IEEE P802.11
Wireless LANs

|  |
| --- |
| Draft technical report on interworking between 3GPP 5G network & WLAN |
| Date: 2021-07-14 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Hyun Seo OH | ETRI | Gajeongro 218 YusungguDaejeon, Korea | +82.42.860.5659 | hsoh5@etri.re.kr |
| Hanbyeog CHO | ETRI | Gajeongro 218 YusungguDaejeon, Korea | +82.42.860.5531 | hbcho@etri.re.kr |
| Yoohwa Kang | ETRI | Gajeongro 218 YusungguDaejeon, Korea | +82.42.860.6364 | yhkang@etri.re.kr |
| Chang Han OH | allRadio Co. Ltd | 280, Seobusaet-gil, Geumcheon-gu, Seoul, Korea | +82.2.801.1310 | choh@allradio.co.kr |
| Shinho CHO | allRadio Co. Ltd | 280, Seobusaet-gil, Geumcheon-gu, Seoul, Korea | +82.10.3351.8424 | shcho@allradio.co.kr |
| Raeman KIM | allRadio Co. Ltd | 280, Seobusaet-gil, Geumcheon-gu, Seoul, Korea | +82.10.5512.9390 | rmkim01@allradio.co.kr |
| Si Young HEO | KT | KT R&D Center, 151, Taebong-ro, Seocho-gu, Seoul, Korea | +82.10.266.4569 | siyoung.heo@kt.com |
| Yangseok Jeong | KT | KT R&D Center, 151, Taebong-ro, Seocho-gu, Seoul, Korea | +82.10.9530.0856 | Yangseok.jeong@kt.com |
| Hyeong Ho LEE | Nevision Telecom Inc., SNUST | 412, 199, Techno2-ro, Yuseong-Gu, Daejeon, 34025, Korea | +82.42.931.4130 | hhlee@netvisiontel.com |
| Youngjae KIM  | TTA | 47, Bundang-ro, Bundang-gu, Seongnam-city, Gyeonggi-do, 13591, Korea | +82.10.5110,2895 | yjkim@tta.or.kr |
| Choon Sik Yim | RCN | 199, Techno2-ro, Yuseong-Gu, Daejeon | +82.10.9531.3610 | Yim253@hnamail.net |
| Yixue Lei | Tencent  | Tencent Building, Kejizhongyi Avenue, Hi-tech Park, Nanshan District, Shenzhen | +86-755-86013388 | yixuelei@tencent.com |
| Xin Zuo | Tencent | Tencent Building, Kejizhongyi Avenue, Hi-tech Park, Nanshan District, Shenzhen | +86-755-86013388 | xinzuo@tencent.com |
| Harry Hwang | Tencent | Tencent Building, Kejizhongyi Avenue, Hi-tech Park, Nanshan District, Shenzhen | +86-755-86013388 | harryhwang@tencent.com |
| Glen Hu | Tencent | Tencent Building, Kejizhongyi Avenue, Hi-tech Park, Nanshan District, Shenzhen | +86-755-86013388 | glennhu@tencent.com |

Edits provided by: Joseph LEVY, AANI SC Chair [InterDigital, Inc.], Stephen McCANN [Huawei Technologies Co., Ltd.], Graham SMITH [SR Technologies]

Clause 4 “Registration and authentication with a 5G core network via a WLAN” contributed by Robert Stacey [Intel.]

Abstract

This contribution is a draft technical report on Wireless Local Area Network (WLAN) interworking to 3rd Generation Partnership Project (3GPP) 5th Generation (5G) network. It describes the interworking reference model and interworking types supported by 3GPP 5G network and WLAN, and defines the necessary functionalities and specific procedures that enable WLAN access networks to interwork with 3GPP 5G network. This technical report on interworking between 3GPP 5G network and WLAN will provide a technical information for stakeholders with interest in standardization and system development.

Revision History

Rev.0 January 2020, Draft technical report on interworking between 3GPP 5G network and WLAN was presented by Hyun Seo Oh.

Rev.1 April 2020, Draft technical report on interworking between 3GPP 5G network and WLAN was updated by Hyun Seo Oh.

Rev.2 June 3, 2020, Harry Hwang added comments on 3.1 WLAN interworking type and N1 signaling forwarding.

Rev.3 June 23, 2020, Joseph Levy added editorial comments and updated to clarify the technical report.

 3 types of TSN bridges were described.

Rev. 4 July 14, 2020, comments were made on the technical report by Binita Gupta and Necati Canpolat.

Revision on the tightly coupled and loosely coupled interworking and the terminal types (UE(User Equipment) and STA(Station)) was made.

Rev. 5 July 28, 2020, rev. 4 of the document was reviewed on the AANI SC teleconference, all changes were discussed. This document accepted the changes and provided some minor editorial changes (spelling/grammar) to align the draft with the 802.11 editorial style (US English – based on the latest edition of Merriam-Webster’s New Collegiate Dictionary), noted that additional edits may be necessary. The document was also converted to PDF format, with line numbers, to support comment collection.

Rev.6. October 20, 2020, rev. 5 of the document was changed according to the comment resolution process from August 21 to October 12 AANI meeting. The update was based on comment resolution sheet: DCN 11-20-1262-05 “CC32-AANI-Report-Comments” by chair Joseph Levy.

Rev. 7. November 1, 2020, rev. 6 of the document was updated to clarify the terminal types: UE and STA. Figure 1 was added and figures 3 and 4 were modified. The figures were renumbered with editorial update by Harry Hwang.

Rev. 8. January 4, 2021, rev. 7 of the document was editorially updated by AANI SC chair Joseph Levy, Stephen McCann, Graham Smith, and reviewed by co-authors.

Rev. 9. January 4, 2021, clean version of Revision 8 (marked version).

Rev. 10. January 11, 2021, rev. 9 of the document was editorially updated to clarify terminals related to STA and UE: Figure 4, 5, 6, 10, 13 were updated to use STA and UE terminals.

Rev. 11 March 15, 2021, clean version of Rev 10 – all redlines removed, some cross references fixed.

Rev. 12 April 28, 2021, terminal types and interworking model were updated by contribution (11-21/0580r0).

Rev. 13 June 22, 2021, Clause 4 “registration and authentication” is added by contribution (11-21/0950r0).

