Private 5G and Wi-Fi Convergence

Key use cases and Requirements

Source:	Wireless Broadband Alliance
Author(s):	WBA 5G Work Group
Issue date:	April 2023
Version:	1.0.0
Document status:	Final for Public

ABOUT THE WIRELESS BROADBAND ALLIANCE

Wireless Broadband Alliance (WBA) is the global organization that connects people with the latest Wi-Fi initiatives. Founded in 2003, the vision of the Wireless Broadband Alliance (WBA) is to drive seamless, interoperable service experiences via Wi-Fi within the global wireless ecosystem. WBA's mission is to enable collaboration between service providers, technology companies, cities, regulators and organizations to achieve that vision. WBA's membership is comprised of major operators, identity providers and leading technology companies across the Wi-Fi ecosystem with the shared vision.

WBA undertakes programs and activities to address business and technical issues, as well as opportunities, for member companies. WBA work areas include standards development, industry guidelines, trials, certification and advocacy. Its key programs include NextGen Wi- Fi, OpenRoaming, 5G, IoT, Testing & Interoperability and Policy & Regulatory Affairs, with member-led Work Groups dedicated to resolving standards and technical issues to promote end-to-end services and accelerate business opportunities.

The WBA Board includes Airties, AT&T, BAI Communications, Boingo Wireless, Broadcom, BT, Cisco Systems, Comcast, Deutsche Telekom AG, Intel, Reliance Jio, Turk Telekom and Viasat. For the complete list of current WBA members, **click here**.

Follow Wireless Broadband Alliance at:

www.twitter.com/wballiance
http://www.facebook.com/WirelessBroadbandAlliance
https://www.linkedin.com/company/wireless-broadband-alliancele

Undertakings and limitation of liability

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement.

In addition, the WBA (and all other organisations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organisations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organisations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third-parties.

CONTENTS

FIGURES

Executive Summary

Enterprises now have the option to expand and increase their wireless coverage density by complementing their IEEE 802.11 based wireless architectures with 3GPP 5G-based systems. The 5G architecture model is a service-oriented system designed for mobile networks. There are various options for fulfilling an enterprise 5G system deployment; it can be deployed through a System Integrator (SI), a mobile operator, a Wi-Fi operator with a cellular partner, potentially a cloud provider or, when the enterprise can leverage its own licensed spectrum, be deployed by the enterprise IT themselves. While the options to enable the basic 5G access connectivity serve as a great starting point, the issues around convergence necessitate a more holistic analysis of how the 5G architecture integrates with the rest of the enterprise systems and processes.

This paper analyses the requirements, use-cases, technical approaches, and challenges for realizing convergence across enterprise private 5G and Wi-Fi access. The stated goal of this convergence is for realizing an access agnostic service layer that enables policies to be enforced for an enterprise user/device across both Wi-Fi and 5G access.

1. Introduction

5G is the fifth-generation communication technology standard for cellular networks. It is an end-to-end system architecture encompassing core network, radio access network, and the new air interface, 5G NR. A significant enhancement delivered in 5G is a switch away from purely targeting deployment by public networks. 5G delivers new capabilities to facilitate deployment in private networks, referred to in 5G as “Non-Public Networks” (NPN).

There is an expectation that 5G will become a key enabling technology for many vertical markets, including manufacturing, mining, public safety, energy & utility, retail, healthcare, smart cities, and enterprise campus. There are some key features in the 5G system that are making it very appealing for private network deployments.

Figure 1: Wireless Applications

ITU has defined three standard 5G service profiles: Massive Machine Type Communications (MMTC), Ultra Reliable Low Latency Communications (URLLC) and enhanced Mobile Broadband (eMBB). The characteristics of these profiles are summarized in Figure 1.

Whereas ITU 5G requirements have helped drive the definition of 5GNR, earlier work from WBA has highlighted how many of the requirements can be met using Wi-Fi 6-based systems, as illustrated in Figure 2.

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 100k bits-per-second) • Variable (non-critical) latency • Limited mobility (particularly with NN-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(50k bits-per-second to 10M bits-per second) • Supports high speed mobility	• Supports at least 100M bits-per-second user rates • Peak data rate of 10 to 20G bits-per-second • High speed mobility of 500km/h • Up to 15 Tbps/km^2 • Downlink and 4Tbps/km^2 • Uplink area traffic capacity

Figure 2: ITU Service Profiles (Source: GSMA)

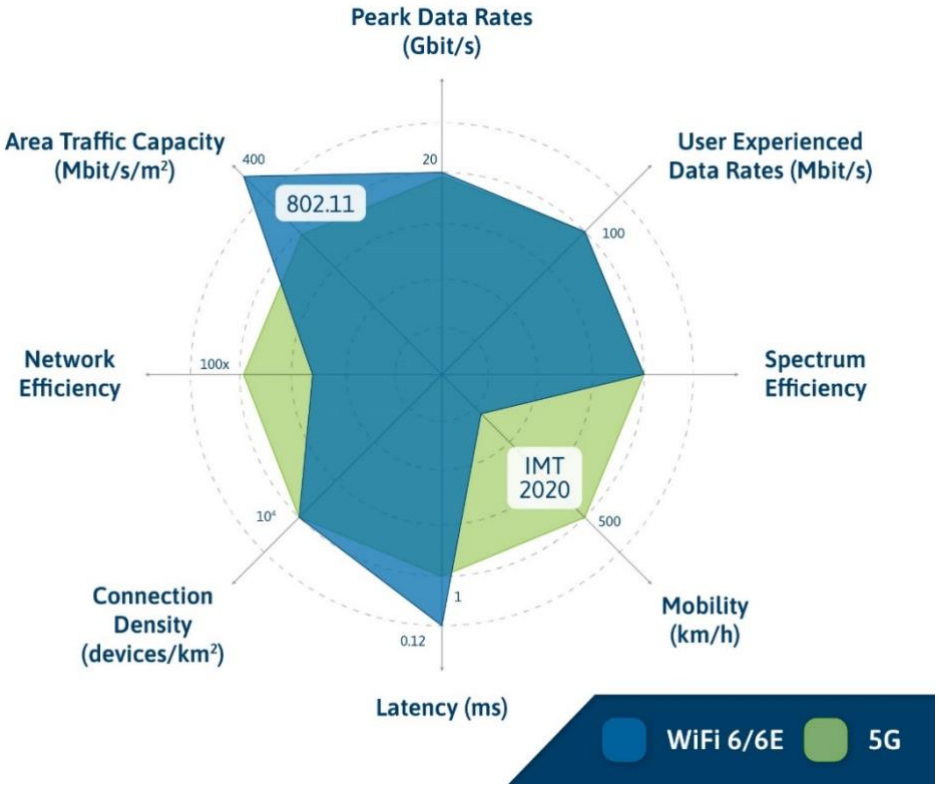


Figure 3: Comparing Wi-Fi 6/6E (802.11) and 5GNR (IMT-2020) Capabilities (Source: WBA)

The 5G service profiles are expected to meet the requirements of most industrial applications and are driving the Wi-Fi 6 and 5G adoption for industrial use-cases.

There are other industry trends which are driving the 5G adoption. The availability of dedicated spectrum, roadmap for a mature device eco-system, and industry investments is making 5G an enterprise-access option. As the manufacturing industry transitions to Industry 4.0 architectures, both 5G and Wi-Fi 6, are showing the promise to meet the factory automation needs.

Many regulatory domains are actively considering enabling private use of cellular spectrum. In the United States there is 150 MHz of allocated spectrum in the 3.5 GHz band (3550-3700 MHz) that has been licensed to facilitate adoption by private networks. Similar approaches to private spectrum allocations are occurring in EU and other regions, which are paving the way for 5G adoption.

Given this larger context, we can reasonably assume that 5G will enter the enterprise realm. 5G is going to be another mainstream access technology incorporated in enterprise architectures. However, with an estimated 628 million Wi-Fi networks in 2023 (source: Cisco), much of the smartphone traffic (74%) still being carried on Wi-Fi networks (source: Ofcom) it is certain that 5G will need to complement and coexist with its equally powerful twin, the Wi-Fi 6. The growing needs of enterprise IT for a robust, secure, high-throughput and reliable connectivity service can potentially be realized with 5G and Wi-Fi 6. This leads to the key question of how can 5G be integrated into existing enterprise architectures? Will it be a “ships in the night” approach with no interworking with Wi-Fi 6 or will there be convergence with Wi-Fi 6 and other enterprise elements for realizing an access agnostic service layer with improved user experience?

This goal of this paper is to describe key use cases, architectural goals, requirements, and technical approaches for Wi-Fi and 5G convergence, while also identifying key gap items that the industry needs to address.

