SMALL CELL FORUM

Solving the HetNet puzzle

Wireless Broadband Alliance

Driving next generation Wi-Fi experience

Industry perspectives, trusted WLAN architectures and deployment considerations for integrated Small-Cell Wi-Fi (ISW) networks

Version 1.00
Issue date February 2016

About the Wireless Broadband Alliance

Founded in 2003, the mission of the Wireless Broadband Alliance (WBA) is to champion the development of the converged wireless broadband ecosystem through seamless, secure and interoperable unlicensed wireless broadband services for delivering outstanding user experience. Building on our heritage of NGH and carrier Wi-Fi, WBA will continue to drive and support the adoption of Next Gen Wi-Fi and other unlicensed wireless services across the entire public Wi-Fi ecosystem, including IoT, Big Data, Converged Services, Smart Cities, 5G, etc. Today, membership includes major fixed operators such as BT, Comcast and Time Warner Cable; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Microsoft, Huawei Technologies, Google and Intel. WBA member operators collectively serve more than 2 billion subscribers and operate more than 25 million hotspots globally.

The WBA Board includes AT&T, Boingo Wireless, BT, China Telecom, Cisco Systems, Comcast, Intel, KT Corporation, Liberty Global, NTT DOCOMO, Orange and Ruckus Wireless. For a complete list of current WBA members, please click here.

Follow Wireless Broadband Alliance at:

www.twitter.com/wballiance
http://www.facebook.com/WirelessBroadbandAlliance
http://www.linkedin.com/groups?mostPopular=&gid=50482
https://plus.google.com/106744820987466669966/posts

About the Small Cell Forum

Small Cell Forum accelerates small cell adoption to drive the wide-scale adoption of small cells and accelerate the delivery of integrated HetNets.

We are not a standards organization but partner with organizations that inform and determine standards development. We are a carrier-led organization. This means our operator members establish requirements that drive the activities and outputs of our technical groups.

We have driven the standardization of key elements of small cell technology including Iuh, FAPI/SCAPI, SON, the small cell services API, TR-069 evolution and the enhancement of the X2 interface.

Today our members are driving solutions that include small cell/Wi-Fi integration, SON evolution, virtualization of the small cell layer, driving mass adoption via multi-operator neutral host, ensuring a common approach to service APIs to drive commercialisation and the integration of small cells into 5G standards evolution.

The Small Cell Forum Release Program has now established business cases and market drivers for all the main use cases, clarifying market needs and addressing barriers to deployment for residential, enterprise and urban small cells. The theme of Release 6 is Enterprise, with particular emphasis on real world and vertical market deployments, and the role of neutral host solutions to drive the mass adoption of small cells in business environments.

Small Cell Forum Release website can be found here: www.scf.io

Undertakings and Limitation of Liability

This document and all the information contained in this document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement. In addition, the WBA (and all other organisations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organisations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

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

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

SMALL CELL FORUM
Solving the HetNet puzzle

Wireless Broadband Alliance
Driving next generation Wi-Fi experience

Contents

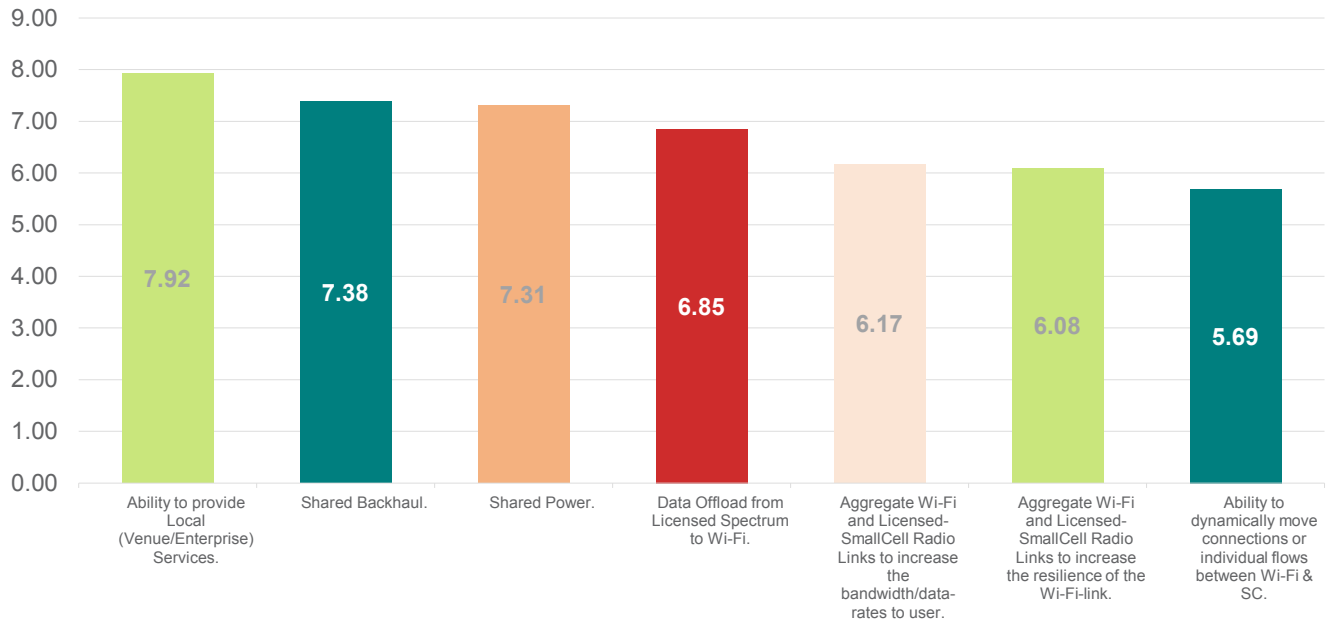
Tables

Figures

Executive Summary

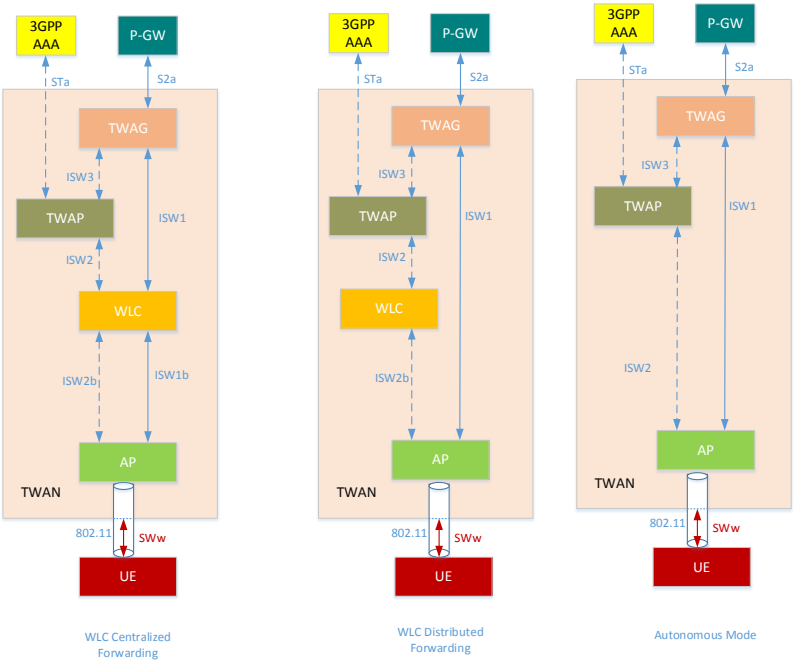
This white paper is the second deliverable of the ongoing collaboration between the Small Cell Forum (SCF) and Wireless Broadband Alliance (WBA) in the area of integrated Small-Cell Wi-Fi (ISW) networks. The first white paper provided an overview of the various ISW network architectures and highlighted various deployment aspects. It was then observed that an important part of the architecture, namely the Trusted WLAN that connects the Wi-Fi access points, access controllers and 3GPP-defined gateways (TWAG/TWAP), was not being addressed by any standards development organization (SDO) or by any industry body. So, SCF-WBA Joint Task Force (JTF) took up the task of examining and documenting the architectural options, interfaces and deployment aspects of the TWAN. The JTF also took this opportunity to conduct a comprehensive survey of a number of MNOs, MSOs, integrated operators and vendors to understand the industry perspective on the business and deployment status and plans of ISW networks. This white paper is a result of these efforts and contains the results of this comprehensive industry survey, as well as TWAN architecture, interface and deployment details.

Specifically, the survey consisted of 13 in-depth questions with multiple options, to which 17 member companies responded. One of the questions related to the perceived benefits of ISW-networks; the response is shown below.

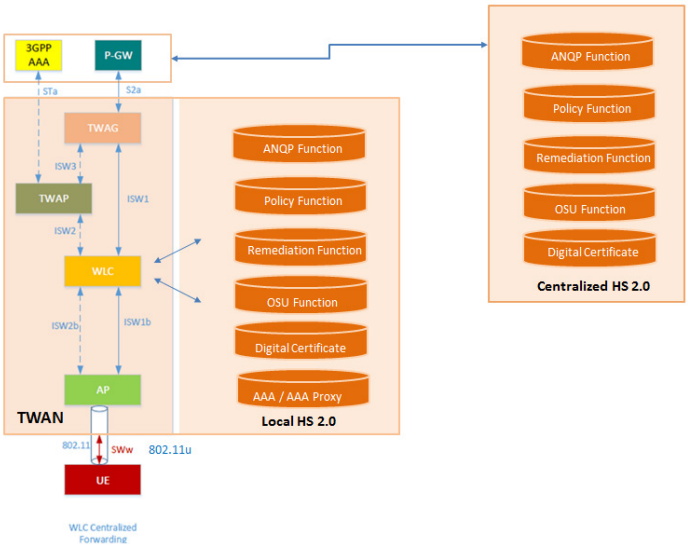


The graph shows that the greatest value is seen to be for enterprises providing local services, closely followed by shared backhaul and power.

The main technical contribution of the paper is in discussing the definition of the various TWAN interfaces, named as ISW1, ISW2 and ISW3 as shown below and analysing various tunnelling options on these interfaces, including L2GRE, L3GRE and L2TP.



Finally, the white paper discusses various deployment considerations, including encryption (for which different techniques IPSec/DTLS are used traditionally) and coexistence of the TWAN architecture with HotSpot 2.0 architecture, shown below.



The white paper concludes by commenting on the recent developments in the RAN-level tight integration of SC and Wi-Fi, such as LWA which is being pursued by 3GPP currently. This is seen as the next evolutionary step in the ISW technologies and it is recommended that SCF-WBA continue their collaboration in this and similar areas.

1. Introduction

The need for ubiquity and mobility has driven the shift in data usage from wireline to wireless, which will be accelerated further as users start to use a great variety of wirelessly connected devices, not only in the consumer world, but in other industries, such as automotive, retail and enterprise. Both Cellular and Wi-Fi will play a key role in enabling this new world of connected devices, supporting the anticipated explosion of data usage.

