IEEE P802.11
Wireless LANs

|  |
| --- |
|  Technical report on the interworking between 3GPP 5G system and WLAN |
| Date: 2020-08-31 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Binita Gupta | Intel | San Diego, CA, USA 92127 |  | binita.gupta@intel.com |
| Necati Canpolat | Intel | Hillsboro, OR, USA 97124 |  | necati.canpolat@intel.com |

Abstract

This contribution is a technical report on interworking between 3GPP 5G system and WLAN. It describes 5G and WLAN interworking architecture, related functions, procedures, protocols and interfaces as defined by 3GPP Release 15 and 16. It highlights some key technical gaps and challenges related to enabling the interworking of WLAN with the 5G system and provides guidance for addressing those gaps in IEEE 802.11 and/or 3GPP. This report can provide a reference for WLAN interworking with the 5G system and serve to guide and facilitate standardization efforts to address interworking related gaps and issues in IEEE 802.11 standard and/or create liaison to address relevant issues in 3GPP 5G standard.

**Revision History**

|  |  |  |
| --- | --- | --- |
| Rev.0 | August 31, 2020  | First upload of the Technical report on the interworking between 3GPP 5G system and WLAN  |

Contents

1 Scope 4

2 Objective 4

3 Acronyms and Abbreviations 4

4 Introduction 7

5 Interworking Architecture Reference Model 8

5.1 Untrusted WLAN Integration Architecture 8

5.2 Trusted WLAN Integration Architecture 9

5.3 Support for Wi-Fi only devices 10

5.4 Reference Points 10

6 Interworking Functions 11

6.1 WLAN Access Network Selection 11

6.2 Registration and Authentication 12

6.2.1 IPsec SA over Untrusted WLAN Access 12

6.2.2 IPsec SA over Trusted WLAN Access 14

6.3 PDU Session Management 16

6.4 Access Traffic Steering, Switching and Splitting (ATSSS) 17

6.4.1 ATSSS Steering Functionality 18

6.4.2 ATSSS Rules 19

6.5 5G QoS Model 20

6.5.1 QoS Profile 20

6.5.2 QoS Rules and QoS Flow Descriptions 21

6.5.3 Packet Detection Rules 22

6.5.4 5G QoS Characteristics 23

6.6 User Data Transport 24

7 Interworking Challenges and Gaps 25

7.1 Trusted WLAN Integration 25

7.2 QoS Differentiation over WLAN for 5G Flows 26

7.2.1 DSCP Marking based QoS Mapping 27

7.2.2 Device Centric QoS Management 28

7.2.3 Network Centric QoS Management 30

7.3 Support for Wi-Fi only Devices 31

8 Technical Recommendations 33

9 Possible Future Enhancements 35

9.1 Dynamic Traffic Distribution for ATSSS 35

9.2 TSN support for Integrated 5G and Wi-Fi network 36

10 Conclusion 37

11 References 37

# Scope

This document describes the interworking approaches, architecture, related functions, procedures, protocols and interfaces as defined by 3GPP for interworking of WLAN access network with the 5G system. The document highlights technical issues and gaps related to WLAN interworking with 5G system and provides technical recommendations and guidance to address identified gaps.

# Objective

The objective of this report is to provide a reference document for WLAN interworking with the 5G system, and to highlight technical issues and gaps related to the interworking to guide and facilitate standardization effort to address those gaps in IEEE 802.11 standard and/or create liaison to address relevant issues in 3GPP 5G standard.

# Acronyms and Abbreviations

5G AN 5G Access Network

5G NR 5G New Radio

5QI 5G QoS Identifier

AAA Authentication Authorization and Accounting

AC Access Category

AKA Authentication and Key Agreement

AMBR Aggregate Maximum Bit Rate

AMF Access and Mobility Management Function

ANDSP Access Network Discovery and Selection Policy

ANQP Access Network Query Protocol

AP Access Point

AR/VR Augmented Reality/Virtual Reality

ARP Allocation and Retention Policy

ATSSS Access Traffic Steering, Switching and Splitting

ATSSS-LL Access Traffic Steering, Switching and Splitting Low Layer

AUSF Authentication Server Function

CN Core Network

DL Downlink

DSCP Differentiated Services Codepoint

DS-TT Device Side TSN Translator

EAP Extensible Authentication Protocol

EAPoL EAP over LAN

eATSSS Enhanced Access Traffic Steering, Switching and Splitting

EDCA Enhanced Distributed Channel Access

ePDG evolved Packet Data Gateway

ESP Encapsulating Security Payload

GBR Guaranteed Bit Rate

GFBR Guaranteed Flow Bit Rate

GRE Generic Routing Encapsulation

HCCA HCF Controlled Channel Access

HCF Hybrid Coordination Function

IIoT Industrial Internet of Things

IKE Internet Key Exchange

IKEv2 Internet Key Exchange Version 2

IMSI International Mobile Subscriber Identity

IPsec IP Security

LWA LTW WLAN Aggregation

LWIP LTW WLAN Integration with IPsec tunnel

MAR Multi-Access Rule

MA PDU Multi Access PDU

MCC Mobile Country Code

MDBV Maximum Data Burst Volume

MFBR Maximum Flow Bit Rate

MNC Mobile Network Code

MPTCP Multi-Path TCP

MPQUIC Multi-Path QUIC

MSDU MAC Service Data Unit

NAI Network Address Identifier

NAS Non Access Stratum

N3IWF Non-3GPP Interworking Function

N5CW Non-5G-Capable over WLAN

NG-RAN Next Generation-Radio Access Network

NW-TT Network Side TSN Translator

PCC Policy and Charging Control

PCF Policy Control Function

PDB Packet Delay Budget

PDR Packet Detection Rule

PDU Protocol Data Unit

PLMN Public Land Mobile Network

PMF Performance Measurement Function

PMK Pairwise Master Key

QCI QoS Class Identifier

QFI QoS Flow Identifier

QRI QoS Rule Identifier

RADIUS Remote Authentication Dial-In User Service

RAN Radio Access Network

RTT Round Trip Time

RQA Reflective QoS Attribute

RQI Reflective QoS Indication

SA Security Association

SDF Service Data Flow

SIM Subscriber Identity Module

SME Station Management Entity

SMF Session Management Function

SNPN Stand-alone Non Public Network

STA Station

SPI Security Parameter Index

SUPI Subscription Permanent Identifier

TCLAS Traffic Classification

TLS Transport Layer Security

TNAP Trusted Non-3GPP Access Point

TNGF Trusted Non-3GPP Gateway Function

TS Traffic Stream

TSN Time Sensitive Network

TSPEC Traffic Specification

TTLS Tunneled Transport Layer Security

TWAG Trusted WLAN Access Gateway

TWIF Trusted WLAN Interworking Function

TWT Target Wake Time

TxOP Transmission Opportunity

UE User Equipment

UL Uplink

UP User Priority

UPF User Plane Function

USIM Universal Subscriber Identity Module

VLAN Virtual Local Area Network

WLAN Wireless Local Area Network

WLANSP WLAN Selection Policy

# Introduction

The 5G era brings new emerging usages including AR/VR, edge computing, autonomous driving and industrial automation (IIoT). New set of 5G use cases and verticals have varied set of requirements on throughput, latency, coverage, availability and reliability which can benefit from combined resources from both 5G and Wi-Fi access networks. Integration and interworking of Wi-Fi with the 5G system would enable leveraging capabilities of both access networks to provide seamless services and applications across NR and Wi-Fi to the end-users.

Interworking between Wi-Fi and cellular networks has been specified by 3GPP starting from 4G LTE system and now for the 5G system. In general, the interworking between Wi-Fi and cellular system can be achieved at three different levels:

* Cloud/App Level Interworking between Wi-Fi and cellular network is achieved in the cloud/app using above IP multipath protocols e.g. MPTCP or MPQUIC. This approach enables multipath over cellular and Wi-Fi links with deployment of MPTCP or MPQUIC proxies or MP-TCP capable servers in the cloud e.g. as used by Apple iTunes music service.
* Core Network (CN) Level Interworking between Wi-Fi and cellular network is achieved within the 3GPP Core Network. 3GPP 4G LTE defines CN level interworking through ePDG and TWAG gateway functions for untrusted and trusted WLAN access respectively. 3GPP 5G Release 15 and 16 defines CN based interworking between 5G Core and WLAN as described in sections 5 and 6.
* RAN Level Interworking between Wi-Fi and cellular network is achieved within the radio access network (RAN). 3GPP 4G LTE has defined RAN level interworking with LWA and LWIP solutions. 3GPP 5G release has not defined RAN level interworking between Wi-Fi and 5G NR access networks.

This report focuses on core network level interworking between WLAN and 5G system.

NOTE: in this report, the terms WLAN, 802.11 and Wi-Fi are used interchangeably.

