5G and Wi-Fi RAN Convergence

Aligning the Industry on Opportunities and Challenges

Source: Wireless Broadband Alliance
Author(s): WBA 5G Work Group
Issue date: April 2021
Version: 1.0
Document status: Final

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 AT&T, Boingo Wireless, Broadcom, BT, Cisco Systems, Comcast, Deutsche Telekom AG, GlobalReach Technology, Google, Intel, Reliance Jio, SK Telecom and Viasat. For the complete list of current WBA members, click here.

Follow Wireless Broadband Alliance:

www.twitter.com/wballiance

http://www.facebook.com/WirelessBroadbandAlliance

https://www.linkedin.com/company/wireless-broadband-alliance

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.

CONTENTS

FIGURES

TABLES

EXECUTIVE SUMMARY

With the continued evolution of Wi-Fi and 5G technologies, convergence between these two technologies will enable new use cases and business opportunities for the industry to undertake. Some key use cases which can benefit from and leverage Wi-Fi and 5G convergence include verticals/enterprises, industrial IoT and connected cities.

This paper on Wi-Fi and 5G convergence builds and further expands on the previous RAN Convergence paper published in September 2019, jointly authored by WBA and NGMN [1]. It continues to explore the topic of 5G and Wi-Fi convergence with an in-depth look at 3GPP defined solutions to support the integration of WLAN with the 5G system and identifies some key challenges and gaps in current solutions.

This paper is organized into three main parts:

Part I (Chapter 2): Focuses on 3GPP state-of-the-art on integrating WLAN with the 3GPP 5G system as defined by 3GPP Release 15 and 16, including WLAN integration architecture, related features, functions, policies and associated procedures.

Part II (Chapter 3): Identifies key challenges and gaps in current 3GPP-defined solutions to support interworking between WLAN and 3GPP 5G system and suggests high-level solutions to address some of the identified gap items.

Part III (Chapter 4-5): Provides recommendations and next steps for the industry and the relevant standard bodies to address the key challenges and gaps related to the 5G and Wi-Fi convergence.

The paper covers WLAN integration architecture for the untrusted and trusted WLAN integration with the 5G Core and identifies some gap areas related to enabling trusted WLAN integration. It captures the establishment of IPsec security associations (SAs) for the transport of signalling and user data over the WLAN access. The 5G policies for access selection and route selection are described, including the Access Network Discovery and Selection Policy (ANDSP) containing WLAN Selection Policy (WLANSP) and the UE Route Selection Policy (URSP). Various aspects of the Access Traffic Steering, Switching and Splitting (ATSSS) feature are covered including ATSSS architecture, steering functionality, ATSSS rules and ATSSS procedures for multi-access traffic steering. A detailed description of 5G QoS model is captured as it applies to 5G flows carried over the WLAN access, including QoS related signalling and the QoS flow data transport over the WLAN access.

An in-depth analysis of the challenges and gaps related to the ATSSS feature is captured. As part of this analysis, a number of important ATSSS related issues have been highlighted including combining ATSSS policy with other UE based policy, deployment limitations of

ATSSS MPTCP converter proxy and incorporation of UE local conditions in ATSSS. Other key issues emphasized include ATSSS support for packet level traffic steering for all traffic types, ATSSS operation with Multi-path capable servers, incorporating RAN level measurements for dynamic traffic steering in ATSSS and interworking challenges of ATSSS MPTCP functionality with the already deployed outer MPTCP on certain device platforms. The importance of key issues identified in the Release 17 ATSSS phase 2 study is underscored.

Further analysis is conducted on the policy interworking across Wi-Fi and 5G, taking into consideration that policies for access selection and/or multi-path selection can be defined by multiple entities including application providers, device manufacturers, end users, and enterprise IT admins as well as the service provider. The issue of choosing a high-quality WLAN network connection based on Wi-Fi QoS metrics is considered and the policy related enhancements needed to enable such a capability are highlighted. Relating to policy, another key issue identified is how to enable an operator to provide differentiated service over 5G and Wi-Fi as part of a converged service bundle.

The paper also examines the key issue of how the end-to-end QoS requirements for 5G applications and services can be satisfied over the WLAN access. It highlights the importance of providing QoS differentiation within WLAN access for 5G QoS flows based on 5G QoS characteristics and QoS parameters. It analyses the issues associated with mapping of 5G QoS to Wi-Fi QoS and underscores the need to define a standardized mapping between 5QI to DSCP values as one of the gap areas to support QoS differentiation. In addition, it identifies some IEEE 802.11 related gaps to support QoS differentiation for 5G flows based on identifying and prioritizing the 5G user traffic carried over IPsec child security associations within the WLAN access.

The importance of supporting 5G connectivity for Wi-Fi only devices is underscored, to be able to provide 5G experiences to such devices in enterprises and verticals. The issues associated with supporting Wi-Fi only devices without USIM in the 5G and WLAN converged system are explored. The need to define full support for non-IMSI based identity and EAP-TLS/EAP-TTLS authentication methods over WLAN access for stand-alone non-public network (SNPN) is highlighted, for enabling Wi-Fi only devices in private 5G networks. Additionally, the important discussion point on the topic of supporting Wi-Fi only devices without USIM over the PLMN networks is highlighted.

Finally, the paper provides recommendations on what the industry can do to address key challenges and gaps identified to fully support the 5G and Wi-Fi convergence. It suggests liaisons with relevant standard bodies as the next step to align the industry on the challenges and issues, and facilitate standardization efforts for addressing these issues, to provide fully deployable end-to-end 5G and Wi-Fi convergence solutions.

1   Introduction

With continued development of 5G networks in 3GPP and continued evolution of Wi-Fi technology with Wi-Fi 6/6E and Wi-Fi 7, the industry stands to benefit a great deal from the continued convergence of Wi-Fi and 5G system. This convergence can enable leveraging capabilities of both access networks to provide seamless and interoperable services to the end-users across a variety of use cases and verticals.

This paper enhances on the previous work done in WBA and NGMN on the RAN Convergence [1] and continues to explore the topic of 5G and Wi-Fi convergence with in-depth look at 3GPP defined solutions to support integration of WLAN with the 5G system and identifies some key challenges and gaps in current solutions which the industry needs to address.

The architecture for integrating Wi-Fi in the 3GPP 5G system is examined and some of the practical limitations of its implementation in the real world scenarios are considered. Specifically, the key gap areas related to enabling trusted WLAN integration with 5G Core are highlighted. The role of ATSSS is examined in-depth and some of its current limitations have been highlighted.

The paper examines the topic of policy interworking and policy combining across Wi-Fi and 5G taking into considerations that policies for access selection and/or multi-path selection can be defined by multiple entities on the device and/or on the network side. It further analyses the key issue of meeting end-to-end QoS requirements for 5G applications and services over the WLAN access taking into account 5G QoS characteristics and parameters. It emphasizes the importance of supporting 5G connectivity for Wi-Fi only devices without USIM capability, to be able to provides 5G experiences to such devices in various enterprises and verticals deployments.

This paper also proposes some possible high level solutions to address identified gaps and suggests possible ways the industry needs to work together to address key convergence related challenges. Finally, it highlights the standard bodies where further work is needed to develop solutions that the industry should adopt, to provide the best service experiences to the end users across different 5G and Wi-Fi converged deployments.

2 3GPP State-of-the-art on 5G and Wi-Fi Integration

The previous RAN Convergence paper by WBA and NGMN Alliance [1] covered integration and interworking between 3GPP 4G and 5G systems and WLAN access networks.

In this section, we focus on 3GPP state-of-the-art on the integration and interworking of WLAN with 3GPP 5G systems as defined by 3GPP Release 15 and 16. This section describes the 5G and WLAN integration architecture, related features, functions, policies and associated procedures as defined by 3GPP, to better understand the interworking between the two technologies and further analyse interworking related challenges and gaps.

2.1 Integration Architecture[1]

In the 3GPP 5G System, WLAN is integrated either as a trusted or untrusted access. An untrusted WLAN access network is connected to the 5G Core (5GC) via a Non-3GPP Interworking Function (N3IWF) and a trusted WLAN access network is connected to the 5G Core via a Trusted Non-3GPP Gateway Function (TNGF) or a Trusted WLAN Interworking Function (TWIF),. WLAN networks may advertise support for trusted 5G connectivity with one or more PLMNs e.g. as part of ANQP protocol in Passpoint ^{TM}. Based on the type of WLAN access discovered, a UE may decide to use untrusted or trusted WLAN access to establish connectivity with the 5G Core per implementation specific procedure. The N1 Interface between UE and 5G Core carries NAS messages and can be transported over 3GPP or WLAN access. For WLAN access, the transport of NAS signaling and user plane data is performed over IPsec tunnels established between N3IWF/TNGF and the UE as described in sections 2.1.3 and 2.1.4.

2.1.1 Untrusted WLAN Integration Architecture

Figure 2-1 shows the architecture for integrating untrusted WLAN access with the 5G Core via the N3IWF gateway function. There is loose coupling between N3IWF and WLAN access over the Y2 interface through generic IP transport and the WLAN layer-2 authentication is independent of the UE 5G core authentication. The NWu interface is based on the establishment of IPsec security associations (SAs) between the UE and N3IWF over WLAN access for securing the transport of both 5G NAS signalling and user data. The IPsec SAs over NWu apply both encryption and integrity protection for 5G signalling and user data, since WLAN layer-2 security is not trusted in this deployment as it is independent of UE 5G authentication.

---

[1] clause 4.2.8 in TS 23.501
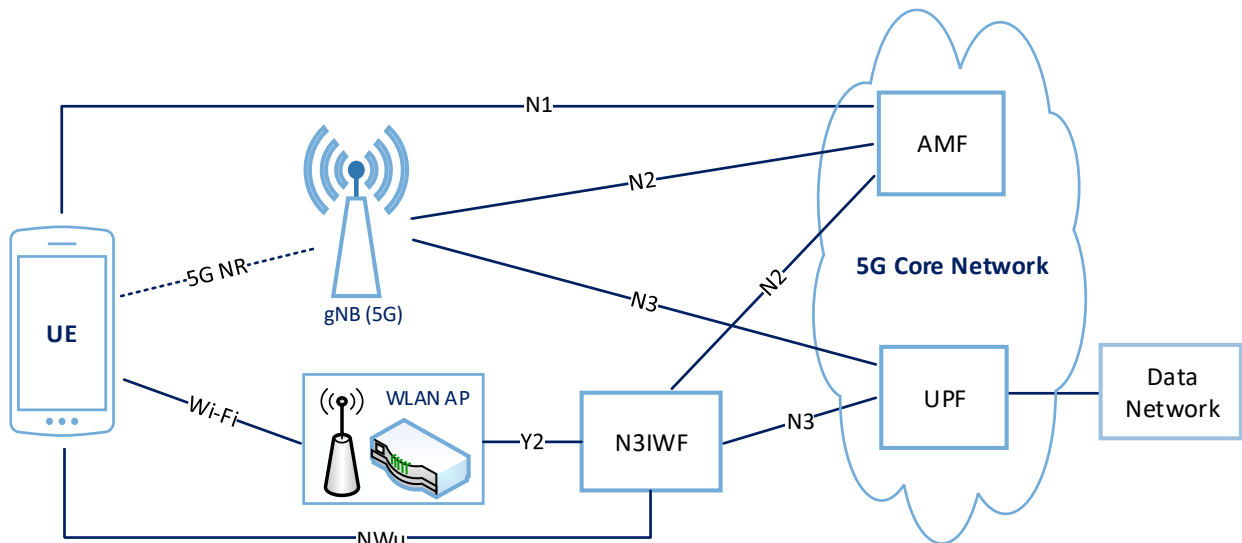
Figure 2-1 Untrusted WLAN integration with 5G Core

2.1.2   Trusted WLAN Integration Architecture

Figure 2-2 shows the architecture for integrating trusted WLAN access with the 5G Core via TNGF gateway function. There is tighter coupling between the TNGF and trusted WLAN AP over a AAA based interface Ta. The WLAN layer-2 authentication is tied to a key derived by TNGF after successful UE authentication with the 5G Core. The NWt interface is based on the establishment of IPsec security associations (SAs) between UE and TNGF over WLAN access for transport of both 5G NAS signalling and user data, similar to NWu. However, the IPsec SAs over NWt apply NULL encryption for signalling and user data to avoid double encryption, since WLAN layer-2 encryption is trusted in this deployment as it is dependent on the UE 5G authentication.
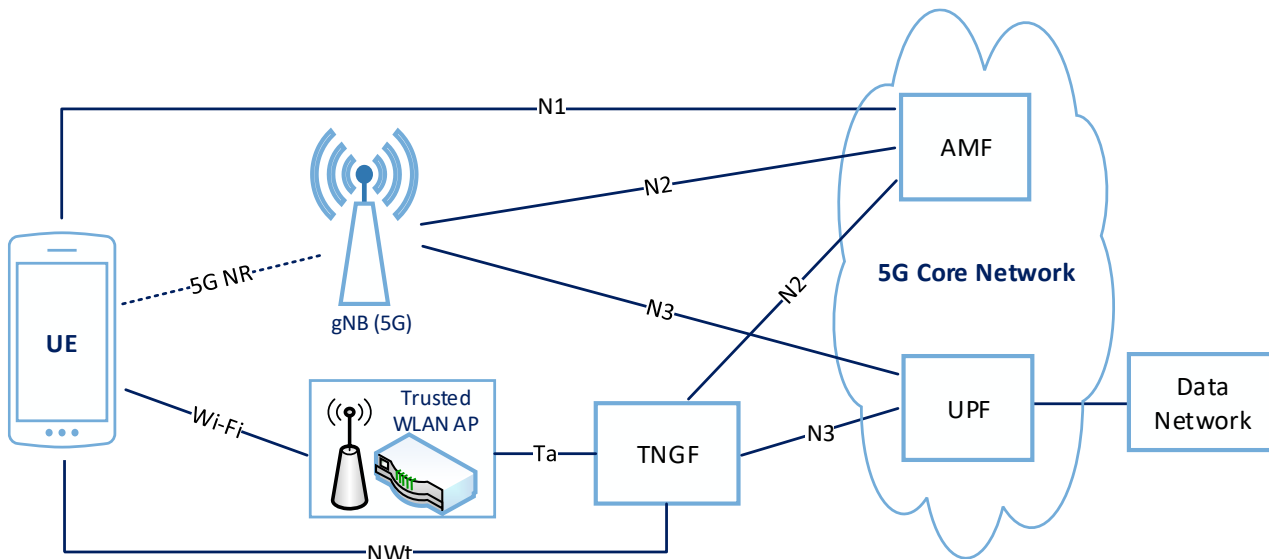
Figure 2-2 Trusted WLAN integration with 5G Core via TNGF

There could be devices which support 5G SIM credentials but do not support 5G NAS signalling over trusted WLAN access, which requires UE to support EAP-5G and IKEv2 protocol. Such devices, referred to as Non-5G-Capable over WLAN (N5CW), can still connect to a 5G Core over trusted WLAN access via the TWIF gateway function as shown in Figure 2-3. TWIF implements the NAS protocol stack and exchanges NAS messages for registration/PDU session management with the AMF on behalf of the N5CW device over the N1 interface. The UE authentication with 5G Core over WLAN access is executed through TWIF function, like the TNGF case, with EAP authentication messages directly transported over Yw interface and the WLAN layer-2 authentication is tied to a key derived based on the UE 5G authentication. The N5CW device is assumed to have a USIM and is authenticated with the 5G Core using EAP-AKA' (clause 7A.2.4 in TS 33.501). The N5CW device may operate as a 5G UE over 5G access network, but those network functions are not shown in Figure 2-3 for simplicity.
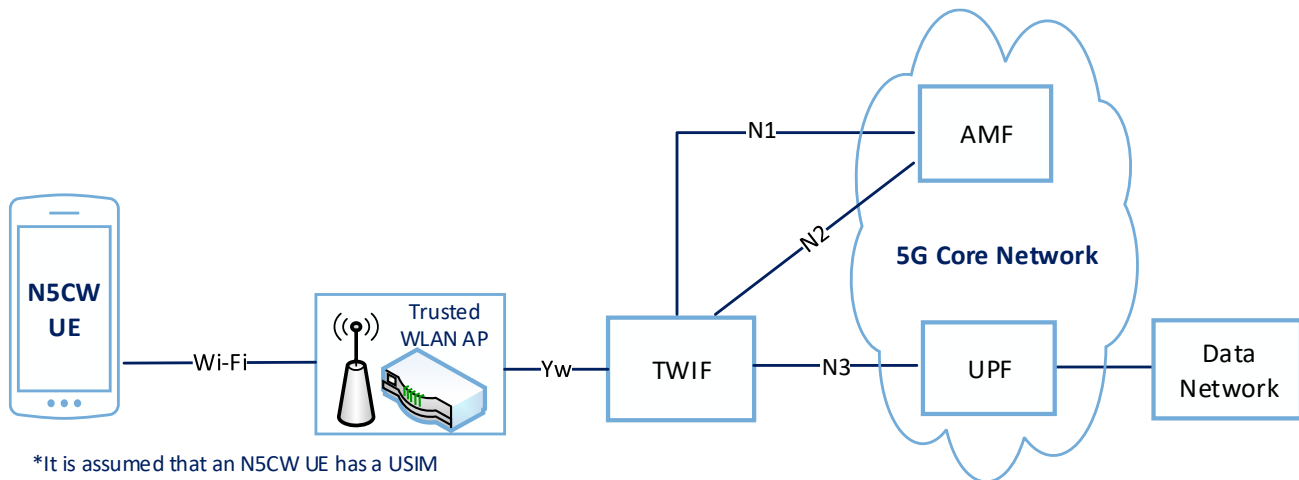
Figure 2-3 Trusted WLAN integration with 5G Core via TWIF for N5CW Devices

To support trusted WLAN integration, the Ta interface between WLAN AP and TNGF, and the Yw interface between WLAN AP and TWIF needs to be specified. These interfaces are considered to be outside of 3GPP scope and need to be addressed within the WLAN scope.