2. Spectrum Availability & Procurement

The primary market driver for Private 5G network adoption is the shift in the policy from regulatory authorities for opening-up spectrum for private / industrial use. This newly available licensed/semi-licensed spectrum can meet the private network goals. Traditionally, the only spectrum available for use by cellular systems was licensed exclusively to Mobile Service Providers with licenses being allocated on an exclusive basis covering a particular geography. The license conditions permit higher transmit powers as there is no possibility of interfering with a neighbouring system using the same channel which is not operated by the same operator.

Moreover, if the licensee does detect any interference from a third party, it can ask the regulator to take enforcement action to remove the cause of the interference. However, there is now spectrum available in various regulatory domains that is licensed based on a non-exclusive and/or regional basis that can be used in deployments of private networks. As the UK regulator describes, the rationale for such was to “enable the deployment of private networks with greater control over security, resilience and reliability”. Table 1 details the available spectrum in different geographies.

Countries/Region	Target Private 5G Spectrum	Band	Power Limits
United States	3.55 – 3.7 GHz (CBRS)	n48, n78	Cat A: 24 dBm, Cat B: 30 dBm
Germany	3.7 - 3.8 GHz	n78	28dBm TRP
Sweden	3.76 – 3.8 GHz	n78	38 dBm TRP per cell
UK	1781.70-1785 MHz 2.39 to 2.40 GHz 3.8 - 4.2 GHz	n3 n40 n77	Lower Power: 24 dBm. Medium Power: 42 dBm
France	2.57-2.62 GHz 3.8 – 4.0 GHz	n38 n77	field limit value of 30 dBµV/m/5 MHz at edge of coverage
Japan	4.6 – 4.9 GHz	n79	
Taiwan	4.8 – 4.9 GHz	n79	

Table 1: Allocation of Spectrum for Private Use

2.1 CBRS Structure & Role of Spectrum Access System

Citizens Broadband Radio Service (CBRS) provides for use of a 150 MHz-wide broadcast band in the 3550 - 3700 MHz frequency range, i.e., Time Division (TD) Long-Term Evolution (LTE) (TD-LTE) band "48." There are three types of users allowed to access this spectrum, including incumbent users, Priority Access License (PAL) users, and General Authorized Access (GAA) users.

The SAS serves to protect incumbents from interference from lower-tier PAL and GAA users and protects PAL users from interference from other PAL and GAA users. The SAS maintains database information of spectrum usage by incumbent, PAL, and GAA users in all census tracts (or areas) and allocates channels to base stations (also referred to as Citizens Broadband Radio Service Devices or "CBSDs") according to a variety of rules.

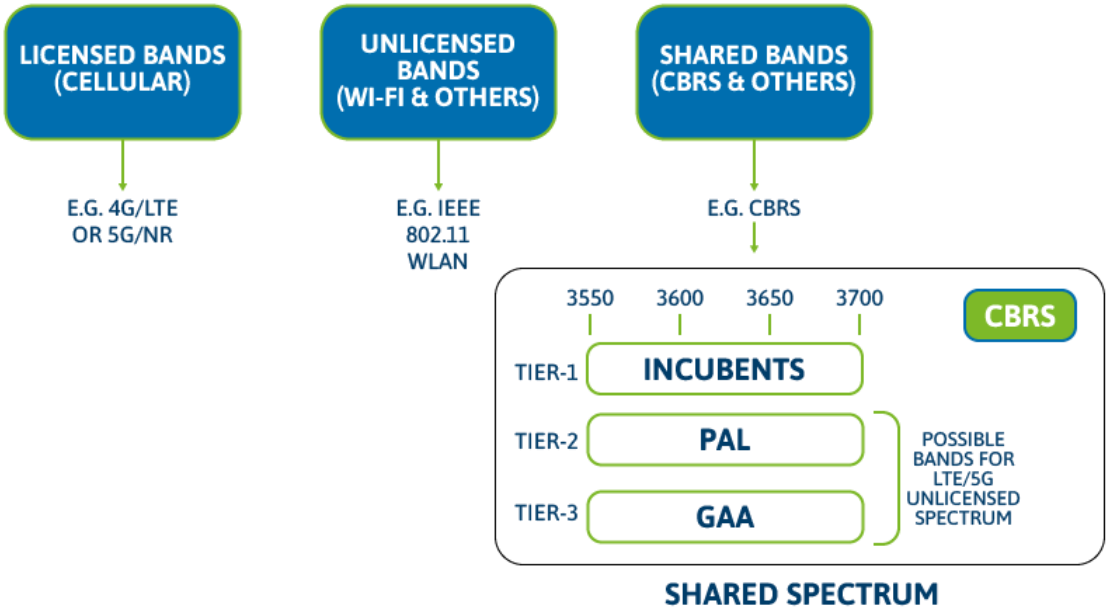


Figure 4: The Three Tier CBRS Structure (Source: Cisco)

For example, a Tier-1 or incumbent users (such as navy ships, military radars, and fixed satellite service earth stations) are allocated access to all the channels at their particular installations. A Tier-2 or PAL users are granted access in the 3550-3650 MHz band and are allowed to use a maximum of seven (7) 10 MHz channels in a census tract (or area). Here, no licensee is allowed to take more than four (4) PAL channels in a census tract. A Tier-3 or GAA users are allowed access to all the channels, but only channels that are not being used by the other above-indicated users.

The SAS makes determinations based on multiple factors and informs CBSDs of allowable operating parameters (e.g., frequency band or channel and maximum Effective Isotropic Radiated Power or "EIRP") that it can use at a given point of time, to ensure compliance with regulations with the Federal Communications Commission (FCC) and other regulatory bodies.

CBRS is one example of radio resource allocations for non-public networks based on spectrum sharing models. There are other spectrum sharing models in other regulatory domains.

2.2 Alternative Shared Access Approaches

Compared with the CBRS-defined SAS approach, other regulators have taken a more incremental approach to licensing spectrum for shared access. Ofcom, based in the UK, charges an annual license fee which starts at £80/year for access to 10 MHz of spectrum, for both low power / medium power licences [REF1]. Each license application form requires the location of the base station antenna to be recorded with a 1 metre accuracy. Information about awarded licenses is available on Ofcom's Spectrum Information System (REF2).

In contrast to Ofcom's approach to license lower power systems on a per base station basis, Germany's Federal Network Agency, BNetzA, allocates licenses based on planned coverage area, with annual license fees calculated as the sum of a variable fee proportional to the required coverage surface area a fixed license fee of €1000 (REF3).

3. Use-Cases

These are some of the leading use-cases for Private 5G and Wi-Fi 6 across Manufacturing, Mining, Venues, Utilities, Healthcare, and other market verticals.

Figure 5: Private 5G & Wi-Fi 6 Applications (Source: Cisco)

4. Deployment Models

There are four possible deployment models for bringing 5G into enterprise networks.

The considerations for choosing a specific model for a given deployment may be based on number of factors, such as the nature of the application, latency on the core network & Radio Access Network (RAN) interfaces, location of the application services and manageability considerations.

The goal here is not to recommend a specific model, but to identify the technical considerations that are at play.

4.1 Core Network & Application Services are On-Prem

In this deployment model, the cellular radio access network (RAN), 5G core network, user-plane elements and application services are on-prem. The UE's (Packet Data Unit) sessions are anchored at the on-prem User Plane Function.

Data sovereignty, site resiliency and application latency requirements are ensured by keeping all traffic on-prem. Access to conventional enterprise cloud-based applications is enabled, subject to normal limitations around resiliency and latency.