Rev. 14 July 14, 2021, Subclause 2.1 overview and subclause 4.3 are updated by contribution (11-21/1102r0).

**Table of Contents**

[1. Definition, acronyms and abbreviations 6](#_Toc75882707)

[1.1 Definitions 6](#_Toc75882708)

[1.2 Acronyms and abbreviations 7](#_Toc75882709)

[2. Introduction 10](#_Toc75882710)

[2.1 Overview 10](#_Toc75882711)

[2.2 Scope 10](#_Toc75882712)

[3. Reference model of interworking between 5G core network and WLAN 11](#_Toc75882713)

[3.1 Overview 11](#_Toc75882714)

[3.2 WLAN interworking functional model in 5G system 11](#_Toc75882715)

[4. Registration and authentication with a 5G core network via a WLAN 13](#_Toc75882716)

[4.1 Overview 13](#_Toc75882717)

[4.2 WLAN connection 13](#_Toc75882718)

[4.2.1 General 13](#_Toc75882719)

[4.2.2 No authentication 14](#_Toc75882720)

[4.2.3 Password authentication using SAE 15](#_Toc75882721)

[4.2.4 Password authentication using PSK 15](#_Toc75882722)

[4.2.5 802.1X authentication 15](#_Toc75882723)

[4.2.6 FT authentication 16](#_Toc75882724)

[4.2.7 Opportunistic key caching 16](#_Toc75882725)

[4.3 5G core network connection over an untrusted WLAN 17](#_Toc75882726)

[4.4 5G core network connection over a trusted WLAN 18](#_Toc75882727)

[5. Untrusted WLAN interworking function and procedures 19](#_Toc75882728)

[5.1 Overview 19](#_Toc75882729)

[5.2 Registration and authentication message procedures 19](#_Toc75882732)

[5.2.1 Registration and authentication function 19](#_Toc75882733)

[5.2.2 Message procedures 20](#_Toc75882734)

[5.3 IP tunneling function and its message procedures 21](#_Toc75882735)

[5.3.1 IP tunneling function 21](#_Toc75882736)

[5.3.2 Message procedures 21](#_Toc75882737)

[6. 5GS QoS management 23](#_Toc75882738)

[6.1 5GS QoS model 23](#_Toc75882739)

[6.2 ATSSS function support 24](#_Toc75882740)

[7. Gap analysis and recommendations 25](#_Toc75882741)

[7.1 Gap analysis 25](#_Toc75882742)

[7.2 Technical recommendations 27](#_Toc75882743)

[7.3 TSN topics 28](#_Toc75882744)

[8. Conclusions 30](#_Toc75882745)

[9. References 31](#_Toc75882746)

**List of Figures**

[Figure 1. Overview of interworking reference model 10](#_Toc65252856)

[Figure 2. Interworking reference model between 5G core network and WLAN 11](#_Toc65252858)

[Figure 3. Untrusted WLAN interworking reference model with 5G core network 12](#_Toc65252859)

[Figure 4. Trusted WLAN interworking reference model with 5G core network 12](#_Toc65252860)

[Figure 5. Establishing a WLAN connection 14](#_Toc65252860)

Figure 6. Fast BSS transition for fast association…………………………………………………………16

[Figure 7. IPsec tunnel establishment (3GPP TS 23.501) 17](#_Toc65252860)

[Figure 8. Trusted WLAN connection with 5G network registration 18](#_Toc65252860)

[Figure 9. Control plane between a TE and N3IWF (3GPP TS 23.501) 19](#_Toc65252861)

[Figure 10. Y2 interface 20](#_Toc65252862)

[Figure 11. NWu interface 20](#_Toc65252863)

[Figure 12. N1 interface 21](#_Toc65252864)

[Figure 13. Data plane between a TE and N3IWF (3GPP TS 23.501) 21](#_Toc65252865)

[Figure 14. QoS flows and mapping to AN resource in user plane (3GPP TS 23.501) 24](#_Toc65252866)

[Figure 15. Architecture reference model for ATSSS support (3GPP TS 23.501) 24](#_Toc65252867)

[Figure 16. QoS mapping and scheduling example of WLAN 27](#_Toc65252868)

[Figure 17. TSN bridge using 5G AN and CN 28](#_Toc65252869)

[Figure 18. TSN bridge using WLAN and 5G CN interworking 28](#_Toc65252870)

[Figure 19. TSN bridge using WLAN only 29](#_Toc65252871)

**List of Tables**

[Table 1. QoS characteristics (3GPP TS 23.501) 23](#_Toc65254358)

[Table 2. Service categories to interwork with 3GPP core network 26](#_Toc65254359)

[Table 3. Gap analysis of GBR service between 3GPP 5G network and WLAN 26](#_Toc65254360)

# Definition, acronyms and abbreviations

##  Definitions

**ANC**  Access network control function of Wireless Local Area Network (WLAN) access network, which refers to IEEE 802 network reference model [18].

**NWt** Reference point between the User Equipment (UE) and Trusted Non-3rd Generation Partnership Project (non-3GPP) Gateway Function (TNGF) in 5th Generation (5G) system [8].

**NWu** Reference point between the User Equipment (UE) and Untrusted Non-3rd Generation Partnership Project (non-3GPP) Inter Working Function (N3IWF) in 5th Generation (5G) system [8].

**N1** Reference point between the User Equipment (UE) and the Access and Mobility Management Function (AMF) in 5th Generation (5G) system [8].

**N2** Reference point between the Access Network (AN) and the Access and Mobility Management

Function (AMF) in 5th Generation (5G) system [8].

**N3** Reference point between the Access Network (AN) and the User Plane Function (UPF) in 5th

Generation (5G) system [8].

**N4** Reference point between the Session Management Function (SMF) and the User Plane Function (UPF) in 5th Generation (5G) core network [8].

**N11** Reference point between the Access and Mobility Management Function (AMF) and the

Session Management Function (SMF) in 5th Generation (5G) core network [8].

**R1**  Reference point for Physical Layer (PHY)/Media Access Control (MAC) layer function between terminal and access network [18].

**R3** Reference point for Physical Layer (PHY)/Media Access Control (MAC) layer function between access network and access router [18].

**R8**  Reference point for control and management signaling between terminal and the access network [18].

**R9**  Reference point for control and management interface between access network and access router [18].

**Y2** Reference point for Physical Layer (PHY)/Media Access Control (MAC) layer function between the untrusted non-3rd Generation Partnership Project (non-3GPP) access network and the Non-3GPP Inter Working Function (N3IWF) which refers to 3rd Generation Partnership Project (3GPP) 23.501 [8].

