Private 5G & Wi-Fi Convergence

Phase 2 – Technical Considerations

Source: Wireless Broadband Alliance

Authors: 5G Work Group

Issue Date: December 2024

Version: 1.0.0

Status: Public

For other publications, visit our website here

To participate in further projects, contact pmo@wballiance.com

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 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 undertakes programs and activities to address business and technical challenges, while exploring opportunities for its member companies. These initiatives encompass standards development, industry guidelines, trials, certification, and advocacy. Its key programs include NextGen Wi-Fi, OpenRoaming, 5G, IoT, Smart Cities, 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.

Membership in the WBA includes major operators, service providers, enterprises, hardware and software vendors, and other prominent companies that support the ecosystems from around the world. The WBA Board comprises influential organizations such as Airties, AT&T, Boingo Wireless, Boldyn Networks Broadcom, BT, Charter Communications, Cisco Systems, Comcast, HFCL, Intel, Reliance Jio, Telecom Deutschland and Turk Telekom.

For the complete list of current WBA members, click here.

Follow Wireless Broadband Alliance:

www.twitter.com/wballiance

www.facebook.com/WirelessBroadbandAlliance

www.linkedin.com/company/2919934/

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 organizations 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 organizations 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 organizations 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.

Table of Contents

1. Executive summary

Private 5G and Wi-Fi are two key wireless-based access technologies. There is a general estimate that private network operators globally will be spending billions of dollars every year on these two wireless technologies. Although the technical capabilities of these two technologies have largely aligned and there is an arguable level of parity now, these two network architectures by no means are in direct competition.

Technological advancements, with WBA OpenRoaming^{TM}, device localization, Quality of Service (QoS), and other features in Wi-Fi, have effectively bridged these disparities. Nevertheless, distinct characteristics exist, making one technology more suitable than the other for specific use cases and market verticals.

Due to their distinct pricing models, deployment preferences, fulfilling models, cell size/density, and spectrum considerations, these two wireless solutions typically address different use-cases. One may be more suited than the other for certain market verticals. However, in many environments, the coexistence of these networks is also given and there is significant value in realizing synergies between these two technologies. Such synergies will lead to reduced operational costs by the way of elimination of redundant functions, simplified management, and greater end-user experience.

The WBA paper, Private & 5G Convergence (Phase-1), was primarily dedicated to examining the requirements, use cases, technical strategies, and challenges related to the realization of convergence between enterprise private 5G and Wi-Fi access networks. The paper prominently emphasized the goal for convergence: realizing an access agnostic service layer that enables polices to be enforced for an enterprise user/device across both Wi-Fi and 5G access, regardless of whether they are connected via Wi-Fi or 5G access.

This document takes the discussion to the next level by presenting the methods for interworking and for achieving the technical objectives identified in Phase-1.

2. Introduction

The following are the key deliverables for phase 2 of the Wi-Fi and Private 5G convergence efforts.

- Analysis, approaches, and potential solutions related to Wi-Fi and Private 5G convergence in enterprise networks as identified in the previously published white paper.
- Provide deployment guidelines for converged Wi-Fi and 5G deployments in private 5G networks.
- To create liaisons as needed with other standards bodies, including 3GPP and IEEE 802.11 SDOs.
- Explore potential trials for Wi-Fi and 5G convergence in private 5G networks.

3. Architecture Considerations

There are multiple factors to be considered for a 5G and Wi-Fi convergence solution; a few of them are captured below.

3.1 Identity Correlation

Identity correlation involves associating a single, unified identity with a user or a device, regardless of whether they are connected through Wi-Fi or Private 5G. This ensures that users have a consistent experience and can access resources without disruption when switching between networks. This is possible only when the network functions can correlate the respective access-specific identities to a common enterprise identity.

3.2 Singular Policy Enforcement Per User/Device

A common policy across Wi-Fi and Private 5G networks is essential for efficient network management, consistent user experiences, and better resource utilization. Enterprise IT defines policies based on device/user classification and group affiliation. These policies define the QoS prioritizations for different traffic and the enforcement of access controls. Enterprise IT should have the ability to define singular policy for a device/user irrespective of the radio access.

3.3 One Authentication and Policy Function Across Wi-Fi and Private 5G

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. Integration of Private 5G into these networks should not require a parallel set of functions which do the same thing. It is a goal to re-use existing deployed infrastructure elements.

3.4 Service Naming

Wi-Fi and Private 5G networks use different service naming constructs. A common service which is accessible over both Wi-Fi and Private 5G, may have different service identifies and the device will have no awareness of the same. It is important to enable the end point to be made aware of the services names that are used in each of the access systems for all sessions.

3.5 Meta-Data Tagging on User Plane Traffic

Service Functions are extensively deployed in most networks, and they provide a range of features. These service functions do not have the visibility into the identity/policy associated with a packet/flow. There is value in building interworking between these service functions and the network elements in the Wi-Fi and Private networks. This interworking can be in the form of meta-data exchange on the service node where classification and policy binding is performed.

3.6 Exchange of Device Connectivity Status

Device authentication/connectivity status or location in one access network, when exchanged with the other access network can be useful for realizing many of the signalling optimizations.

4. RADIUS Extensions for 5G Device Authentication

Authentication and key management are critical for ensuring secure communication within the access network. These mechanisms enable mutual authentication between the device and the access network, verifying identities and establishing trust. By validating the identities of both parties, these procedures ensure that only authorized devices can access the network. Additionally, these procedures derive cryptographic keys that safeguard both signalling and user plane data. By doing so, they protect the integrity and confidentiality of the transmitted information, preventing unauthorized access and maintaining a secure communication environment within cellular networks.

3GPP 5G System architecture has defined support for different authentication methods - 5G AKA, EAP AKA' and EAP TLS and EAP TTLS. The 5G system defines a new service-based architecture together with new network elements (e.g., Authentication Server Function (AUSF), Unified Data Management (UDM)) to support these authentication methods. Appendix A shows signalling exchanges associated with 5G registration between the 5G network functions and the AUSF and UDM.

Integrating this authentication method into RADIUS allows network operators to leverage existing RADIUS infrastructure for user authentication and authorization in enterprise 5G deployments. This document defines new RADIUS attributes to support the 5G-AKA procedure, enabling interoperability between RADIUS servers and 5G network elements.

4.1 Access Architectures

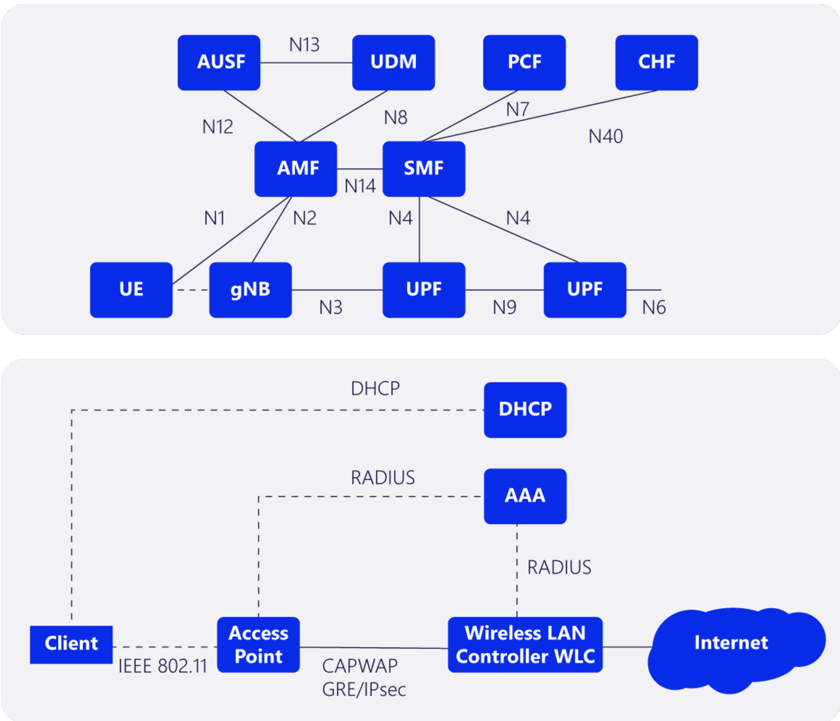


Figure 1 - Access Architectures

Use-Case:

Enterprises can expand and enhance their wireless coverage density by complementing their existing IEEE 802.11-based wireless architectures with 3GPP-based 5G access networks.

There are multiple deployment options available for implementing an enterprise 5G system. It can be deployed through a System Integrator (SI), a mobile operator, a Wi-Fi operator in collaboration with a cellular provider, potentially a cloud provider, or by the enterprise IT themselves if they can access 5G spectrum. While these options provide a strong foundation for enabling basic 5G access connectivity, there is considerable value in achieving convergence across these diverse access architectures and leveraging the already deployed network elements. It is highly desirable for enterprise IT to possess the capability to correlate identities across different access technologies and enforce consistent enterprise policies.