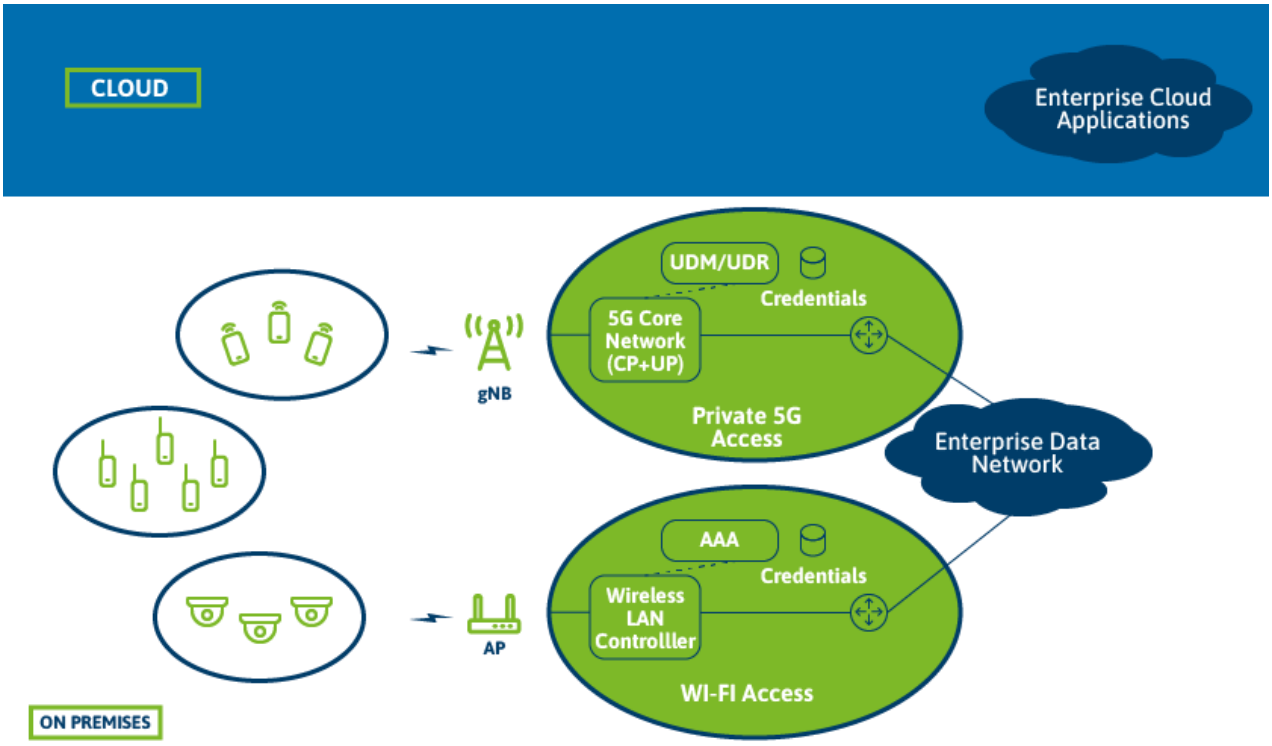


Figure 6: Core Network & Application Services are On-Prem (Source: Cisco)

4.2 User Plane & Application Services are On-Prem

As we shift our focus to the cloud, there are several potentially good reasons to move the control plane to the cloud. One reason could be control plane aggregation in a multi-site 5G core network deployment. All other 5G elements and the application services are on-prem, except the 5G control plane elements.

This approach will not introduce any new latency on the user plane traffic. But there is additional latency on the N4 interface and that may impact the performance of the Packet Forwarding Control Protocol (PFCP); PFCP is the protocol used between the Session Management Function (SMF) and User Plane Function (UPF) over N4 interface.

For example, if the UE is in idle mode, the UPF on detecting a downlink packet will trigger the control plane for activating the paging process. The additional latency introduced on N4 interface may impact the performance of the paging process.

Furthermore, if WAN connectivity is interrupted, access to the cloud-based control plane will be lost and the resulting impact on serving existing devices and new registrations needs to be understood.

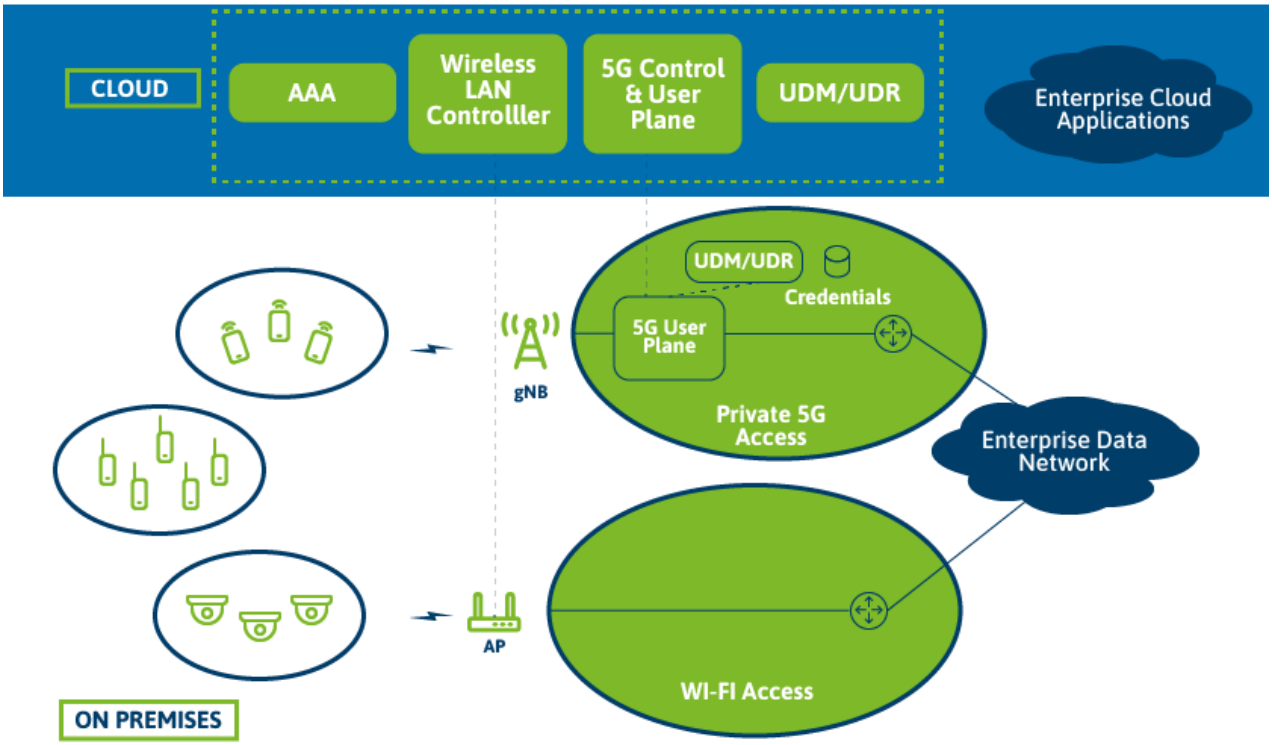


Figure 7: User Plane & Applications are On-Prem (Source: Cisco)

4.3 Core Network & Application Services are in the Cloud

There may be deployments where all the application services are in the cloud. The user plane traffic from the 5G devices will always have to enter the cloud. In such deployment models, it may be possible to move the 5G core network and user plane elements to the cloud where the applications services are located.

If the latency and reliability of the Wide Area Network (WAN) interface used to support the N3 interface meets the application requirements, this may be a reasonable option.

However, for user plane traffic to and from on-prem application services, the traffic takes a zig-zag path. The user plane traffic between the on-prem UE and the on-prem application server will always hit the cloud UPF. All traffic will hit the security firewall and may have to pass through Network Address Translation (NAT) devices. This may be undesirable for some applications.

