placed at the operator edge or central (and public) clouds. In the second situation, the multi-tenant shared control plane is located at the operator domain, most likely at the edge, reducing CAPEX and OPEX. With a local UPF and convergence units, data processing can be done locally or at the operator's edge, possibly under 5G traffic steering control. The third situation is the one with fewer costs for the enterprise. Only the minimum required infrastructure is locally deployed to ensure local accesses, with all the computational processing delegated to the operator or Internet domains.

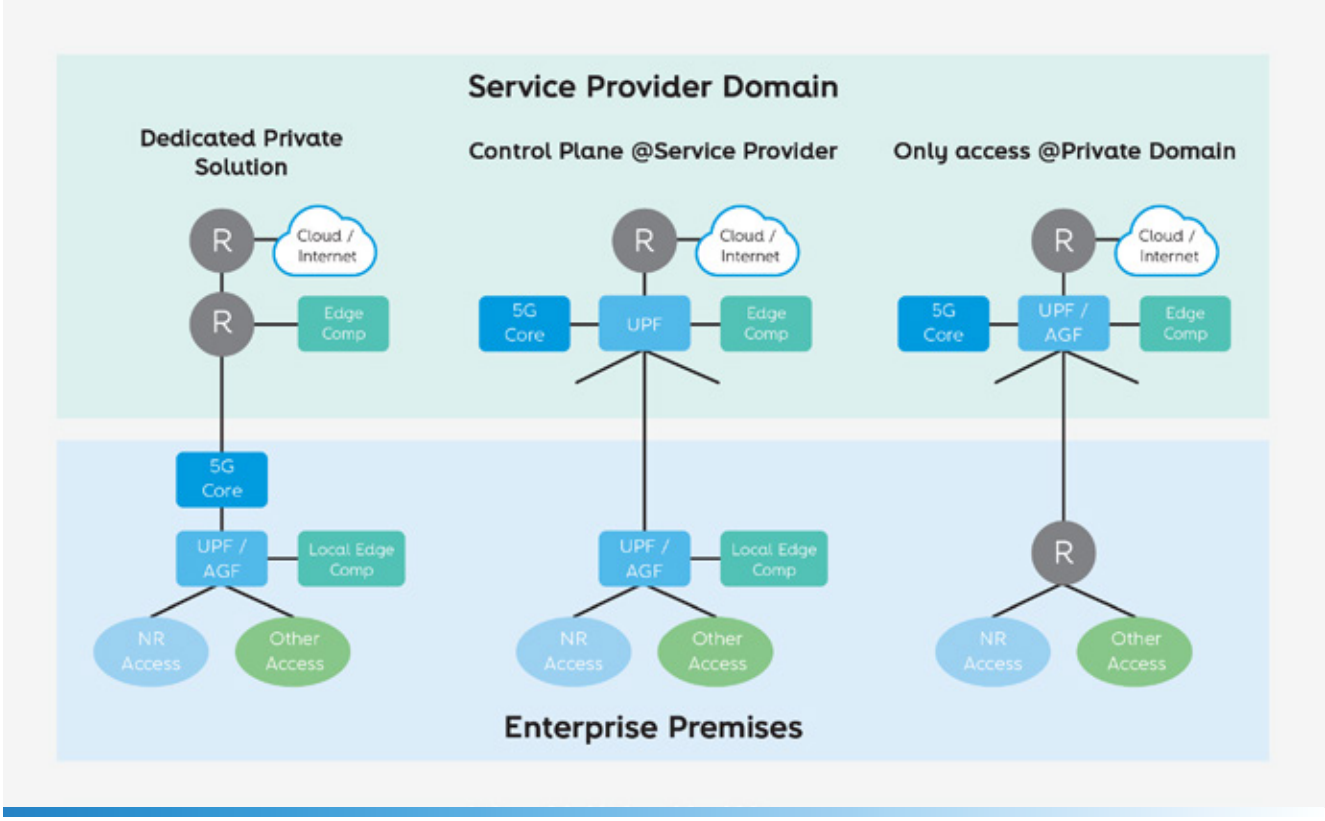

Figure 4 – Different NPN deployment configurations, distributed between public and private domains