**Ta** Reference point between the trusted non-3rd Generation Partnership Project (non-3GPP) access network and the Trusted Non-3GPP Gateway Function (TNGF), which is used to support an Authentication Authorization Accounting (AAA) interface which refers to 3rd Generation Partnership Project (3GPP) 23.501 [8].

##  Acronyms and abbreviations

**3GPP** 3rd Generation Partnership Project

**5G** 5th Generation

**5G-AN** 5th Generation Access Network

**5GS** 5th Generation System

**AAA**  Authentication Authorization Accounting

**AIFS** Arbitrary Inter-Frame Spacing

**AN** Access Network

**ANC**  Access Network Control

**AMF**  Access and Mobility Management Function

**AP**  Access Point

**AS**  Application Server

**ATSSS** Access Traffic Steering Switching and Splitting

**AUSF** Authentication Server Function

**BSS** Basic Service Set

**CN** Core Network

**DHCP**  Dynamic Host Configuration Protocol

**DNS** Domain Name System

**DRB** Data Radio Bearers

**DS** Distribution System

**EAP-5G** Extended Authentication Protocol-5th Generation

**EDCA** Enhanced Distributed Channel Access

**ESS** Extended Service Set

**FT** Fast Transient

**GBR** Guaranteed Bit Rate

**GRE** Generic Routing Encapsulation

**HCCA** Hybrid Controlled Channel Access

**IKEv2** Initial Key Exchange Protocol Version 2

**IP** Internet Protocol

**IPsec** Internet Protocol Security

**MAC** Media Access Control

**MSDU** MAC Service Data Unit

**NAS** Non-Access Stratum

**N3IWF** Non-3GPP Inter Working Function

**OWE**  Opportunistic Wireless Encryption

**PCF** Policy Control Function

**PDU** Packet Data Unit

**PER** Packet Error Rate

**PHY**  Physical Layer

**PSA** Pre-Shared Key

**PTKSA** Pairwise Transient Key Security Association

**RAN** Radio Access Network

**RAT** Radio Access Technology

**QoS** Quality of Service

**SAE** Simultaneous Authentication Equals

**SMF** Session Management Function

**TE** Terminal

**TEC** Terminal Control

**TEI** Terminal Interface

**TNGF** Trusted Non-3GPP Gateway Function

**TSPEC** Traffic Specification

**TSN** Time Sensitive Network

**UE**  User Equipment

**UPF**  User Plane Function

**V2X** Vehicle to Anything

**WM** Wireless Module

**WLAN** Wireless Local Area Network

# Introduction

##  Overview

This technical report provides an overview of the IEEE 802.11 Working Group’s understanding of Wireless Local Area Network (WLAN), based on IEEE Std 802.11, interworking with the 3rd Generation Partnership Project (3GPP) 5th Generation (5G) core network. This report refers to terminologies and architectural models from 3GPP (TS 23.501, etc.), IEEE 802.1CF, and IEEE 802.11 standards.

Clause 3 describes the functional interworking reference models of the untrusted and trusted accesses to 5G core network. Clause 4 introduces registration and authentication with 5G core network via a WLAN for both untrusted and trusted accesses. To understand an untrusted access in the aspects of control and data planes, Clause 5 describes in detail the WLAN interworking function and specific procedures regarding registration, authentication, and IP tunneling. Clause 6 describes the 5th Generation System (5GS) QoS model and Access Traffic Steering Switching and Splitting (ATSSS) function support. Clause 7 describes technical gap analysis, technical recommendations, and Time Sensitive Network (TSN) topics. Conclusions are summarized in Clause 8.

##  Scope

The high-level interworking reference model consists of a terminal, an access network, the 3GPP 5G core network and a data network as shown in Figure 1.



Figure 1. Overview of interworking reference model

This report considers an interworking reference model, two types of network access (trusted and untrusted) and two types of terminals (User Equipment (UE) and Terminal (TE)). The interworking reference model defines how coupled the 3GPP network is to the WLAN access network. The architectural model, necessary functionalities and specific procedures that allow WLAN access networks to interwork with 3GPP 5G core network are discussed for the trusted as well as untrusted case, as defined in TS 23.501 [8]. In this report, a UE is a device that is capable of communicating with 3GPP 5G access network, and a TE is a device that is only capable of communicating with WLAN access network.

# Reference model of interworking between 5G core network and WLAN

## Overview

Interworking model between 5G core network and WLAN, as shown in Figure 2, consists of data network, 3GPP core network, two independent access networks (3GPP 5G access network and WLAN access network), and two types of terminals (UE and TE). A TE can only support WLAN access to interwork with 5G core network. A UE can support both 3GPP access and WLAN access to interwork with 5G core network.



Figure 2. Interworking model between 5G core network and WLAN

The 3GPP 5G system allows WLAN access network connection as a non-3GPP Radio Access Technologies (RAT) and the WLAN access network can be directly connected to the 5G Core Network (CN) via the Non-3GPP Inter Working Function (N3IWF) or the Trusted Non-3GPP Gateway Function (TNGF), depending on whether the WLAN is trusted or untrusted [8].

##  WLAN interworking functional model in 5G system

3GPP describes the 5G system-WLAN interworking function model as consisting of a UE/TE, a 3GPP/WLAN access network and the 3GPP core network as shown in Figures 3 and 4.

Functions of TE are divided into a terminal interface (TEI) entity and a terminal control (TEC) entity, and WLAN access network functions are divided into WLAN access data path and access network control (ANC) according to the WLAN network reference model of IEEE 802.1CF-2019 [18]. 3GPP 5G network functions are divided into a UE, a 3GPP access network, and the 5G core network, and their signaling interfaces are described according to the 3GPP specification [8-9].

For untrusted WLAN to 3GPP core network interworking, as shown in Figure 3, 3GPP NWu interface signaling shall be processed in the WLAN domainand N1 signaling is transparently forwarded in the WLAN domain. The N1 interface provides the signaling procedures between the UE or TE and 3GPP 5GS core network to support Access and Mobility Management Function (AMF). The NWu interface provides the signaling procedures between the TE and N3IWF of 3GPP core network to support a secured IP channel.