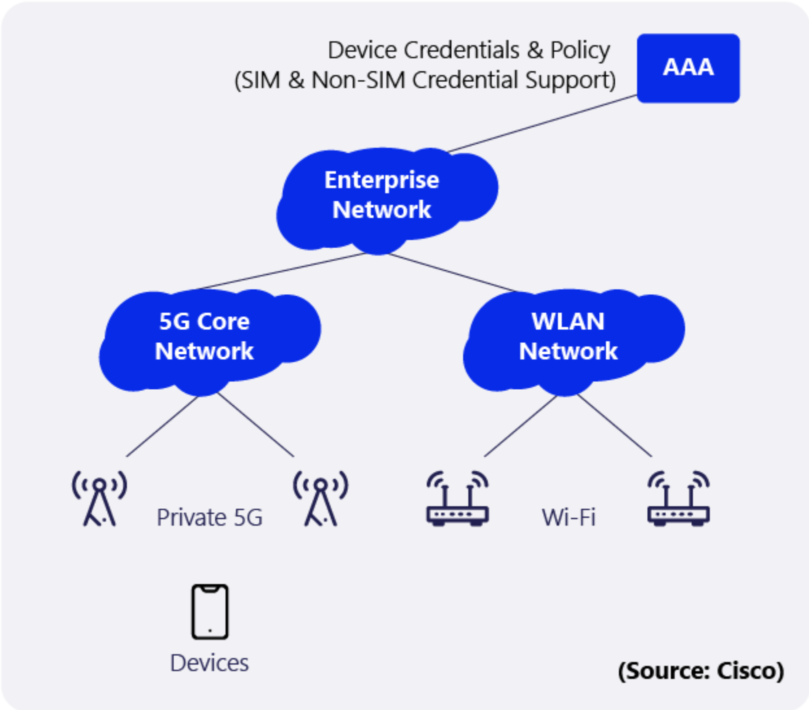


Figure 2 - Enterprise Network

Enterprise network architectures have undergone extensive evolution over an extended period, resulting in intricate structures. These architectures are designed to be technology-agnostic, accommodating both Ethernet and Wi-Fi-based connections seamlessly. RADIUS-based infrastructure is widely employed for authentication and policy management purposes. As 5G-based private networks become integrated into enterprise environments, it is a natural progression to consider private 5G as another access technology, allowing the utilization of the existing RADIUS infrastructure to authenticate 5G devices. The adoption of a unified authentication and policy infrastructure across different access technologies enables the realization of identity correlation and ensures consistent policy enforcement.

We therefore put forward proposals for extending the RADIUS protocol to support the 5G-AKA authentication method.

Figure 3 - 5G Device Authentication Based on AUSF/UDM Interfaces

Figure 4 - 5G Device Authentication Based on RADIUS Interfaces

In the proposed approach, the RADIUS server will implement the 5G-AKA algorithm. Furthermore, it is assumed that as this is a private 5G deployment, there are no requirements to support inter-operator roaming.

4.2 5G-AKA with AAA

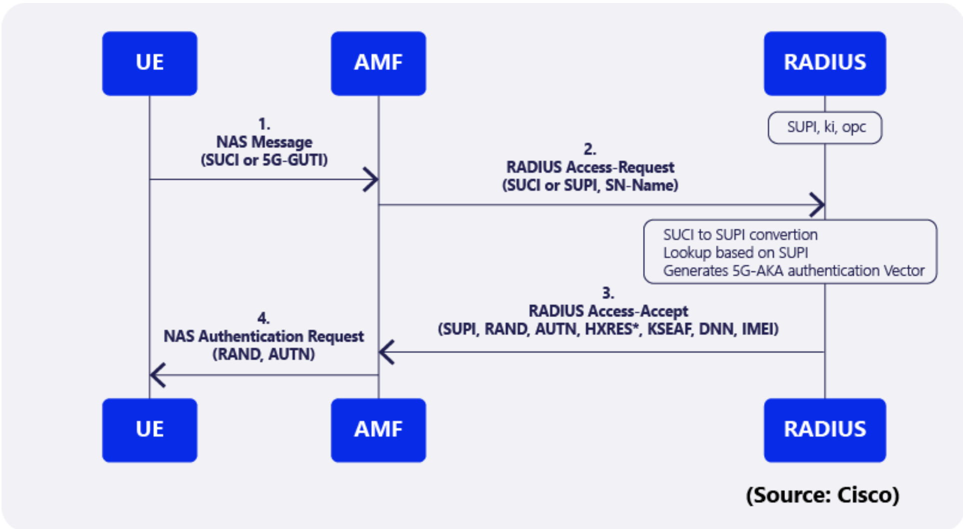


Figure 5 - 5G-AKA with AAA

In the proposed approach, the RADIUS server will be the primary authentication function. Following are the interactions between the 5G system and the RADIUS Server.

- Step-1: User Equipment (UE) Sends the Non-Access Stratum (NAS) Registration Request message to the Access and Mobility Management Function (AMF) which includes Subscriber Concealed Identifier (SUCI) or 5G-GUTI (Global Unique AMF ID).
- Step-2: AMF creates a RADIUS Access-Request message, which includes the RADIUS User-Name attribute that contains the 5G subscriber identifier in format SUCI or Subscriber Permanent Identifier (SUPI) and the RADIUS 5G-SN-NAME attribute that identifies the serving network name.
- Step-3: Once the RADIUS server receives the request it converts the SUCI to SUPI using Subscription Identifier De-Concealing Function (SIDF). The RADIUS server consults the database of users to find the user whose name matches with SUPI in the request. This is equivalent to the

Authentication Credential Repository and Processing Function (ARPF) in the Unified Data Management (UDM). The RADIUS server generates an Authentication Vector using the 5G-AKA algorithm. This vector consists of RAND, AUTN, HXRES* and KAUSF parameters. The AUSF function takes KAUSF and generates KSEAF. The RADIUS server responds with a RADIUS Access-

Accept message containing authentication vector attributes 5G-Auth-RAND, 5G-Auth-AUTN, 5G-Auth-HXRES-STAR, 5G-Auth-KSEAF, 3GPP-IMSI, 5G-DNN, 3GPP-IMEISV. All key derivations for 5G-AKA shall be performed using the key derivation function (KDF) specified in Annex B.2.0 of TS 33.220.

On successful lookup of 5G subscriber identity in the database and calculation of resulting 5G-AKA authentication vector, the RADIUS server sends Access-Accept message that contains the resulting authentication vector in 5G authentication RADIUS attributes specified in section 6 of this document.

If the RADIUS server fails to execute one or more operations, it sends a RADIUS Access-Reject message indicating that 5G-AKA authentication failed.

Note-1: The RADIUS server must be provided with the 128-bit long K and the 128-bit long OPC 5G-AKA parameters per subscriber identity SUPI to perform authentication vector calculations according to 5G-AKA algorithm.

Note-2: The RADIUS server must be provided with the SQN-HN parameter that represents a 48-bits long sequence number. The initial value of SQN-HN for 5G subscriber should be 1. The SQN-HN parameter is increased on every 5G-AKA authentication for the specific 5G subscriber and when it reaches 0x7FFFFFFFFFFF it is rolled over to 1 as specified in TS 33.102 section C.3.2

4.3 RADIUS Attributes Used for 5G AKA Authentication Support

NAME	TYPE	DESCRIPTION
5G-Auth-RAND	String	Random number part of the authentication vector.
5G-Auth-AUTN	String	Authentication token part of the authentica-tion vector.
5G-Auth-HXRES-STAR	String	It is a hash expected response which is part of the authentication vector.
5G-Auth-KSEAF	String	Security anchor key used to derive KAMF key.
5G-SN-NAME	String	Network Identifier includes PLMN and NID.
5G-Auth-RAND	String	Value of authentication token used for resync.
5G-DNN	String	5G Construct for service name.

(Source: Cisco)

Figure 6 - RADIUS Attributes Used for 5G AKA Authentication Support

ARPF (Authentication Credential Repository for Procession Function)

ARPF is part of UDM as per the standard. ARPF contains subscriber credentials, i.e. long term keys and Subscriber Identifier (SUPI). Subscriber credentials may alternatively be stored in UDR [TS23003].

AMF (Access and Mobility Management Function)

The AMF is a control plane function in the visited network. It is UE responsible for providing registration (authentication and authorization) services as well as connectivity and mobility management services.

AUSF (Authentication Server Function)

It is standalone NF located in subscriber's home network. It is handling authentication in home network based on information received from UE and UDM/ARPF

SEAF (Security Anchor Function)

SEAF is functionality provided by the AMF It is handling authentication in serving network based on information received from UE and AUSF.

SIDF (Subscriber Identifier De-Concealing Function)

SIDF is a service offered by UDM in home network. It is responsible for resolving the SUPI from the SUCI.

UDM (Unified Data Management)

UDM is responsible for managing all user data. In 5G UE is authenticated by home network (AUSF) and serving network (SEAF).

5. Wi-Fi Fast Transition Domain to Include Private 5G

As we move closer towards Private 5G commercial deployments, enterprises will be seen deploying Private 5G and Wi-Fi in different configurations. For example, deployment of P5G in outdoor parking lots and Wi-Fi indoors is one such example configuration. It is reasonable to assume that both these radio technologies will co-exist in many deployments for providing blanket coverage with no gaps; furthermore, there will be interworking between the control plane elements of these access networks with a unified policy layer and for delivering better user experience.