Some key indicators (based on well-known industry sources, such as WBA Industry Report, Cisco VNI) are:

- Wireless data usage is estimated to rise exponentially, (as exemplified by a Cisco estimate of 12.5 times between 2013 and 2019, starting from 1.5 Exabytes in 2013)
- Mobile data consumption will increase at an impressive rate (as exemplified by Cisco's quarterly VNI that predicts it will increase at a CAGR of 61%, resulting in an eleven fold increase between 2013 and 2018, with average device usage growing from 600MB per month in 2013 to 2.2GB in 2018. Around 45% of that data is currently offloaded from cellular to Wi-Fi, and is expected to rise to 52%)
- The volume of Wi-Fi traffic will exceed that of wireline very soon (as exemplified by Cisco, it should be in 2016).
- The Internet of things (IoT) will add further huge numbers of devices to the wireless networks as the decade progresses, with those devices (Wi-Fi or cellular) crossing the 10bn mark by 2018.

MNOs originally regarded public Wi-Fi as a threat, enabling companies with no licensed spectrum assets with the tools to provide affordable wireless broadband. However, in recent years, MNOs have increasingly embraced the economics of solutions based on unlicensed spectrum, recognizing how they can add much-needed capacity without having to pay for expensive spectrum licenses as well as CAPEX and OPEX which may be subsidized by alternative value propositions. The main approach has been mobile data offload (MDO), a fairly straight forward offering in which high bandwidth, low value traffic was pushed off the precious cellular network and on to Wi-Fi, thus improving the experience for customers left on 3G/4G, and reducing the MNO's cost of data delivery.

The next step was to recognize that Wi-Fi could be fully integrated into the MNO's network via the emergence of the HetNet. When fully formed, this consists of a mixture of base stations in different spectrum bands (licensed and unlicensed), different cell sizes (both indoors and outdoors), and supporting different air interfaces (Wi-Fi, 3G, 4G). These create a seamless pool of capacity, with the exact technology used to support the connection being invisible to the user. The MNO's fear of losing the ability to track and monetize the users as soon as they moved from the cellular network onto the Wi-Fi network is also being addressed by mobile core platforms, BSS/OSS and by policy/analytics engines, which can support all users equally, whether they are connected by Wi-Fi or 3G/4G.

Finally, the advent of Small Cells enables the real possibility of integration of the Cellular and Wi-Fi technologies by exploiting the synergies of Small Cell and Wi-Fi Access Networks, such as similar coverage and deployment scenarios.

Critical enabling components of such an integrated Wi-Fi/cellular network are the WBA's Next Generation Hotspot (NGH), the Wi-Fi Alliance's Passpoint/HotSpot 2.0 specifications and 3GPP/SCF's small cell standards/technologies. These complementary technologies promise to make the seamless network a reality, and recent years have seen the beginnings of significant deployments.

To accelerate the understanding of various technical and business challenges and opportunities as well as to promote the speedy and wide-spread deployment of such integrated small cell Wi-Fi networks, Small Cell Forum and Wireless Broadband Alliance came together in a collaborative relationship in 2012-13 and formed a WBA-SCF JTF. The first phase of the JTF's collaboration resulted in a paper presenting an analysis and overview of the relevant elements of the Integrated small cell Wi-Fi (ISW) environment [53].

Based on the next steps identified by this initial paper and subsequent brainstorming discussions, the following were identified as potential topics for further collaboration:

- Focused project based on gap(s) identified in the WP
  - Recommendations for TWAN Architecture
  - Simplified ISW Architecture for Internet Access
- Study project of topics not adequately addressed in the WP
  - Policy & intelligent network selection/mobility
  - ISW for existing enterprise/venue Wi-Fi Networks

Recommendations for TWAN architecture was prioritized to be addressed on this follow-up white paper given the following considerations:

- 3GPP has developed standards for accessing operator core network (OCN) via Wi-Fi (both trusted & untrusted)
- Essential component of the integration architecture is the 'WLAN-GW' (TWAG/TWAP for trusted Wi-Fi & ePDG for untrusted Wi-Fi)
- Well-defined 3GPP standards exist for 'north-side' connectivity of WLAN-GW to OCN
- Well-defined IEEE/WFA standards exist for 'south-side' connectivity of Wi-Fi-AP (i.e. radio interface to User Equipment)
- However, the network between trusted Wi-Fi-AP & WLAN-GW (i.e. TWAN) is not addressed by any SDO/industry forum
- As many as six different architectural possibilities have been identified by the Joint SCF-WBA ISW WP

The team reached a consensus that JTF between SCF-WBA is ideally positioned to address this network space, evaluate various TWAN architectures, generate consensus and provide recommendations and focus for the Industry.

1.1 Scope and outline

The scope of the white paper is as follows:

- The network connecting Wi-Fi APs to the trusted WLAN-GW (namely TWAG/TWAP), referred to as TWAN henceforth.
- Wi-Fi access controllers, when used

A practically relevant subset of the 6 configurations identified by the ISW white paper

- produced by SCF-WBA JTF [53].

The outline of the white paper is as follows:

- Section 1 introduces the current market context and drivers leading to this white paper
- Sections 2 presents a brief introduction to integrated small cell Wi-Fi (ISW) Networks and recaps key results from the earlier SCF-WBA JTF white paper [53].
- Section 3 describes the results of a comprehensive survey conducted by the SCF-WBA-JTF on perspectives on various aspects of ISW-Networks from a broad range of MNO, non-MNO & integrated operators.
- Section 4 addresses the work done by 3GPP, SCF and SCF-WBA in the general area of ISW-Networks and focusses on the Trusted WLAN (TWAN) component, which has yet to be addressed comprehensively by any SDO. In particular, a useful set of 3 architectures is chosen and discussed in great detail, including various interface options.
- Section 5 analyzes some deployment considerations, including encryption, quality of service, and coexistence with the HotSpot 2.0 architecture. It also discusses the accepted flavors of commonly

deployed Wi-Fi, namely carrier Wi-Fi and business/enterprise Wi-Fi in the context of small cell integration.

- Section 6 provides some concluding remarks and suggestions for future work.

2. Integrated small cell Wi-Fi (ISW) networks

1.2 ISW access point

Wi-Fi integration with small cells is an evolving topic of development and standardization such that at the time of writing, alternate frameworks are emerging in the industry as well as in standardization bodies. We present some of these alternatives now, with the cautionary remark that further standardization activities are in progress in 3GPP (e.g. LWA, LAA).

The architecture framework in Section 2.3 is well-standardized and may be termed as core network (CN) based Wi-Fi Integration architecture framework. When Wi-Fi is being integrated into small cells, other interesting alternatives are possible, namely integration in the SC-APs (i.e. RAN-based integration) and/or in SC-gateways (i.e. GW-based integration). These were introduced in an earlier SCF document [5] and the concepts are reproduced here in Figure 2.1.

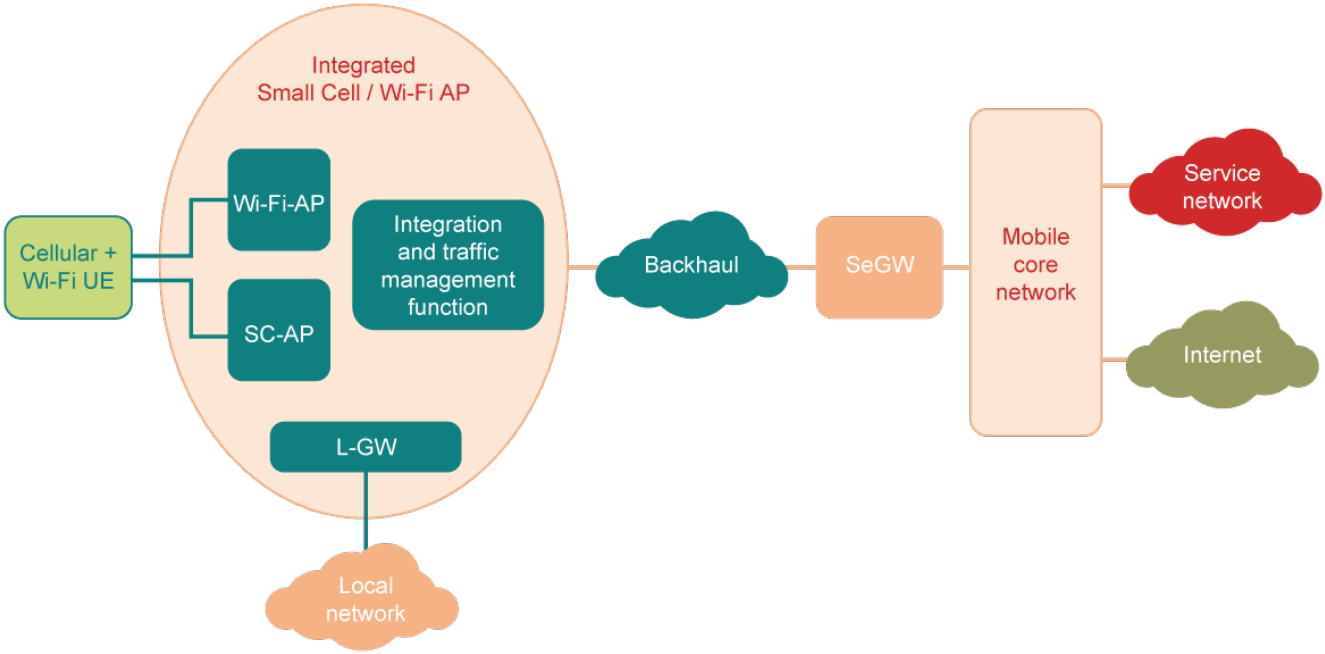


Figure 2.1 Integrated small cell/Wi-Fi access point

Here, the Integration function resides at the edge, possibly in an integrated ISW-AP. RAN-based integration of licensed/unlicensed access is now being addressed by 3GPP release 13, including approaches for RAN based integration of Wi-Fi and LTE.

Finally, architectures that integrate Wi-Fi and SCs at the gateway level are possible. For example, the SC-GW (i.e. H(e)NB-GW) as well as Wi-Fi GW (i.e. ePDG and/or TWAG/TWAP) may be realized together, along with associated integration functions. At the time of writing, these architectures are still in consideration and development.

1.3 3GPP cellular and Wi-Fi network integration architectures

This section describes architectures where the cellular and Wi-Fi integration takes place in the OCN with Wi-Fi access achieved via a trusted WLAN access network (TWAN) managed by the MNO. Only LTE small cells are

considered for the sake of simplicity, recognizing that the concepts apply to 3G cases also, with possible minor modifications.