# Interworking Architecture Reference Model

3GPP 5G architecture supports UE connecting to the 5G core network over WLAN access including connectivity over both untrusted and trusted WLAN access [1]. The 5G architecture also supports a UE connecting to 5G Core over WLAN access only without requiring primary connectivity over cellular access. An untrusted WLAN access is integrated with 5G Core via a Non-3GPP Interworking Function (N3IWF) and a trusted WLAN access is integrated with 5G Core via a Trusted Non-3GPP Gateway Function (TNGF) [1]. The 5G Core is designed to be access neutral where N3IWF and TNGF gateway functions interface with 5G Core using same N2/N3 interfaces as used by the 3GPP access. In both models, the transport of NAS signaling and user plane data is done over IPsec tunnels established between N3IWF/TNGF and the UE.

WLAN networks may advertise support for trusted 5G connectivity with one or more PLMNs e.g. as part of ANQP protocol. Based on the type of WLAN access network discovered, a UE may decide to use untrusted or trusted WLAN access to establish connectivity with the 5G Core, using implementation specific procedures.

## Untrusted WLAN Integration Architecture

Figure 5‑1 shows the architecture for integrating untrusted WLAN access with the 5G core network via N3IWF gateway function. There is loose coupling between N3IWF and WLAN access over Y2 interface through generic IP transport. The NWu interface establishes IPsec security associations (SAs) between UE and N3IWF for secure transport of 5G NAS signaling and user data. The IPsec SAs over NWu apply both encryption and integrity protection for 5G signaling and user data since WLAN is untrusted in such a deployment.



Figure 5‑1 Untrusted WLAN integration with 5G Core via N3IWF

## Trusted WLAN Integration Architecture

Figure 5‑2 shows the architecture for integrating trusted WLAN access with the 5G Core network via TNGF gateway function. There is tighter coupling between TNGF and trusted WLAN AP over a AAA based interface Ta, tying WLAN layer-2 authentication to a derived key from TNGF after successful UE authentication with the 5G Core. The NWt interface establishes IPsec security associations (SAs) between UE and TNGF for transport of 5G NAS signaling and user data like NWu. However, the IPsec SAs over NWt apply NULL encryption for signaling and user data since WLAN layer-2 encryption is trusted in such a deployment.



Figure 5‑2 Trusted WLAN integration with 5G Core via TNGF

There can also be devices which do not support 5G NAS signaling over trusted WLAN access, which requires the 3GPP access on the UE to support EAP-5G, IKEv2 and ESP protocols. Such devices, referred to as Non-5G-Capable over WLAN (N5CW), can still connect to 5G Core over trusted WLAN access if a TWIF (Trusted WLAN Interworking Function) gateway function is supported for that WLAN access network as shown in Figure 5‑3. TWIF performs registration and PDU session management on behalf of N5CW devices with the 5G Core over N1. The UE authentication with 5G Core over WLAN access is executed trough TWIF similar to TNGF case with EAP authentication messages transported over Yw interface. The N5CW device is assumed to have a USIM and is authenticated with the 5G core using EAP-AKA’ (as described in clause 7A.2.4, TS 33.501). The N5CW device may also operate as a 5G UE over NG-RAN, but 3GPP access network is not shown in Figure 5‑3 for simplicity.



Figure 5‑3 5G Core access over WLAN from N5CW devices

## Support for Wi-Fi only devices

Current 3GPP standard does not explicitly define architecture to support Wi-Fi only devices 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 connectivity over both 3GPP and non-3GPP radio per reference architectures in TS 23.501 clause 4.2.8.2. 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 (TS 33.501). A UE is required to support 3GPP IMSI-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 Core control plane (NAS) and user plane functionality (shown by 5G Entity) and includes a USIM (providing 3GPP IMSI-based identity and SIM credentials), can connect to 5G Core as shown in Figure 5‑4. However, this architecture does not work for most Wi-Fi only devices which do not have a USIM included (e.g. legacy/latest devices in enterprise deployments) even if such devices can be upgraded to support 5G NAS functionality.

 

Figure 5‑4 Wi-Fi Only UE requires USIM support for accessing 5G PLMN network

Even for the N5CW (Non 5G Capable over WLAN) UEs 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 TS 33.501 clause 7A.2.4. Hence, the TWIF based architecture as defined currently also does not support Wi-Fi only devices without SIM credentials.

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 across various enterprise/verticals deployments. Technical gaps, challenges and capabilities required for supporting Wi-Fi only devices in the 5G system are covered in section 7.3.

## Reference Points

Following reference points/interfaces are relevant to WLAN and 5G interworking architecture.

**N1** Reference point between the UE and the AMF.

**N2** Reference point between the (R)AN and the AMF.

**N3** Reference point between the (R)AN and the UPF.

**N4** Reference point between the SMF and the UPF.

**N6** Reference point between the UPF and a Data Network.

**N9** Reference point between two UPFs.

**N11** Reference point between the AMF and the SMF.

**N12** Reference point between AMF and AUSF.

**NWu** Reference point between the UE and N3IWF for establishing secure IPsec tunnel(s) between the UE and N3IWF for secure transport of NAS messages and user plane data between the UE and the 5G Core Network over WLAN access.

**NWt** Reference point between the UE and the TNGF to establish secure IPsec tunnels between the UE and TNGF for secure transport of NAS messages and user plane data between the UE and the 5G Core Network over WLAN access.

**Ta** Reference point between the WLAN AP and the TNGF which provides a AAA-based interface.

**Y2** Reference point between the untrusted WLAN access and the N3IWF for the transport of NWu traffic.

**Yw** Reference point between the WLAN AP and the TWIF.

# Interworking Functions

The 5G Core is designed to be access neutral. It uses same N2 and N3 interfaces used by the 3GPP access to also interwork with WLAN access network through N3IWF, TNGF or TWIF gateway functions. This section describes some of the key functions related to WLAN and 5G interworking including functionality needed in the WLAN domain. These functions as described apply for both the dual radio devices and the Wi-Fi only devices, except for the ATSSS function in section 6.4. Specific challenges for supporting Wi-Fi only devices are covered in section 7.3.

## WLAN Access Network Selection

5G defines policies for WLAN access network selection as part of Access Network Discovery and Selection Policy (ANDSP) [3]. The ANDSP specifies set of WLAN Selection Policy (WLANSP) rules and configuration information for connectivity over untrusted WLAN access (clause 6.6.1 of TS 23.503). The 3GPP Access on the UE can use the WLANSP rules to select a preferred WLAN access network which can provide untrusted connectivity to 5G Core via N3IWF. The WLANSP rules are only used by the UE when a WLAN access network can not be selected based on user preferences e.g. when there are no user preferences or when there is no user-preferred WLAN access network available.

The UE may also decide to connect to 5G core via a trusted WLAN access network. 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. First, UE discovers list of PLMNs with which trusted 5G connectivity is supported by available WLAN networks e.g. by using ANQP protocol to query such a 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. Finally, the UE selects a WLAN access network which provides trusted 5G connectivity to the selected PLMN, by using WLANSP rules to prioritize and select a preferred WLAN access network.

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 first discovers list of PLMNs (e.g. over ANQP) with which trusted 5G connectivity without NAS is supported by available WLAN access networks, then UE selects a PLMN network from that list and finally UE selects a preferred WLAN access network (by using WLANSP rules) which provides connectivity via TWIF to that PLMN.

To enable discovery and selection for trusted WLAN networks, the WLAN STA needs to support querying 3GPP Cellular Network Information containing PLMN lists over the ANQP protocol and pass the discovered information to 3GPP Access on the UE.

## Registration and Authentication

UE registration with 5G Core over the WLAN access is based on the registration procedure defined over the 3GPP access. A vendor specific EAP-5G method is defined by 3GPP (clause 9.3.2 in TS 24.502), which is used to encapsulate NAS registration messages between UE and N3IWF/TNGF (EAP-5G is not used for UE authentication). The UE authentication over WLAN access is done using EAP-AKA’ or 5G-AKA authentication method, similar to UE authentication for the 3GPP access. A signaling IPsec ESP security association (SA) is established between the UE and N3IWF/TNGF during registration procedure using IKEv2 protocol (RFC 7296), for transport of NAS messages over the WLAN access.

###  IPsec SA over Untrusted WLAN Access

When the UE decides to connect to 5G Core over an untrusted WLAN access, the UE first connects to and obtains an IP address from the untrusted WLAN access, then the UE selects an N3IWF in a PLMN and initiates procedure to establish IPsec SA with the selected N3IWF as shown in Figure 6‑1 [2].

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. UE then initiates IKE\_AUTH exchange without AUTH payload which indicates to N3IWF to start an EAP-5G session. The EAP-5G protocol is used to encapsulate NAS messages over IKEv2 protocol between UE and N3IWF. UE authentication over untrusted non-3GPP access is executed using either EAP-AKA’ or 5G-AKA authentication method. After successful UE authentication, both N3IWF and UE have a common N3IWF key and EAP-5G session is completed with an EAP-Success sent to UE. Next, IKE\_AUTH exchange with AUTH payload is used to establish a signaling IPsec SA for ESP protocol between UE and N3IWF using the common N3IWF key, over the NWu interface. The signaling IPsec SA applies both encryption and integrity protection for secure transfer of NAS messages. UE establishes a TCP connection with the N3IWF for reliable delivery of NAS messages. All subsequent NAS messages, including the Registration Accept message, are carried over the TCP connection within the signaling IPsec SA.