Convergence and 5G

5G may not be the best connectivity solution for all use cases, even if technically feasible. Considering the different connectivity requirements, other wireless (e.g., WLAN) and wired (copper or fiber) technologies may, currently, be more cost-effective and less complex for some of the use cases and, most likely, be already deployed. Considering 5G characteristics, it shall be adopted in demanding ultra-reliable and low-latency communications (URLLC) use cases, providing connectivity in specific functional and geographic areas. With convergence, private industrial networking continues being a heterogeneous environment, but with common management and operation of all accesses as a single network, via a common 5G control plane and traffic aggregation entities. The 5GC control and data planes have the capability to serve other access technologies. In the scope of private deployments, potential 5GC shared services include:

Common and consistent authentication/registration and global assignment of security policies;

- Unique IP address management;
- Consistent traffic management (e.g., routing, forwarding, inspection, policy enforcement, QoS handling, and reporting) across all access types;
- Transversal slicing/virtual networking management;
- Exposure to external entities as a single network.

Additionally, convergence enables multi-technology endpoints to choose the access technology to use at each time (traffic steering and switching) and even to connect simultaneously via different access technologies (traffic splitting). Starting with multi-radio dual connectivity (MR-DC) in Release 15, this is now specified as access traffic steering, switching and splitting (ATSSS), currently part of 5G standards.

Fixed-mobile convergence (FMC) or, more recently, wireline-wireless convergence (WWC) has long been addressed by 3GPP [7] and other organizations like the Broadband Forum [8], defining solutions for a shared common mobile core, serving wired and wireless access technologies. Already addressed in 4G/LTE scope, this gained higher relevance with 5G due to its intended broader scope.

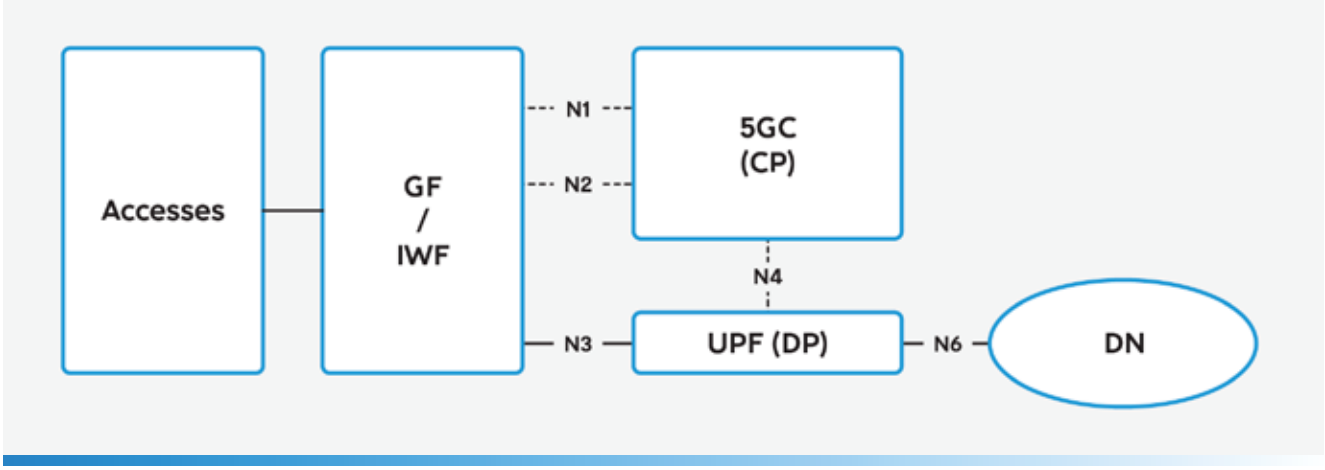

Figure 5 – Access networks integration with a 5GC

Convergence in 5G is achieved at the core via functional entities placed at the 5G domain entrance, which adapt access specific protocols to standard N2 interface control plane (CP) and N3 interface data plane (DP). The N1 interface, used to convey non-radio signaling between the UE and the 5GC, may not be supported by the terminal equipment, forcing the adaptation entities to handle it on behalf of the terminal (as shown in **Figure 5**, on the previous page). That is the case for most of the residential gateways and WLAN-only devices.