3GPP has defined two architectural approaches in TS 23.402 [7] for integrating Wi-Fi into existing MPC components. They are distinguished based on where the mobility architectures are, for facilitating mobility of UEs between Wi-Fi and cellular networks. We first note that essential components of any mobility architecture are the mobility anchors, one of which is in the PGW/HA in both cases. The other mobility anchor in either the UE or WLAN gateway. The former may be referred to as the UE-based mobility architecture and the latter network-based mobility architecture. In this section, we focus on network based mobility architectures. The WLAN gateway is either the ePDG or the TWAG/TWAP, depending on whether the WLAN is considered untrusted or trusted by the operator of the MCN. Again, in this section, we shall focus mainly on the trusted WLAN case. The interface between the PGW/HA and the WLAN gateway is either S2a or S2b depending on whether the Gateway is TWAG/TWAP or ePDG.

Both the ePDG and TWAG provide a similar function in the network, namely providing access to the EPC-based services for UEs residing on a non-3GPP access network which may be trusted or untrusted.

In the untrusted use case, a UE requesting access to EPC services resides on a non-3GPP access network outside the span of control of the EPC operator. UE access to the non-3GPP access network is granted independently of/and prior to requesting access to the EPC network. It is the function of the evolved packet data gateway (ePDG) to act as a secure access gateway to the EPC network. The ePDG receives UE access requests (via IKEv2/IPsec remote access tunnel), authenticates the UE's credentials against the operator's 3GPP AAA server (via SWm), and establishes connectivity with the appropriate PDN-GW over S2b. Mobility within the untrusted network that causes a change in the IP Point of Attachment is not supported in the ePDG application, unless MOBIKE (RFC 4555) is implemented by both the UE and the ePDG, standard handover procedures exist between the cellular and untrusted non-3GPP networks where the PDN-GW preserves the UE IP address between radio access types to ensure session continuity on a per-PDN basis.

In the trusted use case, a UE requesting access to EPC services resides on a non-3GPP access network within the span of control of the EPC operator (or a trusted partner), so granting access to the TWAN and the EPC is granted at the same time. The function of the TWAG is to authenticate the UE gaining access (via the TWAP) and establish connectivity with the appropriate PDN-GW over the S2a interface, or provide local traffic offload. In managing the individual UE sessions, the TWAG needs to be the enforcement point for a subscriber policy, to provide anti-spoofing, and, depending on traffic routing, interface to billing and lawful Intercept applications (see Section 5.5). The trusted use case also implies that the TWAG/TWAP, since it forms part of the same network as the TWAN, must be able to manage and track UE mobility events within the TWAN.

The Trusted Wi-Fi authentication proxy (TWAP) provides the AAA proxy functions used to permit UE access to both the TWAN and specific EPC services. The TWAP uses the STa DIAMETER reference point (defined in 3GPP TS 29.273) to provide user authentication information to the 3GPP AAA Server/HSS, signal AAA success/failure and support AAA-triggered session change/termination mechanisms.

When a UE attempts to connect to a specific Wi-Fi SSID using EAP-AKA/AKA'/SIM, the Wi-Fi Access network captures the EAP Identity credentials from the UE EAP Message and generates the AAA request upstream to the TWAP. The TWAP in turn proxies the AAA request to the 3GPP AAA server. Based on the response from the AAA server, the TWAP forwards an accept/reject message to the Wi-Fi access network. The UE is either granted or denied access to the Wi-Fi network. If allowed to connect, the UE initiates network connectivity configuration from the TWAG/AC via DHCP/SLAAC.

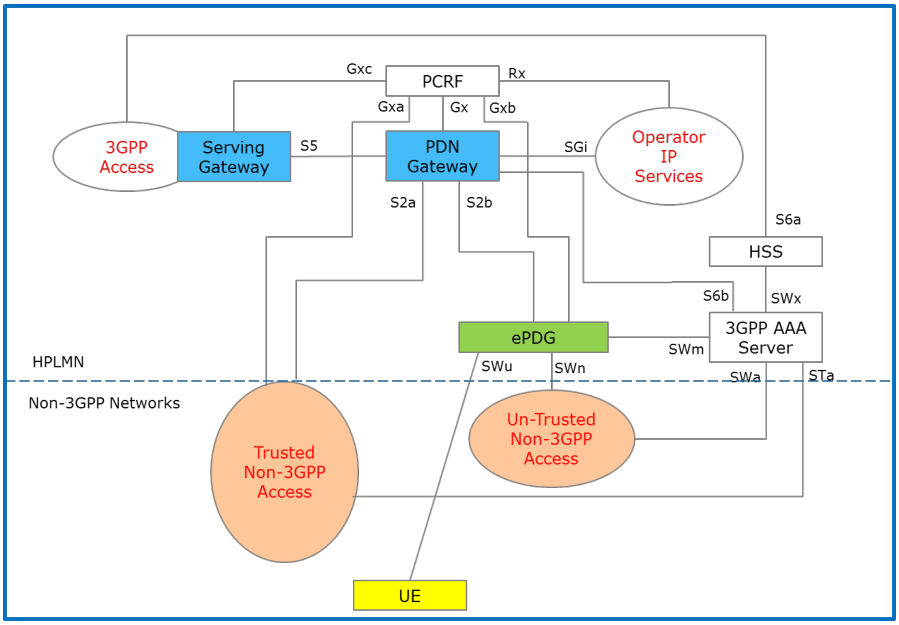


Figure 2.2 Cellular & Wi-Fi integration Network-based (S2a/b) mobility architecture

1.4 Small cell and Wi-Fi network integration architecture

While the architecture in Figure 2.2 above applies to general integration of cellular and Wi-Fi networks, the following Figure 2.3 focuses on small cell and Wi-Fi integration. This represents a non-optimized architecture where each access node, i.e. Wi-Fi AP or small cell, is individually controlled and managed by the OCN. In this case, there is no operational distinction between collocated or non-collocated Wi-Fi and small cell access nodes.

As shown, this architecture may also include intermediate gateway functionality between multiple small cells in the small cell access network and the OCN.

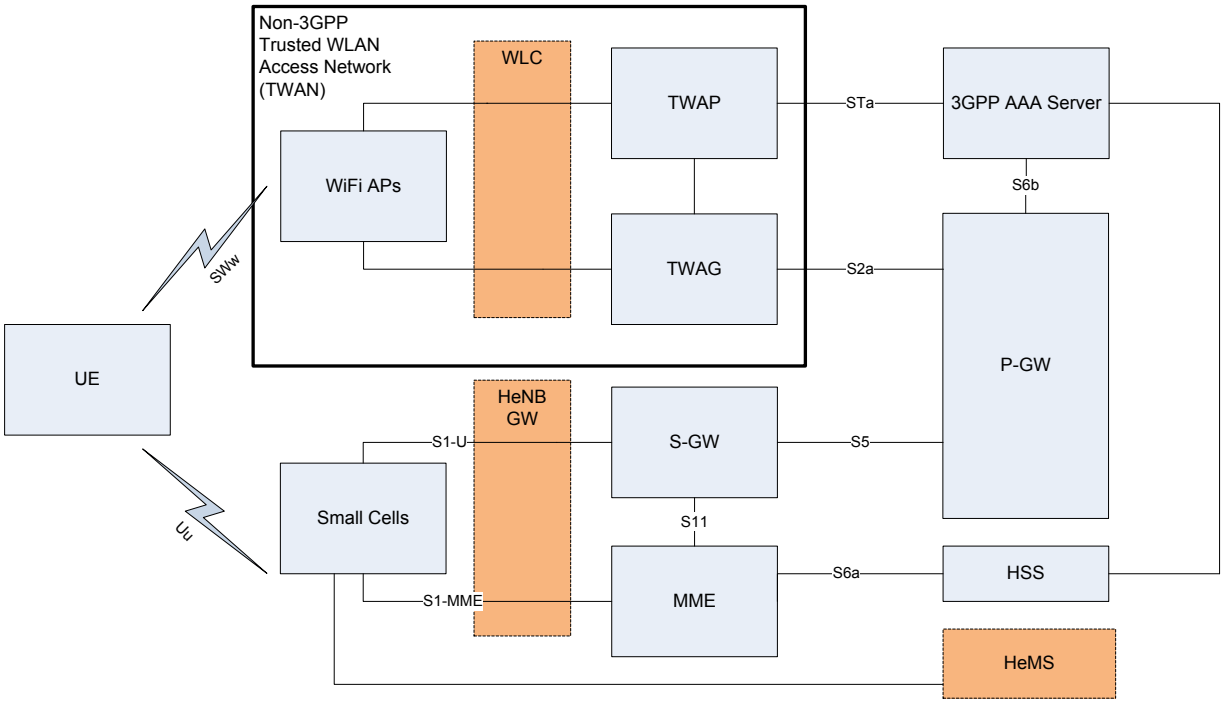


Figure 2.3 Multi-access TWAN and multi-access small cell network

Figure 2.4 below illustrates the optimized case where the small cell and Wi-Fi are integrated into a single access node. Such implementations enjoy the advantage of shared hardware, software, power, backhaul, secure housing etc.

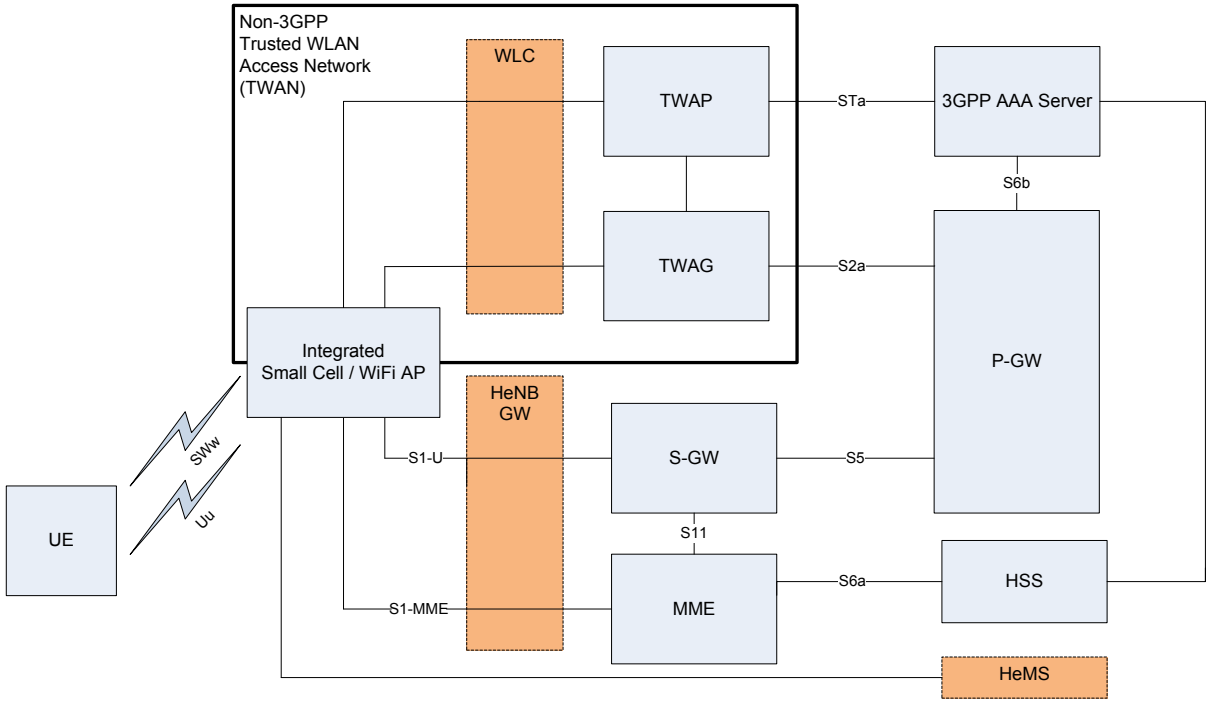


Figure 2.4 Integrated Small Cell / Wi-Fi AP

3. Industry perspectives on ISW networks and services

The SCF-WBA JTF conducted a comprehensive survey of ISW requirements from a broad range of MNO, MSO and integrated operators, with the following main objectives:

- Understand the ISW landscape
- Allow SCF-WBA joint taskforce to better understand operator requirements related to ISW
- Frame current deployments and future evolution
- Identify which are the most important challenges

The joint team agreed on the relevance of launching a survey to retrieve feedback from participating operators/vendors, with regard to the most relevant ISW topics currently being discussed in the industry. In total 17 companies participated in the survey.