In the WLAN domain, R1 and R3 interfaces support the data flow via the Physical Layer (PHY) and Media Access Control (MAC) layers of TE and WLAN access network. In addition to the R1 and R3 interfaces, control and management interfaces R8 and R9 are defined in IEEE Std 802.1CF, which provide Quality of Service (QoS) mapping and MAC scheduling. In Figure 3, the red colored R1/R3 and R8/R9 interfaces are in the domain of WLAN, and they are provided in the TE and the WLAN access network. The Y2 interface is defined for untrusted WLAN interworking in 3GPP domain.



Figure 3. Untrusted WLAN interworking reference model with 5G core network

In trusted WLAN to 3GPP core network interworking, as shown in Figure 4, the NWt interface provides the signaling procedures between the TE and TNGF of 3GPP core network to support a secured IP channel. and the Ta interface is defined for WLAN interworking in the 3GPP domain.



Figure 4. Trusted WLAN interworking reference model with 5G core network

# Registration and authentication with a 5G core network via a WLAN

## Overview

3GPP defines two methods for gaining access to a 5G core network via a WLAN: untrusted and trusted access.

With untrusted access no assumptions are made regarding the WLAN other than that it provides an IP route to a non-3GPP interworking function (N3IWF) on the 3GPP core network. Connecting to the WLAN is a separate and independent process from connecting to the 5G core network, although WLAN connection necessarily proceeds connection to the 5G core network. The UE/TE might connect to the WLAN without connecting to the 5G core network if it does not require 5G core network services and then connect to the 5G core network when it does require 5G core network services. Alternatively, the UE/TE might initiate the 5G core network connection immediately following the WLAN connection to gain data protection and immediate access to 5G core network services.

With trusted access, the WLAN is more tightly coupled to the 5G core network. The WLAN includes a trusted gateway function (TNGF) that couples the WLAN connection process with the 5G core network connection process. With trusted access, connecting to the WLAN necessarily implies connecting to the 5G core network.

This clause is structured as follows:

* 4.2 (WLAN connection) provides an overview of the WLAN connection process.
* 4.3 (5G core network connection over an untrusted WLAN) provides an overview of the 5G core network connection process via an untrusted WLAN.
* 4.4 (5G core network connection via a trusted WLAN) provides an overview of the 5G core network connection process when the WLAN is a part of the 5G network.

It is worth noting the trusted and untrusted are the terms used in 3GPP documents. However, the terms might be misleading since they reference different access procedures and not necessarily the degree to which the WLAN network is trusted for security purposes.

## WLAN connection

### General

An UE/TE connects to a WLAN through a process illustrated in Figure 5.



Figure 5. Establishing a WLAN connection

Key aspects of the process are an initial authentication exchange, an association exchange, 802.1X authentication exchange (if necessary), a 4-way handshake to establish the pairwise transient key security association (PTKSA) (if required) and DHCP exchange to obtain an IP address (if the UE/TE is using IPv4).

The exact frame exchange sequence depends on the security policy in place on the WLAN with various options described in 4.2.2 (no authentication), 4.2.3 (password authentication using SAE), 4.2.4 (Password authentication using PSK), 4.2.5 (802.1X authentication), 4.2.6 (FT authentication) and 4.2.7 (Opportunistic key caching).

A UE/TE can determine the WLAN security policy and association options prior to initiating the connection process from the beacon periodically transmitted by the AP or through a Probe Request/Response frame exchange with the AP.

A UE/TE might also use the connection process itself to discover the security policy, i.e., initiate the connection process and abort the process if the AP does not meet the UE/TE security requirements or the UE/TE cannot meet the AP’s security requirements.

### No authentication

If security policy on the WLAN does not require authentication, then either no encryption (so called open system) is used or opportunistic wireless encryption (OWE) is used. The 802.11 standard recommends that OWE be used rather than no encryption.

For both no encryption and OWE, the connection process begins with a 2-way authentication exchange: the non-AP STA sends an open system Authentication frame to the AP and the AP responds with an open system Authentication frame with the status success.

For the no encryption case, the non-AP STA then sends an Association Request frame that does not select a cypher suite or authentication method (i.e., does not include an RSN element) and the AP responds with an Association Response frame with the status code success. At this point data transfer is possible using unprotected Data frames. A PTKSA is not established and is not needed since the Data frames are unprotected.

For the OWE case, the non-AP STA sends an Association Request frame that includes an RSN element selecting use of OWE and includes a Diffie-Hellman Parameter element in the frame. The AP responds with an Association Response frames that acknowledges use of OWE and includes a Diffie-Hellman Parameter element in the frame. The Diffie-Hellman Parameter elements in the Association Request and Association Response frames contain, respectively, the non-AP STA and AP public keys.

A 4-way handshake follows to establish the PTKSA with pairwise transient keys derived from the public keys. Data transfer using protected Data frames is now possible.

### Password authentication using SAE

Mutual authentication of the non-AP STA and AP can be achieved by demonstrating knowledge of a shared secret, where the shared secret is a password or pass phrase. The 802.11 specification defines a simultaneous authentication of equals (SAE) protocol for this purpose.

The connection process begins with a 4-way authentication exchange comprising a 2-way commit exchange followed by a 2-way confirm exchange. With the commit exchange, the non-AP STA sends an SAE Authentication frame and the AP responds with an SAE Authentication frame. With these two frames each side commits a single guess at the password. This is followed by a second 2-way exchange where the non-AP STA sends an SAE Authentication frame and AP responds with an SAE Authentication frame. These two frames confirm that the other side’s password guess was correct.

Following successful completion of the 4-way authentication exchange, the non-AP STA sends an Association Request frame to the AP and the AP responds with an Association Response frame. Cypher suites are negotiated with this exchange.

This is in turn followed by a 4-way handshake to establish the PTKSA with pairwise transient keys derived from the shared secret. Data transfer using protected Data frames is now possible.

### Password authentication using PSK

Pre-shared key (PSK) is an older form of password authentication that is still widely deployed. The connection process using PSK authentication begins with a 2-way authentication exchange using open system Authentication frames.

The non-AP STA then sends an Association Request frame and the AP responds with an Association Response frame. With this exchange, the non-AP STA and AP negotiate cypher suites and the use of the PSK authentication method.