Security mechanisms for authentication and data encryption are key aspects in convergence since they must be present whenever a terminal attaches to the network. However, they are deeply dependent on the nature of the used access network. A unified authentication framework was defined for 5G, where 5G authentication and key agreement (5G-AKA) and extensible authentication protocol (EAP) for the 3rd generation authentication and key agreement (EAP-AKA') are mandatory 5G primary authentication methods. That framework makes 5G-AKA procedure suitable for both open and access-network agnostic scenarios, relying on three authentication methods: 5G-AKA, EAP-AKA', and EAP transport layer security (EAP-TLS). The framework enables the existence of multiple security contexts that can be established with a single authentication execution, allowing the UE to move from a 3GPP access network to a non-3GPP network without having to be unauthenticated [9].

Different adaptation entities were, so far, defined, mainly differentiating on security aspects. Besides gNB and next-generation e-NodeB (ng-eNB), for native 5G-NR and LTE accesses, respectively, the following four additional 5G access node types exist (detailed in [10] and [11]):

Non-3GPP interworking function (N3IWF), which allows 5G capable terminals, supporting non-access stratum (NAS) to connect from untrusted WLAN or other accesses deployed by third-party entities, out of the scope of 5G network owner control.

Trusted non-3GPP gateway function (TNGF) and trusted WLAN interworking function (TWIF), aimed for trusted non-3GPP and WLAN accesses, but requiring the UE to have 3GPP credentials and, for the first case, to support NAS. They are based on the tight coupling between a trusted access point and a gateway or interworking function.

Wireline access gateway function (W-AGF), which connects a wireline 5G access network (W-5GAN) to the 5GC network. It is similar to the TNGF for 5G residential gateways (5G-RG) and the TWIF for fixed-network residential gateways (FN-RG) but considering the specific characteristics of fixed access networks. 5G-RG units support NAS signaling and authenticate themselves, while FN-RG do not support 5G capabilities and do not have 3GPP credentials in this specific context.

From the previous, it can be observed the lack of standards to support pure WLAN devices connections to the 5GC. This is identified in the 5G work group [10] by the Wireless Broadband Alliance (WBA), stating that “most Wi-Fi-only devices, e.g., devices in enterprise deployments, would not have a USIM included,” recommending that “3GPP needs to define architecture and procedures for supporting Wi-Fi only UE with non-IMSI based identity and EAP-TLS/EAP-TTLS based authentication”. Altice Labs is aware of this limitation and is working towards an interim, proprietary solution, while this is not addressed by 3GPP.

Traffic steering

Depending on the context, terminals located at the private domain need to, transparently and dynamically, be served at the same premises, on the operator edge, or at central clouds. 5G has built-in mechanisms for dynamic traffic steering via API exposed to service platforms or applications functions (AF).

Via the network exposure function (NEF) (using reference point N33 for untrusted services) or directly via the policy control function (PCF) (using reference point N5 for trusted platforms), services may dynamically change the anchor point, or protocol data unit (PDU) session anchor point (PSA) on the network side of running 5G PDU sessions, switching between different UPF instances, and thus providing access to different service platforms (depicted in **Figure 6**). This is particularly interesting for moving terminals (e.g., a change in gNB/centralized unit may trigger a change in the anchoring UPF to keep latency low) or in the scope of edge computing (e.g., to serve users at the right 'distance' for their changing latency requirements, or under periods of network congestion). Despite limited applicability for SNPN, with a small number of UPF in a limited geographical area, it may become crucial for shared 5G control scenarios in which traffic is steered between local and edge data centers (see the middle scenario depicted in previous **Figure 4**).