1.5 Objective of the survey:

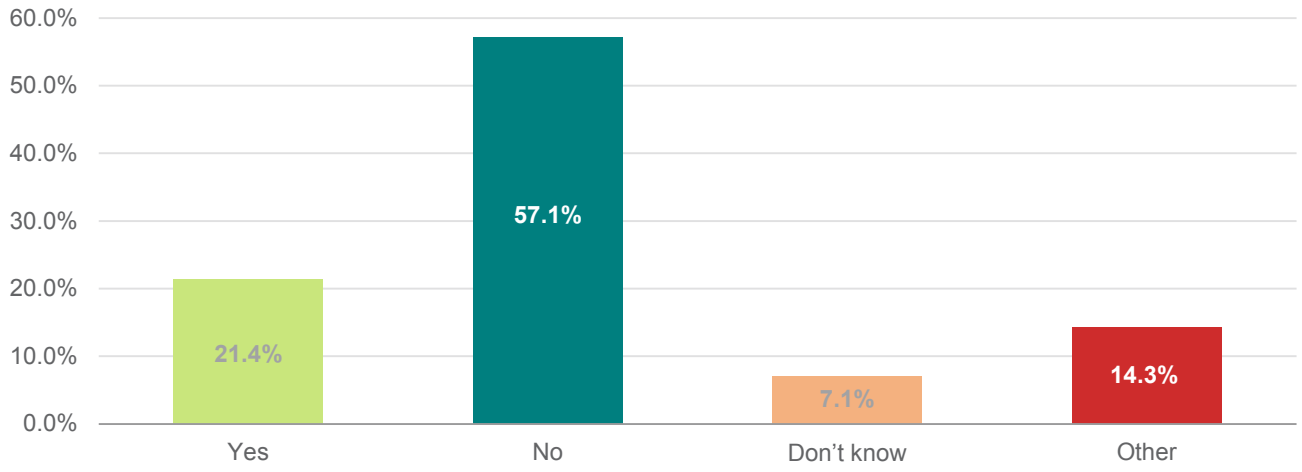
- Understand the ISW landscape
- Allow SCF-WBA joint taskforce to better understand operator requirements related to ISW
- Frame current deployments and future evolution
- Identify which are the most important challenges

1.6 The target audience for this survey:

a. Mobile operators (MNOs)
b. Integrated operators, fixed and mobile
c. Non-mobile operators (ISPs, cable, Wi-Fi, etc.)

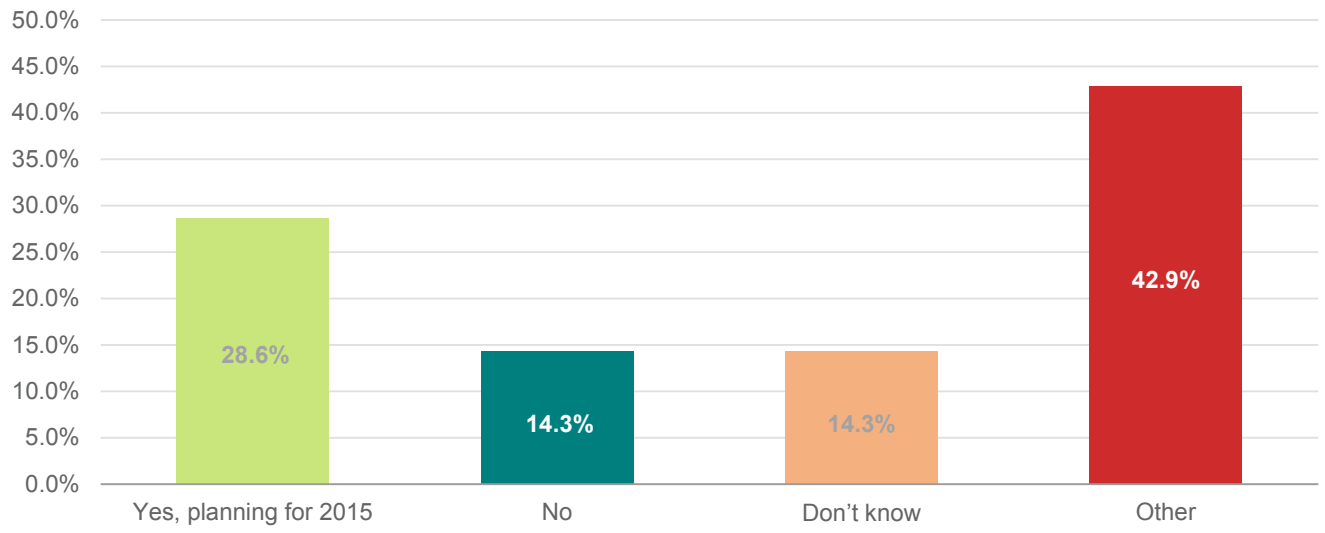
1.7 Survey question results:

Question#1: Has your company deployed ISW networks?



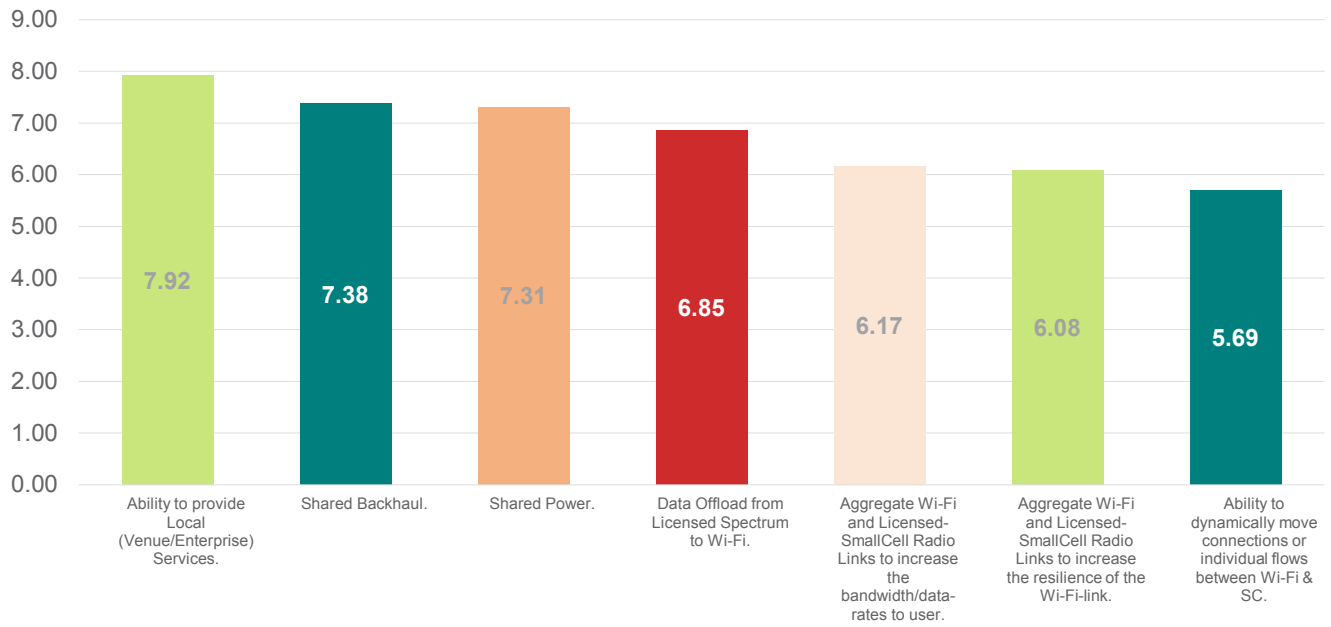
Workgroup analysis: Deployment of ISW networks is still picking up, thus the scope of the white paper being developed will certainly help to foster further deployments.

Question#2: Is the deployment of ISW network on your company roadmap?



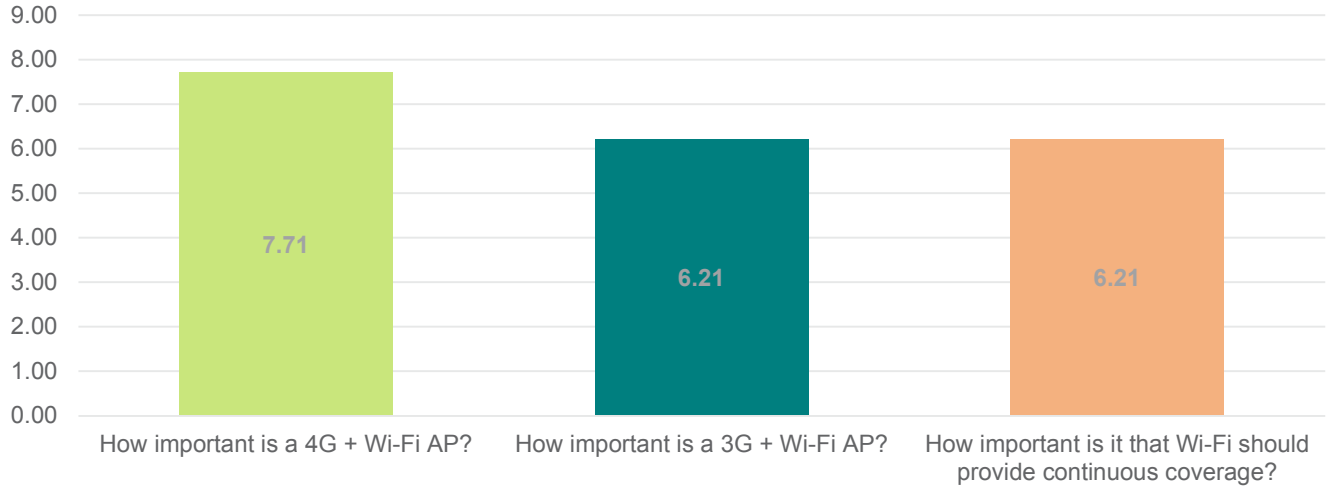
Workgroup analysis: The majority of operators with plans to deploy the technology, either on the referred timeline or later. Field 'Other' mainly selected by vendors to whom this question does not apply or by operators who have already deployed the technology.