2.1.3   IPsec SA Establishment over Untrusted WLAN access[2]

In this case, the UE first connects to and obtains an IP address from the untrusted WLAN access. The UE then selects an N3IWF in a PLMN and initiates procedure to establish an IPsec SA with the selected N3IWF. The IKEv2 and EAP-5G protocols are used to establish a signaling IPsec SA between the UE and N3IWF during the registration procedure, as shown by control plane protocol stack in Figure 2-4.

The UE starts with an IKE_SA_INIT exchange to establish an IKE SA, which enables encryption and integrity protection for all subsequent IKE messages. The UE then initiates an IKE_AUTH exchange without any AUTH payload which indicates to N3IWF to start an EAP-5G session. The EAP-5G protocol is used to encapsulate NAS messages over the IKEv2 protocol between the UE and N3IWF. UE authentication over untrusted non-3GPP access is executed using either EAP-AKA' or 5G-AKA authentication method. NAS messages for UE authentication are encapsulated in EAP-5G signaling sent over IKEv2 protocol. After successful UE authentication, both the N3IWF and UE have a common N3IWF key (provided by the AMF to N3IWF and derived by the UE) and the EAP-5G session is completed with an EAP-Success message sent to the UE.

---

[2] clause 4.12.2 in TS 23.502, clause 7.3 in TS 24.502, clause 7.2.1 in TS 33.501

Next, IKEv2 messaging is used to establish a signaling IPsec SA between the UE and N3IWF using the common N3IWF key. The signaling IPsec SA applies both encryption and integrity protection. The UE establishes a TCP connection with the N3IWF for reliable delivery of NAS messages. All subsequent NAS messages are carried over the TCP/IP connection sent over the signaling IPsec SA.
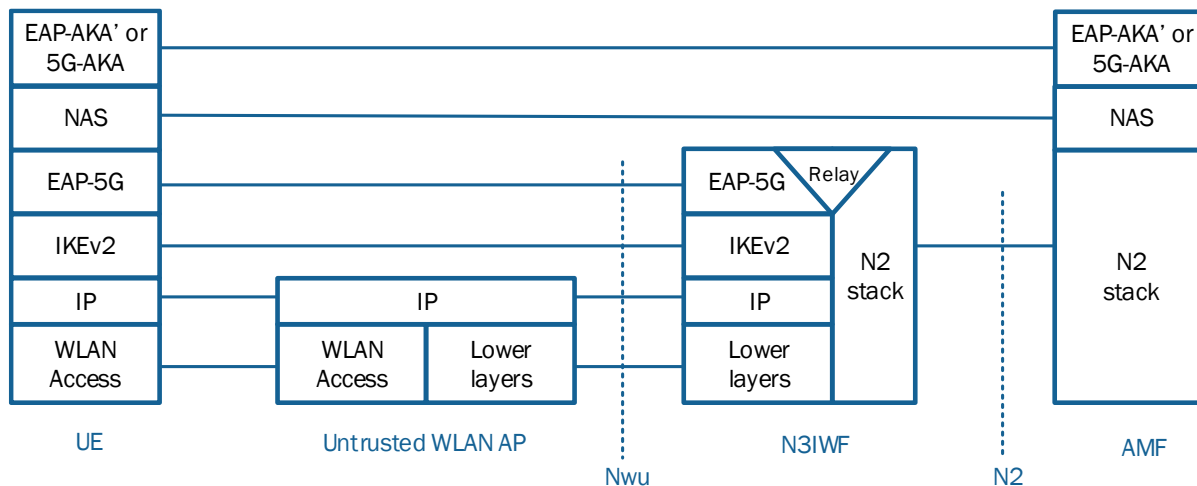
Figure 2-4 Control Plane for Establishment of Signalling IPsec SA over Untrusted WLAN Access

For user plane data transport over untrusted WLAN access, one or more separate IPsec child SAs are established between the UE and N3IWF using IKEv2 messaging as part of PDU session establishment, with both encryption and integrity protection applied over these IPsec child SAs.

2.1.4   IPsec SA Establishment over Trusted WLAN access[3]

In this case, the UE first selects a trusted WLAN access and then establishes a layer-2 association with the WLAN AP (TNAP) within that trusted access. EAP followed by IKEv2 signaling is used to establish a signaling IPsec SA between UE and TNGF as part of the registration procedure, as shown by the control plane protocol stack in Figure 2-5. This procedure requires enhancement on the WLAN AP to support filtering for EAP-5G messages.

An EAP procedure is initiated by the TNAP to request the UE Identity for link layer authentication of the UE. The NAI received from the UE triggers the TNAP to send a AAA request to the TNGF, which operates as a AAA proxy. The TNGF starts an EAP-5G session with the UE. The EAP-5G signaling is used to encapsulate NAS messages between the UE

---

[3] clause 4.12a.2 in TS 23.501, clause 7.3A in TS 24.502, clause 7A.2.1 in TS 33.501

and TNGF, and UE authentication is performed using either EAP-AKA' or 5G-AKA authentication method. NAS messages for UE authentication are encapsulated in EAP-5G messages, which get transported using AAA messages (e.g. using RADIUS EAP-message attribute) between the TNGF and TNAP and are encapsulated over layer-2 protocol (IEEE 802.1x/ EAPoL) between TNAP and UE. After successful UE authentication, a common TNGF key is established between TNGF and UE and an EAP-Success message is sent to the UE completing the EAP-5G session.

The TNGF derives a TNAP key and sends to the TNAP over a AAA message. For WLAN access, the TNAP key is used as the Pairwise Master Key (PMK) to establish layer-2 security between the UE and TNAP by executing the 802.11 4-way handshake. After WLAN layer-2 security is established, the UE receives IP address configuration from the WLAN access network. The UE then establishes a signaling IPsec SA with TNGF using the IKEv2 protocol with the common TNGF key and NULL encryption is negotiated. Similar to the untrusted non-3GPP access case, the UE establishes a TCP connection with the TNGF for reliable delivery of NAS messages. All subsequent NAS messages are carried over the TCP/IP connection sent over the signaling IPsec SA.
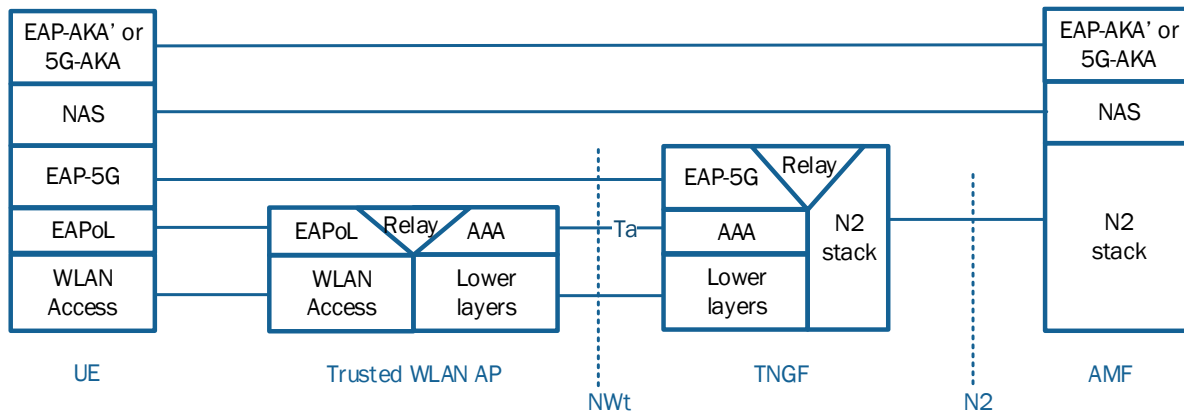
Control plane over Trusted WLAN before UE is assigned IP address
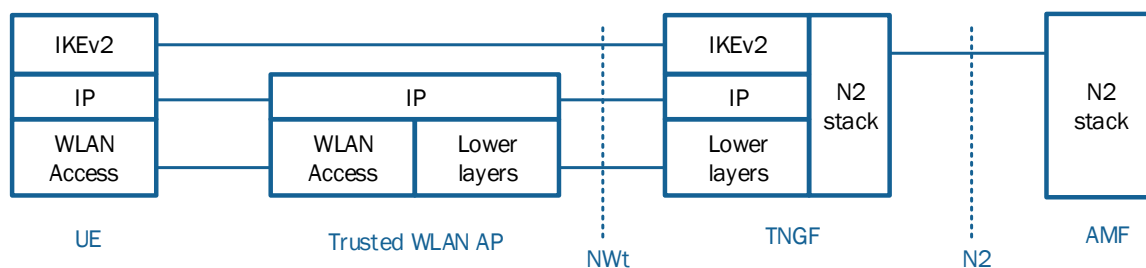
Control plane over Trusted WLAN after UE is assigned IP address

Figure 2-5 Control Plane for Establishment of Signalling IPsec SA over Trusted WLAN Access

For user plane data transport over trusted WLAN access, one or more separate IPsec child SAs are established between the UE and TNGF using IKEv2 messaging as part of PDU session establishment, and NULL encryption is negotiated for these IPsec child SAs.

2.2   5G Policies for Access Network Selection and Traffic Steering

3GPP defines 5G policies for selecting Wi-Fi access networks, for determining whether particular traffic data flows should be routed over Wi-Fi, cellular or both, and, in the final case, how traffic should be divided between the two access networks. The ANDSF WLAN Selection Policy (WLANSP) rules are reused in 5G access network selection policy.

The 5G policies operate in three distinct phases. First, an Access Network Discovery and Selection Policy (ANDSP) is used to influence which Wi-Fi access network the mobile device should connect to as described in section 2.2.1. Next, for each application flow, a UE Route Selection Policy (URSP) is used to determine whether to send the data for that flow over Wi-Fi, cellular, or both (i.e. using a "Multi-Access PDU session") as described in section 2.2.3 below. Finally, if the route selection decision is to use both access networks over a MA-PDU session, an ATSSS policy determines how traffic should be divided between the two accesses. The ATSSS architecture and ATSSS policy/rules are described in section 2.3.

2.2.1 Access Network Discovery and Selection Policy (ANDSP)[4]

The 5G Access Network Discovery and Selection Policy is used to determine which non-3GPP networks the mobile device should connect to. It is not used to prioritize 3GPP cellular networks. Furthermore, Wi-Fi is the only non-3GPP network for which the policy is defined.

An important aspect to note about the ANDSP is that it only applies when a Wi-Fi network cannot be selected on the basis of *user preference*, i.e. where no user preference exists or where no user preferred Wi-Fi network is in range.

This would result in WLAN access selection being made based on the mobile device OEM specified policy for determining what the user preferences are. For example, the OEM policy could count the user manually configuring an SSID (entering the password for an SSID, manually connecting to an open SSID or manually downloading a Passpoint TM profile) as being user preferred networks. The OEM policy could also potentially differentiate PasspointTM networks configured by the cellular operator (perhaps in carrier settings) that use SIM based credentials from the other Passpoint TM networks configured manually by the user.

The ANDSP essentially consists of a set of WLAN Selection Policy (WLANSP) rules (re-using the WLANSP definition introduced in 4G) together with an identifier/address that tells the mobile device where in the mobile core it needs to route the Wi-Fi access traffic for untrusted WLAN connectivity. The WLANSP is used for selecting a WLAN access network which can provide untrusted connectivity to 3GPP core network via N3IWF. The ANDSP is also used as an input to select a preferred WLAN access network providing trusted connectivity to the 5G Core via TNGF or TWIF as described in section 2.2.2.

---

[4] clause 6.6.1 in TS 23.503

The 5G Access Network Selection Policy is summarized in Table 2-1.

Table 2-1 5G Access Network Discovery and Selection Policy

Information Name	Details	
WLANSP Rules	Validity Conditions - time of day, geolocation, network location (e.g. PLMN, Location Area), etc.	
	WLAN Selection Criteria	Attributes defined in the Hotspot2.0 Rel-2 specification: - PreferredRoamingPartnerList, - MinimumBackhaulThreshold, - MaximumBSSLoad, - RequiredProtoPortTuple. - A list of SSIDs as defined in the SPExclusionList
		Additional attributes: - PreferredSSIDList: A prioritized list of SSIDs preferred for selection. - HomeNetwork (as identified using Hotspot 2.0)
ePDG identifier configuration	It provides the FQDN or IP address of the ePDG in the HPLMN (clause 6.3.6.1 in TS 23.501)	
N3IWF identifier configuration	It provides the FQDN or IP address of the N3IWF in the HPLMN (clause 6.3.6.1 in TS 23.501)	
Non-3GPP access node (N3AN) selection information	It provides a prioritized list of PLMNs and for each PLMN provides information to select and discover ePDG or N3IWF for untrusted connectivity. (clause 6.3.6.1 in TS 23.501)	

It should be noted that a number of WLAN Selection Criteria in the WLANSP policy are effectively the same as specified in the Wi-Fi Alliance Hotspot 2.0 Release 2 specification and this was done on purpose to be able to define WLAN access selection policy with metrics similar to HS2.0. This may lead to the possibility of having conflicting requirements if both a 3GPP WLAN Selection Policy and a WFA Passpoint™ Management Object were installed in the same device with different values for the common attributes for the same home network.

2.2.2 Trusted WLAN Access Network Selection[5]

To establish trusted connectivity to 5G Core via TNGF, the UE follows a series of steps to select a trusted WLAN access network as described in clause 6.3.12 in TS 23.501. For example, the UE, before it associates with a WLAN network, queries, using ANQP, the WLAN network about the list of PLMNs to which it can provide trusted connectivity. One or more WLAN networks may be discovered by the UE and the UE may use ANQP to query each of the discovered WLAN network for the list of PLMNs. Next, the UE selects a PLMN to connect to from the list of available PLMNs using the procedure described in clause 6.3.12 in TS 23.501. Finally, the UE selects a WLAN access network which provides trusted 5G connectivity to the selected PLMN. The UE uses WLANSP rules to prioritize available access networks and then selects the highest priority WLAN access network providing trusted 5G connectivity to the selected PLMN.

Similarly, to select trusted access network selection for "Non 5G-Capable over WLAN" devices to connect to 5G Core via TWIF, the UE follows a similar set of steps as described in clause 6.3.12a in TS 23.501. The UE discovers list of PLMNs with which trusted 5G connectivity without NAS is supported by available WLAN access networks e.g. using ANQP, then the UE selects a PLMN network from that list and finally selects the highest priority WLAN access network (by using WLANSP rules) which provides connectivity via TWIF to that PLMN.

2.2.3 UE Route Selection Policy (URSP)[6]

UE Route Selection Policy (URSP) is used by the UE to determine if a detected application can be associated to an established PDU Session, can be offloaded to non-3GPP access outside a PDU Session, or can trigger the establishment of a new PDU Session. It consists of a set of Route Selection Policy Rules. Each rule is made up of three main components: a rule precedence indicator to order the priority of the rules, a Traffic Descriptor which defines which traffic flows the rule applies to and a list of prioritized Route Selection Components which determine how the matching flows should be routed. Each Route Selection Component also has a set of validity criteria to indicate when it is valid.

Each URSP rule is defined as shown in Table 2-2.

---

[5] clause 6.3.12 and 6.3.12a in TS 23.501
[6] clause 6.6.2 in TS 23.503

Table 2-2 UE Route Selection Policy Rule

Information Name	Details
Rule Precedence	Determines the order in which URSP rule is enforced at the UE
Traffic Descriptor	Application Descriptor OSId (Operating System identifier) OSAppId (list) (Operating System specific Application Identifier)
	IP descriptors (list) Destination IP address, port and/or protocol
	Non-IP descriptors (list)
	Domain descriptors FQDN of destination domain
	Data Network Name (DNN)
	Connection Capabilities (list) IMS, MMS, SUPL, Internet
Route Selection Component List	Route Selection Descriptor Precedence
	SSC Mode Selection (Session and Service Continuity Mode) Mode Mode 1 – IP address continuity Mode 2 – Break before make Mode 3 – Make before break
	Network Slice Selection (list) S-NSSAI (Single-Network Slice Selection Assistance Information)
	DNN Selection (list) Data Network Name
	PDU Session Type Selection IPv4, IPv6, IPv4v6, Ethernet or Unstructured

	Non-Seamless Offload Indication
	Access Type preference 3GPP, non-3GPP or Multi-Access PDU session.

	Route Selection Validation Criteria
	
	  Time Window
	
	  Location Criteria (from TS 24.526 (UE Policies))
	
	    E-UTRA cell identities list
	
	    NR cell identities list
	
	    Global RAN node identities list
	
	    TAI list (tracking area)

These rules allow for application or destination specific tailoring of connections. Of particular relevance to Wi-Fi and 5G convergence, is the ability to specify that Wi-Fi and cellular should be bonded into a single "Multi-Access PDU" session with the Access Type preference, thus invoking the Access Traffic Steering, Switching and Splitting functionality.