Altice Labs has demonstrated this functionally [12] by integrating Intel® Smart Edge Open distribution [13] (via OpenNESS AF) with the PCF of Fraunhofer FOKUS' Open5GCore [14].

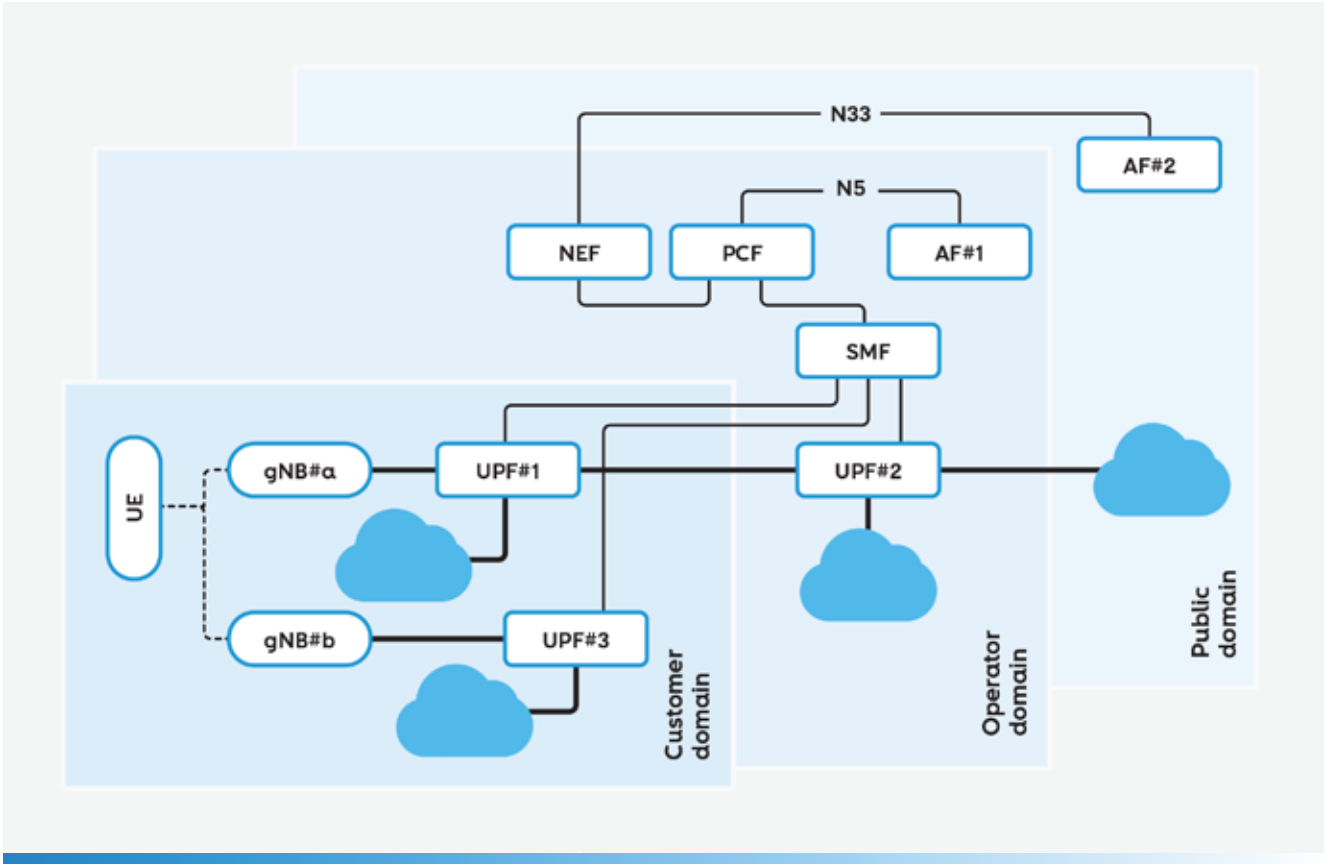

Figure 6 – T raffic steering control scenarios, for trusted and untrusted application functions

Multi-connectivity

The ability to attach multiple access technologies to a 5GC provides significant flexibility in the planning and operation of network environments. Although the physical areas covered by the different access networks may be complementary or overlap, providing the network and terminals with simultaneous multi-connectivity directly promotes that flexibility.