Question#3: Please rate the following benefits of integrating Wi-Fi into Small Cells (10=Strongly Agree; 1=Strongly Disagree)



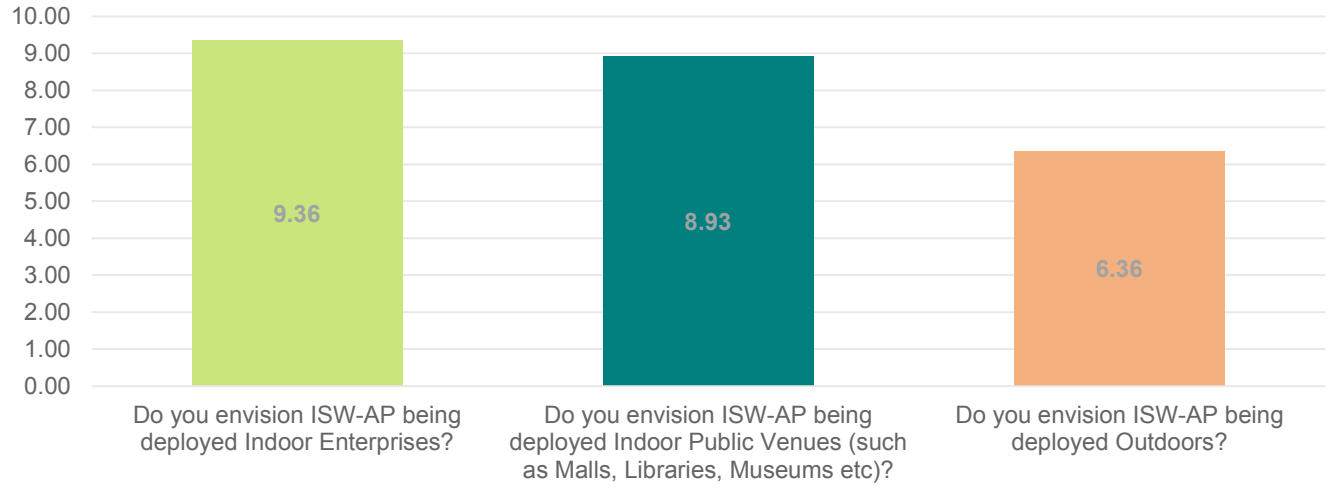
Workgroup analysis: The most relevant benefits to respondents is the ability to provide services to specific venues/enterprises where typically a macro cellular network might not be the best solution. Also, shared backhaul and power are ranked on the TOP3, due to the efficiency and cost-saving they can bring to the equation.

Question#4: Please rate the following Wi-Fi and small cells deployments (10=Very Important; 1=Not at all important)



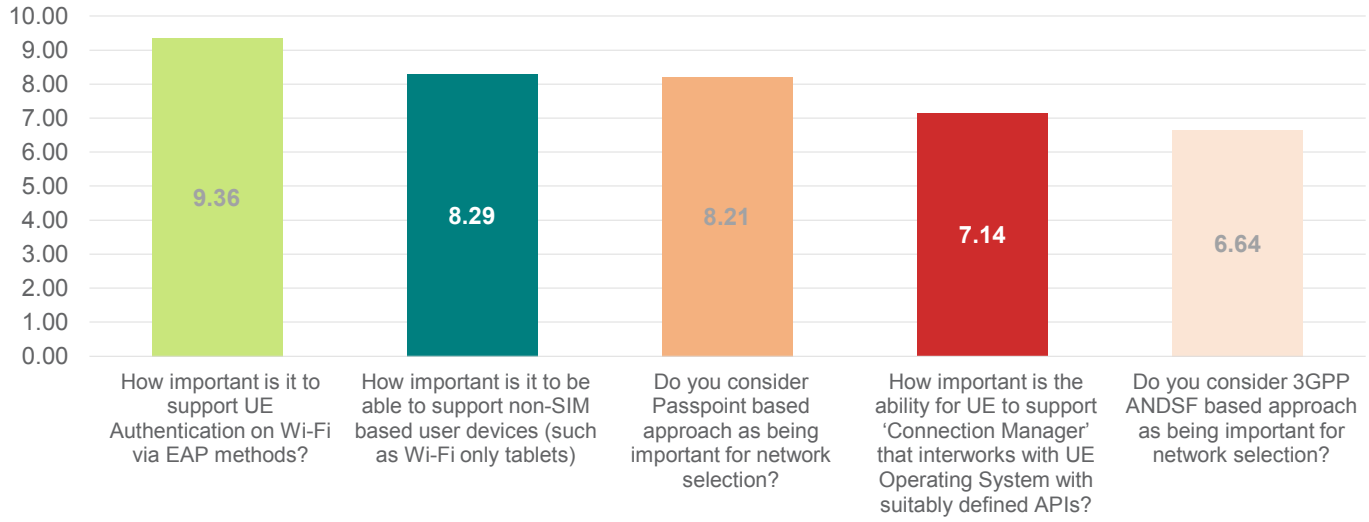
Workgroup analysis: New global deployments of 4G are now more relevant to the ecosystem with regard to their aggregation with Wi-Fi.

Question#5: Please rate the following Wi-Fi and small cells deployment scenarios (10=Strong Yes; 1=Strong No)



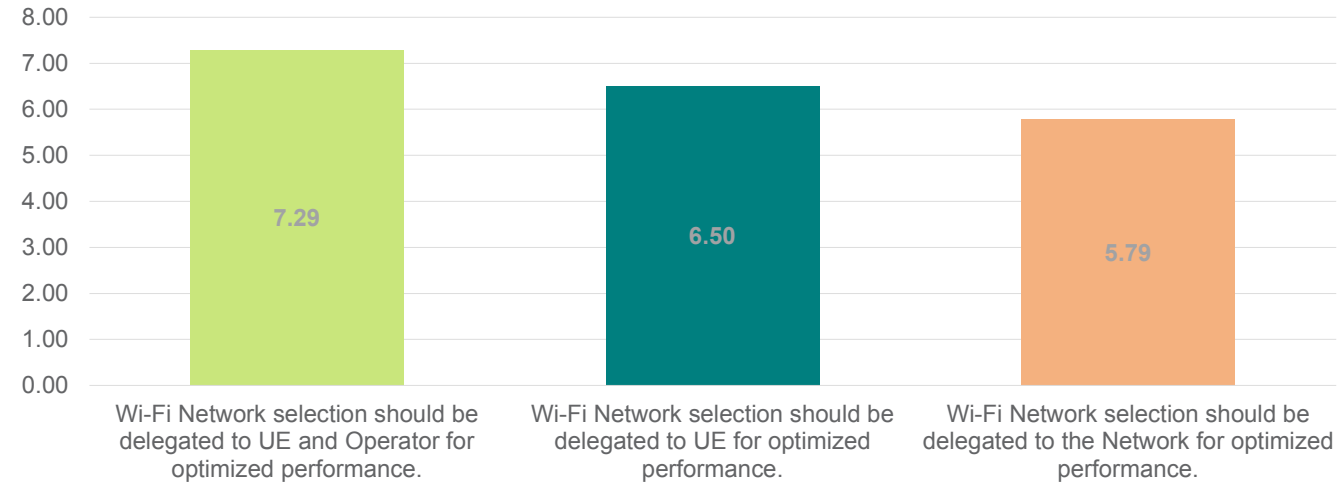
Workgroup Analysis: The scenarios that involve indoor or specific venues are clearly ranked as the most relevant for ISW deployments.

Question#6: Please rate the following Wi-Fi and small cells user experience/user equipment options (10=Very Important, 1=Not at all important)



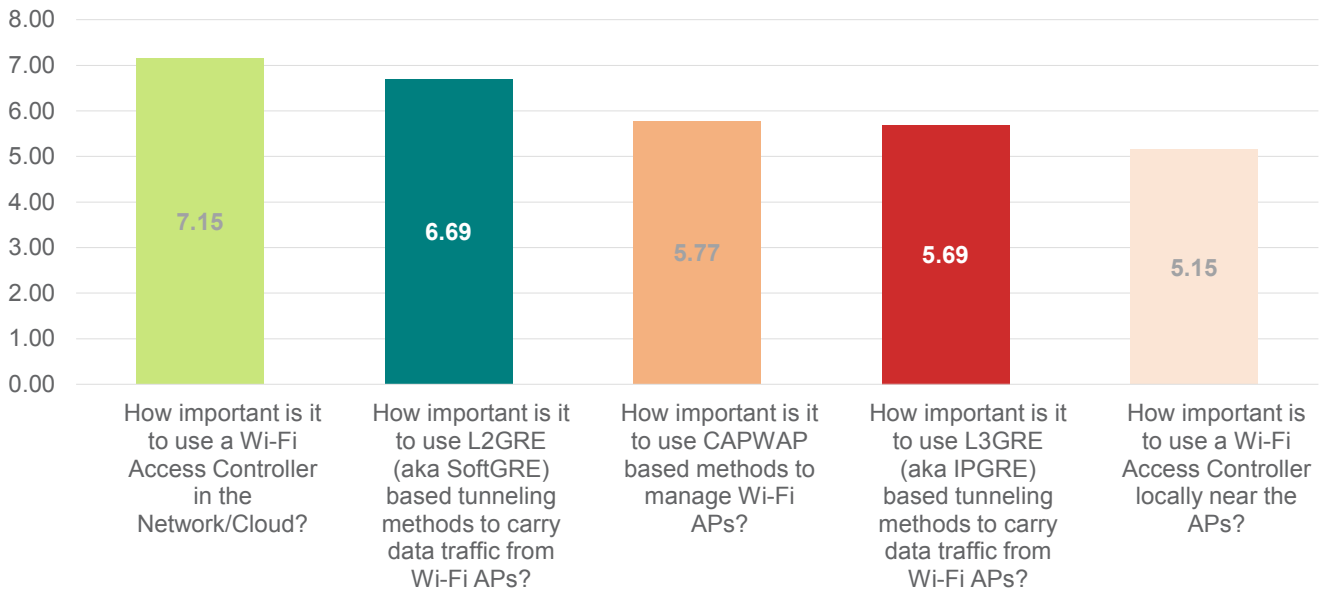
Workgroup analysis: Seamless authentication via EAP methods facilitating user experience and support for a broad range of devices is key.