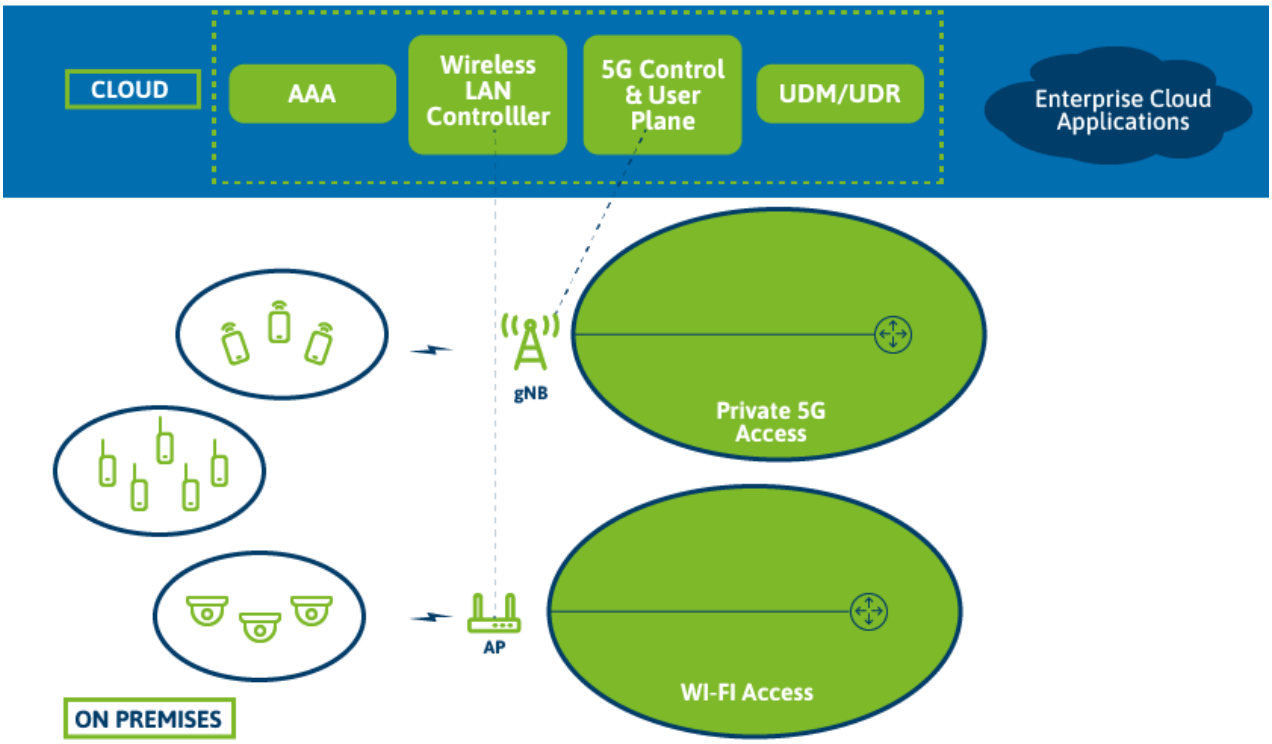


Figure 8: Core Network & Applications in the Cloud (Source: Cisco)

4.4 Hybrid Scenario

The final scenario is a hybrid deployment model. There are some application services in the cloud, and some are on-prem. To support such a model, there can be two different Data Network Names (DNN's), one for supporting applications which are on-prem and another for supporting applications in the cloud. An on-prem UPF will anchor the PDU connections associated with the on-prem DNN, and another UPF in the cloud for the other DNN.

The 5G control plane will push the UE Route Selection Policy (URSP) policy, which will help in application to DNN binding. Applications which require on-prem services will use the local DNN and will use cloud DNN for cloud applications.

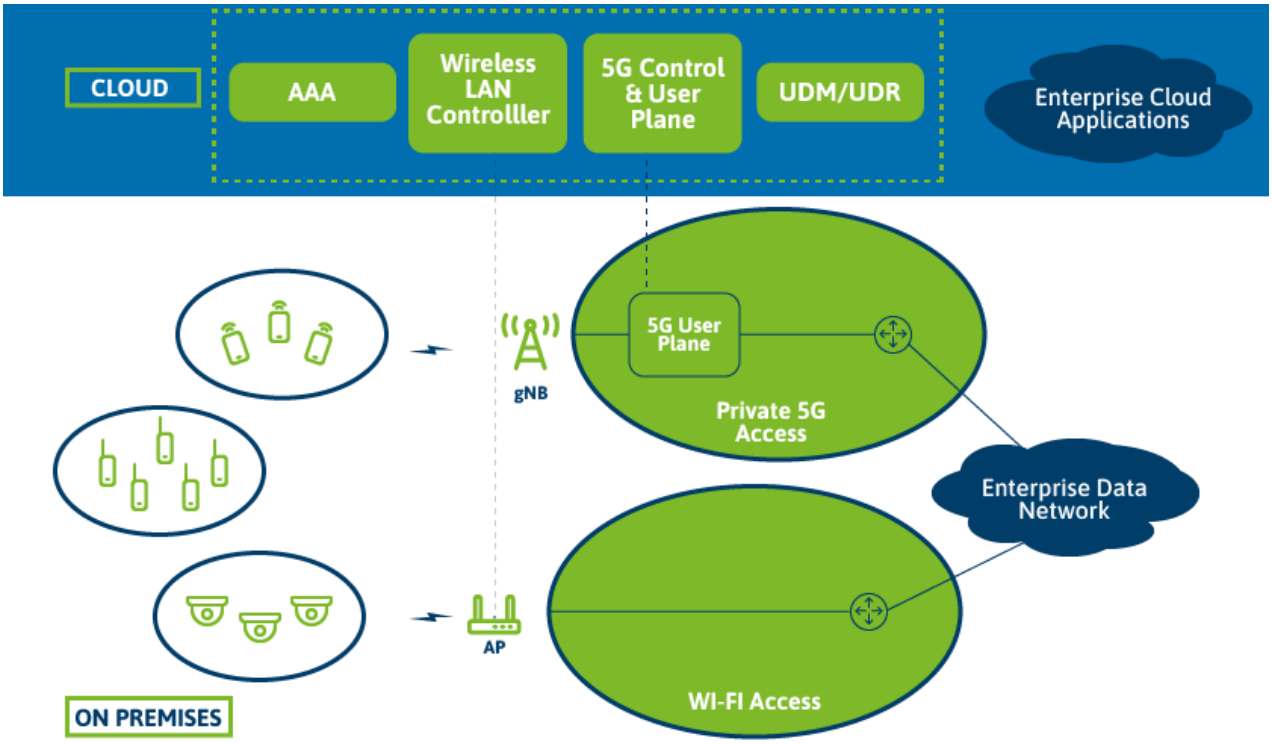


Figure 9: Hybrid Model 9 (Source: Cisco)

5. Enterprise Integration

Enterprises network architectures are very complex and have evolved over a long period of time. These architectures are access-agnostic, supporting Ethernet and Wi-Fi based access technologies. There are existing deployed elements for performing identity, policy, mobility, security, and network management functions.

Figure 10: Enterprise Process Integration (Source: Cisco)

The 5G system encompassing both the RAN and Core Network elements must fit into the above environment.

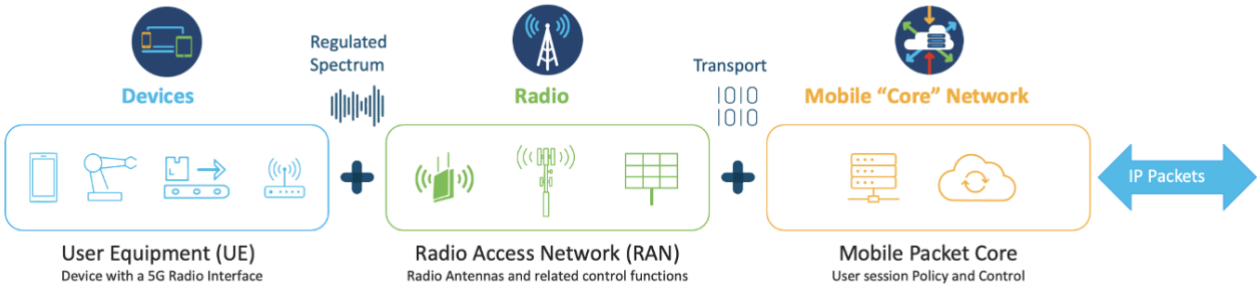


Figure 11: 5G System Architecture (Source: Cisco)

As 5G gets integrated into private enterprise offerings and when these two worlds meet, the question that needs to be answered is what this integration will look like? Will this integration be like ships in the night, resulting in two different identity, policy, routing, mobility, and management domains, or will it be a single service domain?

As private networks based on 5G radio technology make their way into enterprise environments, it would be logical to make private 5G just another access technology. It is a desire for the enterprise IT to have one consistent identity and policy for an enterprise user/device irrespective of the access technology that is in use.

6. Identity & Policy Considerations

Throughout this paper we are documenting the techniques permitting 5G access to private networks, side by side with Wi-Fi access.

The Wi-Fi standards and IEEE 802.1 series in general offer a wide choice of techniques to identify, authenticate and authorize devices (non-Access Point stations - STA) [REF5].

6.1 Identification

As Wi-Fi devices increasingly tend to randomize their link layer address (MAC address) for privacy, device identification has shifted to access-layer credentials, i.e., in the case of 802.1x Extensible Authentication Protocol (EAP) methods a username/password, Public Key Infrastructure (PKI) certificate or cellular International Mobile Subscriber Identity (IMSI).

An attacker posing as the EAP Authenticator can unfortunately catch these permanent credentials when the device does not validate the identity of the network before sharing its credentials. Similar attacks on privacy are possible in 3GPP 5G system.

IMSI is the identity used in the 3GPP EPS architecture. The threats to IMSI Privacy are documented by the Wireless Broadband Alliance's Wi-Fi in REF7, namely in sections 2.1 & 2.2.

Regarding the privacy of the IMSI for Wi-Fi Calling, two levels of protection currently exist for the UE:

1. Avoid revealing the IMSI to the ePDG not having presented a trusted PKI certificate
2. Encrypting the IMSI (EAP Identity) with the Public Key of the trusted PKI certificate presented by the network, providing proof of possession of the matching private key by the network.