3GPP Release-16 5G specifications include the ATSSS functionality. Steering refers to the capacity to select the best link to use for the data plane traffic, according to the service (QoS type for a data flow). Switching allows data plane traffic to switch to another access technology without service interruption. Splitting means the simultaneous use (bonding) of several network connections (PDU sessions). As an example, leveraging simultaneous communication over multiple paths (typically over one 3GPP access and one non-3GPP access) gives 5G systems the mechanisms to provide services with improved user experience, distribute traffic across multiple accesses in a policy-based fashion, and enable new high-data-rate services.

In the 5GC, the ATSSS functionality will be co-located with the UPF, making it a "UPF+ATSSS" node (as depicted in the 'b' option of **Figure 7**). While 5G systems do not natively integrate the ATSSS functionality (to be part of 3GPP Release-17 specifications), this can be enabled by placing the ATSSS gateway in complement to an existing UPF (shown as the 'a' option in **Figure 7**). ATSSS-enabled terminals will still be able to steer, switch or split traffic between two or more accesses, based on rules and information received from the network.

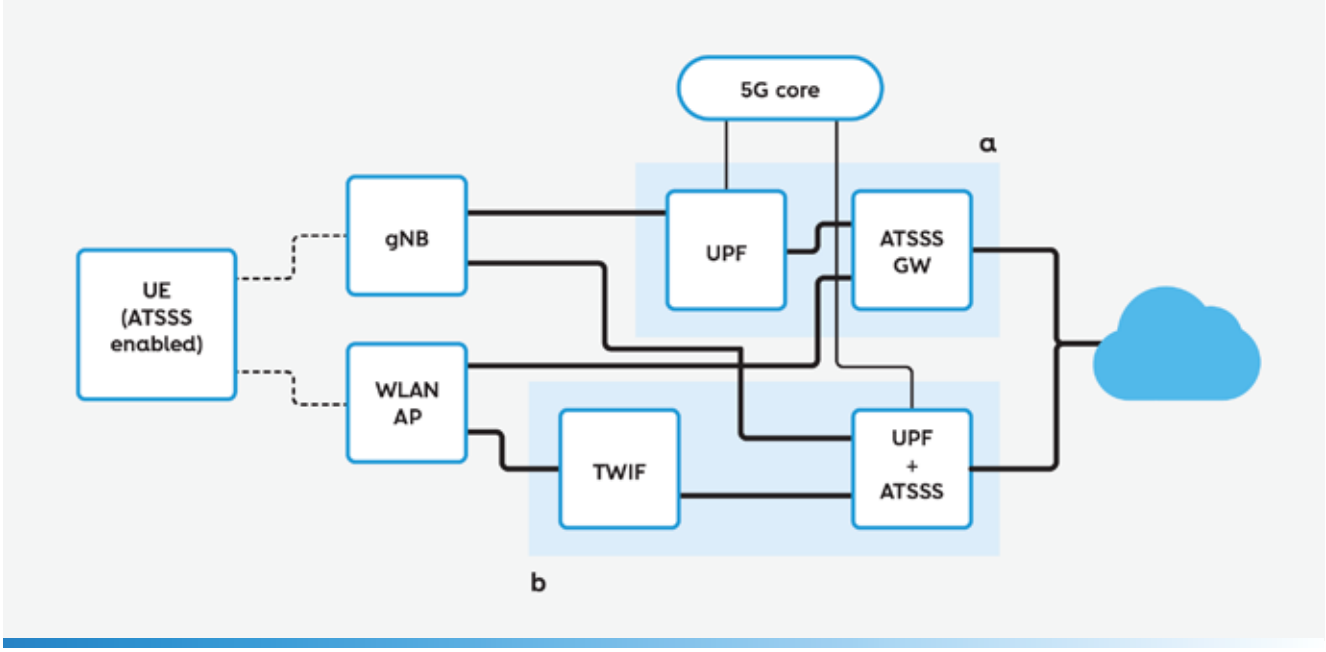

Figure 7 – Different NPN deployment configurations, distributed between public and private domains