When the UE moves to Wi-Fi access from 3GPP access, the UE first must establish 802.11 open authentication and association, followed by 802.1x authentication and then followed by a 4-way handshake to derive the encryption keys. The described steps involve the exchange of multiple messages between UE and the network, and results in latency before the Wi-Fi link is usable.

There is clearly a desire and opportunity to optimize the connection establishment to Wi-Fi access, by leveraging the already existing key material from the UE's authentication to the network over Private 3GPP access.

There is value in standardizing approaches for bootstrapping keys on Wi-Fi access based on the key material generated from the 5G access authentication. This helps in reducing number of messages exchanged during the initial attach.

Proposed is a method and technique for leveraging session keys generated in 3GPP access (5G/LTE) and leveraging 802.11r capability of Wi-Fi infrastructure to derive the Fast Roaming (FT) Keys, as the user moves from private 3GPP access to Wi-Fi access. This technique results in drastic reduction of connection establishment time to Wi-Fi access (upwards of 90% reduction in connection time). This is a significant gain for latency sensitive applications (Ex: URLLC, Industrial IOT, Video, AR/VR, Cloud Gaming) and thereby greatly improving the real-time application experience in enterprise networks.

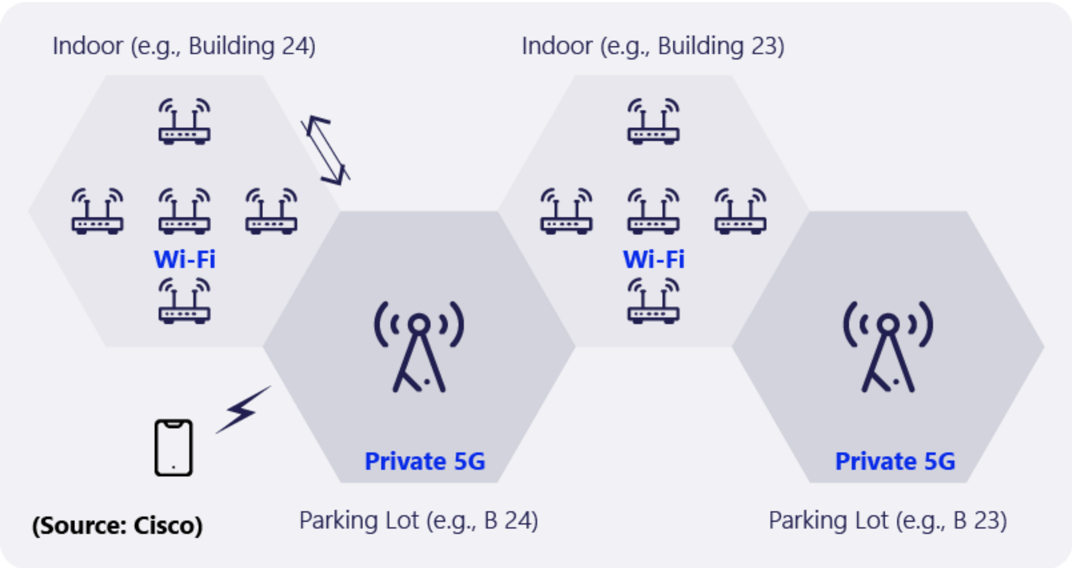


Figure 7 - Fast Transition

The 802.11r designed for fast roaming is well known and widely implemented on smartphones as well as on the infrastructure elements. The scope of the mobility domain is limited to Wi-Fi access points. By maintaining proximity relation between 5G and Wi-Fi radios, it is possible to proactively set up the key states on the APs that are in close proximity to 5G access.

We describe two methods using which UE uses 3GPP generated Session Keys as seed to generate FT hierarchical keys that can be used with Wi-Fi access. One of the methods (Approach#1) is tied to PDU Secondary authentication resulting in a completely new set of claims, and the other method is tied to primary authentication.

In both methods, any form of Primary authentication method can be used (SIM - 5G-AKA, EAP-AKA or Non-SIM based like EAP-TLS, EAP-TTLS). This enables the UE to leverage the 11r messaging to associate to Wi-Fi access network resulting in massive reduction of connection establishment time.

5.1 Fast Transition to Wi-Fi from 3GPP Access – Approach#1

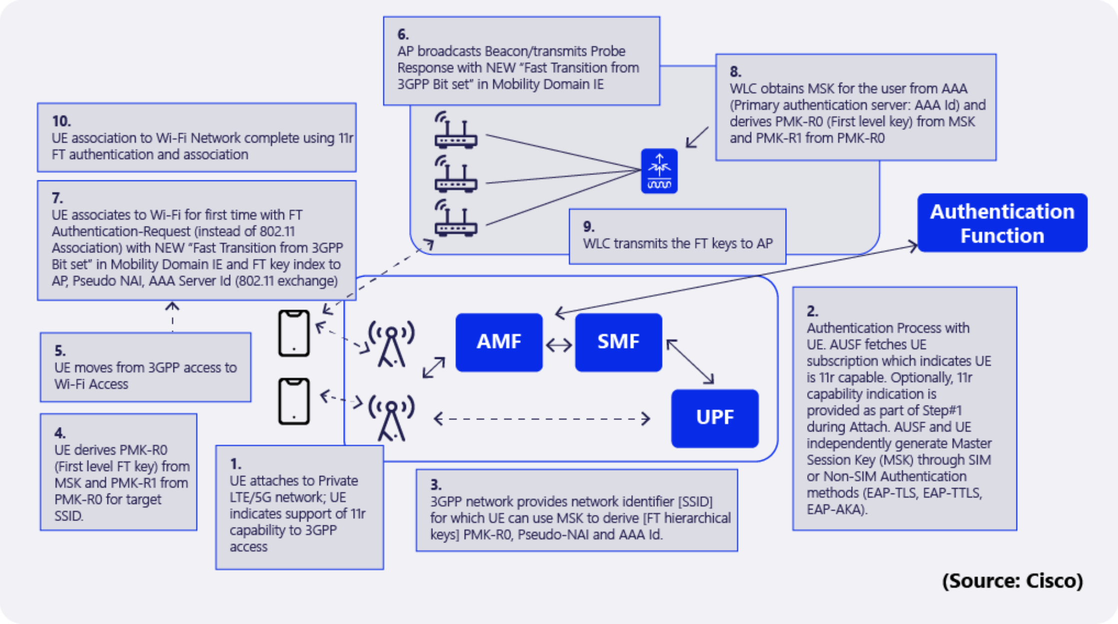


Figure 8 - Fast Transition to Wi-Fi from 3GPP Access – Approach#1

5.2 Fast Transition to Wi-Fi from 3GPP Access – Approach#2

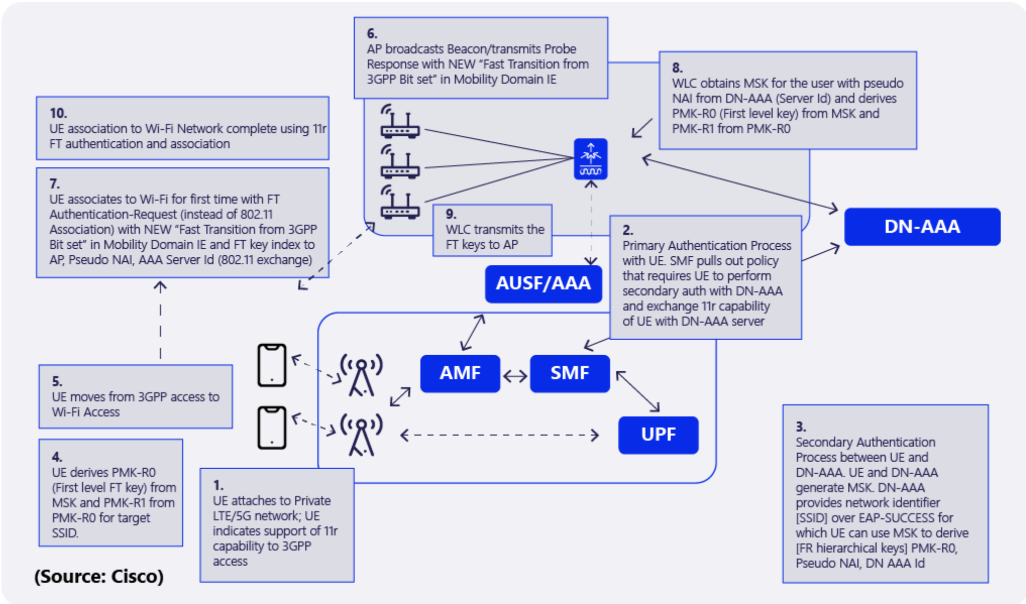
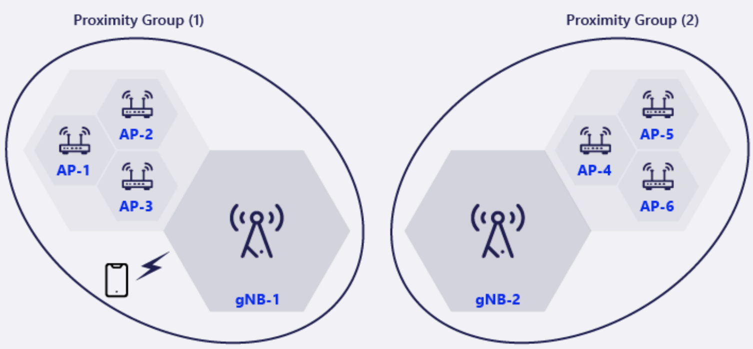


Figure 9 - Fast Transition to Wi-Fi from 3GPP Access – Approach#2

5.3 Proximity Relationships Between Wi-Fi and P5G

Network maintains proximity relation between Wi-Fi APs and 5G gNB. The management plane in the network configures these relationships. For extending FT domain to include both P5G and Wi-Fi access points, these proximity relationships will be essential for key bootstrapping.