For the Evolved Packet System (EPS for 4G and 5G NSA), both protection measures are documented in chapter 3 of REF7.

In the 5G system, Subscription Permanent Identifier (SUPI) is a globally unique 5G subscriber permanent identity that is allocated to each subscriber.

The 5G standard attempts to fix the issue of SUPI leakage by encrypting the permanent identifier (now SUPI) and transmitting the SUCI.

The Subscription Concealed Identifier (SUCI) is a privacy preserving identifier containing the concealed SUPI. Since the encrypted SUCI is re-generated with an ephemeral key for each use, an attacker can no longer derive the user's identity. However, there may be some attack vectors that may allow the leakage of SUCI. For example, the exposure of SUPI to a rogue N3IWF (via 5G AKA over EAP-5G) and/or its IMSI to a rogue ePDG needs further study. Indeed, ePDG interworking with the 5GS is specified as of 3GPP Release 15.

Therefore, in this section we should investigate solutions protecting the end user's permanent identity, either by using a frequently rotating temporary identity, or by avoiding exposure of the permanent identity to rogue identity catchers.

The IPv6 Network Layer (L3) offers new possibilities. For example, IETF RFC 3972 defines Cryptographically Generated IPv6 Addresses (CGA). CGA is an IPv6 address whose interface identifier has been generated according to the CGA generation methods. Contrary to a classic IPv6 address generation schemes where the IPv6 identifier is generated based on EUI-64 of the link-layer identifier, the L3 CGA is independent of the L2 address (MAC address), it can frequently be changed, and could thus ensure privacy even when the MAC address is burnt-in (rather than randomized). An attacker can generate a CGA but cannot spoof a victim's CGA. As such the CGA is a valid self-generated identifier for network layer communication.

A CGA avoids the deployment of a PKI, but the network cannot resist the attack of generating a high number of CGAs, either for a single IPv6 prefix or several.

Other self-generated identities are not only generated in isolation, but also limit the number of valid identities, by imposing a difficulty condition on the shared secret K of an encrypted communication (IPsec, TLS, MACSec…) and/or on the public user identity itself (public D-H value A).

3GPP, IEEE, IETF and other standard bodies are continuously improving security and privacy methods.

6.2 Authentication

With the support for EAP based authentication support on 3GPP and Wi-Fi access, a variety of authentication methods such are now supported. Private 5G support 5G-AKA and EAP-AKA, and similarly various EAP and non-EAP based authentication methods are supported on Wi-Fi access.

6.3 Authorization

The authorization of a network user is the act of limiting the destinations and services which the network makes available to the end user. It involves taking more binary and permanent decisions than policy & charging control (PCC), which is more gradual and temporary.

Whereas Wi-Fi traffic is typically authorized at a rather coarse level in the AP, with additional external firewalls providing the necessary screening, cellular 4G/5G traffic is today more often subject to PCC within the PGW/SMF/UPF.

The authorization of Wi-Fi traffic could become more granular, to be more in line with cellular PCC. Wi-Fi access points themselves are generally not capable of applying L3/L4 Access Control Lists at scale, nor Deep Packet Inspection (DPI) or Heuristic Packet Inspection (HPI).

Therefore, the following two approaches should be compared:

- Data gateways such as the 3GPP N3IWF (with IPsec null encryption) leading to the SMF/UPF, with SMF/UPF performing these DPI/HPI functions
- Stand-alone DPI nodes (3GPP Traffic Detection Function) Wi-Fi Traffic screened, policed, shaped and reported at more granular level, as authorized by either
    - the Wi-Fi AAA system itself (RADIUS/Diameter)
    - a modernized Wi-Fi AAA system using JSON/HTTPS (Service Based Architecture) between AP and AAA API
    - the 3GPP primary authentication (EPS HSS, 5GS AUSF/UDM/UDR) and EPS/PDU session establishment (EPS PGW, 5GS SMF/UPF) if Wi-Fi traffic is guided through the EPC (via S2a/S2b) or 5GC (via ePDG or N3IWF).
    - the 3GPP secondary authentication (EPS SGi AAA server, 5GS DN-AAA server) if Wi-Fi traffic is guided through the EPC PGW or 5GC SMF/UPF

The evolution from RADIUS/Diameter to SBA (with SBI: Service Based Interfaces) would allow Wi-Fi networks to benefit from ongoing investments in 3GPP 5GS AUSF/UDM.

6.4 Leveraging AAA Infrastructure

Compared to 3GPP systems that have conventionally used specialized functions for authentication and authorization, private enterprises typically use generic AAA servers for supporting EAP Server

functionality enabling integration into established identity stores. Importantly, 3GPP release 17 is delivering new capabilities to enable the decoupling of the AAA/EAP server from the specialized 5G functions and as a consequence, enabling a converged AAA/EAP server and identity store that can be used for both Wi-Fi and 5G access systems.

As 5G is integrated into these architectures, it is reasonable to assume enterprises will have the existing means to identify the endpoint and apply a consistent security and QoS policies for that user/device.

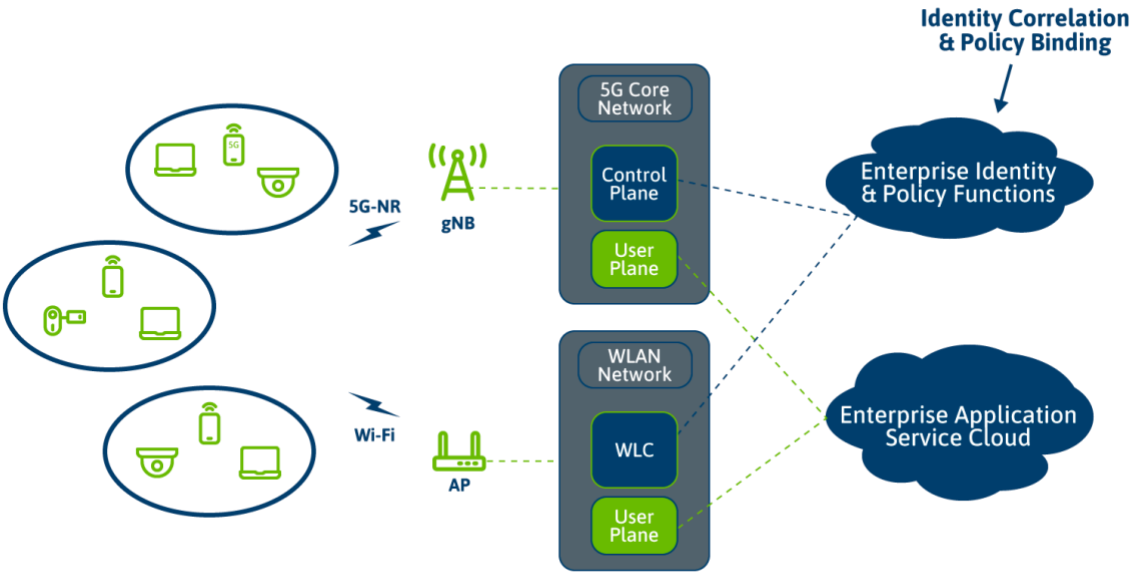


Figure 12: Private 5G and Wi-Fi 6 Network Using a Common Identity & Policy System (Source: Cisco)

The idea of singular identity, policy, and visibility, irrespective of the access technology is the basic essential requirement for integrating private 5G networks into enterprise architectures. Enterprise IT should have the ability to correlate access specific identifiers associated with a device and associate a singular policy profile.

7. IP Mobility Management

7.1 Standalone Private 5G Networks

This approach is more like ships-in-the-night approach. There is no interworking between the two access networks. The UE will have IP addresses configuration on an access basis. The URSP policy on the UE will determine what traffic goes on what access network.

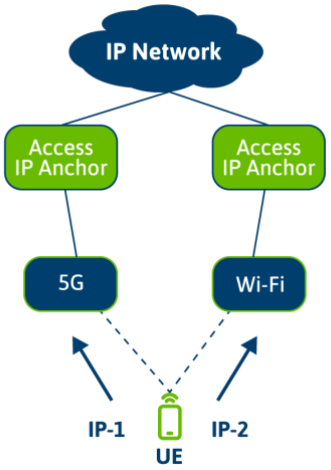


Figure 13: Access-specific Mobility Anchors (Source: Cisco)

7.2 Converged Core Network

In this approach, there is interworking between the two access networks. This interworking can be based on 3GPP defined on non-3GPP interworking interfaces or based on other enterprise specific methods. In one realization the WLC controller in the Wi-Fi access network may interface with the SMF for mobility management. The UE will be able to perform handovers between the two access networks with IP address preservation.