To take benefit of the ATSSS features, the IP transport layer has to adapt to the new multipath environment. As such, multipath transmission control protocol (MP-TCP) [15] was adopted by 3GPP in Release-16 as the solution for ATSSS. However, it only applies to TCP traffic. IETF's Transport Area Working Group (TSVWG) [16] is working in multipath-datagram congestion control protocol (MP-DCCP) to make it a suitable ATSSS alternative to multipath quick UDP Internet connections (MP-QUIC) [17] for IP and UDP traffic, and be adopted in 3GPP Release-18.

With the purpose of having complete and efficient ATSSS solutions in the market for its convergent private network solution, Altice Labs is actively supporting the development and adoption of MP-DCCP as an ATSSS technology in 3GPP Release-18 specifications. Equipped with such functionality, the Altice Labs' solution is ready to always provide the best connectivity.

Conclusions

Exploiting specific technology characteristics, private 5G networks are on the rise, with commercial deployments in more advanced markets but still with a strong experimentation objective. They will only achieve significant numbers in 2024 (as shown in previous **Figure 2**) mainly because they are complex, require specific skills to plan, deploy and maintain, and are still an expensive technology, especially in the RAN. This is expected to change with OpenRAN based solutions, like the Altice Labs' solution. Until then, relevant industry features in 3GPP Release-16 specifications but especially with Release-17 and following ones are not yet implemented in commonly available 5G solutions. Other components to share the control and data planes, reducing customers CAPEX and OPEX, are not yet mature to be considered in the near future.

Still, Altice Labs is building a convergent solution for private networks based on a selected 5GC and integrating its own 5G-NR technology, composed of centralized, distributed, and radio units (CU, DU, and RU), aligned with the OpenRAN architecture. Such convergent solution is presented in the InnovAction 2021 article "Enabling 5G private mobile networks". This complete 5G system, with the addition of gateway and interworking functions, integrates WLAN and xPON, this last one as an access technology (private optical LAN) and as the midhaul for the 5G-NR cells, also based in Altice Labs' technology. Except for RU, optical network unit (ONU), and optical line termination (OLT) components, all run as virtualized software elements, operated as containers in a suitable clustered platform. The proposed solution integrates the features referenced throughout this article:

- Converged wireline and wireless accesses over the same 5GC;
- Network traffic steering to access services transparently at the edge, at the core or in public clouds;
- Traffic steering, switching, and splitting over different accesses;
- Integration with edge computing;
- Cloudification of all its software components.

The following **Figure 8** provides a high-level representation of the overall solution.

In order to have a complete and flexible solution, answering the requirements of customers of all dimensions and from all geographies, other areas, like multi-site private networks, integration and interoperation of private and public networks, or multi-tenant control sharing from the edge, to mention only the most relevant, will be addressed in the near future.