5G NODE	NEIGHBOR WI-FI APS
gNB-1	AP-1, AP-2, AP-3 (Proximity Group 1)
gNB-2	AP-4, AP-5, AP-6 (Proximity Group 2)

(Source: Cisco)

Figure 10 - Proximity Relationships between Wi-Fi and P5G

Summary:

The 802.11r designed for fast roaming is well known and widely implemented on smartphones as well as on the infrastructure elements. The scope of the mobility domain is limited to Wi-Fi access points.

There is value in standardizing approaches for bootstrapping keys on Wi-Fi access based on the key material generated from the 5G access authentication. This helps in reducing number of messages exchanged during the initial attach.

Furthermore, by maintaining proximity relation between 5G and Wi-Fi radios, it is possible to proactively set up the key states on the APs that are near 5G access.

6. Indication of Identical Service on Other RAT

The network will maintain a mapping of Service Name/Network Identifier in one access, with the corresponding identifiers in the other access. Both the Wi-Fi and Private 5G access networks have awareness of these service mappings.

As part of the UE's initial attachment to Wi-Fi access, the Wi-Fi network will send the corresponding Service Name/Network Identifier for the 5G access to the UE. Alternatively, the network can send these identifiers in the 802.11 beacon frame along with the SSID, as 802.11 Probe Request/Response, or using other access protocols.

A UE performing initial attachment to 5G access and upon activating a Packet Data Unit (PDU) session for a given Single – Network Slice Selection Assistance Information (S-NSSAI) / Data Network Name (DNN) / Public Land Mobile Network Identifier (PLMN-ID), the 5G network can send the corresponding identifiers for the Wi-Fi access to the UE as Protocol Configuration Option (PCO) option, or through other protocols.

A service token identifying the service can also be provided to the client, which it can present to the network over the other access. Various other protocols including Dynamic Host Configuration Protocol (DHCP), Domain Name Server (DNS), 802.11/5G access protocols and Security Protocols can be used for delivering this "Identical-Service Availability over other RAT" mapping information to the client.

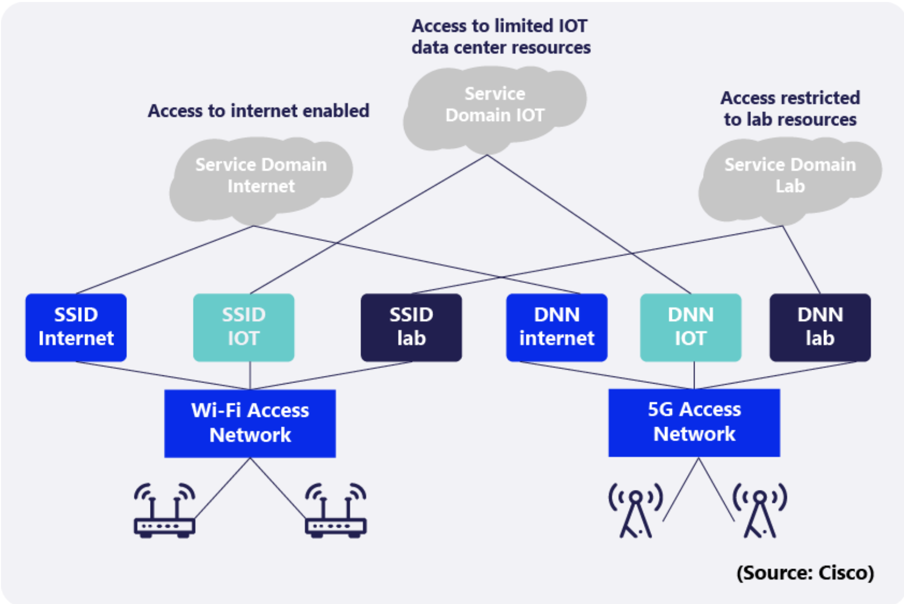


Figure 11 - Indication of Identical Service on Other RAT

There should be a mapping of Service identifiers / Network Identifiers in one RAT with the corresponding identifiers in the other RAT.

- Network should be able to notify the UE about the availability of the other RAT for accessing the same service domain.
- It should be able to provide the Service Name/Network Identifier for the other RAT, or a service token for that service that the UE can use for the lookup.
- Trigger for notifications a.) Initial Attach, b.) Bad Radio Conditions for the client in the current RAT, c.) Network Maintenance of the current RAT, d.) Load Distribution

Service Name / Network Identifier (Wi-Fi)	Service Policy	Data Plane Identifiers	Service Name / Network Identifier (5G))	Service Token
Blizzard	Internet, Engineering Resources; VoIP, Data Center	L2-VNID-1, L3-VNID-1	PLUM Id: 315-010, DNN: blizzard.com	0xabcafede
Lab	Lab, No Internet	L2-VNID-2, L3-VNID-2	PLUM Id: 315-010, DNN: cisco-lab.com	0xbababababa
Guest	Internet, no other access	L2-VNID-3, L3-VNID-3	PLUM Id: 315-010, DNN: guest.com	0xaaaaafood

(Source: Cisco)

Figure 12 - Mapping of Identifiers

7. IP Address Preservations & Seamless Mobility

7.1 Access Specific IP Anchor

A multi-access capable UE will be able to attach to both Wi-Fi and Private 5G access networks and have distinct IP address configuration on an access basis. Application-binding to access is based on the UE policy. Ships-in-the night approach.

1. UE is dual-radio capable, attaches to both Wi-Fi & 5G.
2. The IP anchor for the 5G access is the Userplane Function (UPF). The IP anchor for the Wi-Fi access is typically the Wireless LAN Controller (WLC).
3. Applications based on the device policy will perform the access selection.
4. Fail-over of one access will result in application switch-over to other access with session discontinuity.
5. There is no IP address preservation, or Session Continuity.

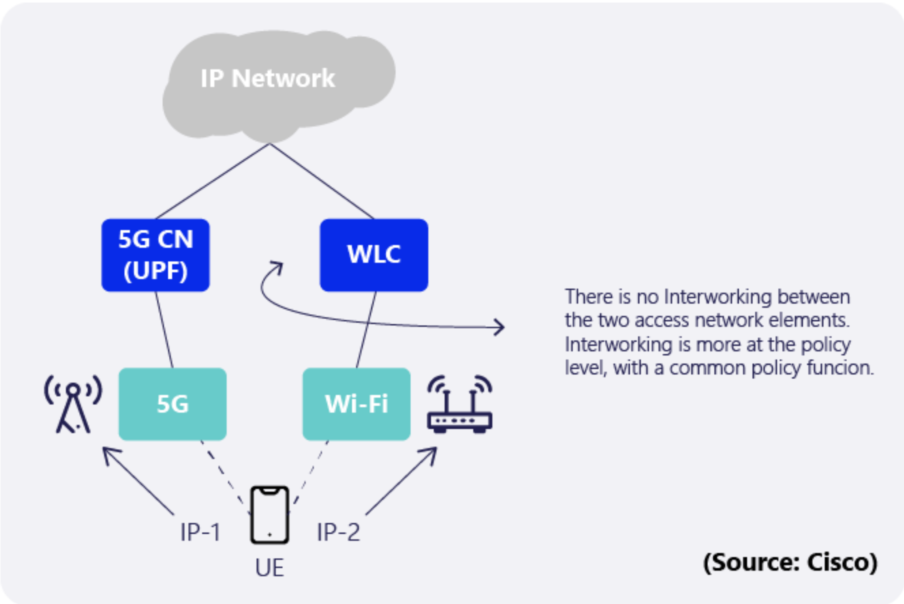


Figure 13 - Access Specific IP Anchor

7.2 3GPP Interworking Approaches

3GPP has defined interfaces for integrating WLAN access into 5G core. There are two models of interworking a.) Trusted and b.) Untrusted Non-3GPP Access.