Figure 6‑1 Signaling IPsec SA establishment over untrusted WLAN access

Figure 6‑2 shows control plane protocol stack for establishment of signaling IPsec SA over NWu interface for untrusted WLAN access. The NAS messages for UE authentication are encapsulated in EAP-5G messages sent over IKEv2 protocol. There is loose coupling between WLAN AP and N3IWF on the network side and between WLAN Access and 3GPP Access on the UE side, over generic IP transport. The EAP-5G and IKEv2 protocols are implemented within 3GPP Access on the UE. No specific enhancements are needed on the WLAN AP or WLAN STA to support untrusted integration of WLAN access with 5G core.



Figure 6‑2 Control Plane for signaling IPsec SA establishment over untrusted WLAN

###  IPsec SA over Trusted WLAN Access

For trusted WLAN integration, there is tight coupling between WLAN AP and TNGF function on the network side and between 3GPP Access and WLAN Access on the UE side, to register and authenticate UE with the 5G Core and thereafter establish WLAN layer-2 authentication as shown by the flow in Figure 6‑3 [2].

The UE first selects a trusted WLAN access network as described in section 6.1 and then establishes a layer-2 association with the WLAN AP (TNAP) within that trusted access. An EAP procedure is initiated between TNAP and UE to request UE Identity for link layer authentication of the UE. The NAI (Network Address Identifier) provided by the UE indicates that the UE requests "5G connectivity" to a specific PLMN, e.g. with NAI="<any\_username>@nai.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org". This triggers WLAN AP to send a AAA based request to the TNGF, which operates as a AAA proxy. TNGF starts an EAP-5G session with the UE by sending an EAP-Request/5G-Start message. The UE authentication is performed using either EAP-AKA’ or 5G-AKA authentication method. The NAS messages for UE authentication/registration are encapsulated in EAP-5G messages, which get encapsulated over AAA messages (e.g. using RADIUS EAP-message attribute) between TNGF & WLAN AP and encapsulated over layer-2 protocol (IEEE 802.1x/EAPoL) between WLAN AP and UE. After successful UE authentication, a common TNGF key is established between TNGF and UE and a TNAP key is derived from the TNGF key and sent to the WLAN AP. An EAP-Success message is sent by TNGF to the UE completing the EAP-5G session.

The TNAP key is used as the Pairwise Master Key (PMK) in the WLAN 4-way handshake to establish Wi-Fi layer-2 security between the UE and WLAN AP. After layer-2 security is established, UE receives IP address configuration from the WLAN access network. UE then establishes a signaling IPsec ESP SA with TNGF using IKEv2 protocol with the common TNGF key and a NULL encryption is negotiated.



Figure 6‑3 Signaling IPsec SA establishment over trusted WLAN Access

Figure 6‑4 shows control plane protocol stack for establishment of signaling IPsec SA over NWt interface for trusted WLAN access. The EAP-5G protocol is implemented as part of 3GPP Access on the UE and on the TNGF. The AAA-based Ta interface is not defined in 3GPP currently. The TNGF function could also be implemented as part of the WLAN Access network connecting with 5G core over N2 and N3 interfaces.



Figure 6‑4 Control Plane for signaling IPsec SA establishment over trusted WLAN

Both for the untrusted and trusted WLAN access, after establishment of signaling IPsec SA, UE establishes a TCP connection with the N3IWF or TNGF for reliable delivery of NAS messages. All subsequent NAS messages, including the Registration Accept message, are carried over the TCP/IP connection within the signaling IPsec SA as shown by the control plane protocol in Figure 6‑5 [1].



Figure 6‑5 Control Plane protocol after signaling IPsec SA is established

## PDU Session Management

The PDU session management over untrusted WLAN access and trusted WLAN access are described in clause 4.12 and 4.12a in TS 23.502. The PDU session establishment procedure over WLAN access is based on the session establishment procedure defined for the 3GPP access. The key difference is that when the PDU session (either single access or multi-access PDU session) is established over a WLAN access, one or more IPsec ESP child SAs are created using IKEv2 protocol between N3IWF/TNGF and UE to transport 5G QoS flows user data over WLAN access.

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 5G QoS flow(s) and QoS profiles associated with each child SA, based on local policies, configuration and the QoS profiles received from the 5G core network. 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 user plane child SA. This message includes a 5G\_QOS\_INFO Notify payload which contains QoS specific parameters for the UE. If additional IPsec child SA(s) needs to be established, a separate Create\_Child\_SA request is sent to the UE for each child SA. Figure 6‑6 shows control plane for establishment of user plane IPsec child SA via N3iWF or TNGF.

The N3IWF or TNGF can optionally 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/TNGF mark all IP packets sent over this child SA with that DSCP value, which can provide QoS differentiation within the WLAN access.

For user plane IPsec SA creation over WLAN access, the endpoints are between 3GPP access on the UE and the N3IWF/TNGF on the network side, and no specific enhancements needed on the WLAN AP or WLAN Access on the UE side.



Figure 6‑6 Control Plane for establishment of user plane IPsec child SA

## Access Traffic Steering, Switching and Splitting (ATSSS)

3GPP ATSSS functionality provides a multi-access PDU Connectivity Service through creation of a Multi-Access PDU (MA PDU) session, which enables PDU data delivery between 5G Core network and the UE over 3GPP and non-3GPP access simultaneously [1]. UE may request establishment of a MA PDU session when it is registered over both 3GPP and non-3GPP access or when it is registered over only one access. In the first case, the user plane resources get established over both accesses as part of MA PDU session establishment. In the second case, user plane resources get established over only one access as part of the MA PDU session establishment and UE can request adding user plane resources over the second access when UE registers over that access. Separate N3/N9 tunnels are established between the UPF and 3GPP access and non-3GPP access for PDU data transfer.

ATSSS supports traffic steering functionality at both high-layer (above IP) and low-layer (below IP). In 3GPP Release 16, the high-layer steering functionality is supported using MPTCP which can be used for steering TCP traffic, and the low layer steering functionality is supported via ATSSS-LL which can be used for steering all types of traffic, including TCP, UDP and Ethernet traffic. Figure 6‑7 shows ATSSS architecture in the 5G system. The UE may support either MPTCP functionality, ATSSS-LL functionality or both. Similarly, the UPF may support one or more of these steering functionalities. The ATSSS-LL functionality is mandatory in the UE and UPF for MA PDU session of type Ethernet. The MPTCP functionality in the UE communicates with an associated MPTCP Proxy functionality in the UPF using the MPTCP protocol. For ATSSS-LL, UPF supports a Performance Measurement Function (PMF), to request access specific performance measurements from the UE over the user-plane of 3GPP access and/or non-3GPP access. The PMF as defined currently provides Round Trip Time (RTT) measurements and access availability/unavailability report from the UE.



Figure 6‑7 ATSSS Architecture

###  ATSSS Steering Functionality

Figure 6‑8 shows ATSSS steering functionality on a UE (clause 5.32.6 in TS 23.501). During MA PDU session establishment, the UE provides its ATSSS Capability to the network indicating supported steering functionalities (MPTCP or ATSSS-LL). The SMF creates ATSSS rules and N4 rules based on the PCC policy. The ATSSS rules are sent from the network to the UE for UL traffic distribution on the UE, and N4 rules are sent to the UPF to apply ATSSS policy for DL traffic distribution. If UE supports ATSSS-LL, then SMF also provides Measurement Assistance Information for PMF measurements reporting to the UE.

If the MPTCP functionality is selected by the network, then the MPTCP Proxy functionality is enabled in the UPF and the SMF provides MPTCP steering functionality related information to the UE which includes link specific IP addresses (IP@1 and IP@2) for two accesses and MPTCP proxy information. The IP@3 is the UE IP address assigned for the MA PDU session. TS 24.193 defines that the IETF TCP converter protocol (RFC 8803) must be used for the MPTCP steering functionality between the MPTCP functionality on the UE and the MPTCP Proxy.



Figure 6‑8 ATSSS Steering Functionality on the UE

###  ATSSS Rules

The UE receives ATSSS rules from the network in an ATSSS container IE as part of the PDU session establishment procedure. The ATSSS rules specify how the UL user data traffic should be distributed across 3GPP and non-3GPP access for the associated MA PDU session. ATSSS rules incudes three key parts (clause 5.32.8 in TS 23.501):

* **Traffic descriptors** to identify the matching user data traffic to determine when the ATSSS rule applies.
* **Steering modes** to specify the traffic distribution policy over 3GPP and non-3GPP access for matching service data flow (SDF). Following steering modes are defined:
	+ Active Standby: It is used to steer an SDF on one access (the Active access), when this access is available, and to switch the SDF to the available other access (the Standby access), when Active access becomes unavailable. When the Active access becomes available again, the SDF is switched back to this access.
	+ Smallest Delay: It is used to steer an SDF to the access that is determined to have the smallest Round-Trip Time (RTT). The RTT measurements can be obtained from the MPTCP protocol RTT measurements or based on PMF RTT measurements for ATSSS-LL.
	+ Load Balancing: It is used to split SDF traffic across both accesses if both accesses are available. It specifies percentage of the SDF traffic that should be sent over the 3GPP access and remaining sent over the non-3GPP access. This mode is only applicable to non-GBR flows.
	+ Priority Based: It is used to steer all the traffic of an SDF to the high priority access, until this access is determined to be congested. Then the traffic of the SDF is sent also to the low priority access, i.e. the SDF traffic is split over the two accesses. 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.
* **Steering functionality** to specify whether the MPTCP functionality or the ATSSS-LL functionality should be used to steer the traffic of matching SDF.