2.3 Access Traffic Steering, Switching and Splitting (ATSSS)[7]

The ATSSS feature provides a multi-access PDU Connectivity Service through creation of a Multi-Access PDU (MA PDU) session, which enables PDU data delivery between the network and the UE over both 3GPP and non-3GPP access simultaneously. ATSSS supports steering functionality at both high-layer (above IP) and low-layer (below IP). In 3GPP Release 16, the high-layer steering functionality is supported via the MPTCP proxy functionality which can be used for steering TCP traffic, and low-layer steering functionality is supported via ATSSS-LL which can be used for steering TCP, UDP and Ethernet traffic. The ATSSS rules specify how the traffic is distributed over cellular and Wi-Fi for an MA PDU session as described in section 2.3.3.

2.3.1 ATSSS Architecture

In order to support the ATSSS feature, the 5G System Architecture is extended as shown in Figure 2-6.

---

[7] clause 5.32 in TS 23.501
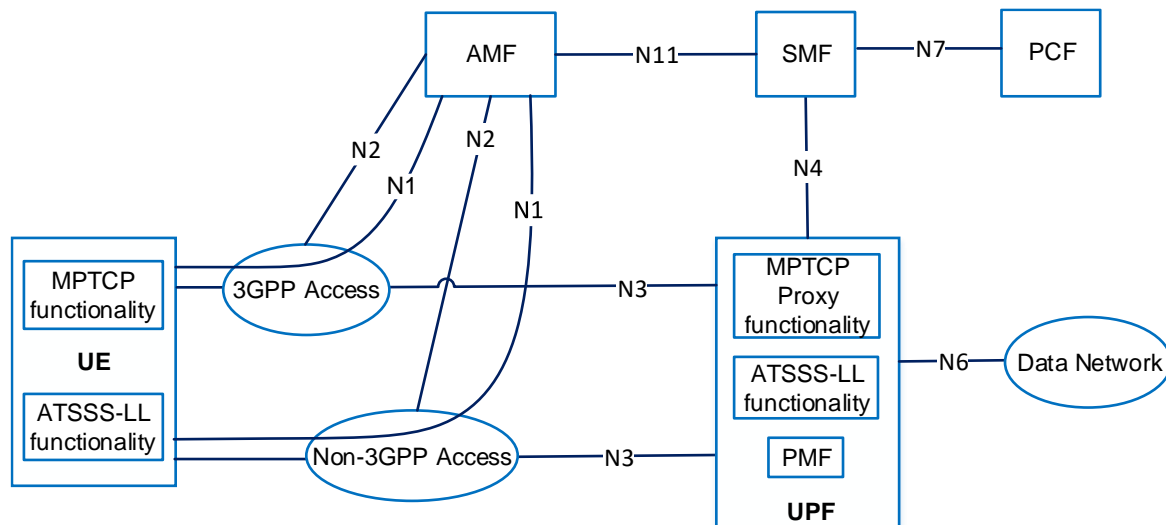
Figure 2-6 ATSSS Architecture

For the ATSSS feature, the following additional functionalities are supported by the UE and the other network functions in the 5G Core:

- The UE supports one or more steering functionalities. In Release 16 the supported steering functionalities are MPTCP and ATSSS-LL. The ATSSS-LL functionality is mandatory in the UE for MA PDU session of type Ethernet.
- The UPF supports one or more steering functionalities. In Release 16 the supported steering functionalities are MPTCP and ATSSS-LL. The MPTCP Proxy functionality within the UPF communicates with the MPTCP functionality in the UE using the MPTCP protocol. The ATSSS-LL functionality is mandatory in the UPF for an MA PDU session of type Ethernet.
- The UPF also supports a Performance Measurement Function (PMF) which may be used to request access specific performance measurements from the UE over the user-plane of 3GPP access and/or non-3GPP access when operating using ATSSS-LL. The PMF provides Round Trip Time (RTT) measurements and access availability/unavailability report from the UE.
- The AMF, SMF and PCF functions within the 5G Core are extended with the ATSSS functionalities as described in section 2.3.4.

2.3.2 ATSSS Steering Functionalities

Figure 2-7 shows ATSSS steering functionalities on a UE as described in clause 5.32.6 in TS 23.501. If the MA-PDU session is an IP session a global IP address IP@3 is assigned to this session. The ATSSS-LL (Low Layer) steering functionality steers each 5G QoS Flow over either 3GPP or non-3GPP access, thereby avoiding out of sequence delivery. The ATSSS High Layer functionality (ATSSS-HL) includes an MPTCP client functionality on the UE and an MPTCP proxy on the UPF. Link-specific IP addresses (IP@1 and IP@2) are assigned to the UE for MPTCP subflows over 3GPP and non-3GPP access between UE and MPTCP proxy.
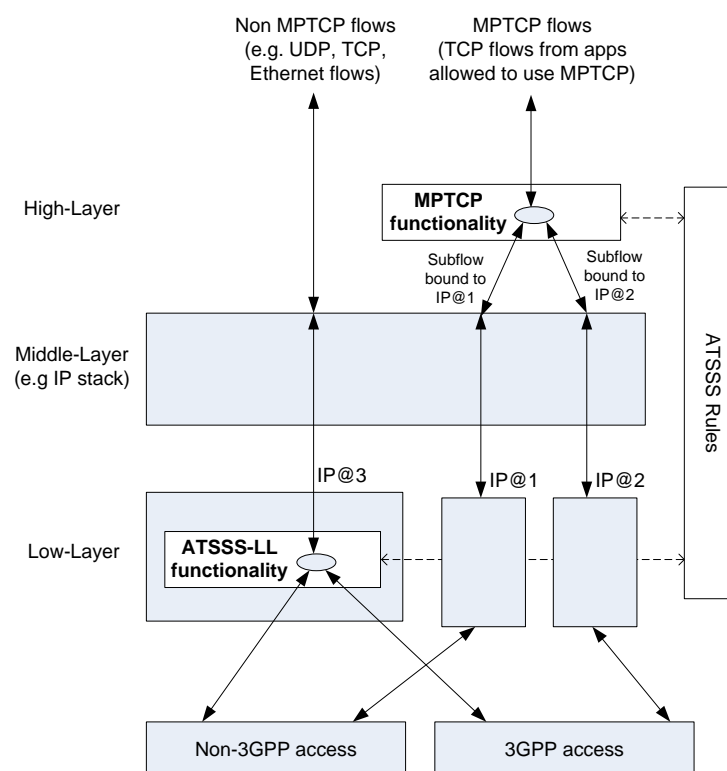
Figure 2-7 ATSSS Steering Functionality on the UE

The ATSSS MPTCP functionality operates using the IETF TCP converter protocol (RFC 8803) as described in TS 24.193. This involves following steps between MPTCP client on the UE and MPTCP Proxy on the UPF:

- The network indicates the IP address, port number and proxy type (converter in Release 16) of one or more MPTCP proxies in the UPF to the UE as part of ATSSS container sent to UE.
- The UE selects and sends TCP SYN with MP_CAPABLE option to the IP address of an MPTCP converter proxy inside the UPF.

- The UE adds the Server's IP address and port in the payload of the TCP SYN as the converter protocol header.
- The UE translates the IP Source Address (IP@3) of uplink traffic to link-specific address IP@1 or IP@2 depending on which link is used as the primary subflow for MPTCP.
- The UPF translates the received link-specific IP address for uplink traffic to IP@3.
- The UE sends TCP SYN with MP_JOIN option to the IP address of the selected MPTCP converter proxy inside the UPF with the second link specific address, for adding the second subflow over MPTCP.

2.3.3 ATSSS Rules[8]

ATSSS rules specify how Wi-Fi and cellular should be bonded together on an application or source/destination specific basis. The rules apply to a specific Multi-Access PDU session and, unlike the ANDSP and URSP rules, these rules are delivered after establishment of the relevant MA PDU session as part of PDU session procedures.

The two most significant parts of an ATSSS rule are the Steering Mode and Steering Functionality fields. These effectively define the traffic distribution policy and which protocol should be used to transport the data.

Steering mode defines how the traffic for a Service Data Flow (SDF) should be carried across 3GPP and non-3GPP access. An SDF is an aggregate set of packet flows that matches traffic filters specified in the Traffic descriptor part in the ATSSS rule.

Four options are supported for the Steering Mode:

- <u>Active Standby</u>: One access is identified as the default/active access and the SDF traffic is routed over this unless that access becomes unavailable, in which case the traffic is routed over the other access. When the active access becomes available again, the traffic is switched back to that access.
- <u>Smallest Delay</u>: The SDF traffic is sent over the access link with the smallest delay. PMF defines procedures for determining the latency of each link or the latency measurements can be obtained from the underlying multipath protocol.
- <u>Load Balancing</u>: A fixed percentage is specified for the fraction of the SDF traffic that should be sent over the 3GPP network, with the remainder of the traffic sent on the non-3GPP network. This mode is only applicable to non-GBR QoS flow.

---

[8] clause 5.32.8 in TS 23.501

- Priority Based: The SDF traffic is transmitted over a specified high priority access (Wi-Fi or 3GPP) until that access becomes congested. The traffic then overflows onto the other access. Also, when the high priority access becomes unavailable, all traffic is switched to the other access. The determination of when an access is considered "congested" is implementation specific.

An ATSSS policy consists of a set of ATSSS Rules as outlined in Table 2-3.

Table 2-3 ATSSS Rules

Information Name	Details		
Rule Precedence	Determines the order in which the ATSSS rule is evaluated in the UE.		
Traffic Descriptor	Application Descriptor (list)		
	IP descriptors (list) 5-tuple: IP source and destination addresses and ports and protocol		
	Non-IP descriptors (list) Destination of non-IP (Ethernet) traffic		
Access Selection Descriptor	Steering Mode	Active Standby Active = 3GPP | non-3GPP	
		Smallest Delay (see 5.32.5 of 23.501 for Access Network Performance Measurements)	
		Load-Balancing 3GPP% = Percentage Non-3GPP% = 100% - 3GPP%	
		Priority-based Priority Access = [3GPP | non-3GPP]	
	Steering Functionality MPTCP or ATSSS-LL		

As far as the Steering Functionality is concerned, in Release 16 the MPTCP is the only viable option for packet level switching and splitting, as the ATSSS-LL only provides flow based data switching between two accesses.

2.3.4 ATSSS Procedures for Traffic Routing[9]

For ATSSS based traffic distribution, an MA PDU session can be created only when both the terminal and the 5G Core are ATSSS capable. The UE may request an MA PDU session when the UE is registered via both 3GPP and non-3GPP accesses, or when the UE is registered via one access only. The traffic of an MA PDU session can be transferred over 3GPP access or over non-3GPP access or over both accesses. How the traffic is transferred over the available accesses of an MA PDU session is controlled by the applicable ATSSS policy created by the 5G Core.

The PDU Session Establishment Request message is initiated by the UE and sent either over the 3GPP access or over the non-3GPP access and it includes both an MA PDU Request indication as well as an ATSSS Capability (e.g. an "MPTCP Capability" or "ATSSS-LL Capability" or both). The AMF, on receiving this message, informs the SMF that the request is for an MA PDU Session and whether the UE is registered over both accesses.

Based on the user subscription, the SMF determines if the MA PDU session is allowed and which ATSSS capabilities are supported for the MA PDU session and sends this information to the PCF. Based on operator policy and subscription data, the PCF creates PCC rules for the MA PDU session that include ATSSS policy control information and sends to the SMF. From the received PCC rules, the SMF derives (a) *ATSSS rules*, which are sent to UE for controlling the traffic steering, switching and splitting in the uplink direction, and (b) *N4 rules*, which are sent to UPF for controlling the traffic steering, switching and splitting in the downlink direction.

If the UE indicates support of "ATSSS-LL Capability", the SMF may derive the Measurement Assistance Information for PMF measurements and send to UE. If the UE indicates support of "MPTCP Capability" and network accepts enabling that functionality, the SMF provides MPTCP related steering functionality information which includes link specific IP addresses for 3GPP and non-3GPP access and MPTCP proxy information. The ATSSS rules, the Measurement Assistance Information and the MPTCP steering functionality information are sent to UE as part of an ATSSS container IE in the PDU Session Establishment Accept message.

---

[9] clause 4.22.2 in TS 23.502

The SMF establishes the user-plane resources over the requested accesses per UE registration status. When the UE is registered over both accesses, two separate N3/N9 tunnels are established between the 5G Core and 3GPP access and the 5G Core and non-3GPP access for PDU data transfer.

After the establishment of an MA PDU Session, and when there are user-plane resources on both access networks, the UE applies ATSSS rules and considers local conditions (such as network interface availability, signal loss conditions, user preferences, etc.) for deciding how to distribute the uplink traffic across the two access networks. Similarly, the UPF anchor of the MA PDU Session applies N4 rules and feedback information received from the UE via the user-plane (such as access network Unavailability or Availability) for deciding how to distribute the downlink traffic across the two N3/N9 tunnels for two access networks. When there are user-plane resources on only one access network, the UE may consider the ATSSS rules and local conditions for triggering the establishment or activation of the user plane resources over the other access.

2.4   End-to-End QoS

A UE can establish single access or multi-access PDU session carrying 5G user plane traffic over WLAN access. These PDU sessions carry user data traffic over 5G QoS flows. The 5G QoS model defines QoS requirements for 5G QoS flows which are also applicable when these flows are carried over WLAN access. This section describes the 5G QoS model as well as QoS related signalling and flow data transport behaviour defined for WLAN access.

2.4.1   5G QoS Model for non-3GPP Access[10]

The 5G QoS model, as used over the 3GPP access, is also followed when UE accesses the 5G Core over non-3GPP access. The QoS flow, identified by a QoS Flow Identifier (QFI), differentiates QoS at the finest granularity for the non-3GPP access, both for the single-access PDU sessions established over non-3GPP access and also for the multi-access (MA) PDU sessions carrying traffic over both 3GPP access and non-3GPP access.

For an MA PDU session, a QoS flow is not associated with specific access i.e. it is access agnostic, and the same QoS is supported for the QoS flow when the traffic is distributed over the 3GPP access and/or the non-3GPP access. A QoS flow can be either guaranteed bit rate flow (GRB QoS flow) or non-guaranteed bit rate flow (Non-GBR QoS flow).

---

[10] clause 5.32.4 and 5.7 in TS 23.501

A QoS flow carried over WLAN access has the following associated information:

- A <u>QoS Profile</u>, provided to the N3IWF or TNGF
- One or more <u>QoS Rules</u>, either signaled to the UE or derived by the UE by applying Reflective QoS control, and <u>QoS Flow Descriptions</u> for QoS flows sent to the UE
- One or more <u>Packet Detection Rule (PDR)</u> provided to the UPF

A QoS Profile is defined for each QoS flow and includes QoS parameters as specified in Table 2-4. The QoS Profile is sent to the N3IWF or TNGF as part of the PDU session establishment or modification procedure. For a non-GBR flow, for a MA PDU session, the QoS profile is sent to both 3GPP and non-3GPP access networks over N2, if the UE is registered over both accesses. For a GBR flow, the QoS profile is sent to only one access network based on PCC rules. Currently, no traffic splitting is supported for the GBR flow. The QoS Profile information is used by the N3IWF and TNGF to map QoS flows to IPsec child security associations (SAs).

Table 2-4 QoS Profile parameters

Parameters	Description
5G QoS Identifier (5QI)	A 5QI is a scalar that is used as a reference to 5G QoS characteristics, which are used by the access network to control packet forwarding treatment for the QoS Flow. Standardized 5QI values have one-to-one mapping to a standardized combination of 5G QoS characteristics (Table 5.7.4-1 in TS 23.501).
5G QoS Characteristics	(Optional) 5G QoS Characteristics are included for dynamically assigned 5QI and describe the end to end packet forwarding treatment that a QoS Flow receives between the UE and the UPF.
Allocation and Retention Priority (ARP)	The ARP specifies the relative importance of a QoS flow compared to other QoS flows for allocation and retention of RAN resources.
For Non-GBR QoS Flow only	
Reflective QoS Attribute (RQA)	(Optional) The RQA indicates that certain traffic carried on this QoS Flow is subject to Reflective QoS. When RQA is signalled, the 5G access network enables the transfer of RQI marking for the QoS Flow to the UE. For non-3GPP access, RQA is not used. N3IWF and TNGF transparently include RQI marking for the packet, if received over N3.
For GBR QoS Flow only	
Guaranteed Flow Bit Rate (GFBR) – UL and DL	GFBR denotes the bit rate that is guaranteed to be provided to the QoS Flow over the Averaging Time Window.
Maximum Flow Bit Rate (MFBR) – UL and DL	Highest bit rate that is expected by the QoS Flow.
Maximum Packet Loss Rate – UL and DL	(Optional) Indicates maximum rate for lost packets that can be tolerated in the UL and DL direction.
Notification Control	(Optional) Indicates whether notifications are requested from the RAN when the GFBR can no longer (or can again) be guaranteed for a flow.

The QoS Rules are specified per PDU session and are used by the UE to map UL traffic to QoS flows for that PDU session. The QoS rules may be explicitly signaled to the UE during the PDU session establishment or modification procedure, pre-configured in the UE or implicitly derived by the UE by applying Reflective QoS based on DL traffic. More than one QoS rule can be associated with the same QoS flow. A default QoS rule is signaled for every PDU Session.