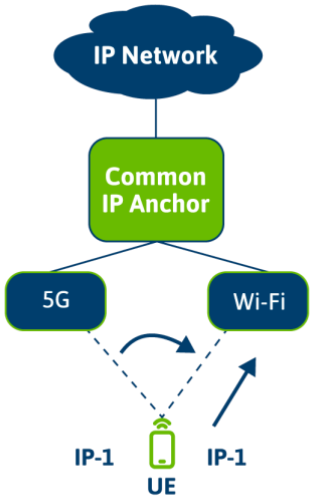


Figure 14: Common Mobility Anchor (Source: Cisco)

7.3 Convergence outside the Access Networks

This approach is similar to the first approach; however, there is convergence outside the access network. In one realization an MP-TCP Proxy, or an MP-QUIC proxy outside the access network may terminate IP sub-flows and allow the UE realize IP mobility.

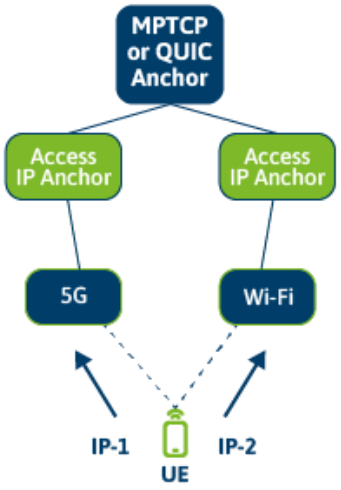


Figure 15: MPTCP / MPQUIC Mobility Anchor (Source: Cisco)

8. Access Traffic Steering, Switching and Splitting & Multipath

Access Traffic Steering, Switching and Splitting (ATSSS) is a defined in Release-16 of the 3GPP architecture. It allows a UE connected to core network over both 3GPP and non-3GPP access to perform traffic steering across both the access connections. The details of ATSSS can be found in 3GPP TS 23.501 specification. An interworking function is used for allowing access to 3GPP core network over a non-3GPP access.

ATSSS functionality has been comprehensively analyzed in WBA's earlier deliverable on 5G and Wi-Fi convergence [REF6]. In particular, ATSSS has been specifically designed for deployment in multi-access environments. Of particular relevance to convergence between private 5G and Wi-Fi is ATSSS' ability to enable Wi-Fi and 5G to be "bonded" into a single "Multi-Access PDU" session and enabling data delivering over both 3GPP and WLAN access simultaneously.

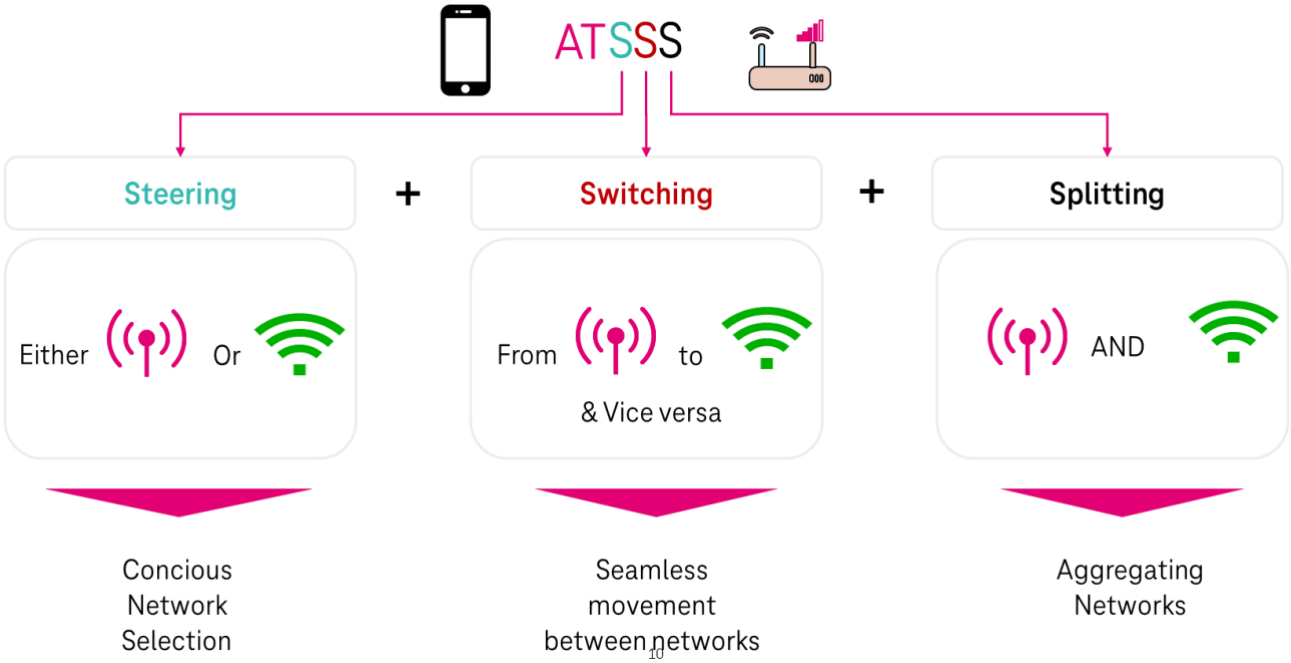


Figure 16: ATSSS Architecture (Source: Telekom Deutschland GmbH)

8.1 ATSSS Value

The value of having ATSSS stems from the long-lasting use of Wi-Fi, where almost all enterprises are using Wi-Fi and evolving it towards Wi-Fi6 and beyond.

1. **Utilizing Wi-Fi infrastructure**: ATSSS allows the use of Wi-Fi infrastructure without jeopardizing the quality of the connection or solely depending on Wi-Fi.

2. **Simultaneous use of 5G and Wi-Fi capacity**: In a private context, having ATSSS allows enterprises to use both 5G and Wi-Fi across their supported devices to increase effective Campus capacity and distribute traffic efficiently.
3. **Improved User experience**: Another key value of ATSSS is to enhance user experience by securing connectivity through times of congestion, as well as transitions between Indoor/outdoor, or when one the connections fail (Wi-Fi or even cellular), being able to connect to the two bearers and use their capabilities interchangeably without manual intervention and sluggish response is of a great value.
4. **Resilience**: Using this technology allows parallel use of cellular and Wi-Fi, letting the unavailability of one of them not leading to loss of connectivity. This becomes highly relevant to mission critical devices, that requires five 9s and beyond.
5. **Campus traffic Engineering**: Having access to both bearers allows distribution of devices and applications across them, making the most out the infrastructure dynamically and according to the conditions.

9. QoS Considerations

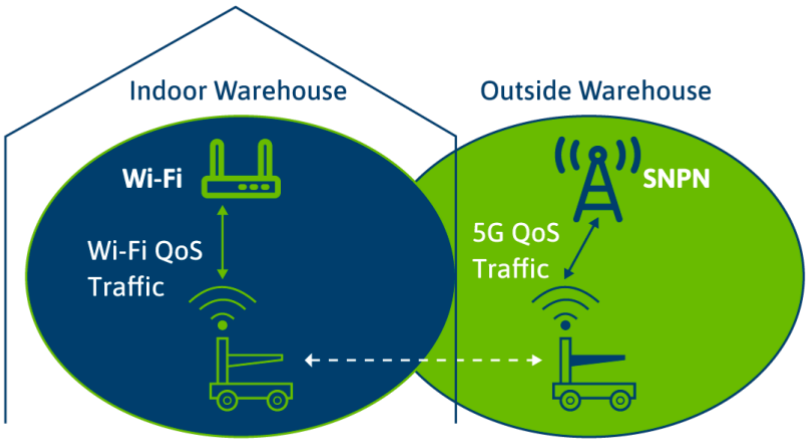


Figure 17: QoS Support in Converged Network

9.1 QoS in 3GPP 5G Access Networks

A private 5G network implements the 5G QoS which is introduced in 3GPP TS 23.501, Section 5.7. In a 5G System the QoS is controlled by the network via SMF. The lowest granularity at which QoS is implemented is the QoS Flow.

Any QoS Flow is characterized by 1) a QoS Profile either preconfigured or provided by the core network to the access, 2) one or more QoS rules and optionally QoS flow level QoS parameters which can be provided to the terminal devices via NAS signaling or deducted in the case of reflective QoS.

The UPF for downlink traffic and the terminal devices for uplink traffic map the service data flows (SDFs) to the QoS flows based on packet filters which are either preconfigured or provided by the 5G Core either at the PDU Session Establishment or dynamically after interaction with various applications (e.g., Voice call setup, etc.) via PDU Session Modification.