To support the ATSSS functionality as defined currently, no enhancements are needed on the WLAN STA and AP side. Some possible future enhancements to ATSSS functionality could result in some impacts to WLAN domain as described in section 9.1.

## 5G QoS Model

The 5G QoS model is defined in clause 5.7 of TS 23.501. The 5G QoS model, as used over the 3GPP access, is also followed when the UE accesses the 5G core over the non-3GPP access. The QoS Flow is the finest granularity of QoS differentiation within the PDU session, both for single access and multi-access (MA) PDU sessions. As part of PDU session establishment procedure, one or more QoS Flows get associated with the PDU session based on binding of PCC rule to a QoS Flow. The QoS Flow is uniquely identified by a QoS Flow Identifier (QFI) within a PDU session. User plane traffic with the same QFI for a PDU session receives same traffic forwarding treatment within the access network. The QFI may be dynamically assigned or may be set to 5QI value (section 6.5.1).

For a MA PDU session, a QoS Flow is not associated with specific access i.e. it is access agnostic and the same QoS is supported when the flow 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).

A 5G QoS Flow carried over WLAN access has following associated information:

* **QoS Profile**, provided to the N3IWF or TNGF
* **QoS Rules**, either signaled to the UE or derived by the UE by applying Reflective QoS control, and the **QoS Flow Descriptions** for the QoS flows sent to the UE
* **Packet Detection Rule(s)** (PDR) provided to the UPF

###  QoS Profile

A QoS profile is defined for each QoS Flow of a PDU session and includes QoS parameters as specified in Table 6‑1. The QoS profile and the QFI of all the QoS Flows of a PDU session are provided to the N3IWF or TNGF over N2 as part of the PDU session establishment/modification procedure. For an MA PDU session, for a Non-GBR QoS Flow the QoS profile is sent to both 3GPP and non-3GPP access networks over N2, if UE is registered over both accesses. For a GBR QoS Flow, the QoS profile is sent to only one access network based on the PCC rules. No traffic splitting is supported for GBR QoS Flows in ATSSS in 3GPP Release 16. The QoS profile information is used by the N3IWF and TNGF to map QoS Flows to IPsec child SAs.

Table 6‑1 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 as specified in Table 5.7.4-1 in TS 23.501.  |
| 5G QoS Characteristics | (Optional) 5G QoS Characteristics are only included for dynamically assigned 5QI and provides complete set of QoS characteristics as specified in clause 5.7.3 in TS 23.501. |
| 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 the RQA is signaled, the NG-RAN enables the transfer of the RQI marking for the QoS Flow to the UE. For non-3GPP access, RQA is not used. N3IWF/TNGF transparently include RQI marking for the packet, if received over the N3 interface.  |
| 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 QoS Flow. |

###  QoS Rules and QoS Flow Descriptions

The QoS rules are used by the UE to map UL traffic to QoS Flows within a PDU session and these rules are specified per PDU session. The QoS rules may be explicitly signaled to the UE during the PDU session establishment/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 and will get evaluated based on precedence order. 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) per clause 6.2.5.1 in TS 24.501, if such a derived QoS rule does not exist already. A QoS rule contains parameters as specified in Table 6‑2.

Table 6‑2 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 can be sent to the UE as part of the PDU session establishment or modification procedure and includes parameters as specified in Table 6‑3. These QoS parameters are used by the UE to provide QoS differentiation for the indicated QoS Flow.

Table 6‑3 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 & 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 & DL | Highest bit rate that is expected by the QoS Flow. |
| Averaging Window | (Optional) The duration over which the GFBR and MFBR is calculated. |

As part of PDU session establishment/modification procedure, the N3IWF/TNGF establishes user plane IPsec child SAs with the UE for user data transport over WLAN access. The N3IWF/TNGF includes a 5G\_QOS\_INFO Notify payload which contains QoS specific parameters as part of the Create\_Child\_SA request sent to the UE to establish a child SA. This provides QoS information as captured in Table 6‑4 to the UE for QoS Flow(s) to be carried over that IPsec child SA.

The decision to map QoS Flows to IPsec child SAs is left up to the N3IWF/TNGF implementation. If TNGF decides to aggregate multiple GBR QoS Flows or multiple Non-GBR QoS Flows into the same IPsec child SA, the TNGF needs to derive, 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.

Table 6‑4 5G\_QOS\_INFO Notify Payload

|  |  |
| --- | --- |
| Parameters | Description |
| PDU Session ID | Identifier for the PDU session associated with the IPsec 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 IPsec 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 only for trusted non-3GPP access as defined currently. It includes QoS characteristics associated with 5QI and GBR QoS flow information as provided in the QoS profile. Can be used by the UE to reserve resources on trusted WLAN access.  |

###  Packet Detection Rules

The Packet Detection Rule(s) are used to classify a user plane packet arriving at the UPF (clause 5.8.2.11.3 in TS 23.501). 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 6‑5 lists some of the relevant information contained in a PDR. 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 6‑5 Packet Detection Rule – some 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. 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 signaled 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 RAN in DL and UL direction. The N3IWF or TNGF does not perform any bit rate enforcement for DL or UL traffic.

###  5G QoS Characteristics

Each 5QI value is associated with a set of QoS characteristic as described in Table 6‑6. These QoS characteristics are used to determine packet forwarding treatment for a QoS flow within the 5G system (core, access network and the UE). Standardized 5QI values and associated QoS characteristics are defined for frequently used services in Table 5.7.4-1 of TS 23.501 for GBR, Delay-critical GBR and Non-GRB resource types, for signaling optimization. Dynamically assigned 5QI values and associated characteristics can be defined for services for which standardized 5QI values can not be used.

Table 6‑6 5G QoS Characteristics

|  |  |
| --- | --- |
| QoS Characteristic | Description |
| Resource Type | Indicates the GBR, Delay-critical GBR or Non-GBR resource type for a QoS Flow. A GBR QoS Flow uses either the GBR or Delay-critical GBR resource type. For GBR QoS Flows, dedicated network resources are allocated in the 5G-AN to guarantee the bit rate.  |
| Priority Level | Indicates a priority in scheduling resources among QoS Flows. The lowest Priority Level value corresponds to the highest priority. It is used to differentiate between QoS Flows within the same UE and across different UEs. |
| Packet Delay Budget (PDB) | Defines an upper bound for the time that a packet may be delayed between the UE and the UPF that terminates the N6 interface. The PDB is used to guide configuration for scheduling functions in the 3GPP access network. |
| Packet Error Rate | Defines an upper bound for a rate of non-congestion related packet losses. This is used to determine appropriate link layer protocol configurations in 3GPP access network. The PER is same in the UL and DL.  |
| Averaging Window | Represents the duration over which the GFBR and MFBR shall be calculated. |
| Maximum Data Burst Volume (MDBV)  | MDBV is applicable only for Delay-critical GBR resource type. It denotes the largest amount of data that the 5G-AN is required to serve within a period of 5G-AN PDB. |

When 5G flows are carried over the WLAN access, the QoS differentiation needs to be provided over Wi-Fi link to support 5G QoS over WLAN. Currently, the QoS differentiation over WLAN can be provided by 802.11e defined QoS enhancements schemes. The key issue for supporting 5G QoS over WLAN is how QoS differentiation can be provided within WLAN domain based on 5G QoS characteristics and parameters for GBR QoS Flows and Non-GBR QoS Flows. Details on QoS related gaps and challenges are captured in section 7.2.

## User Data Transport

For UL user data, the UE associates the flow data to a QFI (QoS Flow Identifier) within the associated PDU session based on packet filters specified by the QoS rules. If there is a specific user plane IPsec child SA associated with the matching PDU session and QFI, the UL data will be transported on that IPsec SA, else the UL data will be transported on the user plane IPsec SA indicated as default child SA [5].

The UE encapsulates the UL packet inside a GRE packet, with the GRE header carrying the QFI. The UE further encapsulates the GRE packet into an IP packet and sends to the N3IWF/TNGF over the IPsec child SA selected for the QFI in a tunnel mode. If a DSCP value is associated with the IPsec child SA, then UE marks the IP packet with that DSCP value.