This is followed by a 4-way handshake, that both demonstrates that each side has knowledge of the shared secret and establishes a PTKSA with pairwise transient keys derived from the shared secret.

Data transfer using protected Data frames is now possible.

### 802.1X authentication

For 802.1X authentication, the connection process begins with the non-AP STA sending an open system Authentication frame to the AP. The AP responds with an open system Authentication frame with status code success.

The non-AP STA then sends an Association Request frame and the AP responds with an Association Response frame. With this exchange, the non-AP STA and AP negotiate cypher suites and the use of the 802.1X authentication method.

802.1X authentication follows and is performed using EAPOL messages encapsulated in Data frames. The Data frames are unprotected, however, the EAP exchange carried in the EOPOL messages will protect sensitive content. The data exchange is with the AP but the EAPOL message content is relayed to an authentication server (AS) over a secure connection.

Successful 802.1X authentication results in master key distribution from the AS to the non-AP STA and AP. The non-AP STA and AP then use the 4-way handshake to establish a PTKSA with pairwise transient keys derived from the master keys.

Data transfer using protected Data frames is now possible.

### FT authentication

The 802.11 standard defines a streamlined protocol called fast BSS transition for fast association following an initial association and for fast transition between APs in an ESS. The initial connection process is similar to that in 4.2.3 (Password authentication using SAE), 4.2.4 (Password authentication using PSK) and 4.2.5 (802.1X authentication) with some modifications to the details of the exchange to support key caching. Subsequent transitions by the non-AP STA to other APs in the ESS (reassociation) and/or subsequent associations by the non-AP STA with an AP in the ESS then incur minimal overhead due to key caching.

The fast BSS transition for fast association is shown in Figure 6.



Figure 6. Fast BSS transition for fast association.

### Opportunistic key caching

An alternative to FT authentication is opportunistic key caching. A non-AP STA that has previously connected to the WLAN using one of the procedures described in 4.2.3 (Password authentication using SAE), 4.2.4 (Password authentication using PSK) or 4.2.5 (802.1X authentication) can opportunistically determine if a cached PMKSA is in place with the AP.

The non-AP STA performs an initial 2-way authentication exchange using open system Authentication frames.

The non-AP STA then identifies the PMKSA (by its PMKID) from a previous authentication in the Association Request frame. If the AP supports key caching and the PMKSA identified by the PMKID is available, then this is indicated in the Association Response frame. If the PMKSA is in place, authentication is not needed (possession of the PMKID confirms identity).

The non-AP STA and AP then use the 4-way handshake to establish a PTKSA based on the cached PMK.

Data transfer using protected Data frames is now possible.

## 5G core network connection over an untrusted WLAN

If the UE/TE requires services from a 5G core network and the WLAN over which it is transiting is untrusted, then the UE/TE establishes an IPsec tunnel to the N3IWF that provides access to that network. The entire procedure occurs after the WLAN connection has been established.

The specific N3IWF to which the UE/TE connects is preconfigured, although the IP address might be resolved through a DNS lookup (a service provided by the access network). The procedure used to establish the IPsec tunnel is illustrated in Figure 7.



Figure 7. IPsec tunnel establishment (3GPP TS 23.502)

The connection to the N3IWF, is established with an initial IKEv2 message exchange. This initial IKEv2 exchange establishes contact and secures the signaling between the UE/TE and N3IWF. 5G NAS messages encapsulated over a 3GPP defined EAP method called EAP-5G can then be securely exchanged.

Using these 5G NAS messages, the UE/TE identifies itself and receives a 5G-Start packet that provides further information on the 5G core network. The UE/TE then sends a 5G NAS message that includes access network (AN) parameters and a registration request.

The N3IWF selects an AMF based on local policy and the received AN parameters and forwards the registration request to the selected AMF in an N2 message.

The AMF may request further identification from the UE, select an AUSF and invoke authentication with the UE/TE. If so, the UE/TE and AUSF mutually authenticate using messages relayed through the AMF. If successfully authenticated, the AUSF sends an anchor key to the AMF from which the AMF derives NAS security keys and the N3IWF security key.

The N3IWF security key is used to establish the IPsec tunnel through a subsequent IKE AUTH exchange. The resulting IPsec tunnel provides both encryption and integrity protection.

In Clause 5, the untrusted access method for TE only is described in the aspects of the control and data planes.

## 5G core network connection over a trusted WLAN

If the UE/TE is gaining access to a 5G core network over a WLAN that is trusted, then the WLAN is effectively part of the 5G core network and the authentication process for the WLAN connection is the authentication process for access to the 5G core network with an additional step after the WLAN connection established to create the NAS messaging channel. This process is illustrated in Figure 8.



Figure 8. Trusted WLAN connection with 5G core network registration

# Untrusted WLAN interworking function and procedures

## Overview

The radio channel access and communication procedures must be specified to enable WLAN interworking with 5G core network. Initial registration and authentication procedures between a TE and AMF of 5G core network are described in 5.2. Examples of IP secure transport and data exchange procedures between a TE and User Plane Function (UPF) of 5G core network are described in 5.3.

## Registration and authentication message procedures

A TE monitors WLAN access network usage to determine if the WLAN radio channel is busy or idle. If the radio channel is idle, a TE may attempt to send control or data traffic through the WLAN radio channel. If the radio channel is busy, a TE will not send control or data traffic through the WLAN radio channel, and it will wait until the radio channel is idle.

A TE must initially support registration and authentication to establish a connection between a TE and N3IWF. NWu for registration and authorization involves IP protocol, IKEv2 and EAP-5G protocol, and secured signaling tunnel over N1 (a.k.a. signaling radio bearer) is required to exchange Non-Access Stratum (NAS) signals.

### Registration and authentication function

Registration and authentication services provided by the IEEE 802.11 Distribution System (DS) allow the N3IWF to perform the required registration and authentication of individual IEEE 802.11 TEs within an Extended Service Set (ESS). Figure 9 shows the control plane interface between a TE and N3IWF, which includes the following protocols.

* IP communication protocol
* IKEv2 authorization protocol
* EAP-5G protocol



Figure 9. Control plane between a TE and N3IWF (3GPP TS 23.501)

### Message procedures

* **Y2 interface**

The Y2 interface is a control and data transport between WLAN access network and N3IWF (see Figure 9). Y2 interface includes data link signal, NWu, and N1 signals for untrusted WLAN interworking. Fig. 10 shows Y2 interface.