For Reflective QoS, the UE derives a QoS rule when it receives a DL packet marked with the Reflective QoS Indication (RQI), if such a derived QoS rule does not exist already. Each derived QoS rule has an associated timer and the rule is deleted upon timer expiry. A QoS rule contains parameters as specified in Table 2-5

Table 2-5 QoS Rule parameters

Parameters	Description
QoS Flow Identifier (QFI)	Indicates QoS flow associated with the QoS rule.
QoS Rule Identifier (QRI)	(Optional) Included only for signaled QoS Rule. QRI is unique within the PDU Session.
Default QoS rule indication	(Optional) Applicable only for signaled QoS Rule.
Packet Filter Set	(Optional) Zero or more packet filters to identify packet flow(s). Packets Filter Set could be IP Packet Filter Set (for IP PDU Session type) or Ethernet Packet Filter Set (for Ethernet PDU Session type). Packet Filter Set may not be included for default QoS rule.
Precedence Value	Determines the order in which the QoS rule is evaluated. Set to 80 (decimal) for derived QoS rule.

The QoS Flow Descriptions information is optionally sent to the UE as part of the PDU session establishment or modification procedure and includes parameters as specified in Table 2-6. These QoS parameters are used by the UE to provide QoS differentiation for the indicated QoS flow.

Table 2-6 QoS Flow Descriptions parameters

Parameters	Description
QoS Flow Identifier (QFI)	Indicates QoS flow associated with the QoS rule.
5QI	(Optional) Included if the QFI is not the same as 5QI.
For GBR QoS Flow only	
Guaranteed Flow Bit Rate (GFBR) - UL and DL	The bit rate that is guaranteed to be provided to the QoS flow over the Averaging Time Window.
Maximum Flow Bit Rate (MFBR) - UL and DL	Highest bit rate that is expected by the QoS Flow.
Averaging Window	(Optional) The duration over which the GFBR and MFBR is calculated.

The Packet Detection Rule(s) are used to classify a user plane packet arriving at the UPF. PDRs are used by the UPF to map and forward traffic over the N3/N9 core network tunnel (CN tunnel) created with the N3IWF or TNGF. Table 2-7 lists some of the relevant information contained in a PDR (clause 5.8.2.11.3 in TS 23.501). The PDR also includes an optional Multi-Access Rule ID, included for a MA PDU session, and refers to a Multi-Access Rule (MAR) which specifies steering mode and steering functionality for ATSSS. For DL user data mapped to a PDR, the associated MAR (if any) is used by the UPF to determine how the DL data will be routed over 3GPP access and non-3GPP access.

Table 2-7 Packet Detection Rule - selected parameters

Parameters	Description
Rule ID	Unique identifier for the rule
Precedence	Determines the order in which detection information of PDRs is applied
CN Tunnel Info	CN tunnel info on N3, N9 interfaces for forwarding user plane traffic to access network
Packet Filter Set	One or more packet filters to identify packet flow(s). Packets Filter Set could be IP Packet Filter Set (for IP PDU Session type) or Ethernet Packet Filter Set (for Ethernet PDU Session type).
Application ID	(Optional) Provides an index to a set of application detection rules configured in the UPF.
QoS Flow Identifier	Indicates QoS flow associated with the PDR rule. Contains the value of 5QI or non-standardized QFI. QFI is inserted in the N3/N9 tunnel header for DL packets.
Multi-Access Rule ID	(Optional) Identifies a Multi-Access Rule (MAR) to be applied for handling packet forwarding for a MA PDU session. The MAR Indicates steering mode and steering functionality.
List of QoS Enforcement Rules (QER)	Define how packet is treated in terms of bit rate limitations and packet markings for QoS purposes. Controls marking of RQI in the packets. (clause 5.8.2.11.4 in TS 23.501)

Each PDU session is also associated with per Session Aggregate Maximum Bit Rate (Session-AMBR). The Session-AMBR limits the aggregate bit rate that can be expected to be provided across all Non-GBR QoS Flows for a specific PDU Session, and is signalled to the UPF, the UE and to the access network. The UPF and UE perform Session-AMBR enforcement.

Each UE is also associated with per UE Aggregate Maximum Bit Rate (UE-AMBR). The UE-AMBR limits the aggregate bit rate that can be expected to be provided across all Non-GBR QoS Flows of a UE and is enforced by the 3GPP RAN in DL and UL direction.

2.4.2 QoS Signaling on N3IWF and TNGF[11]

The N3IWF and TNGF provide QoS signaling to support QoS differentiation over the untrusted WLAN access and trusted WLAN access respectively. During the PDU session establishment procedure, the N3IWF/TNGF determines the number of user plane IPsec child SAs to establish with the UE and the QoS profiles associated with each child SA, based on local policies, configuration and the QoS profiles. One IPsec child SA can be associated with one or more QoS flows of the PDU session. The N3IWF/TNGF sends a Create_Child_SA request to the UE to establish a child SA. This message includes a 5G_QOS_INFO Notify payload which contains QoS specific parameters as captured in Table 2-8. If additional IPsec child SA(s) need to be established, a separate Create_Child_SA request is sent to the UE for each child SA.

The N3IWF or TNGF can associate a DSCP value with an IPsec child SA, in an implementation specific way. If a DSCP value is associated with the child SA, then the UE and the N3IWF or TNGF mark all IP packets sent over this child SA with that DSCP value.

As an example scenario, if a MA PDU session has two associated QoS flows with different QoS Profiles (e.g. one for video streaming and one for real time gaming), then the N3IWF/TNGF can determine to create two separate IPsec child SAs for these QoS flows and set the DSCP value differently for those child SAs.

If TNGF aggregates multiple GBR flows or multiple Non-GBR flows into the same IPsec child SA, the TNGF derives, in an implementation specific way, the QoS Characteristics and/or the GBR QoS Flow Information of the aggregated flow by considering information provided for individual flows as part of the QoS Profile. This information is provided as Additional QoS Information to the UE for that child SA.

For trusted WLAN access, TNGF may reserve WLAN access network QoS resources for the IPsec child SA based on the associated QoS profiles. In addition, the UE may reserve WLAN access network resources based on the Additional QoS Information received for the associated IPsec child SA. However, how these resource reservations can be done to provide QoS differentiation on the WLAN access network is not specified and is left to the implementation.

---

[11] clause 4.4 and 7.5 in TS 24.502, clause 4.12.5 and 4.12a.5 in TS 23.502

Table 2-8 5G_QOS_INFO Notify Payload

Parameters	Description
PDU Session ID	Identifier for the PDU session associated with the child SA.
QFI(s)	(Optional) If included, indicates list of QoS flows associated with the IPsec child SA.
DSCP value	(Optional) A DSCP value associated with the child SA.
Default Child SA indication	(Optional) For a given PDU session, there can be only one default child SA. All QoS flows for which no specific mapping to a child SA is specified, are sent over the Default child SA.
Additional QoS Information	(Optional) Included for trusted WLAN access. It includes QoS characteristics identified by 5QI and GBR QoS flow information as provided in the QoS profile. It can be used by UE to reserve resources on trusted WLAN access.

2.4.3   QoS Flow Data Transport over WLAN Access[12]

For UL traffic over both trusted and untrusted WLAN access, the UE associates UL user data with a QFI based on packet filter matching between QoS rules and the UL packet. The UE then encapsulates the UL packet inside a GRE packet, with the GRE header carrying the QFI. The UE further encapsulates the GRE packet into an outer IP packet and sends to the N3IWF/TNGF over the IPsec child SA associated with the QFI. If a DSCP value is associated with the IPsec child SA, then the UE marks the IP packet with that DSCP value.

For DL over both trusted and untrusted WLAN access, the UPF maps the user data packet to a QoS flow based on packet filter matching between PDRs and DL packet. UPF includes QFI, and RQI in the GTP-U encapsulation header on the N3 interface. Upon receiving a DL packet for a PDU session over N3, the N3IWF/TNGF uses the PDU session and QFI information to find the associated IPsec child SA to use for sending the DL packet. The N3IWF/TNGF encapsulates the DL packet into a GRE packet, with the GRE header carrying the QFI and RQI information. The GRE packet is further encapsulated into an outer IP packet and sent to the UE over the selected IPsec child SA. If a DSCP value is associated with the IPsec child SA, then the N3IWF/TNGF marks the IP packet with that DSCP value.

---

[12] clause 4.4.2.3 and 8.3 in TS 24.502

2.4.4   Interworking between QoS Rules and ATSSS Rules[13]

For user traffic delivered via an MA PDU session, both ATSSS rules and QoS rules are applied.

For an MA PDU session, the UE receives ATSSS rules as part of the PDU session establishment or modification procedures. The ATSSS rules are used by the UE to govern traffic distribution over 3GPP access and non-3GPP access for MA PDU sessions as described in 2.3.3. The UE evaluates ATSSS rules to determine the steering mode and steering functionality for the UL traffic, based on UL packet matching with Traffic Descriptor specified in ATSSS rules. For a GBR QoS flow carried over an MA PDU session, the ATSSS rules only specify a single access where that flow can be transmitted. If the network wants to move that GBR QoS flow to the other access, the network needs to update the ATSSS rules on the UE to indicate the new access.

The UE receives QoS rules as part of the PDU session establishment or modification procedure as described in 2.4.1. For an MA PDU session, the QoS rule(s) received by the UE over one access are used for both 3GPP access and non-3GPP access, so the QoS classification for traffic is independent of ATSSS rules. The UE evaluates QoS rules to determine which QoS flow can be used to deliver the UL traffic within the MA PDU session, based on UL packet matching with Packet Filters specified in the QoS rules.

The UL traffic gets delivered over the selected QoS flow which gets distributed over the 3GPP access and/or the non-3GPP access based on the steering mode and steering functionality of the matching ATSSS rule.

3   Challenges and Gaps with 5G and Wi-Fi Interworking

This section identifies some key challenges and gaps in the current 3GPP defined solution to support the interworking between WLAN and 3GPP 5G system and suggests high level solutions to address some of the gap items. These identified gaps and issues need to be addressed by the industry and standards bodies within the cellular and/or the WLAN domain (e.g. 3GPP, IEEE or WFA) to fully enable interworking between WLAN and 5G systems.

3.1   Access Network Selection Challenges

The UE uses the WLANSP rules specified in the ANDSP policy to select a preferred WLAN access network in case of both untrusted and trusted WLAN access. The WLANSP rules specify MaximumBSSLoad and MinimumBackhaulThreshold as selection criteria, among

---

[13] clause 5.32.4 and 5.32.6 in TS 23.501

other WLAN access attributes. However, the WLAN selection criteria specified in WLANSP do not consider other Wi-Fi QoS metrics such as the estimated average or minimum throughput in UL and DL per band, maximum number of connected clients per band, supported frequency bands etc. Hence, even after using the WLANSP rules, the UE may still end up selecting a preferred WLAN access network which may not provide a high quality connection to the end user.

It would be desirable to take into account some of the Wi-Fi QoS metrics as listed above in the WLAN access network selection at the UE to select a high quality WLAN connection. Following key components need to be considered for enhancing WLAN access selection:

- Enhancement to WLANSP rules to consider additional Wi-Fi QoS metrics e.g. estimated throughput in UL and DL per band, maximum number of connected clients per band, supported frequency bands.
- Exposing Wi-Fi QoS metrics APIs to provide AP and STA QoS measurements to be used for WLAN access selection at the UE.
- Exposing IP Service Level metric APIs to provide WAN measurements to be used for WLAN access selection at the UE.

The WBA paper on 'Quality of Service on Carrier Grade Wi-Fi' [22] lists a number of Wi-Fi QoS metrics and thresholds. That paper also describes options for Wi-Fi QoS metrics APIs at different levels of capabilities including expanding ANQP protocol with Wi-Fi QoS fields as well as defining a RESTful API to provide QoS metrics. More recently, WBA OpenRoaming™ has included concepts of sharing real-time QoS information between federation members to enhance authorization decisions [24]. In the context of 5G system, it becomes important to revisit those aspects from the WBA QoS paper [22] to enable selection of a preferred WLAN access network providing high quality connection based on considering Wi-Fi QoS metrics.

3.2 ATSSS Challenges

3GPP ATSSS is a new feature added in Release 16 which enables transfer of the PDU session data between the 5G Core network and the UE over 3GPP and non-3GPP access simultaneously. In this section we examine challenges and gaps related to various aspects of the ATSSS feature.

3.2.1 Policy Combining

The 3GPP ATSSS architecture assumes that all Service Provider and Application Provider multi-path policies are "combined" using the 5G defined Service Based Architecture (SBA) before being signaled to the Policy Enforcement Points, i.e., the UPF in the 5GC for enforcing down-link policies and the UE for enforcing up-link policies.

However, 3GPP is opaque when it comes to how policies signaled to the UE using the ATSSS container are combined with other UE-based policies. For example, TS 24.193 specifies that the UE can take into account "local conditions" that include user preferences, when enforcing up-link policies. However, "local-conditions" could include application polices signaled using enhanced transport services APIs within the device, or policies delivered using "enterprise-agents" that are used to configure enterprise IT Admin policies. This can result in the path-selection decisions enforced in the UE being different from the path-selection decisions enforced by the UPF.
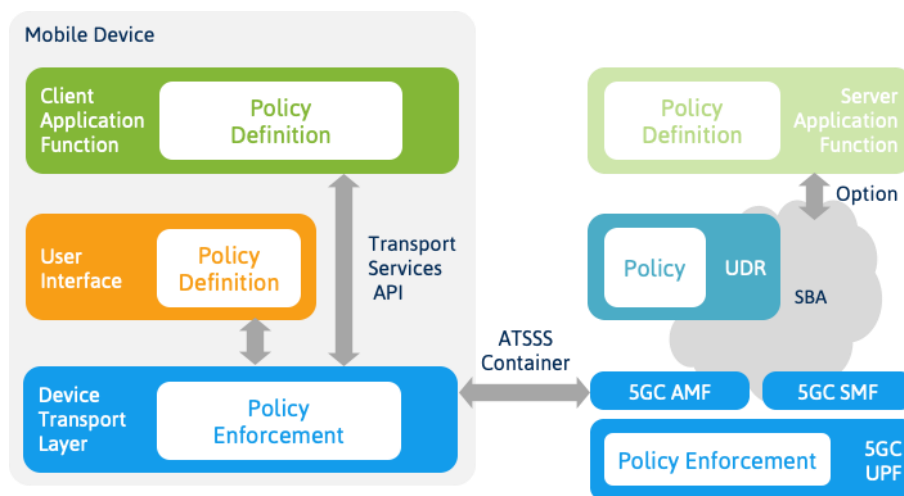
Figure 3-1: Handling ATSSS Policy Combining with Policies from other Stakeholders

One of the challenges with the current ATSSS architecture is to provide more clarity regarding how various policies get combined on the UE, including recommendations of how to deal with policy conflicts.

3.2.2 Multi-Path Server Proxy Deployment

3GPP defines use of IETF converter protocol (RFC 8803) for ATSSS MPTCP functionality. The use of the IETF converter functionality is based on the requirement that all network attachments are managed by the same administrative entity, ensuring that anti-spoofing filters are enforced. This means that the entity offering the connectivity service must be identical to the entity that operates the transport converter proxy, with transit over third party networks explicitly forbidden. However, the use of MPTCP converter proxy for ATSSS supports WLAN access networks which may be third party owned because IPsec tunneling is used to traverse such networks.

This approach is in contrast to earlier realization based on the SOCKSv5 protocol that benefit from authentication exchanges between the client and the proxy which then enables the proxy service to be realized independently of the 5GC operator.

Moving forward, many enterprises are now integrating multi-path into their software Defined Wide Area Network (SD-WAN) solutions, meaning that the proxy may need to be able to be operated by a third party independent of the 5GC administrative domain. Hence, enhancing the architecture and/or protocols to enable flexibility in deployment of the Multi-Path Server proxy can broaden the use-cases where ATSSS can be applied.

3.2.3   Incorporating UE Local Conditions in ATSSS

Current ATSSS policy does not adequately take into account UE local conditions (e.g., battery state, access cost, and thermal conditions). As a result, the network may configure a UE with ATSSS rules that select an access that is not favored by the UE due to local conditions. For example, due to power consumption concern, a UE may prefer Wi-Fi access over cellular access. However, a network without having knowledge of UE local conditions may configure ATSSS rules requiring the UE to use cellular access.

Local conditions at the UE should also influence the access used for downlink traffic. As mentioned in the previous example, if the UE prefers a specific access due to power consumption concern for UL traffic steering, the UE may also want the network to use the same access for DL traffic steering.

In addition, ATSSS policy does not take into account exceptional situations that may occur at the UE. For example, the UE may be overheating or its battery may be running low. In these circumstances, the UE should not only be allowed to choose whichever access for uplink it deems best, it should also be able to indicate to the network the current status (e.g., overheating indication) and the preferred access for downlink. Enhancing existing steering modes and signaling exchanges to support these kinds of exceptional situations can be desirable for UE vendors.

3.2.4   Support for Packet Level Traffic Steering for all Traffic Types in ATSSS

ATSSS supports two steering functionalities for delivering application traffic:

- High Layer, which operates above the IP layer; Release 16 supports only one High Layer steering functionality – Multi-Path TCP. This can only be used to deliver TCP traffic flows with all ATSSS steering modes and uniquely, it supports packet by packet traffic splitting for applicable steering modes.
- Low Layer, which operates below the IP layer; Release 16 only specifies one Low Layer steering functionality which is referred to as ATSSS-LL. This can be used to

deliver all traffic types including TCP, UDP and ethernet with all ATSSS steering modes. ATSSS-LL does not apply a specific protocol to carry the traffic. It is a data switching capability which can make use of a Performance Measurement Function (PMF) to assist in making traffic routing decisions. However, unlike Multi-Path TCP, ATSSS-LL does not provide a packet by packet splitting capability. It can only split traffic at the flow level.