For UL traffic delivered via a MA PDU session, both ATSSS rules and QoS rules are applied. The UE evaluates QoS rules to determine which QoS Flow can be used to deliver the UL traffic within the MA PDU session. The UE evaluates ATSSS rules to determine the steering mode and steering functionality for the UL traffic. 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.

For DL user data over both trusted and untrusted non-3GPP accesses, the UPF maps the user data packets to a QoS Flow based on packet filters specified as part of PDRs (Packet Detection Rules) for the associated PDU session [5]. UPF includes QFI, and RQI in the encapsulation header on the N3 interface. Upon receiving a DL packet via 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 GRE header carrying the QFI and RQI information. The GRE packet is further encapsulated into an 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 N3IWF/TNGF marks the IP packet with that DSCP value.

Figure 6‑9 shows user plane protocol for data transport over WLAN access via N3IWF or TNGF.



Figure 6‑9 User Plane via N3IWF or TNGF

# Interworking Challenges and Gaps

This clause identifies specific gaps related to supporting WLAN interworking with 3GPP 5G system and identifies new capabilities which need to be supported within the WLAN domain to enable such interworking. These gaps apply for both the dual radio devices and the Wi-Fi only devices connecting to 5G core over WLAN access. Additional gaps and challenges for supporting Wi-Fi only devices are covered in section 7.3.

## Trusted WLAN Integration

For the trusted WLAN integration, there is tight coupling between 3GPP Access and WLAN STA on the UE and between WLAN AP and TNGF on the network side. A WLAN Access network is said to provide trusted 5G Connectivity to a PLMN when it supports a TNGF function connecting to AMF/UPF in that PLMN. Similarly, a WLAN access network is said to provide trusted 5G Connectivity without NAS to a PLMN network when it supports a TWIF function connecting to AMF/UPF in that PLMN.

Hence, to provide trusted connectivity to 5G Core, the WLAN Access network may need to be enhanced to support TNGF and/or TWIF functions, connecting to 5G Core over 3GPP defined interfaces. The WLAN access network also needs to advertise PLMNs with which it supports trusted 5G connectivity via TNGF/TWIF as part of 3GPP Cellular Network information provided over ANQP (IEEE 802.11u Standard and TS 24.502). The AAA-based Ta interface between WLAN AP and TNGF needs to be defined. The Yw interface between WLAN AP and TWIF is outside of 3GPP scope and needs to be defined to carry EAP messages for UE authentication.

The decision to use trusted WLAN access for connecting to 5G core is made by the 3GPP Access on the UE based on implementation specific criteria and/or the UE configuration/capability. Supporting trusted WLAN integration via TNGF might be preferred over untrusted WLAN integration because it avoids double encryption for 5G user data traffic by using NULL encryption over the IPsec child SAs.

Table 7‑1 summarizes gaps and new capabilities needed to support trusted WLAN integration with 5G Core.

Table 7‑1 New Capabilities to Support Trusted WLAN Integration

|  |  |  |
| --- | --- | --- |
| Entity | New Capability to be Supported | Standard/domain to address the gap |
| WLAN Access Network | * Support TNGF function providing trusted connectivity to a PLMN network
* Support TWIF function providing trusted connectivity to a PLMN network
* Define AAA-based Ta interface and Yw interface
 | WLAN domain |
| ANQP Server in WLAN Access network | * Advertise PLMNs with which WLAN access network supports trusted 5G connectivity via TNGF or TWIF as part of 3GPP Cellular Network information provided over ANQP
 | WLAN domain  |
| WLAN STA | * Support trigger-based discovery of 3GPP Cellular Network information (containing PLMN lists) over ANQP and pass the discovered information to 3GPP Access on the UE
* Support receiving trigger from 3GPP access for connecting to a specific trusted WLAN access
* Support generating and providing 3GPP specific NAI when sending UE identity to WLAN AP for trusted WLAN access via TNGF
* Support providing NAI uniquely identifying a UE when sending UE identity to WLAN AP for trusted WLAN access via TWIF
* Support transport of EAP-5G messages to/from 3GPP access on the UE
 | WLAN and 3GPP(internal UE interface between 3GPP access and WLAN STA)  |
| WLAN AP | * Support Ta interface with TNGF
* Support invoking Ta interface based on 3GPP specific NAI received from UE
* Support filtering EAP-5G protocol messages
* Support using TNAP key received from TNGF for 802.11i 4-way handshake to establish layer-2 security.
 | WLAN domain |

## QoS Differentiation over WLAN for 5G Flows

The IEEE 802.11-2016 Standard defines EDCA and HCCA schemes for QoS management. The EDCA scheme provides prioritized contention-based access and is the most widely adopted QoS management scheme for WLAN traffic prioritization as part of WFA WMM certification.

The EDCA supports 8 User Priorities (UP) for traffic flows, which get mapped to 4 QoS Access Categories (AC) for background, best effort, video and voice traffic (AC\_BK, AC\_BE, AC\_VI, AC\_VO). Differentiated QoS is achieved per access category by employing different values for AIFS (Arbitration Interframe Space) and CW (Contention Window) parameters for each AC. EDCA also supports admission control for QoS traffic streams per AC using ADDTS Request/Response where traffic characteristics is specified with TSPEC element and traffic identification is specified with TCLAS element. Even with 4 QoS ACs and admission control for QoS traffic streams, EDCA still does not provide any guarantees on throughput, latency, jitter etc. Only priority-based bandwidth allocation based on ACs can be provided. Hence it is not possible to provide any guarantees for meeting guaranteed bit rate and latency requirements for 5G GBR flows and Delay-critical GBR flows over WLAN access. IEEE 802.11 standards also supports mapping data packets to 802.11 UP based on DSCP markings in the IP header (clause 11.23.9 in [11]).

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 identified by QFI, based on 5G QoS characteristics (defined by 5QI) and parameters within the already defined EDCA QoS scheme.

There could be 3 possible approaches to providing QoS differentiation within WLAN access for 5G traffic.

1. DSCP marking based QoS Mapping
2. Device centric QoS Management
3. Network centric QoS Management

Both device centric and network centric approaches provide QoS differentiation for 5G flows based on identifying and prioritizing IPsec child SAs carrying 5G traffic. If supported, the IPsec child SA based traffic identification and prioritization should take precedence over the DSCP marking based approach if DSCP marking are also specified for IPsec packets. It is also recommended to map each 5G QoS Flow to a separate IPsec child SA at the N3IWF/TNGF, to be able to provide QoS differentiation within WLAN access per 5G QoS flow.

###  DSCP Marking based QoS Mapping

In the DSCP marking based QoS mapping, the 5G flow packets sent over WLAN access are tagged with DSCP marking in the IP header as defined by DiffServ (RFC 2474)**,** and within WLAN access the DSCP marking gets mapped to 802.11 User Priority (UP) and Access Category (AC) as shown in Figure 7‑1. No QoS negotiation happens between the STA and WLAN AP in this case. The WLAN AP provides 3GPP network specific DSCP to UP mapping to non-AP STA as described in clause 11.23.9 in [11], which is used by the STA to determine UP for uplink packets based on DSCP marking of the packet. 3GPP network specific DSCP to UP mapping is also used by the AP to determine UP for DL packets based on DSCP marking of the packet.

The 5G architecture for integrating WLAN access enables associating a DSCP value with every IPsec child SA created over WLAN access to carry 5G QoS Flow associated with a 5QI value. All IP packets sent over that child SA get marked with the associated DSCP value. For DL traffic, 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 based QoS is applied for the 5G traffic on the segment between N3IWF/TNGF and WLAN AP. The UE and WLAN AP map DSCP to 802.11 UP/AC for UL and DL traffic respectively based on 3GPP network specific DSCP to UP mapping defined (clause R.3 in [11]), and 802.11e EDCA QoS is applied over the WLAN link in both UL and DL direction.



Figure 7‑1 Mapping 5G QoS to WLAN QoS with DSCP Marking based QoS Management

To support DSCP marking based approach, the standardized 5QI values need to be mapped to DSCP values, however this mapping is not defined in the 3GPP spec and is left up to the implementation. For consistent QoS experience it is desirable to define a common mapping between 5QI values to DSCP values to be used across different 5G system deployments. The IETF information draft [19] addresses the mapping between LTE QCI and 5QI to DSCP values. As described in that draft, detailed analysis of QoS characteristics and intended example services of various 5QI values is required to define 5QI mapping to DSCP values and this could result in allocation of new DSCP code points in Pool 1 and Pool 3 defined by IANA [20]. The GSMA IR.34 spec has defined limited mapping between LTE QCI to DSCP values but those are not updated to include mapping for 5G 5QI 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 deployments of WLAN integration with 5G network. Once defined this mapping can be used by N3IWF, TNGF and TWIF for marking DL data packets with DSCP and by the UE for marking UL data packets with the DSCP to enable DSCP marking based QoS differentiation within WLAN. The WLAN AP and UE also need to support updated set of DSCP values to User Priorities mapping.