Figure 10. Y2 interface

* **NWu interface**

The NWu interface is an IP based communication protocol between a TE in the WLAN access network and N3IWF of 3GPP 5G core network and is used to establish a secured data channel. The IKEv2 authorization protocol and EAP-5G protocol for N2 interface are applied as shown in Figure 11.



Figure 11. NWu interface

* **N1 interface**

The N1 interface uses a secured IP communication protocol between a TE of WLAN access network and AMF of 3GPP 5G core network to provide NAS signaling, as shown in Figure 12.



Figure 12. N1 interface

##  IP tunneling function and its message procedures

A TE shall support secured IP transport between terminal unit and UPF, and traffic data is exchanged over the established IP channel.

### IP tunneling function

The TE and N3IWF shall have the following specific functional requirements to interwork with 3GPP 5G core network (see Figure 13).

* IP communication protocol
* IPsec communication protocol
* GRE communication protocol



Figure 13. Data plane between a TE and N3IWF (3GPP TS 23.501)

### Message procedures

A TE and N3IWF shall provide IPsec tunneling and PDU session establishment to interwork with 3GPP 5G core network:

* IPsec tunneling procedures shall be processed via the WLAN access network.
* PDU session establishment shall be processed via the WLAN access network.

# 5GS QoS management

##  5GS QoS model

The 3GPP Quality of Service (QoS) flow is access agnostic. When the traffic is distributed between the 5G access network and the WLAN access network, the same QoS should be supported. Issues arise if the WLAN access network cannot support the QoS treatment required by the 5G access network. QoS flows for Guaranteed Bit Rate (GBR) traffic and Non-GBR traffic are specified in 3GPP TS 23.501 and QoS flows are defined as follows:

* GBR QoS flow: A QoS flow using the GBR resource type or the Delay-critical GBR resource type and requiring a guaranteed flow bit rate.
* Non-GBR QoS flow: A QoS flow using the Non-GBR resource type and not requiring a guaranteed flow bit rate.

Table 1 shows the characteristics of GBR and delay critical GBR QoS flows from 3GPP. Therefore, it is necessary that GBR flows are supported by the WLAN in both directions, e.g., non-AP TE to AP and AP to non-AP TE.

Table 1. QoS characteristics (3GPP TS 23.501)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Resource Type | Default Priority Level | Packet Delay Budget | Packet ErrorRate  | Default Maximum Data Burst Volume | DefaultAveraging Window | Example Services |
| GBR | 20 | 100 ms | 10-2 | N/A | 2000 ms | Conversational Voice |
| 40 | 150 ms | 10-3 | N/A | 2000 ms | Conversational Video (Live Streaming) |
| 30 | 50 ms | 10-3 | N/A | 2000 ms | Real Time Gaming, V2X messagesElectricity distribution – medium voltage, Process automation - monitoring |
| 50 | 300 ms | 10-6 | N/A | 2000 ms | Non-Conversational Video (Buffered Streaming) |
| 7 | 75 ms | 10-2 | N/A | 2000 ms | Mission Critical user plane Push to Talk voice (e.g., MCPTT) |
| 20 | 100 ms | 10-2 | N/A | 2000 ms | Non-Mission-Critical user plane Push to Talk voice |
| 15 | 100 ms | 10-3 | N/A | 2000 ms | Mission Critical Video user plane |
| 56 | 150 ms  | 10-6 | N/A | 2000 ms | "Live" Uplink Streaming (e.g., TS 26.238 [y]) |
| 56 | 300 ms  | 10-4 | N/A | 2000 ms | "Live" Uplink Streaming (e.g., TS 26.238 [y]) |
| 56 | 300 ms  | 10-8 | N/A | 2000 ms | "Live" Uplink Streaming (e.g., TS 26.238 [y]) |
| 56 | 500 ms  | 10-8 | N/A | 2000 ms | "Live" Uplink Streaming (e.g., TS 26.238 [y]) |
| 56 | 500 ms | 10-4 | N/A | 2000 ms | "Live" Uplink Streaming (e.g., TS 26.238 [y]) |
| Delay Critical GBR | 19 | 10 ms | 10-4 | 255 bytes | 2000 ms | Discrete Automation (see TS 22.261 [x]) |
| 22 | 10 ms | 10-4 | 1354 bytes | 2000 ms | Discrete Automation (see TS 22.261 [x]) |
| 24 | 30 ms | 10-5 | 1354 bytes | 2000 ms | Intelligent transport systems (see TS 22.261 [x]) |
| 21 | 5 ms | 10-5 | 255 bytes | 2000 ms | Electricity Distribution- high voltage (see TS 22.261 [x]) |

The Session Management Function (SMF) assigns QoS profile to AN in WLAN domain with QoS Flow Identification (QFI), which defines the QoS parameters for a QoS flow in the PDU session. The QoS flow is then mapped to AN resource for the assigned QFI (see Figure 14).



Figure14. QoS flows and mapping to AN resource in user plane (3GPP TS 23.501)

##  ATSSS function support

Traffic data shall be transmitted over the WLAN access channel and/or 3GPP access channel by using the ATSSS function. In this subclause, a UE is assumed to support the ATSSS function.

* 3GPP supports ATSSS between 3GPP and non-3GPP access networks.
* ATSSS can enable traffic selection, switching and splitting between the 5th Generation Access Network (5G-AN) and WLAN, shown in Figure 15 as 3GPP access and non-3GPP Access, respectively.



Figure 15. Architecture reference model for ATSSS support (3GPP TS 23.501)

Figure 11 shows the reference architecture for supporting ATSSS which handles either Guaranteed Bit Rate (GBR) QoS flow or Non-GBR QoS flow traffic.

# Gap analysis and recommendations

##  Gap analysis

In the technical gap analysis, a TE is assumed to be compatible with the new functionalities and communication protocols necessary to interwork with 5G core network. These new functionalities and communication protocols are assumed to be implemented in a TE and WLAN access network devices.

The higher layer control and protocols (i.e., IKEv2, EAP-5G, IPsec and GRE), provided by the 3GPP 5G core network to support interworking, are defined and specified by the Internet Engineering Task Force (IETF) and modified for interworking by 3GPP. These protocols can be implemented in the TE TEC and WLAN ANC.