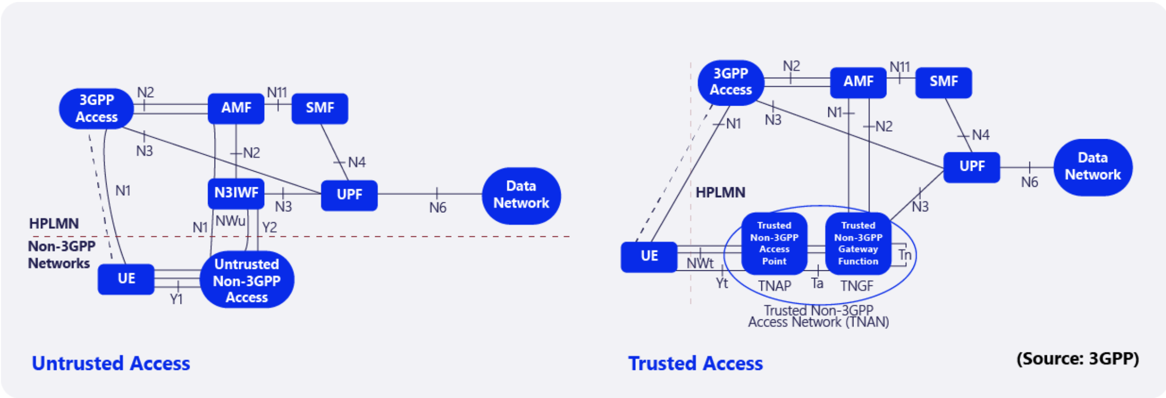


Figure 14 - 3GPP Interworking Approaches

Requiring IPsec gateway nodes in a converged Wi-Fi and Private 5G networks is an expensive proposition and does not make business sense. The complexity it brings in the form of extra node and IPsec + IKE scale requirement makes the case for a non-3GPP approach for interworking.

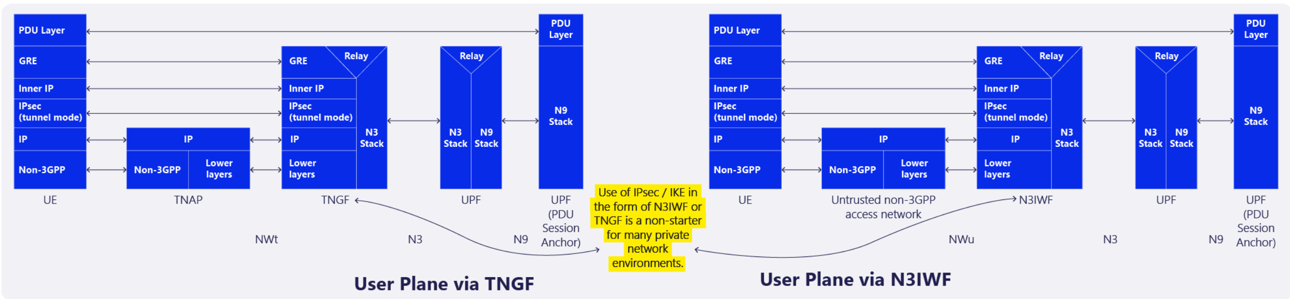


Figure 15 – User Plane protocol stack

7.3 Alternative Approach

What is required is a much simpler approach. Methods that do not require Non-3GPP Interworking Function (N3IWF) / Trusted Non-3GPP Gateway Function (TNGF) type elements, or the need for extending the NAS over Wi-Fi. These approaches do not assume the UPF as the IP aggregation point across Wi-Fi and P5G.

1. There is a common IP anchor for the UE's IP session, and the approach is implementation dependent.
2. Network ensures, UE is given the same address configuration for both the access connections.
3. There is IP address preservation and possibly seamless mobility based on UE capability.
4. Logical interface support (RFC 7847) on the UE stack will ensure seamless mobility.

5. UE can use single/dual Tx/Rx for UL traffic, based on the mode.

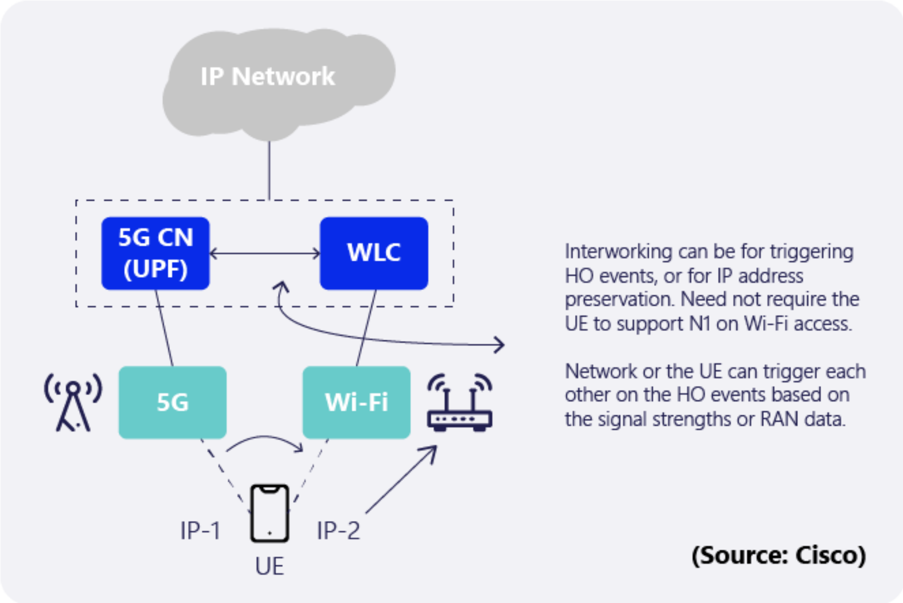


Figure 16 - Alternative approach for interworking

8. Meta-Data Tagging on User Plane Traffic

Enterprise systems manage policies at a group level. These policies can be based on the device type, device identity, user identity, group affiliation or other elements.

The policy can be a simple access control for permitting / denying access to a given network / service, or it could be about the selection of the service chain the packet needs be routed through. The meta-data can be SGT (Secure Group Tag), or specific identifiers that allow the enforcement node to apply identifier-based policies.

In a converged P5G / Wi-Fi network, enterprise should have the control these aspects on consistent manner.

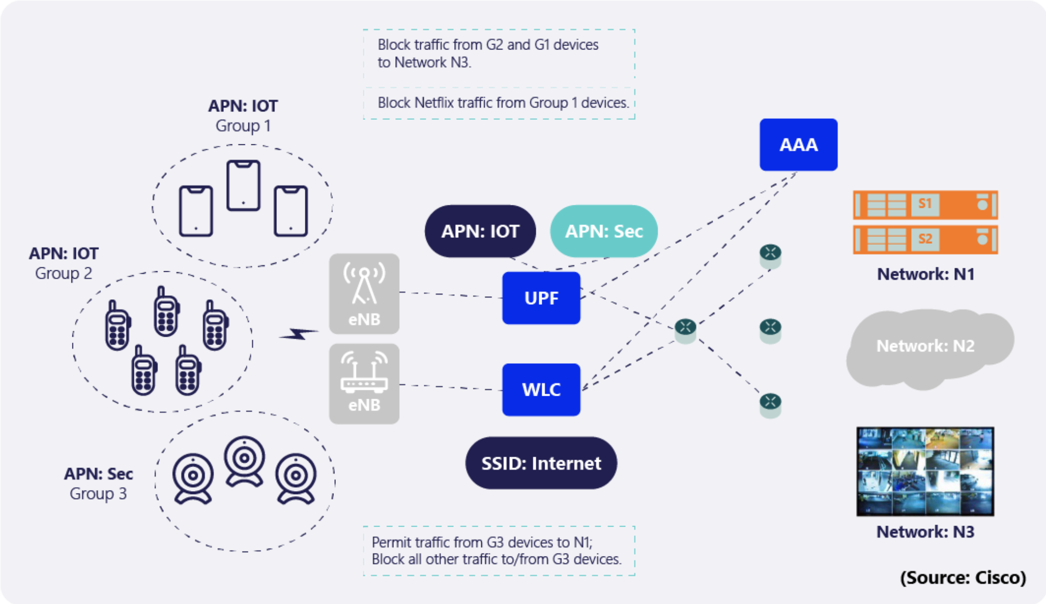


Figure 17 - Meta-Data Architecture Illustration

8.1 Traffic Classification & Meta-Data Tagging

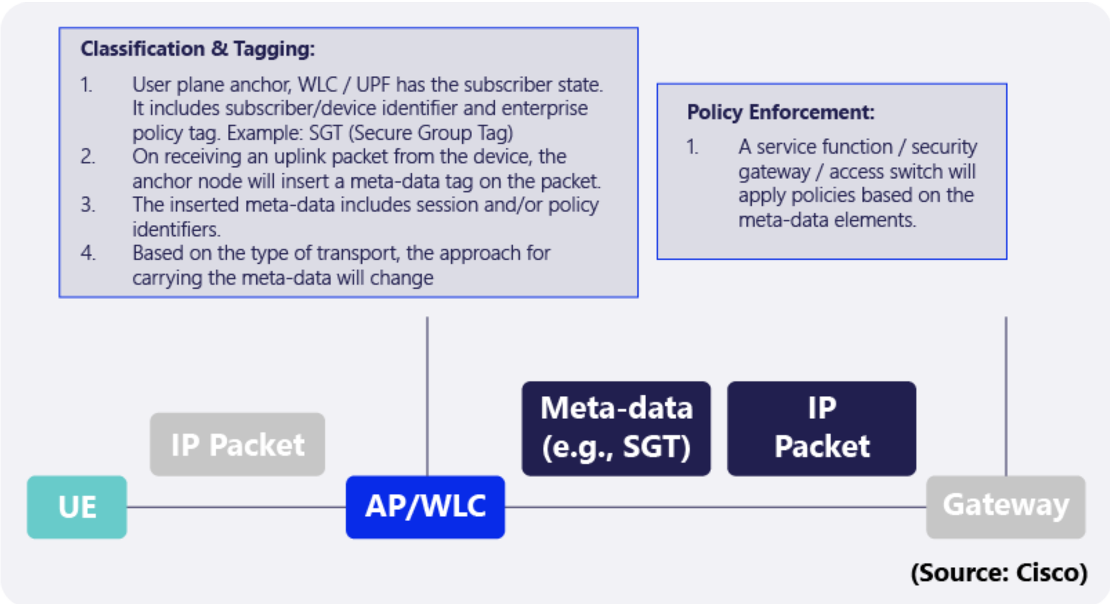


Figure 18 - Traffic Classification & Tagging

9. Optimized UE Paging in Converged Scenarios

Paging is a mechanism in cellular network where the network can wake-up a device which goes into Idle mode, when there is some downlink data to be delivered.