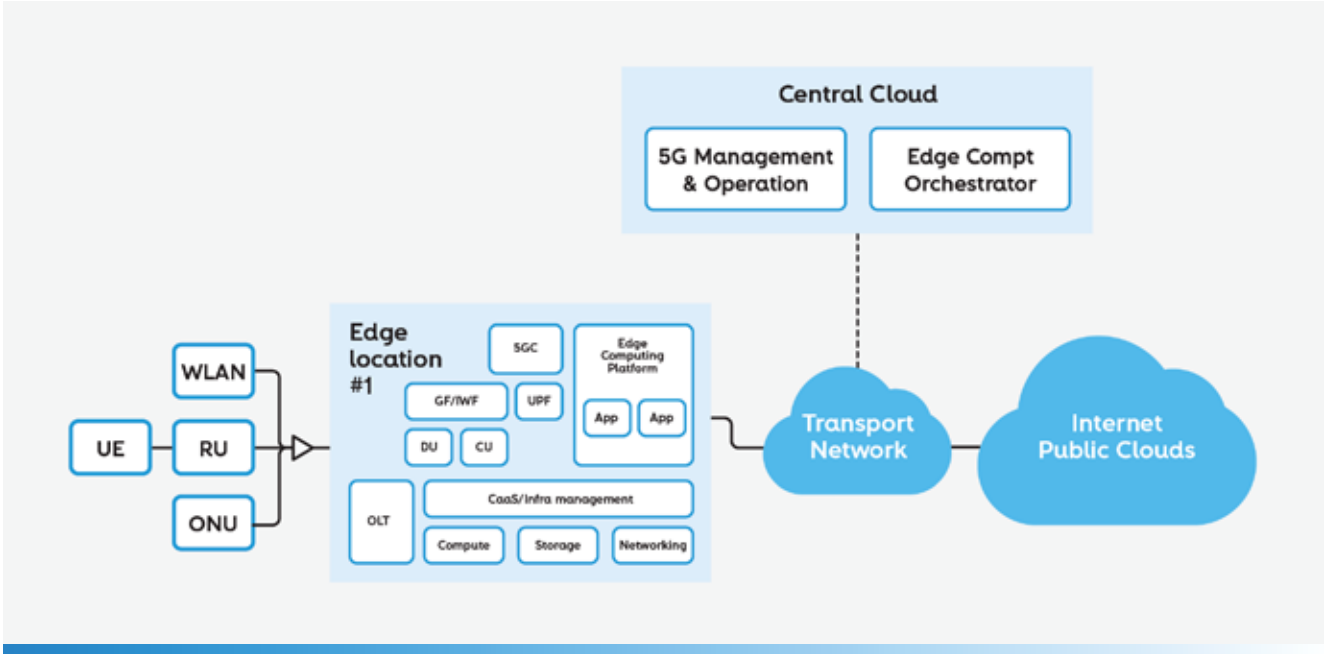

Figure 8 – Global view of current Altice Labs' solution for convergent private networks

References

[1] Polaris Market Research, "Private 5G Network Market Share, Size, Trends," Polaris Market Research, NYC, 2021

[2] D. Manners, "Eletronics Weekly.com," Eletronics Weekly.com, 24 February 2021. [Online]. Available: https://www.electronicsweekly.com/news/business/private-network-5g-pending-outpace-public-network-spending-says-nokia-ceo-2021-02/

[3] H2020 5G Clarity, "5G-CLARITY Deliverable D2.2 - Primary System Architecture," 5G PPP, 2020

[4] Enterprise IoT Insights, "Private 5G Enterprise NOCs - Where and how will mobile operators manage private 5G enterprise networks?," RCR Wireless News, 2021

[5] 3GPP, "Service requirements for the 5G system - TS 22.261," 3GPP Portal, 2017

[6] 5G Americas, "5G Technologies in Private Networks," 5G Americas, USA, 2020

[7] 3GPP, "Wireless and wireline convergence access support for the 5G System (5GS) - TS 23.316," 3GPP Portal, 2019

[8] Broadband Forum, "TR-470: 5G Wireless Wireline Convergence Architecture," Broadband Forum, 2020

[9] TechPlayOn, "5G Authentication and Key Management 5G-AKA," TechPlayOn, 26 March 2021. [Online]. Available: https://www.techplayon.com/5g-authentication-and-key-management-aka-procedure/

[10] WBA 5G Work Group, "5G and Wi-Fi RAN Convergence - Aligning the Industry on Opportunities and Challenges," Wireless Broadband Alliance, 2021

[11] Broadband Forum, "TR-456: AGF Functional Requirements," Broadband Forum, 2020

[12] 5G-VINNI Consortium, "5G-Vinni," 5G PPP, 2019. [Online]. Available: https://www.5g-vinni.eu/