NAS signaling to AMF and packet session control to SMF are specified in 3GPP specifications and can be implemented in TE TEC and WLAN ANC. WLAN QoS management was first introduced in IEEE Amendment 802.11e and is specified in IEEE Std 802.11-2020 and can be adapted to support fine granularity of QoS levels.

The 3GPP specification provides GBR, Non-GBR and delay critical GBR QoS requirements. The delay critical GBR is specified to require low latency (less than 30msec) and low packet error rate (PER) (less than 10-4). 3GPP also specifies QoS management to support packet delay, PER, default maximum data burst volume and default average window for several service types.

3GPP resource types and QoS related parameters are provided to the WLAN using R8 and R9 interfaces. WLAN supports QoS function and related message procedures, which provide QoS mapping, scheduling algorithm and MAC interface that support the QoS requirements. TE TEC and WLAN ANC must provide the necessary functionality to support these requirements.

The EDCA of IEEE Std 802.11-2020 covers four classes of QoS management: background, best effort, audio and video. EDCA QoS is managed according to service class, contention window and Arbitrary Inter-Frame Spacing (AIFS) value. This capability allows WLAN to use EDCA as currently specified to support some GBR as well as non-GBR services. EDCA is contention based and therefore may not be capable of meeting some GBR requirements in a WLAN without low latency access to the Wireless Media (WM). Low latency access is dependent on the load on the WM due to Radio Frequency (RF) interference, the network traffic load and how other users are using the WM. Hybrid Controlled Channel Access (HCCA) relies upon Traffic Specifications (TSPECs) to allocate controlled access and does have the potential to provide low latency and GBR, but will set a limit based on the available WM access latency. 3GPP system specifies QoS profiles and characteristics in the following areas:

* Service priority level
* Packet latency
* Packet error rate
* Guaranteed data rate
* Averaging window

To support 3GPP QoS requirement the TE TEC and WLAN ANC should process QoS management according to the QoS profile provided by 3GPP 5G core network. Table 2 shows service categories and related WLAN specification to interwork with 3GPP core network, and Table 3 shows gap analysis of GBR service between 3GPP 5G network and WLAN.

Table 2. Service categories to interwork with 3GPP core network

|  |  |  |
| --- | --- | --- |
| Service Categories | **Related WLAN function** | **Related WLAN Specification** |
| Non-GBR | 4 service classes; Background, Best effort, audio and video  | IEEE 802.11e |
| GBR | To be defined in fine granularity of service classes and QoS management | Shall specify QoS mapping and scheduling. And IEEE 802.1 TSN is for deterministic Ethernet network. |

Table 3. Gap analysis of GBR service between 3GPP 5G network and WLAN

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resource Type |  Services Examples | Packet Delay Budget | PER | Default Maximum Data Burst Volume | Gap Analysis of WLAN specification |
| GBR | Conversational Voice | 100 ms | 10-2 | N/A | . 802.11ax MAC cannot support 3GPP GBR service requirements of deterministic packet latency, PER and data rate because EDCA is CSMA based MAC and supports only 4 service types of best effort, background, voice and video by controlling TXOP, AIFSN & contention window size. . Enhanced MAC (802.11be) should consider QoS mapping, packet scheduling and related management procedures to support GBR. PHY and MAC should be improved to control packet latency and reliability.  . QoS flow identification and service priority shall be mapped to have fine granularity of service types and QoS parameters. |
| Conversational Video  | 150 ms | 10-3 | N/A |
| Real Time Gaming, V2X messages | 50 ms | 10-3 | N/A |
| Non-Conversational Video | 300 ms | 10-6 | N/A |
| MCPTT | 75 ms | 10-2 | N/A |
| Non-MCPTT | 100 ms | 10-2 | N/A |
| MC-Video | 100 ms | 10-3 | N/A |
| "Live" Uplink Streaming  | 150 ms  | 10-6 | N/A |
| "Live" Uplink Streaming  | 300 ms  | 10-4 | N/A |
| "Live" Uplink Streaming | 300 ms  | 10-8 | N/A |
| "Live" Uplink Streaming  | 500 ms  | 10-8 | N/A |
| "Live" Uplink Streaming  | 500 ms | 10-4 | N/A |
| Delay Critical GBR | Discrete Automation  | 10 ms | 10-4 | 255 bytes | . 802.11ax MAC cannot guarantee 3GPP delay critical GBR service requirements of latency, PER and guaranteed data rate. . Enhanced MAC (802.11be) should consider QoS mapping, packet scheduling and related management procedures to support GBR. PHY and MAC should be improved to control packet latency and reliability.. 802.11bd NGV should consider ITS service requirement. |
| Discrete Automation | 10 ms | 10-4 | 1354 bytes |
| Intelligent transport systems  | 30 ms | 10-5 | 1354 bytes |
| Electricity Distribution- high voltage | 5 ms | 10-5 | 255 bytes |

The definition of 3GPP QoS flow in SMF contains QoS identification and its priority according to resource types, and the QoS information is transferred to AP and TE. QoS mapping from 3GPP QoS to WLAN QoS is necessary. WLAN must support fine granularity for QoS and priority because 5G QoS ID has 6 bits and specifies QoS parameters including GBR, latency and PER. The packet scheduling function in TE and AP should configure the MAC operation to support the required QoS. AP QoS profile and TE Data Radio Bearers (DRB), provided by the 5G Core, contains service QoS identification and parameters to define data rate, packet latency and PER values. The packet scheduler configures data rate, packet latency, PER and packet size for an MSDU packet to support these requirements (see Figure 16).



Figure16. QoS mapping and scheduling example of WLAN

QoS mapping to the WLAN domain relies on the R9 and N1 interfaces to send QoS profile and QoS DRB information, respectively. Alternatively, QoS DRB may be delivered from the AP to a TE over R8 interface if QoS DRB through NAS signaling is not available. It is well known that TSPEC based transmission time scheduling can guarantee low packet latency and that Hybrid ARQ supports PER improvement [19-20]. To support GBR, data rate and bandwidth control are required.