An ATSSS-HL (High Layer) capable UE will contain an MPTCP client and the 5G Core UPF will contain an MPTCP proxy that provide protocol conversion (RFC 8803) of an E2E application's TCP flow to MPTCP (by extending the TCP header with an MPTCP options block). Therefore, it is only possible to deliver TCP traffic using this mechanism. The UE and UPF MPTCP functionality work together to provide packet by packet routing and subsequent recombination for both the uplink and downlink traffic, ensuring that the original TCP flow is delivered in its original form i.e. it operates as a transparent proxy for the E2E traffic.

There is a requirement to be able to use the ATSSS framework to carry all traffic types, where delivery of successive PDUs (Protocol Data Units) can be split across available accesses. This will provide full support of latency sensitive non-TCP traffic such as UDP based real time communications and emerging 5G low latency applications, as well as QUIC based applications, which is likely to grow significantly in usage over the next few years.

In order to support all traffic flows in ATSSS, a supplementary protocol is required that can carry this traffic without adding significant additional latency. This supplementary protocol should satisfy the following requirements:

- Can work in an 'unreliable' mode where lost/late packets are not resent.
- Provide MPTCP like link estimation to allow real time adaptation of packet distribution. This will also be beneficial for fast switching of flows for soft handovers when path degradation has been detected (The PMF capability is unlikely to provide a fast-enough indication of path degradation for soft handovers in ATSSS-LL).
- Does not add significant additional overhead such as encryption – encryption is unnecessary as all traffic delivered over the ATSSS framework will be secured. (This does not have any impact on encrypted E2E application traffic).
- In order (but not reliable) delivery of packets per flow must be supported, but it should be possible to disable this feature for specific applications if required.
- Consideration should also be given to the impact of nesting similar congestion control/reliability mechanisms as in some circumstances this will degrade application performance.

The recently revised IETF charter for QUIC includes extensions to support Multipath and Datagram delivery by December 2021. Together, these two extensions may satisfy many of the requirements for a supplementary ATSSS protocol. The 3GPP, in phase 2 of the ATSSS implementation in Release 17, is studying whether QUIC and its extensions will provide a suitable solution, as described in 3GPP TR 23.700 [25].

3.2.5   ATSSS Operation with MP-CAPABLE Servers

The multi-path TCP proxy functionality used in ATSSS leverages the IETF defined transport convert protocol (RFC 8803). This protocol has been designed to assist the deployment of TCP extensions such as Multipath TCP. The convert protocol specifically enables co-existence with servers that are MP-capable as shown in Figure 3-2, but the operation of ATSSS in such situations is not defined and related gaps in the current 3GPP specification are described here.

The use of the convert protocol enables a UE to discover that a server natively supports the Multi-Path TCP option, enabling a UE to bypass the multi-path TCP proxy for any subsequent Multi-Path TCP connections that it initiates towards the same server. However, for the UE to benefit from the MP-capability of the server, the UE needs to be able to signal the server using unique IP addresses for each sub-flow. The ATSSS architecture does not require the link-specific IP address used by the UE to be routable over the N6 connection, and hence the UE cannot be sure it can benefit from the native Multi-Path support of the server while using the existing MA-PDU Session. Alternatively, the UE may infer that the link-specific IP addresses are not routable over the N6 connection and hence, if the UE is to benefit from the native Multi-Path-capable support of the server, it will need to use a single Access PDU session to access the server over 3GPP access and use the MPTCP client outside of ATSSS to establish multi-path connectivity with the server. In either case, the operation of the UE is not defined.
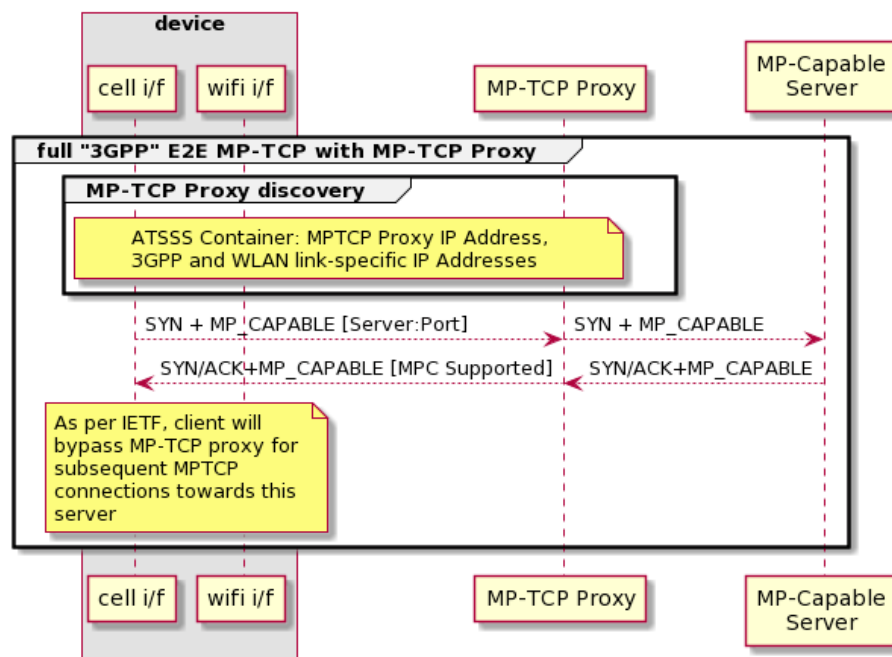
Figure 3-2 ATSSS Operation with an MP Capable Server

Note, as a deployment option, the IETF converter specification enables the operator of the MPTCP proxy to enforce local policies whereby they can define which TCP options to be used when establishing a connection between the MPTCP proxy and the server. Hence, the operator of the ATSSS system is permitted to remove the MP_CAPABLE option from the TCP SYN message sent between the MPTCP proxy and the remote server, which will prevent the discovery of MP-Capable server by the client.

3.2.6   Incorporating RAN Measurements in ATSSS

Current ATSSS rules define four steering modes to steer, switch and split traffic over 3GPP and non-3GPP access as described in section 2.3.3. These rules allow dynamic change of traffic distribution over the two accesses. For ATSSS-HL (MPTCP), traffic distribution can be dynamically updated through MPTCP packet scheduler and congestion control mechanism, and several MPTCP Congestion Control Algorithms (CCA) have been proposed. For ATSSS-LL, change of traffic distribution can be done according to access availability for Active-Standby mode and path delay measurements over PMF for Smallest Delay mode. In addition, ATSSS rules support concurrent use of 3GPP and non-3GPP access for Load Balancing and Priority-Based modes. However, for these two modes ATSSS does not specify any mechanism for dynamic traffic distribution over the two accesses taking into account radio link conditions. For Load Balancing mode, determination of split percentage over 3GPP and non-3GPP access is statically done based on PCC rule and can not be dynamically

adjusted based on access network radio conditions. For Priority-Based mode, determination of congestion on an access for ATSSS-LL is left up to the implementation based on PMF end-to-end measurements and not considering radio link conditions from access networks to determine congestion.

To take full advantage of both 3GPP and non-3GPP accesses, the 5G system should enable distribution of traffic across two accesses in a manner that improves user experience with efficient radio resource usage. Current ATSSS-LL solution can only adjust traffic distribution across 3GPP and non-3GPP access in a reactive manner after detecting noticeable network performance degradation based on PMF measurements, and the time-scales required to make such a determination is not defined. Similarly, the higher layer MP-TCP solution and the QUIC-based solution under discussion in Release 17 depend on end-to-end feedback towards their respective Congestion Control Algorithms to perform congestion and rate control where the time-scales required to adapt to the feedback is a function of the specific algorithm. These congestion control algorithms can detect access network quality degradation based on packet loss and the ACK time out window can limit how fast packet loss can be detected. In addition, due to the lack of knowledge on other TCP/UDP flows, end-to-end feedback based multipath congestion control needs to trade-off between responsiveness and being fair to other flows (RFCs 6182 and 6356 for MPTCP) and as a result can be slow in adapting to the network delay profile.

Radio measurements from RAN nodes (NG-RAN or WLAN AP) can provide timely indication of radio access conditions such as radio link quality, access network load condition and delay statistics of radio links to the 5G Core. In an enhanced architecture, the 5G Core could use RAN measurements to compare different radio accesses and proactively adjust ATSSS traffic distribution across 3GPP and non-3GPP access taking into account RAN measurements along with traffic distribution policies (e.g. from operators or applications). With RAN measurements, radio link degradation can be detected much faster in the order of 10-100msec, as compared to schemes which rely only on end-to-end delay measurements such as MPTCP, MPQUIC and ATSSS-LL, where reaction time could be much higher possibly in the order of seconds. RAN measurements can also be useful for MPTCP and MPQUIC based solution e.g. to determine whether a sub-flow should be added or removed as well as to estimate path characteristics providing input to the Congestion Control Algorithms for selecting packet scheduling policy [21]. RAN measurements taken at the UE can be used for dynamic ATSSS traffic distribution for UL traffic over 3GPP and non-3GPP access. Overall, the RAN measurements based approach can enable more efficient use of access network resources and better QoS guarantees through tight traffic management at the 5G Core across multiple accesses.

RAN measurements can be reported during the session establishment phase from RAN nodes to the 5G Core. Subsequent RAN measurements can be reported periodically or upon certain triggering conditions, such as considerable drop in signal quality. In contrast to PMF which injects traffic over the user plane, the RAN measurements based approach does not add extra traffic over the user plane. RAN measurements from a RAN node may include measurements taken by the RAN node or measurements reported by the UE to the RAN node and can be reported over N2 or N3 interface to the 5G Core. For trusted WLAN, RAN measurements can be reported by the trusted WLAN AP to TNGF. Local RAN measurements from the UE can also be reported directly to the UPF over PMF messaging, an approach which can be used for untrusted WLAN deployments. Many existing RAN measurements in 3GPP and WLAN access are useful for determining dynamic traffic distribution. For example, RSRP (reference signal received power) and RSRQ (reference signal received quality) for 3GPP access and RSSI (received signal strength indicator) for WLAN can indicate radio link quality. The UL and DL data rate estimates can be reported by the NG-RAN and WLAN AP based on past MCS used for transmission. Network load condition can be reflected via PRB (physical resource blocks) usage for 3GPP access and BSS load for WLAN. RAN nodes can also provide L2 latency measurements or queuing latency can be estimated based on RAN resource utilization level.

Overall, enhancing ATSSS steering modes to incorporate RAN measurements for dynamic traffic distribution over 3GPP and non-3GPP access can be beneficial to provide better QoS guarantee and more efficient radio resource usage for 5G services and applications. 3GPP Release 17 ATSSS phase 2 study item is considering enhancements to steering modes and PMF measurements to support dynamic traffic splitting over 3GPP and non 3GPP access. However, the scope of ATSSS phase 2 study item is limited requiring that there be no RAN impact, hence RAN measurements based approach can not be considered in Release 17. Such an approach can be considered in 3GPP Release 18 timeframe to support dynamic traffic distribution for ATSSS where RAN measurements can be used as input for high-layer and/or low-layer ATSSS functionality.

3.2.7   Interworking Challenges with Outer MPTCP

3GPP ATSSS-HL MPTCP should be considered as "Inner" MPTCP since mobile device manufactures, operators and network equipment vendors have already invested in "Outer" MPTCP implementations. The Apple iOS devices have opened up the use of MPTCP to any app developer since iOS 11. These outer MPTCP connections use today's care-of addresses, for example in Figure 3-3 the IP@4 for Wi-Fi communication and the IP@3 for cellular communication. The Data Terminal Equipment (DTE) implements an outer MPTCP client and interfaces with a Data Communication Equipment (DCE) via the AT interface [28].

The DCE includes a cellular chipset compliant to ATSSS, allowing it to communicate via the 3GPP network interface and also via Wi-Fi network interface to an Access Point on the CPE integrated as untrusted WLAN. Over Wi-Fi the DCE can then reach the MNO's 5G Core network (AMF and UPF) via N3IWF gateway function.
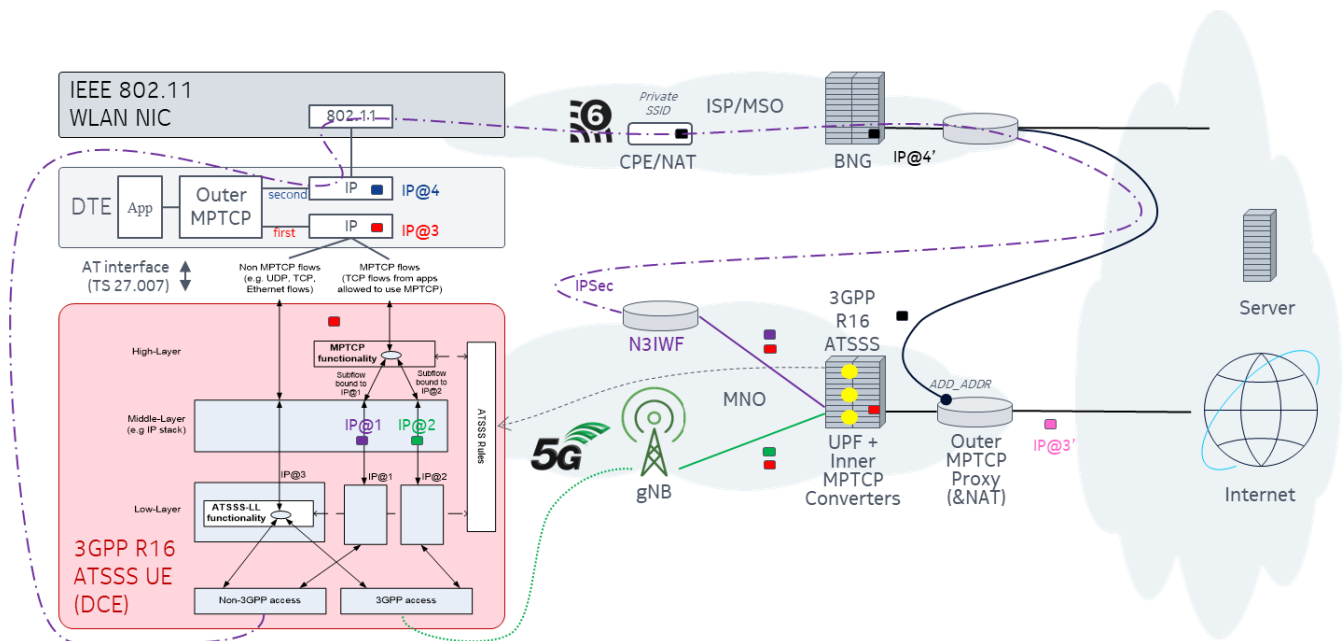
Figure 3-3 Interworking Challenges between Outer and Inner MPTCP

In Figure 3-3, an outer MPTCP client in the DTE splits the traffic between the DCE and the WLAN NIC. The DTE's MPTCP client establishes the first outer MPTCP leg via the 3GPP DCE and via an Outer MPTCP Proxy farm (acting as a transparent on-path multi-path proxy) to the internet destination (the client indicates MP_CAPABLE in TCP SYN). For selected TCP flows (as per the ATSSS rules) the DCE ATSSS-HL steers, switches or splits TCP traffic via 2 paths, namely over link-specific IP addresses IP@1 (for Non-3GPP access) and IP@2 (for 3PPP 5G access). For such flows, the ATSSS-HL will send the TCP SYN (with MP_CAPABLE option) to the IP address of the Inner MPTCP converter proxy (inside UPF) using one of the link specific addresses as per the convert protocol (RFC 8803), rather than to the IP address of the server on the Internet. It is assumed that the ATSSS MPTCP converter proxy does not remove the MP_CAPABLE option from the TCP SYN message sent between the MPTCP converter proxy and the remote server.

As per the IETF convert protocol, after receiving TCP SYN with MP_CAPABLE option, the MPTCP converter proxy on UPF will attempt to establish an MPTCP connection with the server. The on-path outer MPTCP Proxy will intercept and establish TCP connection with the server and return SYN+ACK to the MPTCP converter proxy. The converter proxy returns

SYN+ACK to the ATSSS-HL MPTCP client with TCP options (including MP_CAPABLE) received from the outer proxy in the convert protocol header. At this point in the flow, RFC 8803 does not specify behaviour of the inner ATSSS MPTCP client to pass MPTCP options received from the outer MPTCP proxy up to the outer MPTCP client in the DTE. Per RFC 8684, a unique set of sender and receiver keys need to be exchanged as part of MP_CAPABLE option between outer MPTCP proxy and outer MPTCP client as part of TCP 3-way handshake to establish the outer MPTCP path. However, the convert protocol does not provide a way to send MP_CAPABLE option (with receiver key) from outer MPTCP proxy to the outer MPTCP client on the UE within an inner MPTCP exchange. This breaks the coexistence of inner ATSSS MPTCP with the outer MPTCP.

Thus, the use of TCP converter protocol by ATSSS-HL MPTCP functionality breaks the already deployed outer MPTCP implementation making the two incompatible and the inner and outer MPTCP can't coexist per current specification behavior. Further study is needed in IETF and 3GPP to consider simultaneous operation of ATSSS MPTCP functionality and convert protocol with already deployed outer MPTCP implementations.