When the network needs to send a downlink packet to UE, it first pages the UE so that it establishes the Radio connection and transitions into connected state.

AMF is responsible for the initiation of paging procedure and does that by forwarding NGAP paging message to one or more next generation Node B's (gNBs).

The location of a UE in IDLE mode is known to AMF on a registration area basis. AMF will trigger all or some of the gNBs covering the registration area.

The network adopts a paging strategy starting with the last-known gNB, last-known registration area followed by all the registration area (TAI List).

On receiving the paging request, UE establishes the radio connection with the gNB and transitions to CM-Connected stated, allowing the CN to forward the downlink packets to the UE.

In a Converged P5G+WLAN network, there is an opportunity to greatly optimize the paging procedures. The UE's current association to Wi-Fi network can be useful.

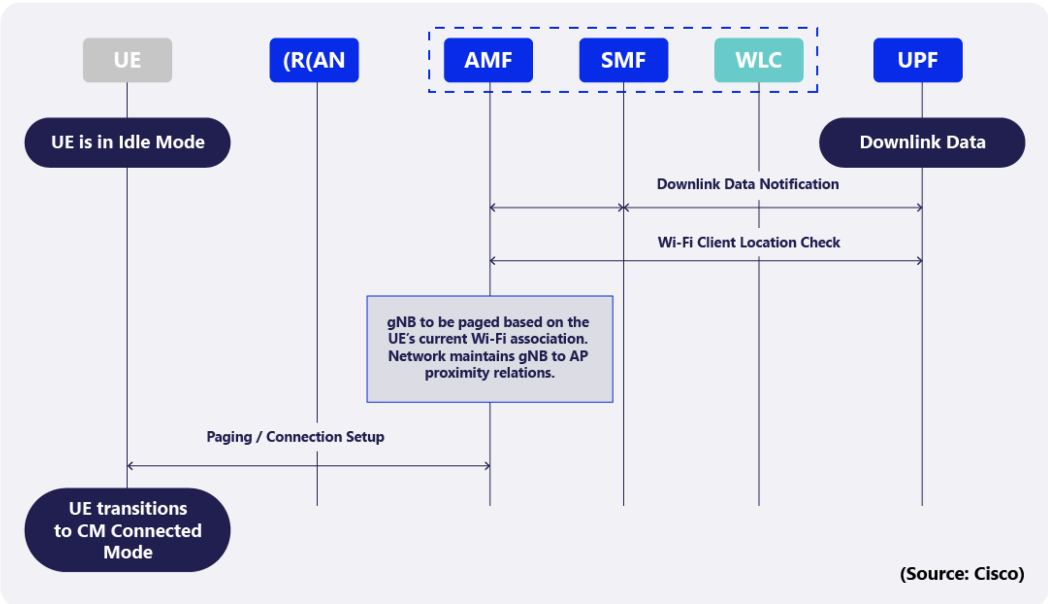


Figure 19 - Optimized UE Paging in Converged Scenarios

Key Points:

- A dual-radio capable UE will be attached to both enterprise Wi-Fi and Private 5G networks.
- The UE's Wi-Fi association state can be the indicator of the UE paging area.
- When AMF/SMF receives a DDN message from the UPF, it can query the WLC for the AP to which UE is currently attached and will be the basis for the paging strategy. There is interworking between the network elements (AMF/SMF and WLC) of each of these access networks.
- The state in each of the access networks will include the UE's current association state, location of the gNB/AP to which the UE is attached and other elements.
- The exchange of states between the network elements will allow us to optimize the signaling procedures and improve the performance. If the network is aware that the UE is currently attached to Wi-Fi access point building 24, the network can page the gNBs in that proximity area, thereby greatly improving the paging latency.

10. Device Identifiers

Network Access Identifier (NAI) is an identifier used by access networks for identifying users requesting access to the network. A user may access the network using more than one device, but all using the same NAI and the associated credentials.

There are various use-cases where an access network needs to unambiguously identify a device used for accessing the network, and NAI is not sufficient for such determination.

A unique identity for the device which is common across all the supported access interfaces allows the network to unambiguously identify the device.

Identifiers on the Device		
Scope	**Identifier #1**	**Identifier #2**
Device Specific	Serial Number	Certificate Id
Wi-Fi Interface Specific	IEEE-48-bit MAC address	NAI
Cellular Interface Specific	IMEI / PEI	IMSI / SUPI

(Source: Cisco)

Figure 20 - Device Identifiers

The use of the currently available stable identifiers such as MAC address, IMEI or Serial number as the unique device identifier is no longer an option for privacy reasons. Furthermore, with the support for MAC rotation, there is no stable MAC address on the endpoint. There are regulations such as GDPR which do not favour the exposure of PII elements to every access network.

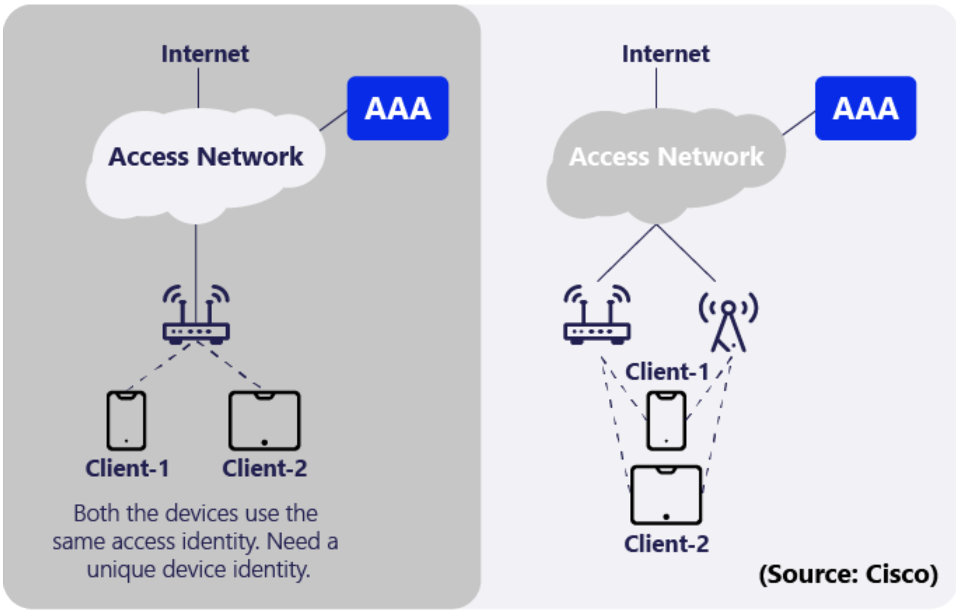


Figure 21 - Comparison on Identifiers Usage

11. Latency Analysis & Comparison Across P5G & Wi-Fi

There is a general expectation that the 3GPP 5G network can offer an end-to-end latency of under one milli-second (ms) for user plane traffic. As the manufacturing industry transitions to Industry 4.0 architecture, this sub-millisecond latency requirement cannot be ignored; 5G is expected to be the key component to that realization.

While we recognize that sub-one-millisecond E2E latency is a very aggressive number (1/1000 sec), the percentage of applications that require such low-latency is very small. Still, it is important to understand what this number means; how its measured, implications on the RAN and core network element placement, and the needed transport and compute. We need to breakdown this number and characterize the cost at each network element so we form a view of how the 5G access network on a factory floor should be designed.

Before we do this latency math, we need to establish the term, “E2E latency”, as it has multiple interpretations based on the SDO; only RAN, RAN+Core Network (CN), or RAN+CN+Data Network (DN) and if its bi-directional. In the context of 5G networks, what is relevant is truly the latency on the air interface, RAN and on the Core Network, and these are the only elements in scope of the 5G access network. Therefore, for this discussion, we will not consider the latency of the application either on the end point, application server, N6 or DN. Finally, we will ignore the slight time delta between UL and DL transmit delays on the air interface.