The UE classifies and marks the traffic to the associated QoS flows based on QoS rules. Each QoS rule contains the QFI of the associated QoS Flow, a Packet Filter Set and a precedence value.

There are essentially three types of resources associated with QoS flows:

1. Guaranteed bitrate (GBR) QoS Flows, for which there is admission control and the signaled bitrate of the QoS flow is guaranteed,
2. Delay-Critical GBR QoS Flows, introduced as a support for URLLC services, which in addition of providing the guaranteed bit rate, the packets which are delayed above the limit indicated in the Packet Delay Budget are marked as “lost”.
3. Non-Guaranteed Bit rate QoS Flows.

The signaled QoS parameters are:

1. The 5G QoS Indicator (5QI),
2. Allocation and retention priority (ARP) for every QoS Flow and,
3. Guaranteed bit flow rate (GFBR) and maximum bit flow rate (MFBR) for GBR QoS Flows, including Delay-critical ones.

The 5QI, same as QCI in 4G System represents a scalar value that is associated with a set of QoS values. These values are:

1. Packet delay budget (PDB),
2. Packet error rate (PER),
3. Averaging window and
4. Priority.

For Delay-Critical GBR 5QIs the maximum data burst volume (MDBV) is also defined. The 5QI value table is typically updated every Release and it can be found in 3GPP TS 23.501, Section 5.7.4.

We provide a summary of QoS rule interpretation and corresponding parameters in Figure below.

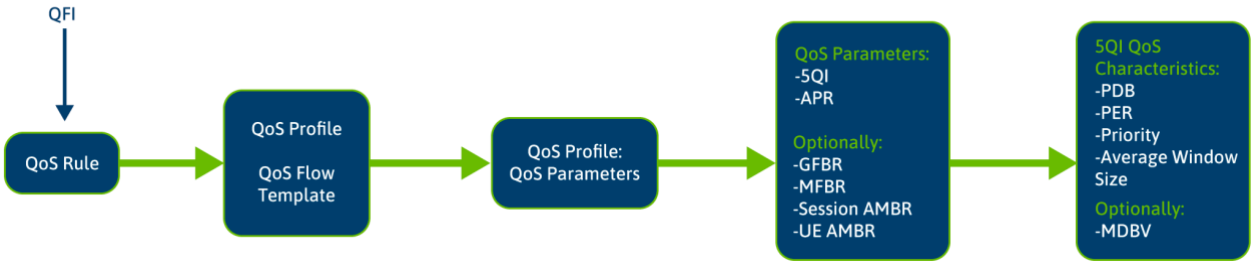


Figure 18: 3GPP 5G QoS Structure

9.2 QoS IEEE 802.11 Access Networks

Wi-Fi has a number of QoS-related work items through IEEE 802.11 [REF5] and WFA.WMM priority media access based on EDCA and supports four QoS access categories voice video, best effort, and background. WMM access categories are the fundamental basis of channel access and transmit for all Wi-Fi generations, including Wi-Fi 6.

WFA and IEEE 802.11 also defined TSPEC to describe the traffic characteristics of flows, but it has not been implemented widely.

WFA also recently released two QoS Management™ certifications in 2020 and 2021. It provides the capabilities for signaling and negotiating QoS requirements between APs and client devices. WFA QoS Management has four key features:

1. Mirrored Stream Classification Service (MSCS): This is simple QoS mechanism. A client negotiates with AP to activate mirroring QoS where client transmits prioritized upstream data packets and AP reflects the same priority for the downstream data packets.
2. Stream Classification Service (SCS): This is mechanism to provide more granular per stream based QoS session establishment and treatment. It also provides QoS supports for 5G child SAs in IPsec tunnels based on the SPIs.
3. DSCP Mapping: Wi-Fi uses a default DSCP-to-UP mapping table, defined in IETF RFC 8325. It also supports non-default QoS mapping to allow network administrators configure their own DSCP-to-UP maps.
4. DSCP Policy: The policies specify DSCP markings based on IP tuples or domain names. Managed Wi-Fi networks may have QoS policies and may request client devices to consider policies when they transmit the uplink data packets for certain flows.

MSCS and SCS are device centric QoS mechanisms where clients initiate the QoS session signaling and negotiation with APs.

DSCP mapping and DCSP Policy are network centric QoS mechanisms supported in QoS Management where network controls the QoS treatment of the flows.

QoS Management features apply to all Wi-Fi generations, and traffic flow prioritization helps Wi-Fi 6 advanced scheduling.

9.3 Identified Gap Items

Followings are the key gap items that are identified, and the industry needs to address in support of private 5G and Wi-Fi networks convergence scenarios.

1. **SCS with exchange of traffic characteristics**

The SCS protocol, as currently supported in "QoS Management" program, enables a STA to establish QoS session based on the IP tuple classification and UP assignment for downlink packets.

We have new emerging applications with relatively deterministic traffic characteristics such as periodicity, max packet size, burst size, delay tolerance etc. and require stringent KPIs.

To support these applications, SCS needs to provide support for parameterized QoS capability where QoS characteristics for a flow can be specified by clients, and APs can use them for better scheduling, resource allocation and QoS treatments.

It is also essential to have such capability in private 5G and Wi-Fi network convergence so that Wi-Fi can support matching 5G QoS attributes when traffic flows move between 5G and Wi-Fi networks.

2. **SCS with 5G QoS mapping table**

SCS currently enables clients to request classification and UP assignment for each IPsec child SA in Wi-Fi access to 5G core network. However, how the STA selects the UP for a given Child SA based on the 5QIs of QoS flows within that Child SA is not defined.

We need a standard based a best-practice mapping table between 3GPP QoS 5QI and Wi-Fi QoS DSCP/UP marking where Wi-Fi can support matching 5QI in private 5G and Wi-Fi network convergence scenarios to ensure consistent behavior.

3. **DSCP Policy Alignment**

DSCP Policy, as defined in Wi-Fi, provides a simple solution assigning a DSCP priority on certain flows based on IP tuples/domain name. For the private 5G and Wi-Fi networks convergence scenarios, it will be important to have consistent matching policies between them as flows move from one network to another one. We need alignment between 5G and Wi-Fi policies and enhance Wi-Fi DSCP policy to handle additional capabilities matching 5G.

10. Application Interfaces

Almost every industry vertical is using location tracking functionalities. Whether it is for manufacturing or logistics, tracking of goods, tools and other moving parts knowing where things are is getting more and more business critical. Today WIFI, BLE, UWB and other combinations of location source data like GNSS has made it easy to adopt the technology. Adding a private 5G network to an

enterprise network, adds also new location telemetry data. 5G & Wi-Fi as access technologies can enrich RTLS processes, especially with massive MIMO, 5G offers very precise location accuracy, taking also into consideration the battery lifetime and consumption.

Figure 19 shows different RTLS systems by location accuracy

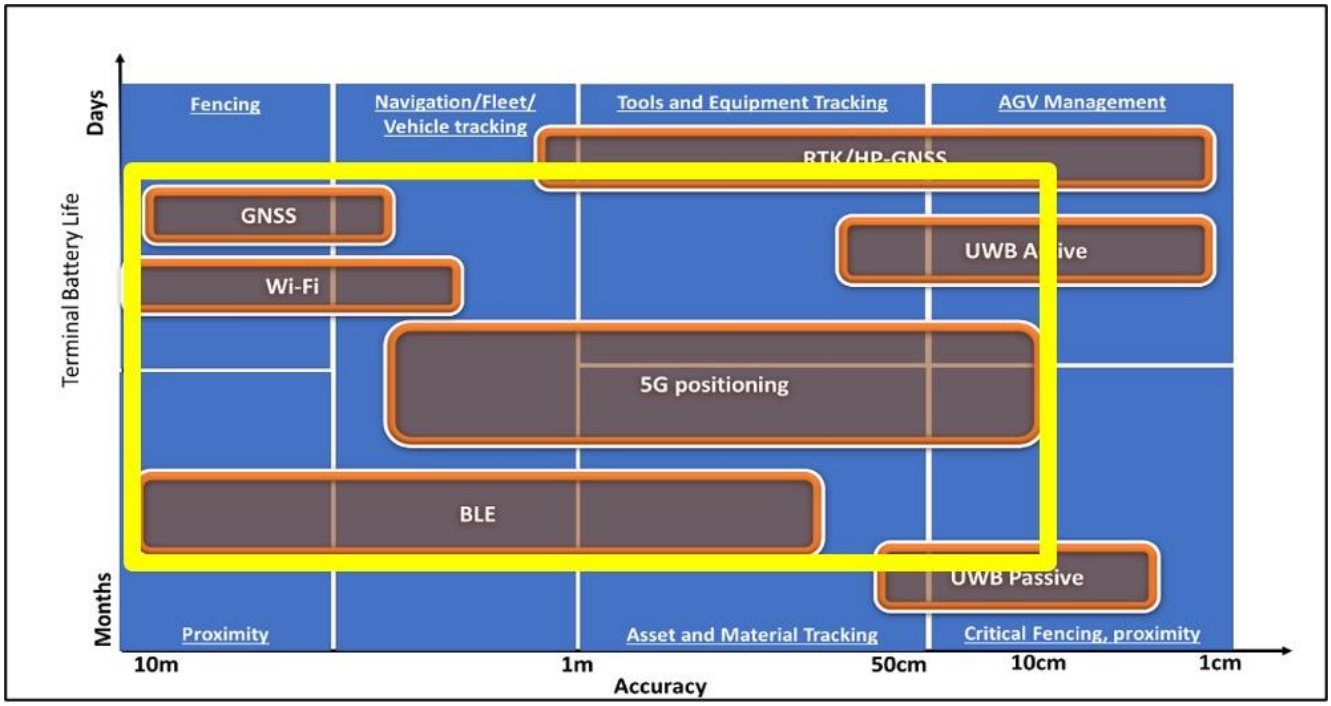
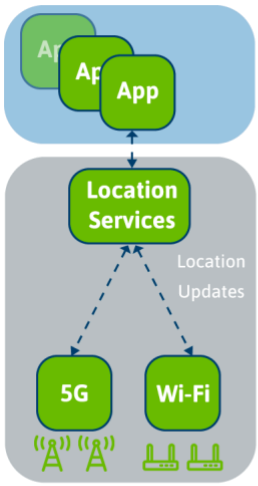