This approach has the limitation of DSCP markings getting reset by on path routers for DL packets, resulting in no QoS differentiation for those packets in WLAN. Also, no resource reservation is done in this approach at the AP. Despite those limitation, the DSCP marking based QoS management approach can be used in deployments where 5G QoS characteristics/parameters and IPsec child SA information can not be made available to WLAN access for QoS management due to limited integration between WLAN and 3GPP access. Also, for trusted WLAN integration deployments with TWIF, this is the only option to provide QoS differentiation within WLAN access since no IPsec child SAs are created. The 5QI to DSCP mapping can also be useful for the device centric and network centric approaches to determine mapping to UP in those approaches.

Table 7‑2 summarizes gaps and enhancements needed to support DSCP marking based QoS Management approach.

Table 7‑2 Enhancements needed to support DSCP marking based QoS Management

|  |  |  |
| --- | --- | --- |
| Entity | New Capability to be Supported | Standard/domain to address the gap |
| General | Define 5QI values to DSCP mapping | IEEE 802.11 or GSMA or IETF or 3GPP |
| N3IWF, TNGF, TWIF, 3GPP Access on UE | Requirement to tag 5G user data packets with appropriate DSCP value based on standardized 5QI to DSCP mapping | 3GPP |
| WLAN STA, WLAN AP | Define mapping between updated DSCP values to 802.11 User Priorities | IEEE 802.11 or 3GPP |

###  Device Centric QoS Management

In the device centric QoS management approach, the WLAN STA initiates QoS management within WLAN for 5G flows carried over IPsec child SAs. The WLAN STA can make use of EDCA admission control procedure to request admission of specific QoS traffic streams (TS) to attempt to provide some resource reservation for 5G traffic carried over IPsec child SAs.

An IPsec child SA carrying 5G traffic is identified using the unique identifiers for IPsec SA - the SPI (Security Parameter Index), the destination IP address and the security protocol ID (RFC 2401). Also, the IPsec SAs always exist in pair with one SA in each direction for inbound and outbound traffic exchange between IPsec end points (RFC 2401). For 5G Flows over WLAN, there will be two separate IPsec child SAs for UL and DL direction, each identified by the set of unique identifiers for an IPsec SA.

For trusted WLAN access, the 5G QoS characteristics (5QI) and parameters are provided by TNGF to the UE as part of the IPsec child SA creation for 5G QoS flows. However, for untrusted WLAN access, 3GPP spec does not require N3IWF to provide 5G QoS information to the UE, which is a gap and should be addressed in 3GPP. How the 5G QoS information is used by the WLAN access for resource reservation and mapping 5G QoS to 802.11 UP and traffic specification (TSPEC) needs to be defined.

Figure 7‑2 shows an example architecture for device centric QoS management for 5G flows within WLAN access. A higher layer ‘5G QoS Entity’ can be co-located within the WLAN STA to provide interworking with 3GPP access for supporting device centric QoS management for 5G traffic. The 5G QoS Entity receives 5G QoS related information from the 3GPP stack for 5G flows. The 5G QoS related information includes 5G QoS characteristics and parameters for 5G Flows, IPsec SA information to identify associated IPsec child SAs and any assigned DSCP value for IPsec SAs. The IPsec SA info includes information to identify IPsec security associations in each direction for UL and DL traffic. For each IPsec SA (uplink SA and downlink SA) the SPI (Security Parameter Index), the destination IP address and security protocol ID information is provided.



Figure 7‑2 WLAN Example architecture for Device Centric QoS Management for 5G flows

The 5G QoS Entity maps the 5G QoS characteristics and parameters to 802.11 QoS Traffic Specification (TSPEC) and 802.11 User Priority. Any DSCP value received can be considered to determine mapping of 5G QoS to 802.11 User Priority. The 5G QoS Entity also creates two separate 802.11 Traffic Classification (TCLAS) elements, one each for UL and DL traffic, from the IPsec SA information received from the 3GPP stack to indicate traffic filters for the IPsec SAs carrying 5G traffic. The 5G QoS Entity on the WLAN STA initiates QoS negotiation with the local SME for IPsec SAs carrying 5G traffic. The SME on WLAN STA triggers QoS negotiation and traffic stream (TS) setup for IPsec SAs both in the UL and DL direction (using Direction field in TSPEC) by invoking the Non-AP-initiated TS Setup procedure (clause 11.4.4.2 in [12]) with ADDTS Request/Response messages.

The 5G QoS characteristics and parameters need to be mapped to TSPEC parameters for QoS TS setup. Some required TSPEC parameters (e.g. MSDU size) are not specified in 5G QoS parameters. Hence, there is a gap on how to map 5G QoS parameters to TSPEC parameters and needs to be addressed. Also, the complete set of 5G QoS characteristics and parameters can be provided to WLAN AP to consider for resource reservation. This can be achieved either by defining a new 5G\_TSPEC element or by extending the TSPEC element. The TCLAS element needs to be enhanced to specify filtering and classification for IPsec SA traffic based on unique identifiers for the IPsec SA (SPI, destination IP address and security protocol ID).

The 5G QoS Entity on the WLAN STA can provide device centric QoS management for 5G traffic for both trusted and untrusted WLAN access integrated within a 5G system. The device centric QoS management model can also be used for Wi-Fi only devices where 3GPP stack is providing 5G NAS and user plane functionality.

###  Network Centric QoS Management

In the network centric approach, the QoS management within WLAN is initiated by the network side for 5G flows carried over IPsec child SAs. This approach is applicable for trusted WLAN access integration via TNGF as this requires tight integration between TNGF and WLAN AP to send 5G QoS information to WLAN AP and trigger network centric QoS management from WLAN AP.

Figure 7‑3 shows an example architecture for network centric QoS management for 5G flows within WLAN access. A higher layer ‘5G QoS Entity’ is co-located within the WLAN AP and receives 5G QoS related information from the TNGF for 5G flows. The 5G QoS related information includes 5G QoS characteristics and parameters for 5G flows, IPsec SA info to identify associated IPsec child SAs, any assigned DSCP value for IPsec SAs and associated 5G PDU Session ID. Similar to the device centric approach, the 5G QoS Entity uses the 5G QoS related information to generate 802.11 TSPEC element, TCLAS (to identify IPsec SA traffic) element, the User Priority for 5G flows and possibly the 5G\_TSPEC element.



Figure 7‑3 WLAN Example architecture for Network Centric QoS Management for 5G flows

The 5G QoS Entity on the WLAN AP initiates QoS negotiation with the local SME for IPsec SAs carrying 5G traffic. The SME on WLAN AP triggers QoS negotiation and traffic stream (TS) setup for IPsec SAs (in UL and DL direction) using the AP-initiated TS Setup procedure as described in 802.11-2016 standard (clause 11.4.4.3) with ADDTS Reserve Request/Response and ADDTS Request/Response messages. The Higher Layer Stream ID for the AP-initiated TS setup for 5G flows can be set to the 3GPP PDU Session ID received from the TNGF.

The network centric QoS management model can also be used for Wi-Fi only devices where the 3GPP stack is providing 5G NAS and user plane functionality. The network centric model can provide more control to the operators over the QoS differentiation for 5G flows and signaling in the WLAN access, with less reliance on device specific implementation for QoS management for 5G flows.

Table 7‑3 summarizes gaps and enhancements needed to support device centric and/or network centric approach for QoS differentiation within WLAN for 5G flows based on identifying and prioritizing IPsec SAs.

Table 7‑3 Enhancements needed to support QoS differentiation in WLAN based on IPsec SAs

|  |  |  |
| --- | --- | --- |
| Entity | New Capability to be Supported | Standard/domain to address the gap |
| N3IWF, 3GPP Access on UE | * Support providing 5G QoS Information for 5G flows carried over untrusted WLAN access to the UE as well, similar to trusted WLAN access
 | 3GPP |
| WLAN STA | * Support a 5G QoS Entity for interworking with 3GPP access to provide device centric QoS management for 5G flows over WLAN
 | IEEE 802.11  |
| WLAN AP | * Support integration with TNGF to receive 5G QoS information for network centric QoS management
* Support a 5G QoS Entity on the WLAN AP for network centric QoS management for 5G flows over WLAN
 | IEEE 802.11 |
| WLAN STA, WLAN AP | * Define mapping of 5G QoS parameters to TSPEC parameters for TS setup. Address how any required TSPEC parameters not specified by 5G QoS need to be handled (e.g. MSDU size)
* Consider providing all 5G QoS parameters to WLAN AP for resource reservation either in a new 5G\_TSPEC element or by extending TSPEC element.
* Enhance TCLAS element to specify filtering and classification for IPsec SA traffic based on unique identifiers for the IPsec SA (SPI, destination IP address and security protocol ID)
 | IEEE 802.11 |
| WLAN AP | * Support AP-Initiated TS setup for 5G flows carried over IPsec child SAs with Higher Layer Stream ID set to the 3GPP PDU Session ID.
 | IEEE 802.11 |

Additionally, the WLAN access needs to support finer grain QoS granularity to meet flow priority, data rate, latency and PER requirements as defined by 5QI characteristics, specially for GBR flows. Further analysis is needed on how new MAC/PHY capabilities in 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 next major Wi-Fi release 802.11be is considering QoS enhancements and new capabilities including TSN support, Multi-link operation and Multi-AP capability. These should consider how fine grain QoS mapping, scheduling and prioritization can be provided for 5G flows based on 5G QoS characteristics and parameters.