## Technical recommendations

WLAN supports high data rates that are necessary to meet the performance goals of the 5G network in the low mobility scenarios, and WLAN needs to support interworking capability to 3GPP 5G network for ATSSS function. Therefore, the 802.11 Working Group should consider adding some new functional entities and signaling procedures to enhance the support of interworking with the 3GPP 5G network. Enhancements to the following 802.11 services and facilities should be considered:

* Active scanning and association
* Registration
* Authentication
* QoS facility

The key areas to be considered are:

* Radio scanning and association process is specified in WLAN 802.11. However, additional radio scanning for ATSSS function should be supported.
* IKEv2, EAP-5G and IPsec protocol for registration and authentication support should be added in the implementation of TE TEC and the WLAN ANC.
* NAS signaling for connecting to AMF should be added in the implementation of TE TEC and the WLAN ANC.
* Packet session initiation/modification/termination for connecting to SMF should be added in the implementation of the TE TEC and WLAN ANC.
* Packet data QoS management of WLAN shall specify QoS identification, profile and DRB to guarantee packet delay and PER for the required service types.
	+ QoS mapping to WLAN is necessary to support more granularity of QoS ID and parameters.
	+ Packet scheduling in the TE and AP should meet data rate, latency and PER.
	+ Timing scheduling and the introduction of a Hybrid ARQ scheme may be necessary to support GBR.
	+ 802.11ax, as implemented, cannot fully support all 3GPP service QoS requirements. Improvements being developed in 802.11be (EHT) and 802.11bd (NGV) should consider MAC enhancements to support these service requirements.

Consideration of the WLAN interworking model and terminal types to support 3GPP 5G interworking can provide insight to real world requirements and should be considered for 802.11 interworking system design and implementations. For example, the terminal TE type should support both data and control functions to interwork with 5G core network. The UE will support all the control functions for interwork with 5G core network and WLAN access function of UE can be used to support high speed data requirements.

##  TSN topics

3GPP 5G System can be integrated with the external TSN as a TSN bridge. The TSN bridge includes TSN translator functionality for interoperation between TSN System and 5G System both for user plane and control plane. The 5G system TSN translator functionality consists of device-side TSN translator (DS-TT) and network-side TSN translator (NW-TT). 5G system specific procedures in a 5G core network and RAN, wireless communication links, etc. remain hidden from the TSN network [8]

As for TSN applications, such as smart factory and automation field, TSN bridges can be configured in three different types. The first type is to use 5G system as a TSN bridge (see Figure 17). 3GPP domain needs to consider the timing synchronization and TSN translator (TT) function in UE and 5G CN. The second type is to use WLAN and 5G CN interworking as a TSN bridge (see Figure 18). The third type is to use WLAN only as a TSN bridge (see Figure 19).



Figure17. TSN bridge using 5G AN and CN



Figure18. TSN bridge using WLAN and 5G CN interworking



Figure19. TSN bridge using WLAN only

# Conclusions

The IEEE 802.11 Standard can support interworking with the 3GPP 5G network and is able to support high data rates to meet the performance goals of 5G network vision in the low mobility scenario. The new functional entities and signaling procedures have been identified:

* Registration and authentication
* NAS signaling messages
* Packet session initiation/modification/termination
* Packet data QoS management

The TE TEC and WLAN ANC use IETF specification such as IKEv2, EAP-5G, and IPsec for implementation. The TE TEC and WLAN ANC should contain the function for NAS signaling, ATSSS and QoS management functions, and should follow the guidance of the 3GPP specifications.

In the interworking model, a UE or TE takes the role of the required functional entities and signaling procedures to interwork with 5G core network. A UE supports all of the described control and signaling functions. A TE should be augmented so that it can support all the control and signaling functions required by the interworking with 5G network.

As for QoS management, IEEE 802.11 must specify enhancements to its QoS mapping and MAC scheduling that include QoS identification and profiles to guarantee QoS in terms of deterministic packet delay, low PER and data rate. The new WLAN interfaces R8 and R9 have been defined to deliver QoS profiles between 5G CN (N3IWF, TNGF) and a WLAN TE to be supported.

Regarding TSN applications, WLAN domain should consider introducing or enhancing capabilities to achieve timing synchronization required to operate in the TSN domain, and how to implement TSN translation in WLAN TEs interworking with the 3GPP 5G CN.

# References

1. 3GPP TS 22.261 V15.5.0 (2018-06) “Service requirements for the 5G system (Stage 1)”
2. 3GPP TS 22.278 “Service requirements for the Evolved Packet System (EPS)”
3. 3GPP TS 23.401 “EPS Architecture and Procedures”
4. 3GPP TS 23.402 "Architecture enhancements for non-3GPP accesses”
5. 3GPP TR 23.716 “Study on the Wireless and Wireline Convergence for the 5G System Architecture”
6. 3GPP TR 23.793 “Study on Access Traffic Steering, Switching and Splitting support in the 5G system architecture”
7. 3GPP TR 23.799 “Study on Architecture for Next Generation System”
8. 3GPP TS 23.501 “System Architecture for the 5G System (Stage 2)”
9. 3GPP TS 23.502 “Procedures for the 5G System (Stage 2)”
10. 3GPP TS 24.302 “Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks (Stage 3)”
11. 3GPP TS 24.501 “Non-Access-Stratum (NAS) protocol for 5G System (5GS) (Stage 3)”
12. 3GPP TS 24.502 “Access to the 3GPP 5G Core Network (5GCN) via Non-3GPP Access Networks (N3AN) (Stage 3)”
13. 3GPP TS 33.501 “Security Architecture and Procedure for the 5G System”
14. 3GPP TR 33.899 “Study on the Security Aspects of the Next Generation System”
15. 3GPP TS 37.324 “Service Data Adaptation Protocol (SDAP) Specification”
16. 3GPP TS 38.300 “NR and NG-RAN Overall Description”
17. RAN convergence paper, WBA and NGMN alliance, September 2019.
18. IEEE Std 802.1CF-2019 “IEEE Recommended Practice for Network Reference Model and Functional Description of IEEE 802® Access Network,” 2019.
19. L. W. Lim, et al., “A QoS scheduler for IEEE 802.11e WLANs, “First IEEE Consumer Communications and Networking Conference,” 2004 (CCNC 2004), January 2004.
20. Christopher Lott, et al., “Hybrid ARQ: Theory, state of the art and future directions,” 2007 IEEE Information Theory Workshop on Information Theory for Wireless Networks, July 2007.
21. 5G and Wi-Fi RAN Convergence, WBA, December 2020.
22. IEEE Std 802.11-2020 “IEEE Standard for Information technology—Telecommunications and information exchange between systems local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” Dec. 2020.