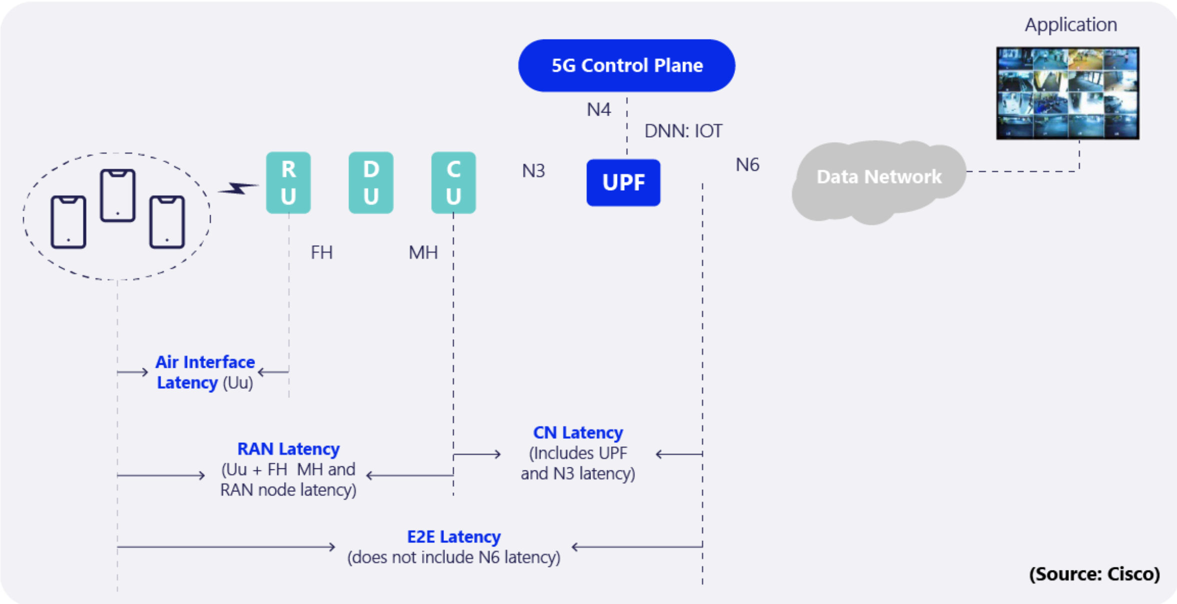
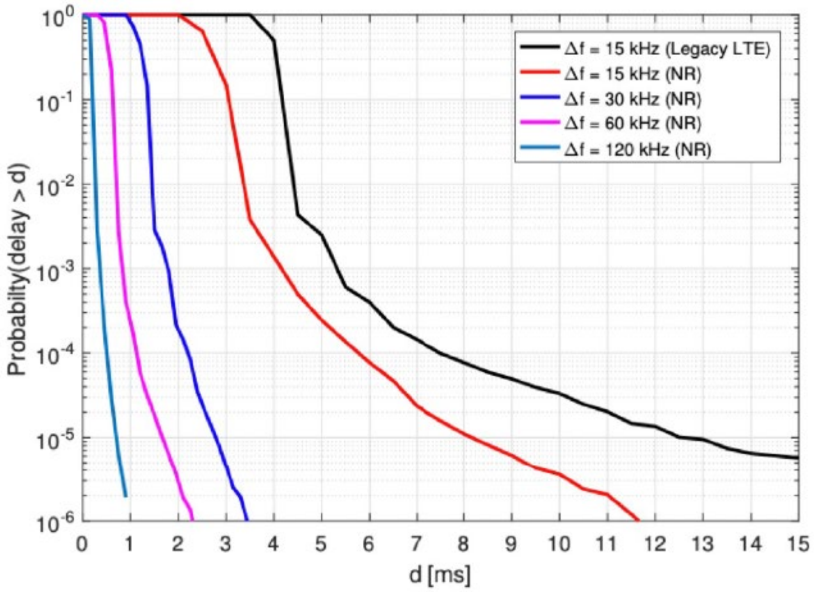


Figure 22 - Latency Analysis & Comparison Across P5G & Wi-Fi

We only care about the latency involved in moving the packet from left to right, and that includes the transport latency on the air interface (uu), RU – DU fronthaul path, DU – CU midhaul path and the N3 latency on RAN – UPF path. Furthermore, we will only consider one-way latency and describe "E2E latency" as the time it takes for moving a packet from the UE to the egress interface of the UPF.

There have been numerous published studies on the 5G NR user-plane latency. It largely depends on the chosen sub-carrier spacing. For 120 kHz (NR), we can assume it will be 0.75ms. for downlink. (Reference: Maaz, D. et al., "Userplane Latency Performance in New Radio").



(Source: Maaz, D. et al., "Userplane Latency Performance in New Radio")

Figure 23 - Complementary Cumulative Distribution Function (CCDF) of the Latency

When estimating the userplane packet processing load on a UPF, we need to understand that it largely varies based on the type of user plane features enabled for that UE / DNN / Slice and the box capability. Generally, we can safely say that an enterprise grade UPF may hold on to an UL/DL packet for anywhere from 0.3 to 0.5ms. Extending the same math to vRAN elements, we can say that the total packet handling time on the vRAN elements can be estimated to be anywhere from 0.2 to 0.8ms.

Moving on to the final component of this latency math, we will review the transport network latency on front-haul (FH), mid-haul (MH), and N3 (RAN-CN) paths. The baseline requirement for RAN disaggregation comes with a stringent latency requirement of 0.25ms on the front-haul. This requirement can be met with multi-Gig-Ethernet wiring, or Fiber. We can generally assume mid-haul latency will be around the same. While we are tempted to cut down the latency of N3 by moving the UPF closer to RAN, we must be careful here as UPF is an aggregation node. Collapsing UPF with RAN elements comes at a cost. Unless we miniaturize the UPF, it may be impractical to place a UPF at every CU/gNB.

We therefore give an estimate of 0.5 – 2.0ms for N3 latency. It is also to be noted that 3GPP specifications assume 1ms delay between RAN and UPF for delay critical bearer (e.g., 5QI 82, Ref 3GPP TS 23.501).

Transport Segment for User plane Packet	Latency (ms)
Uu	0.75 - 4.0
RU-DU	0.25 - 0.5
DU-CU	02.5 - 0.5
N3	0.5 - 2.0
Total:	1.75 - 7.0

Packet Processing Delay at different nodes	Latency (ms)
RU+DU+CU	0.2 - 0.8
UPF	0.3 - 0.6
Total:	0.5 - 1.4

Groupings	Latency (ms)
Total transport latency	1.75 - 7.0
Total Packet Processing Latency at all the nodes	0.5 - 1.4
Total:	2.25 - 8.4

Figure 24 - Latency Assessment

Based on the above analysis, we can say that realizing an E2E latency of 2.25ms is possible, only when we can afford to go with a specific radio configuration, and a very low-latency transport. But, going below the 2.25ms mark requires some level of network re-architecture, perhaps moving UPF closer to the RAN, or maybe with collocation of RAN and CN elements. One may even wonder, if elimination of FH and MH, with small cell another option. These optimizations may cut down the transport latency on the vRAN interfaces, but each of these come at a cost that needs to be carefully studied.

12. Summary & Conclusions

In this whitepaper, we have explored the key architectural approaches and the basic essential features for building tighter interworking between Private 5G and Wi-Fi access networks.

The paper proposed techniques for using RADIUS based AAA infrastructure for supporting 5G device authentication. Integrating 5G authentication such as 5G AKA support into RADIUS-based AAA infrastructure allows network operators to leverage existing AAA infrastructure for user authentication and authorization of private 5G devices. This allows the private network operators including enterprises to achieve identity correlation across access specific identities (e.g., SIM identity and enterprise username), and enforce a singular policy on all sessions originating from a given device.

Also, proposed is an approach for extending the Wi-Fi Fast Transition Domain to include Private 5G access. This approach identifies methods for bootstrapping keys on Wi-Fi access using key material generated from the 5G access authentication, and vice versa. This approach results in drastic reduction of connection establishment time to Wi-Fi access, upwards of 90% reduction in connection time. This is a significant gain for latency sensitive applications (Ex: URLLC, Industrial IOT, Video, AR/VR, Gaming) and thereby greatly improving the real-time application experience in private networks.

We looked at approaches for showing relation between service identifiers used in Wi-Fi and Private 5G systems. Both Wi-Fi and Private 5G network use different service naming constructs. It is important to enable the end point to be made aware of the services names that are used in each of the access systems for all common services that are accessible through both the access networks. This allows the network operator to steer users between radio technologies based on network conditions are other requirements.

The paper analysed different mobility management models for supporting IP address preservation and seamless mobility. Arguments have been made as to why 3GPP's approach of Wi-Fi interworking with 3GPP's access has no path and is a failed architecture. A lightweight interface between Wi-Fi and Private 5G without extending NAS support to Wi-Fi or requiring IPsec functions is sufficient; it is realizable and will have no loss of functionality.

Service Functions are extensively deployed in most networks and play a key role. These Service Functions provide a range of features such as security, WAN acceleration, and server load balancing. The paper explained how the context data from access networks when relayed to these service functions can be invaluable tool for enforcing the right security policies on the user traffic.

The paper also explained how the device connectivity status in one access network can be used by the elements in the other access network for optimizations. Example of optimizations in UE paging was used as an example.