## Support for Wi-Fi only Devices

Most Wi-Fi only UEs do not include USIM to provide SIM based identity and credentials. To support such Wi-Fi only devices, 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 (TS 23.501 clause 5.30.1) and the procedure defined for EAP-TLS authentication for SNPN is specified for 3GPP access only (TS 33.501 clause B.2). 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 shown in the example reference architecture in Figure 7‑4(a). Similarly, for Non-5G-capable (N5GC) Wi-Fi only UEs without 5G functionality (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 shown in the example reference architecture in Figure 7‑4(b).

Overall, to facilitate adoption of Wi-Fi only UEs for private 5G network 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 for accessing 5G SNPN core via N3IWF, TNGF or TWIF functions as shown in Figure 7‑4.



Figure 7‑4 Wi-Fi Only devices accessing 5G Standalone Non-Public Network

Assuming, 5G SNPN networks can provide support for 5G-capable Wi-Fi only devices via N3IWF or TNGF, such 5G-capable Wi-Fi only devices need to support a logical 5G Entity providing 5G network control plane (NAS) and user plane functionality. The 5G entity needs to support EAP-5G, IKEv2, IPsec/ESP and 5G NAS protocols to provide 5G control plane functions and needs to support GRE and IPsec/ESP protocols to provide 5G user plane transport function as described in section 6. The non-5G-Capable Wi-Fi only devices do not support 5G control plane (NAS) and user plane functionality and are connected to 5G SNPN core over TWIF gateway function. Both types of Wi-Fi only devices use EAP-TLS/EAP-TTLS authentication method for UE authentication with the 5G core. There are no specific enhancements needed on the WLAN AP to support Wi-Fi only devices.

Once the support for Wi-Fi only devices is added for SNPN network, 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. 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 Wi-Fi only UEs across different geographic deployments.

Table 7‑4 summarizes gaps and new capabilities needed to support Wi-Fi only devices to connect to SNPN and PLMN networks.

Table 7‑4 Enhancements needed to support Wi-Fi Only devices connecting to 5G Core

|  |  |  |
| --- | --- | --- |
| Entity | New Capability to be Supported | Standard/domain to address the gap |
| 5G Core, N3IWF, TNGF, TWIF, UE | * Define architecture and procedure details for supporting 5G-Capable Wi-Fi only UEs with non-IMSI based identity and EAP-TLS/EAP-TTLS based authentication to access 5G SNPN core via N3IWF or TNGF
* Define architecture and procedure details for supporting Non-5G-Capable Wi-Fi only UEs with non-IMSI based identity and EAP-TLS/EAP-TTLS based authentication to access 5G SNPN core via TWIF
* Consider requiring support for EAP-TLS/EAP-TTLS for Wi-Fi only devices in PLMN networks
 | 3GPP |
| 5G-Capable Wi-Fi only device | * Support a logical 5G Entity providing 5G network control plane (NAS) and user plane functionality as defined in 3GPP
* Support EAP-5G, IKEv2, IPsec/ESP and 5G NAS protocols to provide 5G control plane functions as defined in 3GPP
* Support GRE and IPsec/ESP protocols to provide 5G user plane transport function as defined in 3GPP
 | WLAN domain |

# Technical Recommendations

The interworking between IEEE 802.11 WLAN and 3GPP 5G system can enable new deployment opportunities in enterprises and verticals providing seamless 5G services over both access networks. To support such deployment scenarios where WLAN access is integrated with the 5G system, there are certain gaps and challenges as identified and described in detail in section 7 which needs to be addressed within 802.11 standard and/or 3GPP standard.

There are three main gap areas where new capability and enhancements are needed within the WLAN domain to enable WLAN interworking with 5G system:

1. Support for trusted WLAN integration
2. Support for QoS differentiation over WLAN for 5G flows
3. Support for Wi-Fi only devices without USIM connecting to 5G Core

Enhancements needed in each of these areas are summarized below. If implemented, these enhancements may lead to standards and/or deployment related changes within WLAN domain.

To support trusted WLAN integration with 5G system, following key capabilities should be considered within WLAN domain:

|  |
| --- |
| * Support the TNGF and/or TWIF functions within WLAN access network
 |
| * Define AAA-based Ta interface and Yw interface and add support for these on WLAN AP
 |
| * Advertise in the ANQP 3GPP Cellular Network information the list of PLMNs with which WLAN Access supports trusted 5G connectivity
 |
| * Integration with 3GPP access on the UE to enable trusted network discovery, selection and UE authentication
 |
| * Support EAP-5G message filtering on WLAN AP
 |
| * Use the TNAP key provided by TNGF for 802.11i 4-way handshake
 |

To support QoS differentiation over WLAN access for 5G Flows, following key capabilities should be considered within WLAN domain:

|  |
| --- |
| * Define 5QI values to DSCP values to User Priority mapping and/or raise this issue in other relevant standard bodies
 |
| * Support a 5G QoS Entity on the WLAN STA for device centric QoS management for 5G flows based on identifying and prioritizing IPsec SAs carrying 5G traffic, using Non-AP-initiated TS setup
 |
| * Support a 5G QoS Entity on the WLAN AP for network centric QoS management for 5G flows based on identifying and prioritizing IPsec child SAs carrying 5G traffic, using AP-initiated TS setup
 |
| * Support integration with TNGF to receive 5G QoS information for network centric QoS management
 |
| * Support mapping of 5G QoS parameters to TSPEC parameters for QoS traffic stream setup
 |
| * Enhance TCLAS element to specify filtering/classification for IPsec SAs carrying 5G traffic based on unique identifiers for the IPsec SA – SPI, destination IP address and security protocol ID
 |
| * Consider providing all 5G QoS parameters to WLAN AP for resource reservation either in a new 5G\_TSPEC element or by extending TSPEC element
 |
| * Analysis of how 802.11ax MAC/PHY capabilities such as TWT scheduling, OFDMA and MU-MIMO can provide fine grain QoS for 5G flows based on 5QI characteristics, specially for GBR flows
 |

To support Wi-Fi only devices without USIM connecting to 5G Core, following key capabilities should be considered within WLAN domain:

|  |
| --- |
| * Support a logical 5G Entity on the Wi-Fi only UE providing 5G network control plane (NAS) and user plane functionality as defined in 3GPP
 |
| * Support EAP-5G, IKEv2, IPsec/ESP and 5G NAS protocols to provide 5G control plane functions in the 5G entity as defined in 3GPP
 |
| * Support GRE and IPsec/ESP protocols to provide 5G user plane transport function in the 5G entity as defined in 3GPP
 |

Furthermore, there are also following capabilities identified which need to be considered within 3GPP to further enhance the interworking between WLAN and 5G system:

* Support for using standardized 5QI to DSCP mapping within N3IWF, TNGF and on the UE
* Support for providing 5G QoS Information for 5G flows carried over untrusted WLAN access to the UE, to enable device centric QoS differentiation for untrusted WLAN access as well
* Support mapping each 5G QoS flow to a separate IPsec child SA at the N3IWF/TNGF, to be able to provide QoS differentiation within WLAN access per 5G QoS flow.
* Defining architecture and procedures for supporting 5G-capable Wi-Fi only devices without USIM connecting to 5G SNPN via N3IWF/TNGF
* Defining architecture and procedures for supporting non-5G-capable Wi-Fi only devices without USIM connecting to 5G SNPN via TWIF
* Considering support for EAP-TLS/EAP-TTLS for Wi-Fi only devices as a requirement for PLMN networks

#  Possible Future Enhancements

##  Dynamic Traffic Distribution for ATSSS

In current 5G architecture, the ATSSS traffic distribution for a MA-PDU session is controlled by PCC policy which results into ATSSS rules and N4 rules provided to the UE and UPF respectively to steer, switch and split user traffic. There are four steering modes supported within ATSSS as described in section 6.4.2. For ATSSS-LL, traffic distribution can be done according to access availability for Active-Standby steering mode and RTT measurements recorded by PMF for Smallest Delay steering mode. For Load Balancing mode, determination of split percentage over 3GPP and Wi-fi access is statically done based on PCC rule and can not be dynamically adjusted based on access network radio link conditions. For Priority-Based mode, determination of congestion on an access for ATSSS-LL is left up to the implementation without accounting for radio link conditions to determine congestion.

To take full advantage of both 3GPP and WLAN access and provide efficient radio resource usage and improved QoS performance, the ATSSS should support mechanism to dynamically adjust traffic distribution over 3GPP and Wi-Fi access based on access network radio link conditions. Current ATSSS-LL solution can only adjust traffic distribution across 3GPP and non-3GPP access in a reactive manner after detecting noticeable performance degradation based on PMF measurements. Similarly, the higher layer MP-TCP solution and the QUIC-based solution under discussion in eATSSS in 3GPP Release 17 depend on end-to-end feedback to perform congestion and rate control, where access network quality degradation can be detected based on packet loss, however, the ACK time out window limits how fast packet loss can be detected.