Another possible issue is that, when operating over untrusted WLAN Access Networks, the UL traffic sent using ATSSS-HL or ATSSS-LL must use IPsec encryption and integrity protection to reach the N3IWF, but in certain implementation this IPsec functionally may not be hardware accelerated. This may result in lower throughput via IP@1 (over Wi-Fi access) than via IP@2 (over cellular access), which could result in more traffic being sent via cellular access. If outer MPTCP connectivity is established, then the outer MP-TCP proxy may also react to the relatively high 3GPP access throughput by also reducing traffic via non-3GPP access. This could result in more traffic being concentrated on 5G in preference to Wi-Fi access.

3.2.8   ATSSS Phase 2 Study in Release 17

3GPP Release 17 is currently studying the enhancements to the ATSSS architecture in study item [26]. The scope includes studying whether and how to support additional steering modes as well as whether and how to support additional steering functionality, i.e., using protocols other than MPTCP and ATSSS-LL. At the time of writing this report, the 3GPP study is still on-going, however key issues with the current ATSSS have already been identified in TR 23.700-93 [25] and these include:

- Whether additional steering modes need to be supported between the UE and the network
- Support for Traffic splitting for Ethernet and UDP based traffic
- How to support MA-PDU sessions when the 3GPP access leg is over EPC

These are important issues to study and address in ATSSS. Significantly, the current draft candidate solutions being analysed focus on the use of IETF's QUIC protocol, with solutions being proposed that use QUIC and MP-QUIC as a lower layer method, together with other solutions being proposed that use QUIC and MP-QUIC as higher layer protocols. Details on the support for traffic splitting for Ethernet and UDP traffic is covered in section 3.2.4.

Importantly, the candidate solutions benefit from the re-use of the quic-datagram IETF draft [27], enabling the capability to be used to either transport encapsulated PDU frames (when used for supporting a lower layer method), or used to transport UDP traffic (when used for supporting a higher layer method). IETF's quic-datagram work is specifically targeted at being able to support real-time applications that can then benefit from sharing a common security context with other non-real time/reliable data streams.

One of the key issues highlighted in the ATSSS phase 2 study is the security framework of QUIC and whether IETF will agree to update the QUIC specification to enable a NULL encryption option to be defined and hence avoiding double encryption for user data.

3.3   End-to-end QoS Challenges

To satisfy end-to-end QoS requirements for 5G applications and services, it is important to ensure that the QoS differentiation within WLAN access can be provided for 5G QoS Flows carried over WLAN access based on the 5G QoS characteristics (defined by 5QI) and QoS parameters. This section captures specific challenges and gaps related to mapping 5G QoS to Wi-Fi QoS for providing QoS differentiation over WLAN.

3.3.1   Mapping 5G QoS to Wi-Fi QoS

The N3IWF and TNGF receive QoS profile information for 5G QoS flows from the AMF as part of PDU session procedures. These QoS flows are mapped to IPsec child SAs to tunnel user plane traffic over the WLAN access. The QoS differentiation in WLAN can be provided by the 802.11e defined EDCA QoS management scheme which specifies mapping of 802.11 User Priorities (UP) to four QoS Access Categories (AC) for background, best effort, video and voice traffic (AC_BK, AC_BE, AC_VI, AC_VO) [8]. The IEEE 802.11-2016 standard also supports mapping data packets to 802.11 UP based on the DSCP marking in the IP header. It is important to ensure that the QoS differentiation within WLAN access can be provided for these 5G QoS flows taking into account 5G QoS characteristics (identified by 5QI as described in 2.4.1), to satisfy end-to-end QoS requirements for applications and services no matter which access carries the user traffic.

One way to achieve QoS differentiation for 5G traffic flows over WLAN access is to tag 5G data packets with DSCP marking in the IP header as defined by DiffServ architecture (RFC 2474), and within the WLAN access map DSCP to 802.11 User Priority (UP) and Access Category (AC) as shown in Figure 3-4. Similar solution is used for Wi-Fi calling over LTE where ePDG/TWAG maps LTE QCI to DSCP marking [18]. The 5G architecture enables associating a DSCP value with every IPsec child SA and all IP packets sent over that child SA get marked with that DSCP value. The DSCP value for an IPsec SA can be determined based on mapping 5QI to DSCP for flow(s) carried over that IPsec SA. For DL traffic, the mapping of 5QI to DSCP marking is done at the N3IWF or TNGF and for UL traffic, the mapping of 5QI to DSCP marking is done at the UE. The DiffServ QoS is applied for the 5G traffic on the segment between N3IWF/TNGF and WLAN AP. The UE and WLAN AP map DSCP to IEEE 802.11 UP/AC for UL and DL traffic as specified in [8] and the 802.11e Access Category based QoS is applied over the WLAN link for UL and DL.
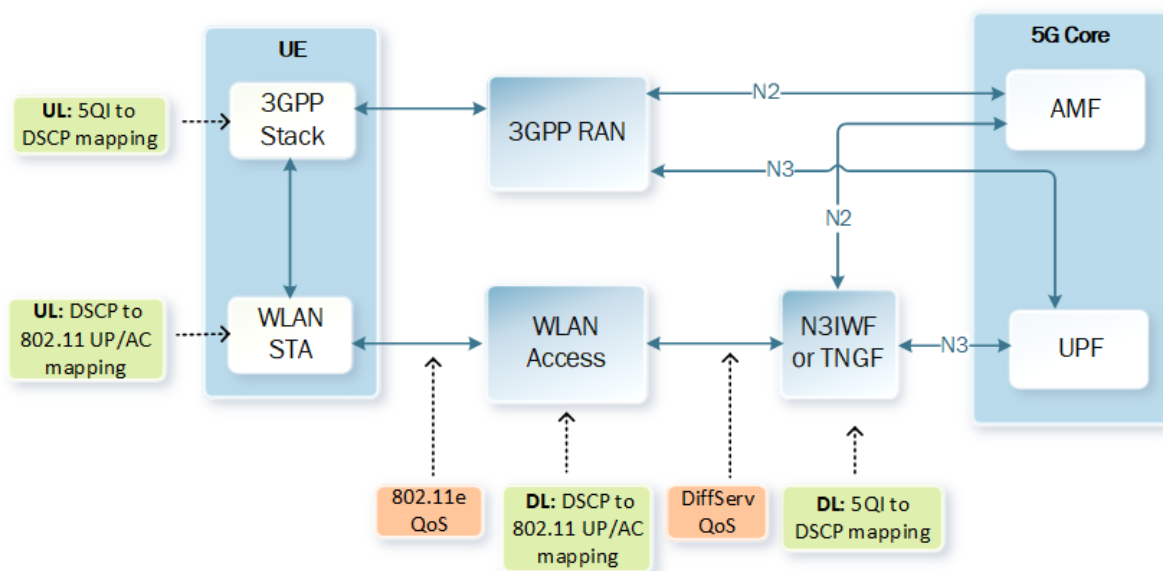
Figure 3-4 Mapping 5G QoS to WLAN QoS based on DSCP Marking

For supporting GBR and non-GBR QoS flows, 5G QoS model defines three resource types – GBR, Delay-critical GBR and Non-GBR. A total of 26 5QI values are specified with standardized set of QoS characteristics for frequently used services as defined in clause 5.7.4 in TS 23.501. However, 3GPP specs do not provide any recommendation for mapping these standardized 5QI values to DSCP values and it is left up to the implementation. This could lead to inconsistent QoS experience across different 5G and Wi-Fi integration deployments, if standardized 5QI values get mapped to different DSCP values in these

deployments. Hence it is desirable to define a common set of mapping between 5QI values to DSCP values which can be used as a recommendation across various deployments.

The IETF draft [15] addresses the mapping between LTE QCI and 5G 5QI to DSCP values. As described in the draft, the cellular QoS characteristics take into account multiple dimensions such as resource type, flow priority, packet delay budget and PER and these do not map well to the traffic classification and PHBs (Per Hop Behaviour) defined by DiffServ architecture which is characterized based on delay, jitter and loss requirements. Detailed analysis of QoS characteristics and intended example services of various 5QI values is required to define mapping to DSCP values and this could result in allocation of new DSCP code points in Pool 1 and Pool 3 defined by IANA [16]. The GSMA IR.34 specification [17] has defined limited mapping between LTE QCI to DSCP values but has not been updated to define mapping of 5G 5QI to DSCP values.

Overall, there is a gap and a need to define standardized recommendation for mapping 5QI values to DSCP values to be used across different trusted and untrusted WLAN integration deployments in 5G system. Also, for trusted WLAN integration deployments via TWIF, the DSCP marking is the only option to provide QoS differentiation within WLAN access since no IPsec child SAs are established over WLAN access.

Another approach for QoS differentiation within WLAN access can be based on identifying and prioritizing IPsec child SAs traffic carrying 5G flows. Such an approach would also work for deployments where the DSCP marking based approach may not fit well. e.g. in cases where the DSCP markings may get reset by the routers before data packets reach the WLAN domain. For this IPsec child SA based approach, there is a need to enhance traffic identification/classification (TCLAS) element within IEEE 802.11 [29] to support IPsec SA traffic filtering and prioritization based on the unique identifiers for IPsec SA which include the SPI (Security Parameter Index), the destination IP address and the security protocol ID per RFC 2401.

For trusted WLAN access, the 5G QoS characteristics (5QI) and parameters associated with 5G QoS flows (identified by QFI) carried over WLAN access are provided by TNGF to the UE as part of the IPsec child SA creation. The 5G QoS information and associated IPsec SA information need to be provided to WLAN access on the UE to reserve resources and prioritize associated 5G traffic carried over IPsec child SAs using a device centric QoS management. How the 5G QoS information is used by the WLAN access to reserve resources and map 5G QoS parameters to 802.11 UP and traffic specification (TSPEC) is undefined and need to be addressed within the 802.11 standard. The 5QI to DSCP mapping can also be used here to map 5QI to a DSCP value which can then be mapped to a UP. For untrusted WLAN access, N3IWF does not provide 5G QoS information to the UE, hence device centric QoS management can not be used for 5G flows carried over untrusted WLAN

access. It is desirable to provide 5G QoS information to the UE for untrusted WLAN case as well to support QoS differentiation for 5G flows in such deployments.

Additionally, there are multiple efforts in WFA OCE and IEEE 802.11 for improving WLAN QoS capabilities to support new breeds of applications (e.g. AR/VR, Industrial IoT, TSN, edge computing) and also for providing additional tools for a new network centric WLAN QoS management paradigm where policies, resources, rules, and priorities along with QoS flow characteristics and parameters can be integrated in end-to-end WLAN QoS management solution. Such network centric approach can enable WLAN QoS management capability from both device and network side and can provide opportunity for better QoS management for 5G flows between TNGF and WLAN AP. Such an approach will require integration between TNGF and WLAN AP to send 5G QoS information to WLAN AP to trigger network centric WLAN QoS management for 5G flows.

Finally, to support QoS requirements for emerging 5G breed of applications over WLAN access in a converged deployment, the WLAN access needs to support finer QoS granularity to meet flow priority, data rate, latency and PER requirements as defined by 5QI, specially for GBR flows. Further analysis is needed on how new MAC/PHY capabilities in IEEE 802.11ax such as TWT scheduling, OFDMA and MU-MIMO can be leveraged to provide fine grain QoS for 5G flows over WLAN. Also, the IEEE 802.11be QoS enhancements and new capabilities being considered including TSN support, Multi-link operation and Multi-AP capability should consider how fine grain QoS mapping, scheduling and prioritization can be provided for 5G flows based on 5G QoS characteristics and parameters.

3.4   Policy Interworking Across Wi-Fi and 5G

When it comes to policy use cases, it is evident that any converged system needs to be able to support fine grain policy, not just on a per network technology basis, where holistic policies are defined based on RF physical layer characteristics, e.g., preferring Wi-Fi or 5G/Cellular, not just on a per networking implementation basis, where polices are defined based on whether a particular access technology has additional policy enforcement mechanisms defined, e.g., preferring an enterprise or service provider network which has been architected to support quality of service guarantees, but rather on a "per-application, per-network, per-access technology" basis.

Agreeing to define policies on an application basis aligns with the evolution of transport services. Already iOS's URL Session class enables applications to signal their required MultipathServiceType, enabling applications to indicate whether they beneficially operate over a transport service configured for multi-path, including signalling whether those paths should be configured for delivering handover capabilities, improved application interaction, or

improved aggregate throughput. Moving forward, the IETF TAPS working group is redefining the conventional APIs that are used for exposing transport protocol features to applications, in the Transport Services (TAPS) Working Group. The IETF TAPS Working group is tasked with helping application and network stack programmers by describing an interface for applications to make use of Transport Services. The Transport Services architecture defines a general model of interaction, aiming to both modernize the API surface presented to applications by the transport layer and enrich the capabilities of the transport system implementation [23].
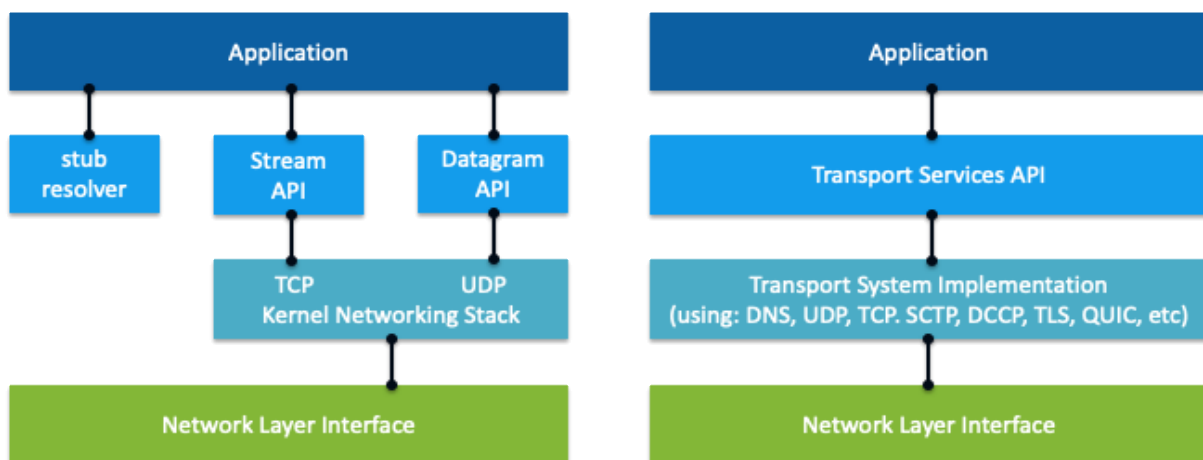
Figure 3-5: Contrasting Conventional Socket API model with Transport Services API Model

The Transport Services API defines a pre-establishment phase where an application can signal pre-selection information, including intent, requirements, prohibitions, and preferences for its networking operations. The TAPS architecture calls out examples, including the ability to influence selection of interface type (such as a Wi-Fi connection, or a cellular connection), preferences for throughput and latency properties, as well as options that influence the transport protocol selection, including multi-path support. Moreover, the TAPS API highlights that interface type should not be treated as a proxy for properties of interfaces such as metered or unmetered network access. Instead, if an application wants to signal that use of a metered access is prohibited or should be avoided, then this should be specified by a separate property distinct from interface type.
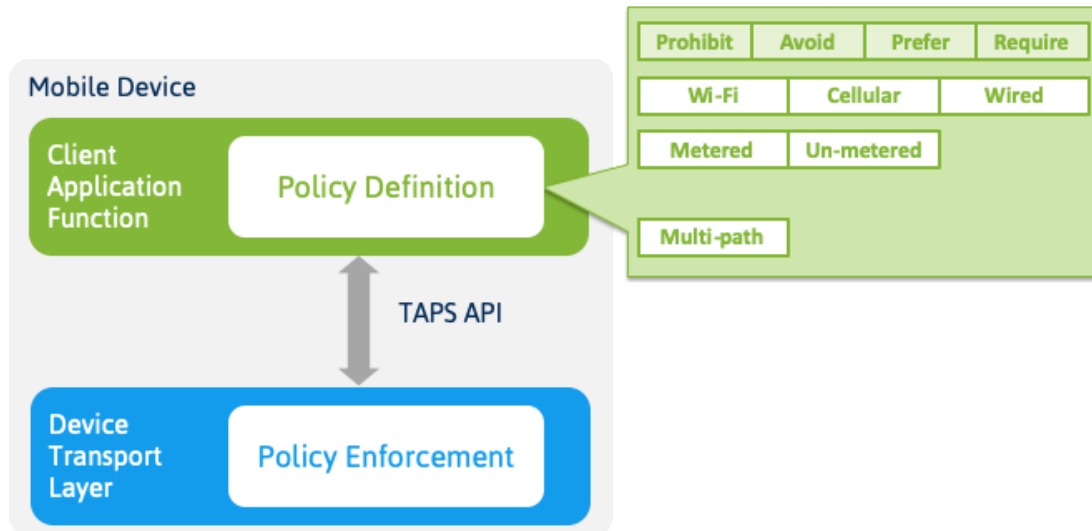
Figure 3-6: Policy Definition and Enforcement in a TAPS Environment

However, exposing APIs for enhancing the selection of paths during a connection pre-establishment phase and/or for how to transfer data over the plurality of selected paths still does not solve the critical issue of who defines the policy? Hence, one of the key challenges in setting a policy between Wi-Fi and 5G is the possible existence of multiple policies. As described in section 2, policies that influence path selection may be defined by application providers, device manufacturers (e.g. policy to determine user preferences for WLAN access selection), end users, enterprise IT admins as well as the service provider defined policy that has been the focus of 3GPP standardization efforts.