Question#7: Please rate the following Wi-Fi and small cells user experience/user equipment options (10=Strongly Agree; 1=Strongly Disagree)



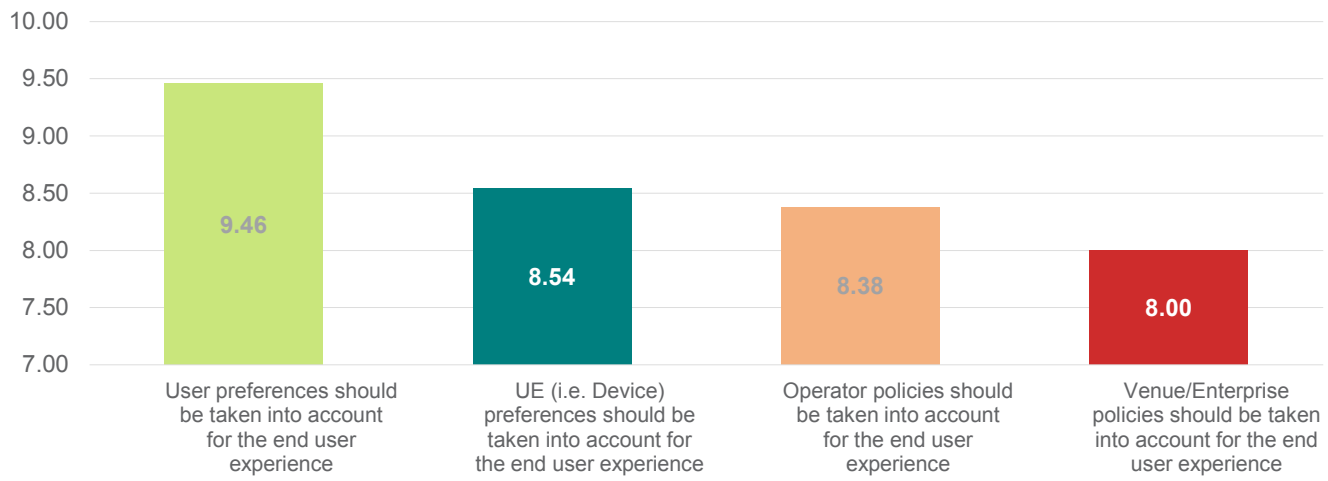
Workgroup Analysis: A hybrid combination of UE and operator policy is regarded as the most prominent vehicle for optimized performance.

Question#8: Please rate the following Wi-Fi and small cells provisioning and management options (10=Very Important, 1=Not at all Important, NA=Not Applicable)



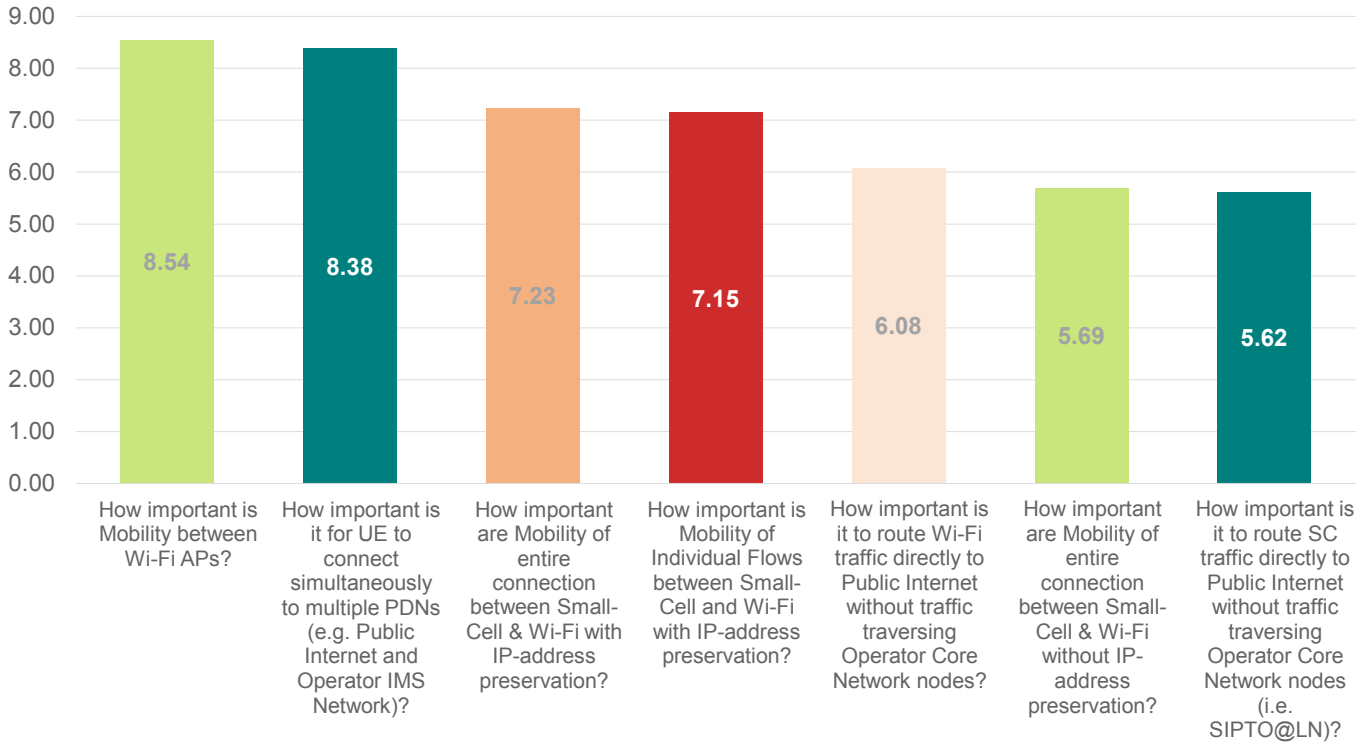
Workgroup analysis: Usage of network/Cloud WLC and L2GRE based tunnelling methods to carry data traffic from Wi-Fi APs as most voted.

Question#9: Please rate the following Wi-Fi and small cells policies options (10=Strongly Agree; 1=Strongly Disagree; No value=No Opinion)



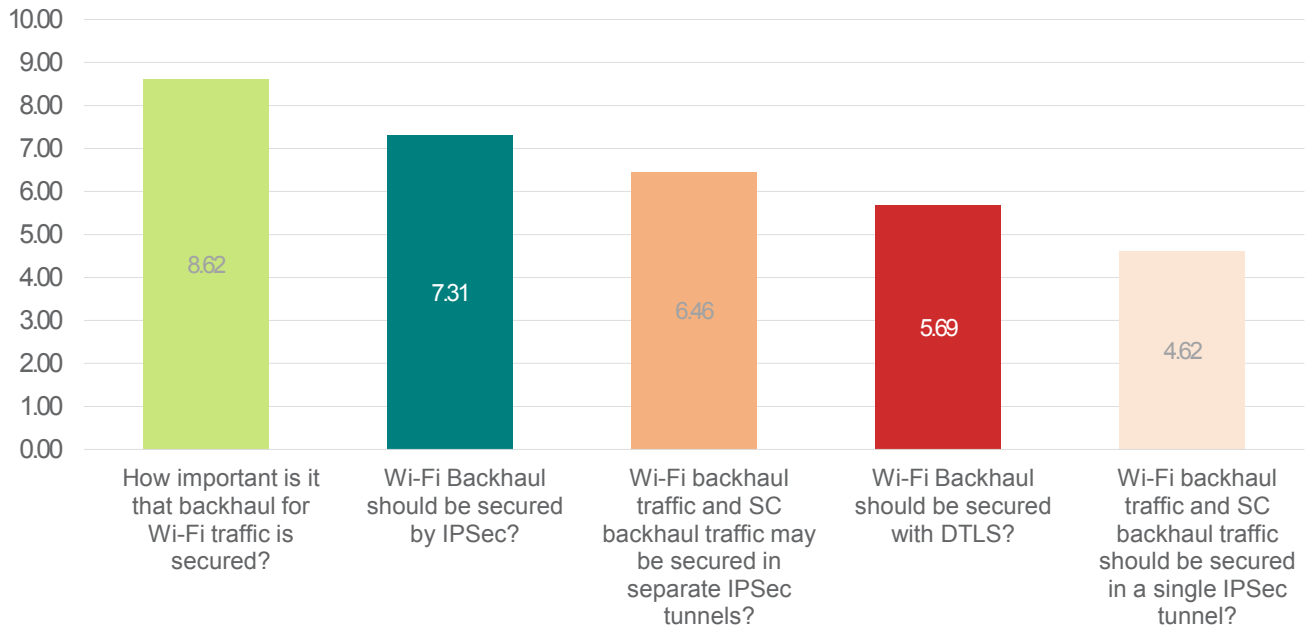
Workgroup analysis: It is consensual that user-based preferences/equipment owned, should have the most prominent role for defining the user experience.

Question#10: Please rate the following Wi-Fi and small cells traffic management options (10=Very Important; 1=Not at all Important; NO=No Opinion)



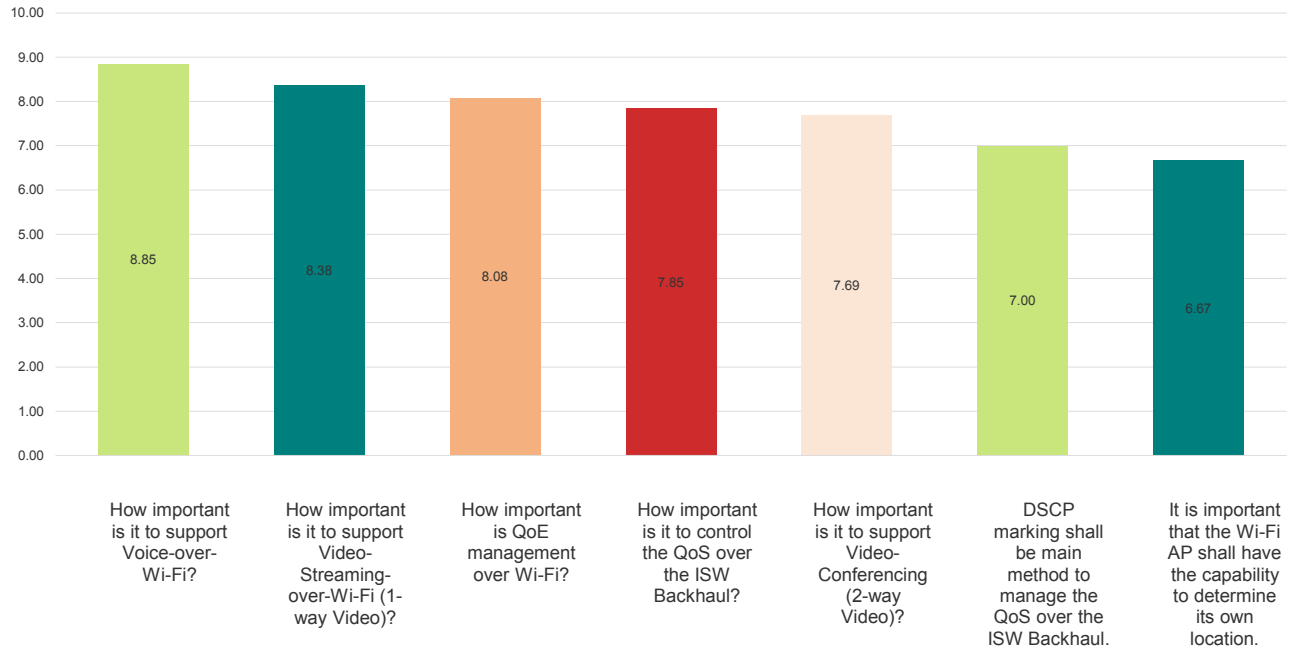
Workgroup analysis: Mobility between Wi-Fi APs and UE simultaneous connection to multiple PDNs as most important options.