Radio measurements from RAN nodes (NG-RAN or WLAN AP) can provide timely indication of radio access conditions such as radio link quality, network load condition and delay statistics to 5G core. The network can use RAN measurements to compare different radio accesses and proactively adjust ATSSS traffic distribution across 3GPP and Wi-Fi access. With RAN measurements provided to ATSSS, radio link degradation can be detected much faster as compared to only using schemes which rely on end-to-end delay measurements such as MPTCP, ATSSS-LL and MPQUIC. The RAN measurements can be used for MPTCP and MPQUIC to determine whether a subflow should be added or removed as well as to estimate path characteristics which can be useful for selecting packet scheduling policy. RAN measurements based approach can provide improved performance with minimal user plane impact. RAN measurements taken at the UE can be used for dynamic ATSSS traffic distribution for UL traffic over 3GPP and Wi-Fi access and can also be sent to the UPF over PMF messaging in certain deployments such as over untrusted WLAN access.

RAN measurements from RAN nodes (NG-RAN or WLAN AP) may include measurements taken by the RAN node or measurements reported by the UE to the RAN node. Many existing RAN measurements in 3GPP and Wi-Fi access are useful for determining traffic distribution across multi-access. For example, RSRP (reference signal received power) and RSRQ (reference signal received quality) for 3GPP access and RSSI (received signal strength indicator) for WLAN are good metrics to indicate radio link quality. Data rate estimate can be another candidate RAN measurement that can be estimated by more intelligent 3GPP RAN nodes and WLAN access points. Network load condition can be reflected via PRB (physical resource blocks) usage for 3GPP access and BSS load for WLAN. Also, RAN can provide L2 latency measurements or queuing latency can be estimated based on RAN resource utilization level.

Overall, there is a gap in the current ATSSS to support dynamic traffic distribution over 3GPP and non-3GPP access based on changing radio link conditions. Incorporating RAN measurements in ATSSS traffic distribution is one approach to address this gap, providing better QoS guarantee and overall efficient radio resource usage. 3GPP Release 17 eATSSS study item is considering enhancements to steering modes and PMF measurements to support dynamic traffic distribution over 3GPP and non 3GPP access. However, the scope of eATSSS study item is limited requiring that there be no RAN impact, hence RAN measurements-based approach can not be considered in Release 17. The RAN measurements-based approach for ATSSS traffic distribution can be beneficial to consider in 3GPP Release 18 timeframe.

To enable such RAN measurements based approach for ATSSS for the WLAN access, RAN measurements for WLAN access can be reported from WLAN AP to TNGF to 5G Core for trusted WLAN access. An interface needs to be defined for WLAN AP to provide Wi-Fi RAN measurements to the TNGF. For untrusted WLAN access, there is no integration between WLAN AP and N3IWF. For untrusted WLAN integration, additional PMF messaging can be defined to report RAN measurements from the UE to 5G Core over the user plane.

##  TSN support for Integrated 5G and Wi-Fi network

IEEE 802.1 TSN standards are designed to operate over IEEE 802 LAN (MAC/PHY) transport, with Ethernet (802.3) used as the main LAN transport in most TSN deployments. Extending TSN to wireless requires providing TSN capabilities like time synchronization (IEEE 802.1AS), time aware scheduling (802.1Qbv) and resource reservation (e.g. IEEE 802.1Qca) over the wireless network which poses several challenges due to unique characteristics of wireless links. There are ongoing industry efforts on supporting TSN functionality over Wi-Fi and 5G wireless links as described here.

3GPP 5G standard has defined architecture to integrate 5G System as a logical TSN bridge with an external TSN system (clause 4.4.8 in TS 23.501) to provide integration of 5G System with TSN networks. The TSN architecture defined for the 5G system includes TSN Translator functionality for the Network-side (NW-TT) and the Device-side (DS-TT) providing TSN ingress and egress ports respectively for 802.1AS time synchronization functionality. A TSN application function (TSN AF) is deployed to exchange TSN bridge information with the TSN central network controller (CNC) (TS 24.519). The DS-TT and NW-TT functions include delivery of generalized precision time protocol (gPTP) messages. The 5G System functionality remains hidden from the TSN System. Besides IEEE 802.1AS time synchronization function, the 5G system does not define support for any other TSN functions in Release 16.

For Wi-Fi, since 802.11 is one of the 802 LAN transport, extensions of 802.1 TSN protocols over 802.11 is architecturally well aligned with the overall TSN architecture. The 802.11 already supports 802.1AS time synchronization capability to distribute time using Timing Measurements (TM) and Fine Timing Measurements (FTM) capabilities defined in 802.11-2016 standard. TSN traffic classification can also be achieved in 802.11 using VLAN tagging (802.1Q) since 802.11 TSPEC and TCLAS support VLAN tag specific traffic differentiation. The TWT scheduling capability in 802.11ax along with OFDMA and MU-MIMO can be used to provide low latency and high reliability for TSN applications. Next major Wi-Fi release 802.11be is also addressing integration with other 802.1 TSN standards and providing TSN grade performance using new features like priority access for time-sensitive traffic, Multi-link operation and Multi-AP capability. Detailed discussion of TSN support over wireless networks can be found in [22].

In private network deployments with Wi-Fi integrated in 5G System (e.g. Industrial IoT), a TSN architecture needs to be defined to integrate the converged 5G and Wi-Fi network with the external TSN system. This TSN architecture should take into account that many 802.1 TSN standards can be natively supported over 802.11 standard. 3GPP next releases should address defining a TSN architecture for integrating external TSN system with a 5G system with integrated WLAN access.

#  Conclusion

With continued evolution of IEEE 802.11 Wi-Fi standards with Wi-Fi 6, Wi-Fi 6E and Wi-Fi 7, the Wi-Fi technology is well positioned as a strong wireless access to carry new breed of 5G applications including AR/VR, edge computing, autonomous driving and industrial IoT. The interworking between WLAN and 3GPP 5G system will enable leveraging capabilities of both access networks to provide seamless services and applications across 3GPP access and WLAN access to the end-users.

There are a number of gaps and challenges which need to be considered and addressed within the WLAN domain to enable interworking with the 5G system. These gaps are related to supporting trusted WLAN integration with the 5G Core, supporting QoS differentiation over WLAN for 5G flows and supporting Wi-Fi only devices without USIM connecting to 5G Core. New capabilities needed within WLAN domain to address the identified gaps related to interworking with 5G system are described in detail, to guide and facilitate standardization efforts to address these gaps in IEEE 802.11 standard and/or other Wi-Fi related standards such as Wi-Fi Alliance.

Certain gaps and new capabilities are also identified for consideration within 3GPP related to QoS differentiation for 5G flows over WLAN and related to support for Wi-Fi only devices without USIM. These may result into liaison to 3GPP to address relevant issues in 3GPP 5G standard.

A possible future enhancement is highlighted for consideration to support dynamic traffic distribution over 3GPP and WLAN access in ATSSS taking into account radio conditions. This would result into Wi-Fi related RAN measurements to be sent to the 5G Core to be considered for making traffic scheduling decisions in ATSSS. Another possible future enhancement is highlighted related to supporting wireless TSN over integrated WLAN and 5G system which needs to consider that many 802.1 TSN standards can be natively supported over 802.11 standard due to 802.11 being one of the 802 LAN transport. These future enhancements are captured for consideration in IEEE 802.11 standard and may lead to a liaison to 3GPP to address relevant issues.

#  References

[1] 3GPP TS 23.501: “System architecture for the 5G System (5GS); Stage 2”

[2] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2"

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

[4] 3GPP TS 24.501: “Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3”

[5]3GPP TS 24.502: “Access to the 3GPP 5G Core Network (5GCN) via Non-3GPP Access Networks (N3AN); Stage 3”

[6] 3GPP TS 33.501: “Security architecture and procedures for 5G system”

[7] 3GPP TS 38.413: “NG Application Protocol (NGAP)”

[8] 3GPP TS 24.526: “User Equipment (UE) policies for 5G System (5GS); Stage 3”

[9] 3GPP TS 24.302: “Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3”

[10] 3GPP TS 38.415: “PDU Session User Plane Protocol”

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

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

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

[14] IEEE Std 802.1AS™‐2020, Timing and Synchronization for Time Sensitive Applications

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

[16] RFC 8803, 0-RTT TCP Convert Protocol

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

[18] RFC 2401, Security Architecture for the Internet Protocol

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

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

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

[22] Avnu Alliance® White Paper, Wireless TSN – Definitions, Use Cases & Standards Roadmap, Version #1.0 – Mar 4, 2020

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

[24] 3GPP TS 24.519: “Time-Sensitive Networking (TSN) Application Function (AF) to Device-Side TSN Translator (DS-TT) and Network-Side TSN Translator (NW-TT) protocol aspects; Stage 3”