Figure 3-7: Multiple Policies at the UE

Distributing policy definition, together with decoupling policy signalling from its enforcement then highlights that a key challenge is being able to define a coherent framework for policy meta-data definition that can be used by the different policy originators. The challenge still remains in terms of how potential conflicts can be resolved across different policy definitions leveraging a common policy definition framework, and that behaviour may be device OEM specific.

3.5 Support for Converged Service Bundle

Recognition of ownership of the service provider networks on the mobile device is another area where there is insufficient provision in the current standards. A service provider who owns both the 5G and Wi-Fi networks may wish to offer differentiated services over their own network (including 5G and owned and partner Wi-Fi networks) when compared to 3rd party Wi-Fi networks. This may be part of a 'converged services' bundle where the 5G and Wi-Fi are treated as a single network service and billed for accordingly. To deliver such a service, an operator may wish for greater control over how traffic is delivered across the two networks in order to manage operational costs.

For example, because any converged service that makes use of MA PDU Sessions will require anchoring in the cellular network operator's 5G Core network, there is the potential to hugely increase the traffic volumes routed through the operator's 5G Core with corresponding cost increases. This is especially true if home Wi-Fi is included, as it currently carries the majority of the data consumed on a large proportion of mobile devices.

There are three key requirements that will help in addressing these issues:

- The ability for a mobile device to securely identify Wi-Fi networks that are owned by the cellular network operator or with which it has a commercial roaming relationship
- The ability for a converged network operator to specify device and network policy to deliver differentiated services depending on Wi-Fi access network attachment
- The mobile device recognising the relationship/ownership of the 5G and Wi-Fi networks and respecting the operator policy for traffic routing and potentially influencing network selection by choosing an operator preferred Wi-Fi network that the differentiated service can be delivered over

To achieve this, one possible approach applicable to Passpoint Wi-Fi networks, would be to enhance the UE Route Selection Policy (URSP) by extending the location validity criteria for MA PDU session establishment to include specifying valid Wi-Fi networks e.g. by using a subset of the ANDSP WLAN Selection Criteria (such as PreferredRoamingPartnerList and PreferredSSIDList). The associated URSP rule would only become active when the UE has associated with one of the valid Wi-Fi networks – it does not influence network selection. Enhancement to the ANDSP policy to indicate network relationships/ownership could be a way of influencing network selection to support 'converged services' if this is also required.

Implementations should note when the Wi-Fi networks and the 5G network form part of a converged service and give greater weight to these URSP rules relative to other local user or application level policies. The UE could determine whether the Wi-Fi and 5G networks form part of a converged service either by a new policy element that explicitly identifies the 5G and corresponding Wi-Fi networks (e.g. through ANDSP) or possibly by inference from the enhanced URSP validity selection criteria above.

Note, this does not prevent the PreferredRoamingPartnerList or PreferredSSIDList from being spoofed by a Wi-Fi network wanting to influence policies enforced by UEs. This also leaves open the question on how these network validity criteria could be specified for non-Passpoint networks such as a broadband ISP's home Wi-Fi access points.

3.6   Support for Wi-Fi Only Devices

Current 3GPP standard does not define architecture to support Wi-Fi only devices without USIM connecting to 5G Core. For a UE connecting to 5G Core over WLAN access via N3IWF or TNGF, the UE is shown as a dual radio device supporting both 3GPP and non-3GPP radio per reference architectures in TS 23.501 clause 4.2.8.2, even though connectivity over the 3GPP access is shown as optional. Similar to Wi-Fi, the 5G system has adopted EAP authentication framework for UE authentication with the 5G Core. It supports EAP-AKA' and 5G-AKA authentication methods for UE authentication over both 3GPP and non-3GPP access in PLMN networks. A UE is required to support SIM based identity (SUPI based on IMSI) and SIM credentials to connect to 5G Core over WLAN access.

Given that the 5G architecture supports a UE connecting to 5G Core over WLAN access only without requiring primary connectivity over cellular access, a Wi-Fi only UE which supports 5G NAS functionality and includes a USIM (providing 3GPP IMSI based identity and SIM credentials), can still connect to 5G Core as shown in Figure 3-8. However, most Wi-Fi only devices, e.g. devices in enterprise deployments, would not have a USIM included even in cases where these devices can be upgraded to support 5G control plane (NAS) and user plane functionality. Hence, it is important to enable Wi-Fi only devices without 3GPP IMSI based identity and SIM credentials to connect to 5G Core, to provide 5G services and experiences across different enterprise and verticals deployments.
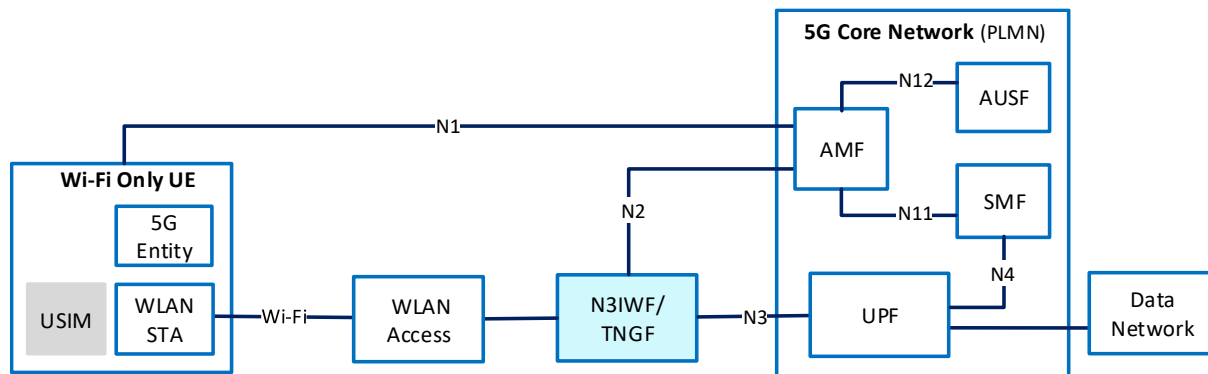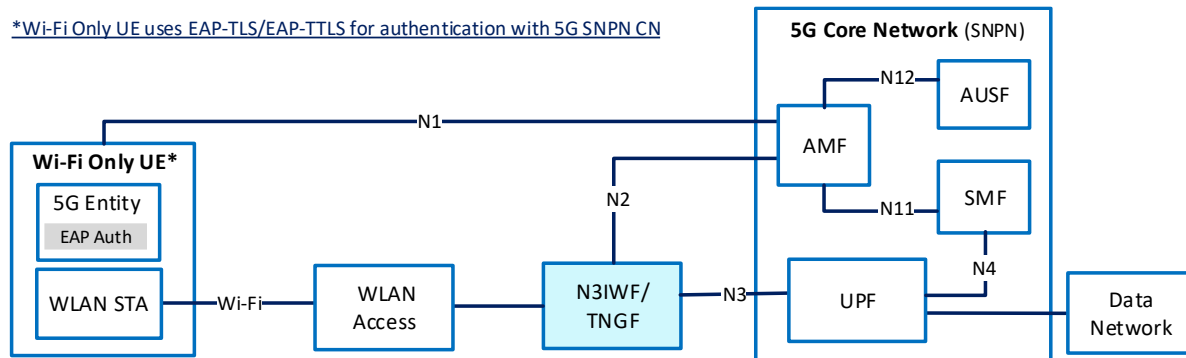
Figure 3-8 Wi-Fi Only UE with USIM Connecting to 5G PLMN

Also, for N5CW UE connecting to 5G Core via TWIF, 3GPP spec requires such UEs to support SIM based credentials since such devices are authenticated using EAP-AKA' as described in clause 7A.2.4 in TS 33.501 and clause 7.3A.4.2 in TS 24.502. Hence, the TWIF based architecture as defined currently also does not support Wi-Fi only devices without 3GPP IMSI based identity and SIM credentials.

The Wi-Fi only UEs may or may not support 5G NAS functionality and typically do not include SIM based identity and credentials. The Wi-Fi only UEs with 5G NAS will need to support EAP-5G, IKEv2 and 5G NAS signalling. To support Wi-Fi only devices without USIM, the 5G Core network needs to support non-IMSI based identity in the form of NAI (username@realm) and non-AKA based authentication methods such as EAP-TLS or EAP-TTLS. Current 3GPP standard supports SUPI based on NAI and defines use of EAP-TLS in stand-alone non-public network (SNPN) deployment without roaming. However, in 3GPP Release 16, direct access to SNPN is only specified for 3GPP access (clause 5.30.1 in TS 23.501) and the procedure defined for EAP-TLS authentication for SNPN is specified for 3GPP access only (clause B.2 in TS 33.501). TS 33.501 does not define procedure details for supporting EAP-TLS/EAP-TTLS based authentication over WLAN access via N3IWF or TNGF for 5G-Capable Wi-Fi only UEs, as per proposed reference architecture in Figure 3-9(a). Similarly, for Non-5G-Capable (N5GC) Wi-Fi only UEs (e.g. legacy Wi-Fi only devices), TS 33.501 does not define procedure details to support EAP-TLS/EAP-TTLS based authentication via TWIF, as per proposed reference architecture in Figure 3-9(b).

Many existing and new verticals such as enterprise, industrial IoT, healthcare etc. could have a mix of 3GPP only, dual radio and Wi-Fi only UEs in standalone private 5G network (SNPN) deployments. To facilitate adoption of Wi-Fi only UEs for such SNPN deployments, 3GPP standard needs to define architecture and procedure details for supporting Wi-Fi only UEs with non-IMSI based identity and EAP-TLS/EAP-TTLS based authentication to access 5G SNPN core via N3IWF, TNGF or TWIF functions as shown in Figure 3-9.

*Wi-Fi Only UE uses EAP-TLS/EAP-TTLS for authentication with 5G SNPN CN

5G Core Network (SNPN)

Wi-Fi Only UE*

5G Entity

EAP Auth

WLAN STA — Wi-Fi — WLAN Access — N2 — N3IWF/ TNGF — N3 — UPF

N1 — AMF — N12 — AUSF

N11 — SMF — N4

Data Network

(a) 5G Capable Wi-Fi Only UE accessing 5G SNPN

5G Core Network (SNPN)

Wi-Fi Only UE*

EAP Auth

WLAN STA — Wi-Fi — WLAN Access — TWIF — N3 — UPF

N1 — AMF — N12 — AUSF

N2

N11 — SMF — N4

Data Network
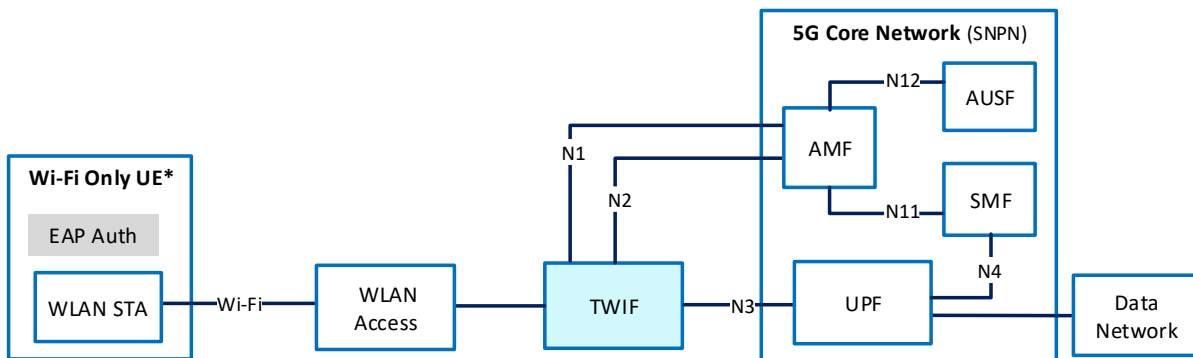
(b) Non-5G Capable Wi-Fi Only UE accessing 5G SNPN

Figure 3-9 Wi-Fi Only UE without USIM Connecting to 5G SNPN

Once the support for non-IMSI based SUPI and EAP-TLS/EAP-TTLS is added for Wi-Fi only devices for SNPN networks, it will be up to the operators to add support for such Wi-Fi only devices in PLMN networks. The main challenge will be supporting EAP-TLS/EAP-TTLS for such devices across roaming partners. To support roaming for such devices, visiting PLMN would need to use UE's NAI realm part for AUSF selection in home PLMN for UE authentication. It may be worthwhile for 3GPP to consider requiring support for EAP-TLS/EAP-TTLS for Wi-Fi only devices in PLMN networks, to enable providing 5G services on such UEs across different geographic deployments.

4 Summary and Recommendations

This WBA paper has closely examined 3GPP defined solutions for the convergence of Wi-Fi with the 5G system including the convergence architecture, WLAN access selection, traffic steering over multiple access and the end-to-end QoS support over WLAN. It has identified and highlighted certain key challenges and gaps associated with supporting the convergence of 5G and Wi-Fi networks and provides some guidelines and high level solutions to address those challenges. Further study and analysis are needed by standard bodies (e.g. 3GPP,

IEEE 802.11) to address identified gaps to fully realize the opportunities presented by the convergence of 5G and Wi-Fi networks across a range of different deployment scenarios.

A summary of key challenges, proposed solutions and associated recommendations are highlighted in the following gap areas related to 5G and Wi-Fi convergence:

- **5G and Wi-Fi Convergence Architecture**

3GPP enables convergence of both untrusted and trusted WLAN access with the 5G system. The trusted WLAN integration has bigger impact on the Wi-Fi access as it requires tight coupling between WLAN AP and TNGF/TWIF functions. There are a number of gaps which need to be addressed within WLAN domain including EAP-5G messages filtering on WLAN AP, use of TNAP key as PMK for 802.11 4-way handshake and ANQP support to advertise list of PLMNs with trusted 5G connectivity. The Ta and Yw interfaces would need to be standardized and the WLAN access network may need to host TNGF/TWIF functions. The trusted WLAN integration may be preferred over untrusted WLAN integration, because it uses NULL encryption over IPsec tunnel avoiding double encryption for user data and it can provide better QoS control for 5G flows over the WLAN access. Additionally, in case of untrusted WLAN integration, the IPsec encryption at the UE may not be hardware accelerated, resulting in much lower throughput over the Wi-Fi access and this might cause more traffic being concentrated over the 5G access, which could be another reason to prefer trusted WLAN integration over untrusted WLAN.

Hence, it is recommended that the Wi-Fi industry considers addressing gaps highlighted for supporting trusted WLAN integration with the 5G system, so that trusted WLAN integration can become a viable deployments option.

- **ATSSS Multi-Access Steering Functionality**

A number of issues and gaps are identified to support ATSSS multi-access steering in different deployment scenarios. To begin with, further study is needed on how ATSSS policy can be combined with the UE-based policy for traffic steering from the applications, enterprise agents or user preferences and how to address any conflicts across these policies. Concern has been raised over the deployment limitations of ATSSS MPTCP converter proxy which limits the proxy deployment by a 3rd party independent of the 5GC administrative domain. Another concern identified is that the UE vendors may desire to incorporate UE local conditions e.g. battery state, access cost, and thermal conditions in selecting access for the UL and DL traffic steering, which is not supported in current ATSSS policy. It is also highlighted that packet level traffic steering across 3GPP and WLAN access is not supported for non-TCP traffic types (e.g. UDP, Ethernet traffic) in ATSSS, which is important to provide

full support for UDP based real time traffic, emerging 5G low latency applications and QUIC based applications. Additionally, there is lack of behavior in terms of ATSSS operation with MP-Capable servers discovered via the IETF MPTCP converter protocol, which means direct connectivity with MP-Capable servers can not be supported in ATSSS as specified by the converter protocol.

Another key issue highlighted is that the traffic steering within ATSSS is more reactive in nature based on end-to-end measurements by the PMF or MPTCP layer which can be slow to react to the changing radio conditions. An enhancement is proposed where RAN measurements from the RAN nodes (NG-RAN or WLAN AP) or the UE can be provided to 5G Core to indicate radio access conditions (e.g. radio link quality, access network load, delay stats) to assist in dynamic traffic steering decisions within ATSSS. It has also been emphasized that the existence of ATSSS MPTCP functionality (the inner MPTCP) breaks the already existing MPTCP functionality on UE devices (the outer MPTCP) because such inner-outer MPTCP model is not supported by the MPTCP converter protocol and no special behavior is defined by 3GPP to address such a scenario. The importance of key issues identified in ATSSS phase 2 study in Release 17 is emphasized and with the QUIC/MP-QUIC based candidate proposals in consideration, the issue of whether QUIC specification will be updated to support NULL encryption to avoid double encryption is highlighted.

Overall, these are some important challenges and gaps brought forth on the ATSSS and it is recommended that these issues be considered in 3GPP for further study.

- **End-to-end QoS**

For end-to-end QoS, the important aspect is to ensure that the QoS differentiation within WLAN access can be provided for 5G QoS flows based on 5G QoS characteristics (defined by 5QI) and other QoS parameters. Defining a standardized mapping of 5QI to DSCP values has been highlighted as one of the gaps to support QoS differentiation over WLAN access. It is also pointed out that the 5G QoS information needs to be provided to the UE for flows over untrusted WLAN access as well (similar to trusted WLAN) to support QoS differentiation for 5G flows for untrusted deployments.