Finally, the paper looked at latency analysis of user plane traffic in Wi-Fi and Private 5G access networks, and explained how the placement of the functions impact the latency. These considerations are important for deployments.

Appendix A

Many architectural methods exist for enterprises seeking a converged 5G and Wi-Fi solution. We have noted these in the below diagram. Each topology has its own unique pros and cons depending on network capabilities and requirements associated with desired use cases.

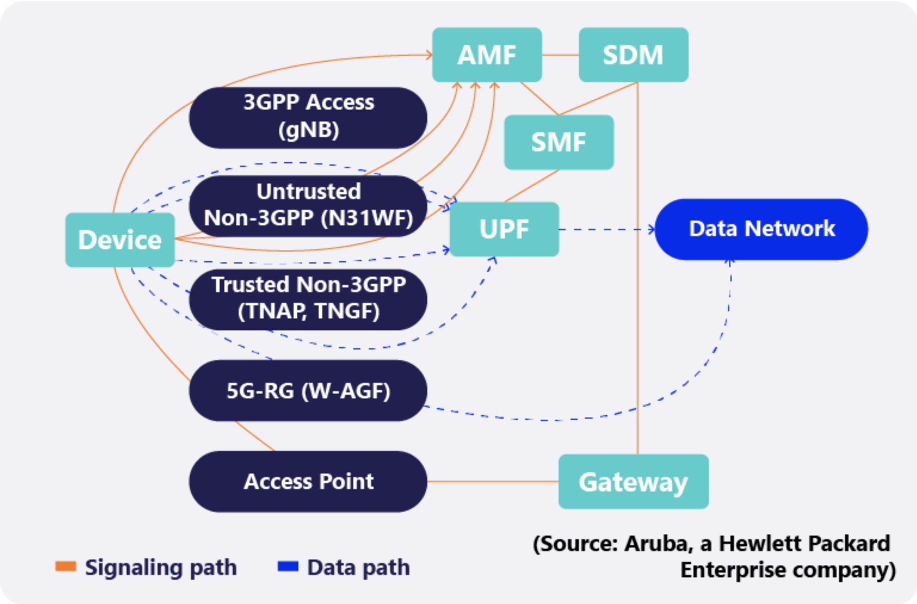


Figure 25 - Options for Enterprise Convergence

Various non-3GPP interworking gateways have been introduced within architectural standards representing untrusted and trusted networks via N3IWF and TNGF, respectively, and these are very well captured in the 3GPP 23.501 and 23.502 specifications.

Each of these convergence solutions requires changes in the network and has its own implementation challenges. Additional consideration should be given to the types of intended use cases identified by the enterprise. Most enterprises or private deployments are looking for a simple and efficient solution without getting into the complexity of selecting an interworking function.

To select a converged solution for an enterprise, some questions should be answered when defining the intended architecture.

- Is it a greenfield or brownfield deployment?

For greenfield deployment, there are some flexibilities to select the required architecture, but for brownfield deployment, either a parallel network or an existing network needs to be evolved. This depends on a case-by-case basis, and there is no generic solution that fits all.

- What kind of devices will be used? Do they support dual connections?

Most of the UEs are supporting 5G NSA architecture, with very few devices available using dual connectivity to support 5G 3GPP and non-3GPP access methods. It will take a couple of years before dual-connection devices are generally available.

- Is there a need for session continuity?

Before session continuity, a common SIM-based authentication mechanism or procedure is preferred for both 5G and Wi-Fi.

If session continuity is mandatory, then there is a need for an interworking function to communicate with the 5G core to provide data session continuity across both access types. It is also possible to leverage 5G capabilities if use cases demand network service slices like MAPDU, ATSSS, session anchoring, etc.

A lightweight gateway can provide some functionality by communicating with standard entities and their interfaces. A simplified architecture can be used where there is no need for session continuity across accesses and just authentication is required to provide device connectivity to valid devices, as depicted in the following figure.

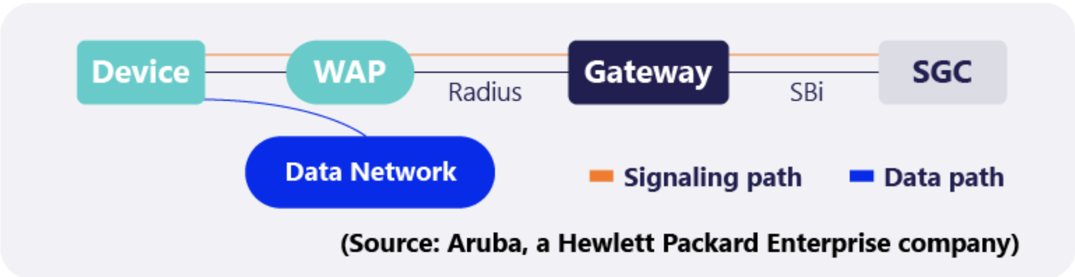


Figure 26 - Lightweight Gateway

Highlights:

- Most private enterprises are either looking for single access or a simplified converged solution without going through the complexity of selecting an interworking solution.
- Lightweight gateways can be of significant value for enterprises utilizing use cases that do not require heavier approaches through interworking functions such as N3IWF and TNGF. The standard-defined non-3GPP procedures (registration, data session establishment, etc.) have defined many more transactions between entities, which results in a higher resource requirement.
- Even if a converged solution is needed, session-continuity requirements by enterprises remain to be seen based on intended use case.

Participant List

Name	Company	Role
Florin Baboescu	Broadcom	Project Leader
Sri Gundavelli	Cisco	Project Co-Leader & Chief Editor
Thierry Van de Velde	Nokia	Project Co-Leader
Ravi Saxena	Aruba, an HPE company	Editorial Team
Blair Bullock	Boldyn Networks	Editorial Team
Mark Grayson	Cisco	Editorial Team
Sangram Lakkaraju	Cisco	Editorial Team
Necati Canpolat	Intel Corporation	Editorial Team
Valerie Parker	Intel Corporation	Editorial Team
Irfan Acar	Airties	Project Participant
Omer Topal	Airties	Project Participant
Anthony Good	Airwavz	Project Participant
Youssef Abdelilah	American Tower	Project Participant
Martin Schwarze	Aruba, a Hewlett Packard Enterprise company	Project Participant
Stuart Strickland	Aruba, a Hewlett Packard Enterprise company	Project Participant
Peter Thornycroft	Aruba, a Hewlett Packard Enterprise company	Project Participant
Pingping Zong	Aruba, a Hewlett Packard Enterprise company	Project Participant
Kevin Franzen	AT&T	Project Participant
Jinhong No	AT&T	Project Participant
Jim Sturges	AT&T	Project Participant
Jessie Manik	Bell Mobility	Project Participant
Romin Jain	Boingo Wireless	Project Participant
George Pejovic	Boldyn Networks	Project Participant
Andy Corston-Petrie	BT	Project Participant
Milan Lalovic	BT	Project Participant
Simon Ringland	BT	Project Participant
Matt Forbes	CableLabs	Project Participant
Lili Hervieu	CableLabs	Project Participant
Neeharika Jesukumar	CableLabs	Project Participant
Luther Smith	CableLabs	Project Participant
Lingaraj Holiyappanavar	Calix	Project Participant
Kyle Johnson	Charter	Project Participant
Loay Kreishan	Charter	Project Participant
Dave Moran	Charter	Project Participant
Patricia Truax	Charter	Project Participant

Gino Corleto	Cisco	Project Participant
Robert Jaksa	Comcast	Project Participant
Ruchi Kothari	Comcast	Project Participant
Hussain Zaheer Syed	Comcast	Project Participant
José Martinez	RDK	Project Participant
Qasim Cheema	COX	Project Participant
Derrick Smith	COX	Project Participant
Harpreet Narula	Dell	Project Participant
Ahmed Hafez	Deutsche Telekom	Project Participant
Hideaki Goto	Cityroam	Project Participant
Natalia Ermakova	ER-Telecom	Project Participant
Brendan Bonner	Extreme Networks	Project Participant
Raymond Lim	Extreme Networks	Project Participant
Souma Badombena	Intel Corporation	Project Participant
John Belstner	Intel Corporation	Project Participant
Dibakar Das	Intel Corporation	Project Participant
Roya Doostnejad	Intel Corporation	Project Participant
Ravi Sinha	Reliance JIO	Project Participant
Edward Wincott	JISC	Project Participant
Yonggang Fang	MediaTek	Project Participant
Jon Buck	Mobilitie	Project Participant
Subir Das	Peraton Labs	Project Participant
SaiDhiraj Amuru	Plume	Project Participant
Bin Hu	Plume	Project Participant
George Hart	Rogers	Project Participant
Betty Cockrell	Single Digits	Project Participant
Michael Sym	Single Digits	Project Participant
Federico Lazzarin	SKY Itália	Project Participant
Chidananda Das	STL	Project Participant
Kishore Rajasekharuni	STL	Project Participant
Les Goldman	Syniverse	Project Participant
Brendan Malay	Telus	Project Participant
Troy Cross	Tessares	Project Participant
Nicolas Keukeleire	Tessares	Project Participant
Bruno Tomás	WBA	Project Participant
Pedro Mouta	WBA	Project Participant