[13] Intel Corporation, "Intel® Smart Edge Open - Streamline networking and application depoloyment at the edge," Intel Corporation, 2021. [Online]. Available: https://www.intel.com/content/www/us/en/developer/tools/smart-edge-open/overview.html

[14] Open 5G Core, "Open 5G Core," Open 5G Core, 2021. [Online]. Available: https://www.open5gcore.org/

[15] Internet Engineering Task Force (IETF), "TCP Extensions for Multipath Operation with Multiple Addresses," Internet Engineering Task Force (IETF), 2014. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6824

[16] Internet Engineering Task Force (IETF), "Transport Area Working Group (TSVWG)," Internet Engineering Task Force (IETF), 2021. [Online]. Available: https://datatracker.ietf.org/wg/tsvwg/about/

[17] UCL - Université Catholique de Louvain, "Multipath QUIC - Website of the Multipath QUIC project," UCL - Université Catholique de Louvain, 2021. [Online]. Available: https://multipath-quic.org/

Acronyms

5G-AKA	5G Authentication and Key Agreement
5GC	5G Core
5G-RG	5G Residential Gateways
AF	Application Function
AGF	Access Gateway Function
AGV	Automated Guided Vehicle
AMF	Access and Mobility Management Function
ATSSS	Access Traffic Steering, Switching and Splitting
CP	Control Plane
CU	Centralized Unit
CaaS	Containers-as-a-Service
DN	Data Network
DP	Data Plane
DU	Distributed Unit
EAP	Extensible Authentication Protocol
EAP-AKA'	EAP Authentication and Key Agreement Prime
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP Tunneled Transport Layer Security
EPC	Evolved Packet Core
FMC	Fixed Mobile Convergence
FN-RG	Fixed-Network Residential Gateways
gNB	Next Generation NodeB
GF	Gateway Function
IMSI	International Mobile Subscriber Identity
IWF	Interworking Function
MOCN	Multi-Operator Core Network
MP-DCCP	Multipath-Datagram Congestion Control Protocol
MP-QUIC	Multipath Quick UDP Internet Connections
MP-TCP	Multipath Transmission Control Protocol
MR-DC	Multi-Radio Dual Connectivity

N3IWF	Non-3GPP Interworking Function
NAS	Non-Access Stratum
NEF	Network Exposure Function
ng-eNB	Next-Generation e-NodeB
NPN	Non-Public Networks
NR	New Radio
OLT	Optical Line Termination
ONU	Optical Network Unit
PCF	Policy Control Function
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
PNI-NPN	Public Network-Integrated NPN
PSA	PDU Session Anchor
RAN	Radio Access Network
RU	Radio Unit
SNPN	Standalone NPN
SMF	Session Management Function
TNGF	Trusted Non-3GPP Gateway Function
TSN	Time-Sensitive Network
TSVWG	IETF's Transport Area Working Group
TWIF	Trusted WLAN Interworking Function
UDP	User Datagram Protocol
UPF	User Plane Function
URLLC	Ultra-Reliable Low-Latency Communication
USIM	Universal Subscriber Identity Module
UE	User Equipment
W-5GAN	Wireline 5G Access Network
W-AGF	Wireline Access Gateway Function
WWC	Wireline-Wireless Convergence
xPON	Designation for several PON technologies

Authors

Francisco Fontes

Seniro Consultant
Altice Labs, Portugal

fontes@alticelabs.com
https://www.linkedin.com/in/franciscofontes/

Miguel Borges de Freitas

Technology Development Manager
Altice Labs, Portugal

miguel-r-freitas@alticelabs.com

Rui Calé

Senior Consultant and Architect
Altice Labs, Portugal

cale@alticelabs.com
www.linkedin.com/in/rui-cal%C3%A9-0306132/

Contacts

Address

Rua Eng. José Ferreira Pinto Basto
3810 - 106 Aveiro (PORTUGAL)

Phone

+351 234 403 200

Media

contact@alticelabs.com
www.alticelabs.com