Device centric and network centric approaches have been identified to achieve WLAN QoS differentiation for 5G flows based on identifying and prioritizing IPsec child SAs traffic within the WLAN access. This involves mapping 5G QoS parameters to 802.11 User Priority and traffic specification (TSPEC) along with extending TCLAS element to support IPsec SA traffic, which are not defined currently, and these gaps need to be addressed in IEEE 802.11 standard. Also, since the QoS differentiation is provided based on IPsec SA, it is recommended that each 5G QoS flow be mapped to a separate IPsec SA on TNGF/N3IWF

to support per 5G flow QoS over WLAN access. The need for further analysis is highlighted on how new MAC/PHY capabilities in 802.11ax such as TWT scheduling, OFDMA and MU-MIMO as well as new capabilities in 802.11be can be leveraged to provide fine grain QoS for 5G flows over WLAN.

It is recommended that addressing these QoS related issues and gaps be considered in IEEE 802.11, 3GPP and/or GSMA & IETF (for 5QI to DSCP mapping) to support QoS differentiation of 5G flows over WLAN.

- **Policy Interworking and Enhancements across 5G and Wi-Fi**

Another key challenge relates to policy interworking across Wi-Fi and 5G, where fine grain policies for access selection and/or multi-path selection can be defined by multiple entities including application providers (e.g. through IETF TAPS APIs), device manufacturers, end users, enterprise IT admins as well as the service provider. It is highlighted that a key issue is being able to define a coherent framework for policy meta-data definition that can be used by different policy originators. Any conflicts across different policies leveraging a common policy definition framework would likely get addressed in a device OEM specific way. Specific policy challenges related to ATSSS are identified under ATSSS challenges and gaps. A potential policy enhancement is suggested for improving WLAN access selection for trusted and untrusted WLAN access by extending the WLANSP rules with additional Wi-Fi QoS metrics for selection criteria and exposing relevant Wi-Fi QoS metrics through ANQP or other means to enable UE to select a high quality Wi-Fi connection.

Relating to policy, another key issue identified is how an operator can provide differentiated service over 5G and specific Wi-Fi networks as part of a converged service bundle. A possible solution proposed includes enhancing URSP rules by extending the validity criteria to specify valid Wi-Fi networks for MA-PDU session, where the URSP rules only become active when the UE has associated with one of the specified Wi-Fi networks. It is suggested that the ANDSP policy could also be enhanced to indicate network relationships/ownership to influence WLAN network selection to support converged services.

It is recommended that the industry considers addressing policy interworking issues and suggested policy enhancements to provide improved operations for converged 5G and Wi-Fi network.

- **Support for Wi-Fi only devices**

Another challenge area emphasized is that the current 5G architecture does not support Wi-Fi only devices without USIM connecting to the 5G Core. Since most Wi-Fi only devices do not have USIM, it is important to support such devices to provide 5G services and experiences across different enterprise and vertical deployments. To facilitate adoption of Wi-Fi only UEs without USIM for private networks in the stand-alone non-public network (SNPN) deployments, it is highlighted that 3GPP needs to define architecture and procedures for supporting Wi-Fi only UEs with non-IMSI based identity and EAP-TLS/EAP-TTLS based authentication to access 5G SNPN core via N3IWF, TNGF or TWIF functions. Another important discussion point highlighted is about supporting EAP-TLS/EAP-TTLS for Wi-Fi only devices for the PLMN networks across roaming partners and enabling that support will depend on the operator's decision.

It is recommended for 3GPP to address issues and gaps highlighted to support Wi-Fi only devices without USIM to access the 5G Core.

5   Conclusion and Next Steps

With continued development of 5G networks in 3GPP Release 16/17 and continued evolution of IEEE 802.11 Wi-Fi technology with Wi-Fi 6/6E and Wi-Fi 7, industry players including cellular and Wi-Fi operators, device manufacturers and end-users stand to benefit a great deal from the continued convergence of Wi-Fi and 5G networks. The convergence of 5G and Wi-Fi enables leveraging unique and complementary capabilities of both access networks to provide seamless and interoperable services to the end-users across a variety of use cases and verticals. Enabling support for converged Wi-Fi and 5G networks presents a new set of challenges which the industry needs to address to provide fully deployable end-to-end convergence solutions.

This WBA paper has highlighted key challenges and proposed high level solutions in the following gap areas to enable 5G and Wi-Fi convergence:

- 5G and Wi-Fi convergence architecture
- ATSSS multi-access steering functionality
- End-to-end QoS
- Policy Interworking and enhancements across 5G and Wi-Fi
- Support for Wi-Fi only devices

The WBA 5G working group recommends aligning the industry on these challenges associated with 5G and Wi-Fi convergence and facilitate standardization efforts to address these challenges through liaisons with following standard bodies, including 3GPP, GSMA, WFA, IEEE 802.11 and IETF.

A. WBA – 3GPP Liaison

Some of the specific challenges for 3GPP considerations may include:

- ATSSS related challenges, including ATSSS policy combining with other UE-based policy, deployment limitations of ATSSS MPTCP converter proxy, incorporating UE local conditions in ATSSS, support for packet level traffic steering for all traffic types, enabling ATSSS operation with MP-Capable servers, incorporating RAN level measurements for dynamic traffic steering decisions in ATSSS, and coexistence of ATSSS inner MPTCP with outer MPTCP on the UE.

- End-to-end QoS related challenges, including considerations for leveraging standardized 5QI to DSCP mapping on TNGF/N3IWF and UE, providing 5G QoS information to the UE for untrusted WLAN access, and considerations for mapping each 5G QoS flow to a separate IPsec SA on TNGF/N3IWF to enable supporting per 5G flow QoS differentiation over the WLAN access.

- Policy related challenges and potential enhancements, including extension to WLANSP rules with additional Wi-Fi QoS metrics for selection criteria and enhancement to URSP rules by extending the validity criteria to specify valid Wi-Fi networks for MA-PDU session.

- Challenges related to supporting Wi-Fi only devices without USIM connecting to the 5G Core, including the need to define 3GPP architecture and procedures for supporting Wi-Fi only UEs with non-IMSI based identity and EAP-TLS/EAP-TTLS based authentication to access 5G SNPN core over WLAN access via N3IWF, TNGF or TWIF.

B. WBA –Wi-Fi Alliance Liaison

Some of the specific challenges for Wi-Fi Alliance considerations may include:

- Challenges related to supporting trusted WLAN access integration with the 5G Core including, tight coupling between Wi-Fi AP and TNGF/TWIF functions over Ta and Yw interfaces, EAP-5G support on the WLAN AP, use of TNAP key as PMK for 802.11 4-way handshake, ANQP to advertise list of PLMNs with trusted 5G connectivity, considerations for standardizing Ta and Yw interfaces and for hosting TNGF/TWIF functions within the WLAN access.

- WBA would like to understand from Wi-Fi Alliance standpoint what are the considerations pertaining to these 3GPP identified interfaces Ta and Yw and its impact to the WLAN vendors.

C. WBA – IEEE 802.11 Liaison

Some of the specific challenges for IEEE 802.11 considerations include:

- Need for further study within IEEE 802.11 on how fine grain QoS for 5G flows can be provided in 802.11ax and 802.11be leveraging new MAC/PHY capabilities of these standards.
- Challenges related to enabling QoS differentiation for 5G flows over WLAN access, especially if the QoS mapping is not addressed by WLAN vendor - one way to address this includes defining 5QIs to DSCP values to 802.11 User Priority mapping, considerations for supporting the device centric and network centric approaches for WLAN QoS differentiation for 5G flows based on IPsec child SAs, defining 5G QoS parameters to 802.11 User Priority and TSPEC parameters mapping and extending TCLAS element to support IPsec SA traffic.

D. WBA – GSMA Liaison

The specific challenge for GSMA consideration includes:

- Consider looking into defining a standardized mapping between the 5G 5QIs and DSCP values, similar to the mapping already defined between LTE QCIs and DSCP in the GSMA IR.34 specification.

E. WBA – IETF Liaison

The specific challenge for IETF consideration includes:

- Consider looking into standardizing 5G 5QIs to Diffserv DSCP mapping, which can be leveraged by 5G and Wi-Fi converged deployments to map 5G QoS to DSCP to WLAN QoS. The Internet Draft 'Diffserv to QCI Mapping - draft-henry-tsvwg-diffserv-to-qci-04' defines 5G 5QIs to DSCP mapping. We request IETF to consider standardization path to RFC for this work.

For more information or to get involved **contactus@wballiance.com**

REFERENCES

[1]   RAN Convergence Paper by WBA and NGMN Alliance, September 2019

[2]   3GPP TS 23.501, System architecture for the 5G System (5GS), Stage 2

[3]   3GPP TS 23.502, Procedures for the 5G System, Stage 2

[4]   3GPP TS 23.503, Policies and Charging control framework for the 5G System (5GS), Stage 2

[6]   3GPP TS 24.501, Non-Access-Stratum (NAS) protocol for 5G System (5GS), Stage 3

[6]   3GPP TS 24.502, Access to the 3GPP 5G Core Network (5GCN) via Non-3GPP Access Networks (N3AN), Stage 3

[7]   3GPP TS 33.501, Security architecture and procedures for 5G system

[8]   IEEE Std 802.11™-2016, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[9]   IEEE Std 802.11u™-2011, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 9: Interworking with External Networks

[10]   IETF RFC 8803, 0-RTT TCP Convert Protocol

[11]   IETF RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

[12]   IETF RFC 2401, Security Architecture for the Internet Protocol

[13]   IETF RFC 8684, TCP Extensions for Multipath Operation with Multiple Addresses

[14]   IETF RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2)

[15]   IETF draft, Diffserv to QCI Mapping, https://tools.ietf.org/html/draft-henry-tsvwg-diffserv-to-qci-03

[16]   IANA DSCP registry, https://www.iana.org/assignments/dscp-registry/dscp-registry.xhtml

[17]   GSMS IR.34, Guidelines for IPX Provider networks (Previously Inter- Service Provider IP Backbone Guidelines) Version 15.0 11 May 2020

[18]   IETF draft, Carrier Wi-Fi Calling Deployment Considerations, **https://tools.ietf.org/html/draft-pularikkal-opsawg-wifi-calling-03**

[19]   RFC 6182, Architectural Guidelines for Multipath TCP Development

[20]   RFC 6356, Coupled Congestion Control for Multipath Transport Protocols

[21]   Impact of Path Characteristics and Scheduling Policies on MPTCP Performance, 2014 28th International Conference on Advanced Information Networking and Applications Workshops, B. Arzani, A. Gurney, S. Cheng, R. Guerin and B. T. Loo

[22]   Wireless Broadband Alliance, Quality of Service on Carrier Grade Wi-Fi, April 2017

[23] IETF draft, An Architecture for Transport Services, **https://tools.ietf.org/html/draft-ietf-taps-arch-07**

[24] Wireless Broadband Alliance, WRIX Umbrella Document, The WRIX Framework Overview and Introduction, Version 1.0

[25] 3GPP TR 23.700-93, Study on Access Traffic Steering, Switch and Splitting support in the 5G system architecture Phase 2

[26] 3GPP Study Item SP-200095, Study on Access Traffic Steering, Switching and Splitting support in the 5G system architecture Phase

[27] IETF draft, An Unreliable Datagram Extension to QUIC, **https://tools.ietf.org/html/draft-ietf-quic-datagram-01**

[28] 3GPP TS 27.007, AT command set for User Equipment (UE)

[29] IEEE P802.11-REVmd™/D3.1, February 2020, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

ACRONYMS AND ABBREVIATIONS

ACRONYM / ABBREVIATION	DEFINITION
3GPP	Third Generation Project Partnership
5G-AKA	5G Authentication and Key Agreement
5GC	5G Core
5QI	5G QoS Identifier
AMF	Access and Mobility Functions
SMF	Session Management Function
AAA	Authentication, Authorization and Accounting
ANDSP	Access Network Discovery and Selection Policy
ANQP	Access Network Query Protocol
API	Application Programming Interface
ARP	Allocation and Retention Priority
ATSSS-HL	Access Traffic Steering, Switching and Splitting - High layer
ATSSS-LL	Access Traffic Steering, Switching and Splitting - Low Layer
AUSF	Authentication Server Function
CCA	Congestion Control Algorithms

CPE	Customer Premise Equipment
DCE	Data Communication Equipment
DiffServ	Differentiated Services
DL	Down Link
DSCP	Differentiated Service Code Point
DTE	Data Terminal Equipment
EAP	Extensible Authentication Protocol
EAP-5G	EAP 5G Authentication and Key Agreement
EAP-AKA'	EAP Authentication and Key Agreement prime
EAPoL	Extensible Authentication Protocol over LAN
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP Tunnelled Transport Layer Security
ePDG	Evolved Packet Data Gateway
FQDN	Fully Qualified Domain Name
GBR	Guaranteed Bit Rate
GFBR	Guaranteed Flow Bit Rate
GRE	Generic Routing Encapsulation
GTP-U	GPRS Tunnelling Protocol – User Data

HS2.0	Hotspot 2.0
IEEE	Institute of Electrical and Electronics Engineer
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange version 2
IMSI	International Mobile Subscriber Identity
IPsec SA	IPsec Security Associations
MA-PDU	Multi-Access PDU session
MAR	Multi-Access Rule
MFBR	Maximum Flow Bit Rate
MNO	Mobile Network Operator
MP-QUIC	Multi Path QUIC
MPTCP	Multi Path Transmission Control Protocol
MU-MIMO	Multi-User, Multiple-Input, Multiple-Output
N3AN	Non-3GPP Access Node
N3IWF	Non-3GPP Interworking Function
N5CW	Non-5G-Capable over WLAN
NAI	Network Access Identifier
NAS	Non-Access Stratum

NGMN	Next Generation Mobile Network
NG-RAN	Next-Generation Radio Access Network
OEM	Original Equipment Manufacturer
OFDMA	Orthogonal Frequency-Division Multiple Access
PCC	Policy and Charging Control
PDR	Packet Detection Rule
PDU	Protocol Data Unit
PHB	Per Hop Behaviour
PLMN	Public Land Mobile Network
PMF	Performance Measurement Function
PMK	Pairwise Master Key
QER	QoS Enforcement Rules
QFI	QoS Flow Identifier
QoS	Quality of Service
QRI	QoS Rule Identifier
QUIC	Quick UDP Internet Connections
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network

RQA	Reflective QoS Attribute
RQI	Reflective QoS Indication
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
RTT	Round Trip Time
SDF	Service Data Flow
SD-WAN	Software Defined Wide Area Network
SIM	Subscriber Identity Module
SNPN	Stand-Alone Non-Public Network
SPI	Security Parameter Index
SSID	Service Set Identifier
STA	Station
SUPI	Subscription Permanent Identifier
TCLAS	Traffic Classification
TCP	Transmission Control Protocol
TNAP	Trusted Non-3GPP Access Point
TNGF	Trusted Non-3GPP Gateway Function
TSN	Time Sensitive Networking

TSPEC	Traffic Specification
TWAG	Trusted WLAN Access Gateway
TWIF	Trusted WLAN Interworking Function
TWT	Target Wake Time
UDP	User Datagram Protocol
UE	User Equipment
UE-AMBR	UE Aggregate Maximum Bit Rate
UL	Up Link
UPF	User Plane Function
URSP	UE Route Selection Policy
USIM	Universal Subscriber Identity Module
WBA	Wireless Broadband Alliance
WFA	Wi-Fi Alliance
WLAN	Wireless Local Area network
WLAN NIC	WLAN Network Interface card
WLANSP	WLAN Selection Policy

PARTICIPANTS LIST

NAME	COMPANY	ROLE
Nigel Bird	Orange	Project Leader
Binita Gupta	Intel	Project Co-Leader & Chief Editor
Mark Grayson	Cisco	Project Co-Leader
Florin Baboescu	Broadcom	Editorial Team
Simon Ringland	BT	Editorial Team
Stephen Johnson	BT	Editorial Team
Necati Canpolat	Intel	Editorial Team
Vivek Gupta	Intel	Editorial Team
Andy Wang	Google	Editorial Team
Ning Zhang	Google	Editorial Team
Thierry Van de Velde	Nokia	Editorial Team
Youssef Abdelilah	American Tower Corporation	Project Participant
Francisco Amaral	American Tower Corporation	Project Participant
Deepa Badgujar	American Tower Corporation	Project Participant
Zahit Sahin	American Tower Corporation	Project Participant
Peter Thornycroft	Aruba Networks	Project Participant

Feng Wang	AT&T	Project Participant
Peter Barany	Boingo Wireless	Project Participant
Johnny Dixon	BT	Project Participant
Kevin Holley	BT	Project Participant
John Barr	CableLabs	Project Participant
Luther Smith	CableLabs	Project Participant
Sandeep Agrawal	C-DOT	Project Participant
Charumati P	C-DOT	Project Participant
Loay Kreishan	Charter Communications	Project Participant
Praveen Srivastava	Charter Communications	Project Participant
Matt MacPherson	Cisco	Project Participant
Matt Melester	CommScope	Project Participant
Angelos Mavridis	Deutsche Telekom	Project Participant
Pavan Nuggehalli	Google	Project Participant
Shu-ping Yeh	Intel	Project Participant
Rajesh Goyal	Nokia	Project Participant
Finbarr Coghlan	Orange	Project Participant
Hemant Jha	Reliance Jio	Project Participant

George Hart	Rogers	Project Participant
Richard Price	Single Digits	Project Participant
Michael Sym	Single Digits	Project Participant
Brendan Malay	Telus	Project Participant
Peter Flynn	Viasat	Project Participant
Bruno Tomás	WBA	Project Participant
Pedro Mouta	WBA	Project Participant
Sarah Markham	WBA	Project Participant
Steve Namaseevayum	WBA	Project Participant
Tiago Rodrigues	WBA	Project Participant