Question#11: Please rate the following Wi-Fi and small cells architectures~~s~~ options (10=Strongly Agree, 1=Strongly Disagree)



Workgroup analysis: Security of Wi-Fi backhaul and usage of IPSEC tunnels as most important options.

Question#12: Please rate the following Wi-Fi and small cells services & QoE options (10=Very Important; 1=Not at all Important)



Workgroup Analysis: Voice and video streaming over Wi-Fi together with QoE management ranked as the most relevant.

Question#13: What are the current (or anticipated) challenges, if any, associated with ISW deployment?

- QoS for Wi-Fi-based services (VoWi-Fi & video)
- Small cell location determination, timing synchronization for other than GPS-based
- Separate the control and user planes
- INFOSEC requirements mandating isolation between small cell and Wi-Fi traffic
- Coexistence between various bands and Wi-Fi

4. Trusted WLAN access network (TWAN) architectures

The aim of this section is to provide details regarding the different options available for the realization of the Trusted non-3GPP WLAN access network. The options will be compared, helping operators wishing to integrate service provider Wi-Fi networks with their 3GPP EPC to decide on how best to deploy such functionality.

1.8 3GPP view of TWAN (TR 23.852)

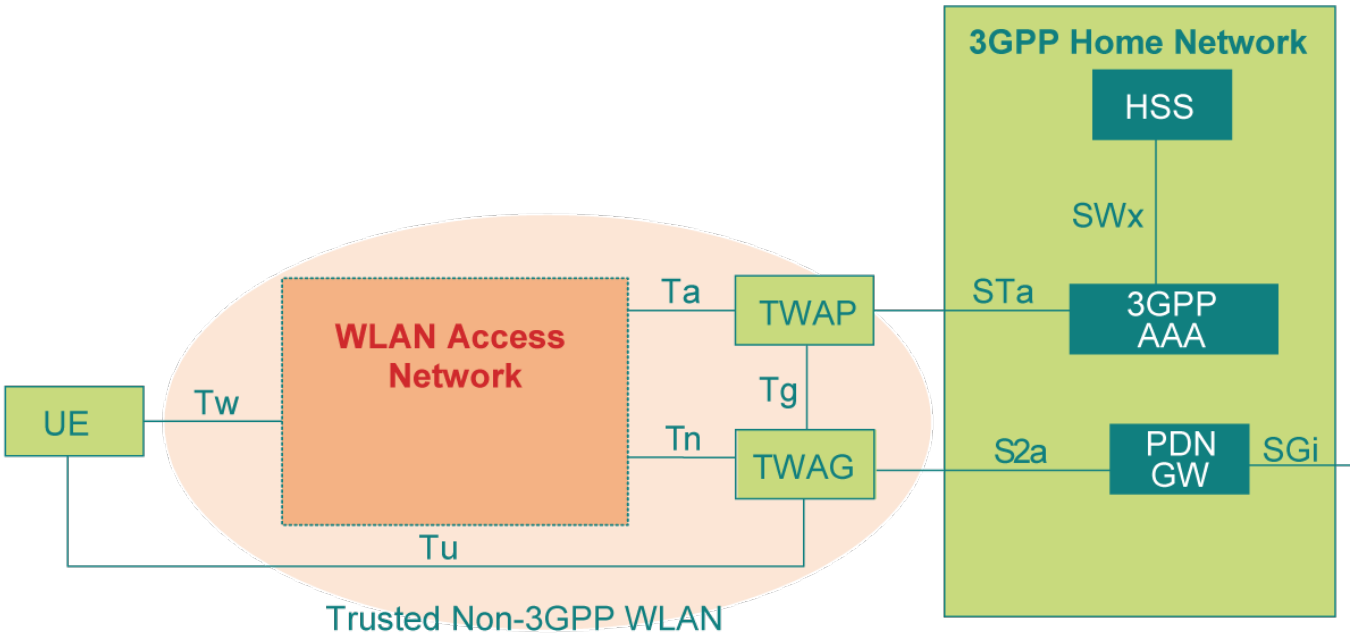


Figure 4.1 3GPP-TWAN interworking reference model [1]

Section 7.1.2.1 of TR 23.852 [1] discusses in detail the internal reference points inside TWAN. Figure 4.1 presents the reference model of the non-roaming case. The shaded area refers to trusted non-3GPP WLAN access functionality. The internal reference points can be summarized as follows.

1.8.1 Ta reference point

The Ta reference point connects the WLAN access network to the trusted WLAN AAA proxy. The prime purpose of the protocols crossing this reference point is to transport **authentication, authorization and accounting** related information. **EAP** authentication shall be transported over the Ta reference point. The functionality of the reference point is to transport AAA frames:

- Carrying data for **authentication** signalling between UE and 3GPP network; as a side effect, allowing the trusted WLAN AAA proxy to detect L2 attach of the UE.
- Carrying data for **authorization** (including the authorization information update) signalling between WLAN Access Network and 3GPP Network.
- Carrying **accounting** signalling per WLAN user, e.g. for charging purposes; As a side effect, allowing the Trusted WLAN AAA proxy to detect L2 detach the UE.
- Carrying **keying** data for the purpose of radio interface integrity protection and encryption;
- Informs WLAN access network of per-UE **encapsulation information** to be used with the trusted WLAN access gateway. The specifics of the encapsulation method in use (e.g. L2 unicasting, IETF RFC 6085, 802.11Q VLAN, MPLS, CAPWAP) and how it is negotiated between the trusted WLAN

access network and the trusted WLAN access gateway via the Trusted WLAN AAA proxy are dependent on the specifics of the WLAN access network deployment and out-of-scope for 3GPP.
- Purging a user from the WLAN access network for immediate service termination.

1.8.2 Tg reference point

The Tg reference point connects the trusted WLAN AAA proxy to the trusted WLAN access gateway. This is a AAA interface used to:

- Trusted WLAN AAA proxy notify Trusted WLAN Access Gateway of **WLAN attach and detach** events.
- Trusted WLAN access gateway Informs trusted WLAN AAA proxy of per-UE **encapsulation** information to be used between the WLAN Access Network and the Trusted WLAN access gateway. The specifics of the encapsulation method in use (e.g. L2 unicasting, IETF RFC 6085, 802.11Q VLAN, MPLS, CAPWAP) and how it is negotiated between the trusted WLAN access network and the trusted WLAN access gateway via the trusted WLAN AAA proxy are dependent on the specifics of the WLAN access network deployment and out-of-scope for 3GPP.

1.8.3 Tn reference point

The Tn reference point connects the WLAN access network and the trusted WLAN access gateway and provides the following functionality:

- Per-UE **encapsulation** between the WLAN access network and the trusted WLAN access gateway. The specifics of the encapsulation method in use (e.g. L2 unicasting, IETF RFC 6085, 802.11Q VLAN, MPLS, CAPWAP, L2oGRE, L3oGRE) and how it is negotiated between the trusted WLAN access network and the trusted WLAN access gateway via the trusted WLAN AAA proxy are dependent on the specifics of the WLAN access network deployment and out-of-scope for 3GPP.

1.8.4 Tw reference point

The Tw reference point connects the UE to the WLAN access network as per IEEE 802.11 specifications. The definition of IEEE physical and medium access control layers protocols (e.g. Layer-1 and Layer-2 defined by IEEE 802.11 standards) is out of the scope of 3GPP. The functionality of the reference point is based on IEEE 802.11 specifications and it is intended to transport **signalling** messages including:

- **Attach and detach** request from the UE to the WLAN access network.
- **Detach** signal from the WLAN access network to the UE.
- Parameters for **authentication** signalling between the 3GPP AAA server and the UE.
- Per-UE **encapsulation** of data frames between the UE and the WLAN access network as per IEEE 802.11 specifications.

1.8.5 Tu reference point

The Tu reference point represents the point-to-point link and per-UE subnet between the UE and the trusted WLAN access gateway. Transport for the Tu reference point is provided by a combination of:

- The Tw reference point provides an IEEE 802.11 association between the UE and a BSSID/ESSID in the WLAN access network, as per IEEE 802.11 specifications.
- The WLAN access network internally provides per-UE encapsulation between the BSSID/ESSID and the Tn endpoint.
- The Tn reference point provides per-UE encapsulation between the WLAN access network and the trusted WLAN access gateway.

1.9 WLAN view of TWAN

Compared with the Small Cell Forum that has successfully provided the industry with a set of "how-to" guides covering the architectural approaches for the deployment of small cells using licensed radio technologies, the approaches taken by operators in deploying small cells using unlicensed Wi-Fi technology has largely lacked any strict architectural definition. Furthermore, the definition of these architectures is deemed to be out of scope of 3GPP. For example, when considering the Tn reference point shown in the Figure 4-1 it is clear that 3GPP views this as out of scope [30]:

"The specifics of the encapsulation method in use (e.g. L2 unicasting, IETF RFC 6085 [48], 802.11Q VLAN, MPLS, CAPWAP [21]) and how it is negotiated between the trusted WLAN access network and the trusted WLAN access gateway via the trusted WLAN AAA proxy are dependent on the specifics of the WLAN access network deployment and out-of-scope for 3GPP."

However, in order to compare the different options for realizing the integration of the Trusted WLAN Access Network with the MPC/EPC, it is necessary to understand the typical Service Provider Wi-Fi access network deployment models and the connectivity of the control plane and data plane in those various models. In the SP Wi-Fi deployment scenarios, the APs are typically coordinated and managed by Wireless LAN Controllers (WLCs), but there may be certain cases where the APs are operating in autonomous mode (local configuration and control).

In the WLC deployment models, there will always be a control plane connection between the AP and the WLC. This control plane communication can be based on IETF CAPWAP [21] or on the use of alternative vendor-specific protocols. In whichever case, the control plane should be secured using robust encryption. It should be clearly noted that even though IETF CAPWAP is standardised, the partitioning of functionality is not clearly defined with a consequential impact to multi-vendor interoperability [Ref RFC 7494].

The TWAN data plane connection may either be via the WLC in what is known as a "centralized forwarding" model, or it may bypass the WLC in what is known as a "distributed forwarding" model. In many implementations the option to use centralized or distributed forwarding is done at the WLAN/SSID level, so data plane traffic for UEs on certain WLANs might be tunnelled to the WLC for forwarding, while traffic for UEs on other WLANs could be forwarded directly from the AP. When centralized forwarding is utilized, the tunnelled data plane traffic between the AP and the WLC may optionally be secured using robust encryption, which will likely be required for TWAN integration.