Figure 19: RTLS Systems by Location Accuracy (Source: ABI Research)

1. This is especially interesting for companies who have already implemented business processes which rely on location services systems.
2. This section describes how Wi-Fi, Private 5G, and other services like BLE, GPS and LIDAR can be brought into one data pond.
3. Convergence of Wi-Fi and private 5G location data will happen in a common Data Base. An API will serve as common data pulling or pushing mechanism.
4. The most important aspect of data convergence is to have a common identity management for all the devices which could roam between Wi-Fi and private 5G.

The 5G location telemetry will come from the RAN. The RAN will detect the Angle of Arrival (AoA) and the Direction of Arrival (DoA), the LMF instance will calculate the location telemetry data, and handoff to the common RTLS Data Base.

The location telemetry and the mobility events can be exposed to the management plane for the consumption of the applications. The client location and mobility data can be used for building smart applications and use-cases related to process automation.



5G Events	ELEMENTS
ATTACH	UE Identifier: SUPI, NAI, User-Name, IMEI UE Classification: Device Type, Policy Group
DETACH	UE Location: gNodeB Identifier, 5GC, UPF Identifier Time: Date & Time in UTC
HANDOVER	Geo-Location: gNodeB Identifier, Geo-Loc: {X,Y,Z}, RAT Change
AUTH_COMPLETE	:

Figure 20: Location & Mobility Events (Source: Cisco)

11. Summary & Conclusions

In this whitepaper, we have explored approaches for introducing Private 5G into enterprise wireless architectures.

The paper looked at the industry trends such as changes in regulatory policy around spectrum allocations, device eco-system readiness, Industry 4.0 adoption, which are driving the use of Private 5G for industrial and other market verticals.

Arguments have been made as to why the introduction of private 5G should not result in ships in the night approach, where each of the access system comes with its own gear and operates independently with no interworking. There are benefits in building a converged core, as that simplifies the network architecture and reduces the operational cost with function re-use. While realizing an access agnostic service layer with one identity, policy, and management plane is the ultimate goal, the paper also recognized that the path to realizing such level of convergence has to come in incremental steps, keeping the initial focus on coexistence, and reuse of functions.

The paper also looked at various mobility models including 3GPP defined Wi-Fi & 5G interworking models, and over the top mobility models based on QUIC and MPTCP. The interworking between the access systems for realizing IP address preservation across inter-access handovers can be realized in simpler terms by collocating 5G core network elements with WLAN controller and can be the preferred option for most deployments with existing Wi-Fi footprint.

Finally, the paper looked at the QoS structure, semantics and the setup models supported in Wi-Fi and 5G access networks. There are some differences in the way QoS is supported in each of the access systems; a client-centric QoS model in Wi-Fi access and network-centric QoS model supported in 5G system. These differences expose some gaps which need to be fixed. An Enterprise IT managing the network would prefer to deliver QoS policies in one consistent manner, and with a singular QoS

policy definition. Therefore, there is value in unifying the QoS delivery models, with the ability to translate a QoS policy defined in generic terms to an access specific QoS policy, preserving the intended application behavior and the user-experience. There is work cut out for addressing these gaps.

The WBA Wi-Fi & Private 5G Convergence group will continue to investigate these topics and address the identified gaps for meeting the stated architectural goals.

References

REF1:
https://www.ofcom.org.uk/manage-your-licence/radiocommunication-licences/shared-access

REF2:
https://www.ofcom.org.uk/spectrum/information/spectrum-information-system-sis/spectrum-information-portal

REF3:
https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/Areas/Telecommunications/Companies/TelecomRegulation/FrequencyManagement/FrequencyAssignment/LocalBroadband3,7GHz.pdf

REF4:
Wi-Fi Alliance QoS Management specification 2021

REF5:
IEEE 802.11 Standards 2020
https://standards.ieee.org/ieee/802.11/7028/

REF6:
https://wballiance.com/wp-content/uploads/2021/04/WBA-5G-and-Wi-Fi-RAN-Convergence-Whitepaper-Online-Version-2021-V1.0.pdf

REF7:
IMSI Privacy Protection for Wi-Fi – Technical Specification:
https://wballiance.com/resource/imsi-privacy-protection-for-wi-fi/

Participant list

NAME	COMPANY	ROLE
Florin Baboescu	Broadcom	Project Leader
Sri Gundavelli	Cisco	Project Co-Leader & Chief Editor
Stuart Strickland	HPE Aruba	Project Co-Leader
Thierry Van de Velde	Nokia	Project Co-Leader
Mark Grayson	Cisco	Editorial Team
Gino Corleto	Cisco	Editorial Team
Ahmed Hafez	Deutsche Telekom	Editorial Team
Valerie Parker	Intel	Editorial Team
Wael Guibene	Amazon	Project Participant
Youssef Abdelilah	American Tower Corporation	Project Participant
Jim Sturges	AT&T	Project Participant
Rommel Novo	AT&T	Project Participant
Sudhir Kora	Boingo Wireless	Project Participant
Simon Ringland	BT	Project Participant
Milan Lalovic	BT	Project Participant
Luther Smith	CableLabs	Project Participant
Lili Hervieu	CableLabs	Project Participant
Daniel Easo	CableLabs	Project Participant
Dave Moran	Charter Communications	Project Participant
Loay Kreishan	Charter Communications	Project Participant
Kyle Johnson	Charter Communications	Project Participant
Dez O'Connor	Cisco	Project Participant
Hussain Zaheer Syed	Comcast	Project Participant
Ana Lucia Pinheiro	Comcast	Project Participant
Robert Jaksa	Comcast	Project Participant
Mark Hamilton	CommScope	Project Participant
Jesus Barrios	CommScope	Project Participant

Derrick Smith	Cox Communications	Project Participant
Angelos Mavridis	Deutsche Telekom	Project Participant
Richard Zhou	Google	Project Participant
Ning Zhang	Google	Project Participant
Ingolf Karls	Intel Corporation	Project Participant
Roya Doostnejad	Intel Corporation	Project Participant
Dibakar Das	Intel Corporation	Project Participant
Necati Canpolat	Intel Corporation	Project Participant
Souma Badombena	Intel Corporation	Project Participant
Ravi Sinha	Jio	Project Participant
Yonggang Fang	MediaTek	Project Participant
Max Riegel	Nokia	Project Participant
Bikas Kar	Rakuten Mobile	Project Participant
Rajesh Goyal	Rakuten Mobile	Project Participant
George Hart	Rogers	Project Participant
Betty Cockrell	Single Digits	Project Participant
Kishore Rajasekharuni	STL	Project Participant
Les Goldman	Syniverse	Project Participant
Brendan Malay	Telus	Project Participant
Graham Turnbull	Tessares	Project Participant
Nicolas Keukeleire	Tessares	Project Participant
Troy Cross	Tessares	Project Participant
Bruno Tomas	WBA	Project Participant
Pedro Mouta	WBA	Project Participant