Table 4.1 below summarizes the different WLAN configurations that are considered for realization of the Trusted WLAN Access Network

WLAN deployment model	CP egress	CP security	DP egress	DP security
WLC centralized forwarding	WLC	Mandatory	WLC	Optional
WLC distributed forwarding	WLC	Mandatory	AP	N/A
AP autonomous mode	AP (local)	N/A	AP (local)	N/A

Table 4.1 WLAN configuration options

1.10 Selected TWAN architectures

When the WLAN configuration examples are considered, 6 different options for realizing TWAG and TWAP functionality were identified and enumerated in the earlier SCF-WBA white paper [53]. They are essentially based on the following architectural characteristics:

a. Centralized forwarding by WLC
b. Distributed forwarding by WLC
c. Autonomous AP
d. Centralized forwarding by WLC + collapsed TWAG/TWAP/WLC

e. Distributed forwarding by WLC + collapsed TWAG/AP & TWAP/WLC
f. Autonomous AP + collapsed TWAP/AP

For the purposes of this white paper, and in particular for the specific purpose of describing the various TWAN interfaces, it was decided to focus on options 1, 2 & 3. Options 4, 5 & 6 were skipped since these are implementation variations which essentially collapsed some functionality.

The selected architectures based on options 1, 2 & 3 are redrawn in the figure below, where the various TWAN interfaces are also named for further elaboration.

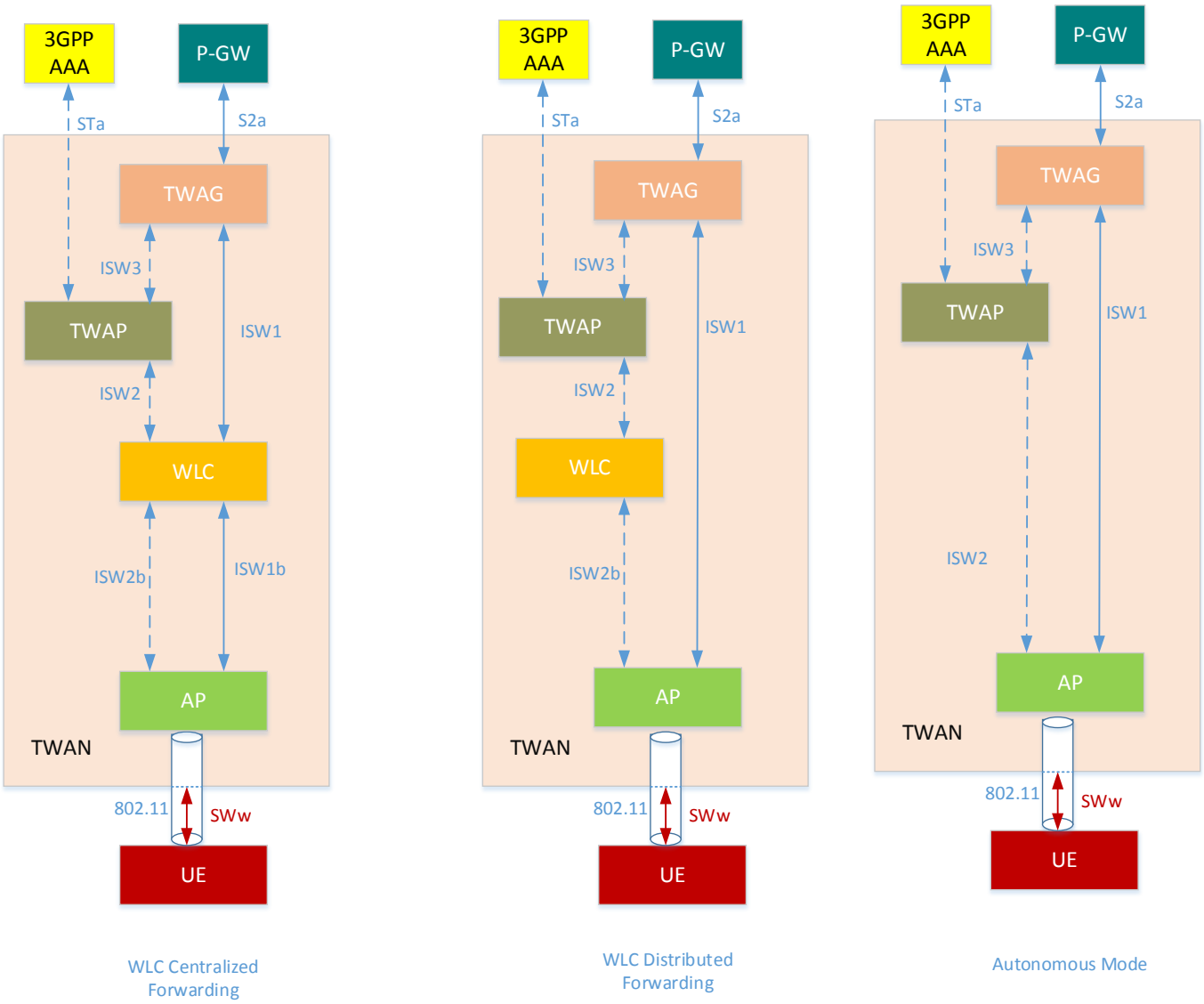


Figure 4.2 Selected TWAN configurations

1.11 TWAN interfaces

1.11.1 Tunnelling protocols

This section explores the different options for tunnelling between the AP and the TWAG, i.e. representing the autonomous mode and WLC distributed forwarding TWAN configurations.

Layer-2 over GRE (L2oGRE) overview

"Layer-2 over GRE" or L2oGRE is the predominant encapsulation technique used to tunnel autonomous AP <-> TWAG traffic. This method brings together two well-understood encapsulation techniques: Ethernet and IP GRE. The benefit of this technique is its simplicity and scalability allowing cost effective deployments while maintaining/preserving the maximum amount of subscriber data at the policy enforcement point (GW). In this mode, regardless of which AP the subscriber is attached to, the GW maintains visibility of the subscriber hardware information (802.11 MAC address).

The general concept of the L2oGRE model is that the AP to which a UE is connected, encapsulates all UE Ethernet frames in a GRE header and sends these frames to the TWAG. The TWAG un-encapsulates the GRE header, at which point it can make a forwarding/policy decision based on the UEs IP/MAC information. All UE-traffic from the AP can run over the same tunnel and traffic from different SSIDs can be delineated using 802.1Q VLAN tags in the Ethernet frame (a common feature supported amongst APs).

The generic encapsulation is as follows:

```
+-----------------------------------------------------+
|                                                     |
|               IP Transport Header                   |
|                                                     |
+-----------------------------------------------------+
|                                                     |
|                     GRE Header                      |
|                                                     |
+-----------------------------------------------------+
|                                                     |
|                UE Ethernet Header                   |
|                                                     |
+-----------------------------------------------------+
```

Figure 4.3 L2oGRE Encapsulation

Where the:

- IP transport header – comprises of the SA/DA of the AP/TWAG. Commonly referred to as the "outer IP".
- GRE header – The shim header used to indicate that the payload carried by this packet is a full Ethernet frame.
  In the GRE header, the protocol type must be set to 0x6558 (transparent Ethernet bridging), and often the checksum, routing, key, sequence, are optional/not used and can be (and usually are) set to zero.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|R|K|S|s|Recur|   Flags | Ver |     Protocol Type = 0x6558    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Checksum (optional)           | Offset (optional)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Key (API) (optional)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Sequence Number (optional)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Routing (optional)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4.4 GRE header

- UE Ethernet header – This is the full (unaltered) Ethernet frame from the UE where the Layer2/Layer3 addressing is as follows:
  - Layer-2:
    - SA/DA MAC@ are the actual UE Wi-Fi MAC layer and the corresponding MAC address of the gateway at the other end of the Layer 2 domain.
    - VLAN-ID (Q tag) can be used to delineate different flows. Typically this VLAN-ID can be used to isolate traffic between different SSIDs.
  - Layer-3: SA/DA IP@ are the actual UE Wi-Fi IP@ (assigned typically via DHCP or SLAAC by the TWAG) and the destination of the IP packet.

L2oGRE considerations:

- Preserves the UE hardware information, simplifies identifying specific UE for policy enforcement, initiating lawful intercept (LI), anti-spoofing, etc.
- Transparent to IP version. UE IPv4/Ipv6 traffic is carried in the same GRE tunnel, although TWAG terminating L2oGRE will need to accommodate DHCPv4, DHCPv6 and/or SLAAC operation.
- Simplified inter-AP/AC mobility as an AP <-> AP mobility event looks to the network as a MAC address relearn on a different tunnel, rather than an IP@ change (more below). On top of the simple MAC address relearn any extra security policy can be implemented to ensure aspects like anti-spoofing or others are safe.
- Supports overlapping UE L3 addressing per AP/SSID, and allows for simplified Layer-2 based wholesale-access.
- Lightweight stateless implementation on AP and TWAG. Can be supported in a “soft-GRE” implementation which removes the need for “always on” tunnels.
- Broad support among AP-vendors.
- When a NAT function exists between an AP/TWAG, additional encapsulation is required to support NAT-traversal (e.g. IPSec).
- L2oGRE is a user-plane encapsulation and relies on out-of-band mechanisms, such as DHCP, RADIUS or CAPWAP to signal subscriber information (e.g. location information) and policy information between the AP/AC/TWAG/TWAP and the AAA infrastructure. A mobility event can either be inferred by MAC@ relearning, or via RADIUS.

L3GRE – protocol/encapsulation overview

L3GRE is another encapsulation option for tunnelling subscriber traffic between the AP and the enforcement point (GW). In this model, user IP payload is encapsulated in a GRE header. In this case, the UE Ethernet frame is stripped from the payload before the AP encapsulates the IP payload in the GRE. The TWAG/GW will terminate GRE header and forward traffic upstream.

The generic encapsulation is as follows:

```
+-----------------------------------------------+
|                                               |
|              IP Transport Header              |
|                                               |
+-----------------------------------------------+
|                                               |
|                   GRE Header                  |
|                                               |
+-----------------------------------------------+
|                                               |
|                  UE IP Header                 |
|                                               |
+-----------------------------------------------+
```

Figure 4.5 L3GRE Encapsulation

Where the:

- IP transport header – comprises of the SA/DA of the AP/TWAG. Commonly referred to as the "outer IP".
- GRE header – The shim header used to indicate that the payload carried by this packet is a full IP datagram. In this header, the "protocol type" is set 0x0800 (or 0x86DD for IPv6).

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|C|R|K|S|s|Recur|   Flags | Ver |     Protocol Type = 0x0800    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Checksum (optional)           | Offset (optional)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Key (API) (optional)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Sequence Number (optional)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Routing (optional)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4.6 IP-over-GRE Header

- UE IP header – This is the IP payload of the UE generated packet, and refers to the UE IP@ and the internet destination IP@ as the SA/DA combination.

L3 tunnelling protocols can also be associated with dedicated signalling capabilities. In particular, this is the case for PMIPv6, an L3 tunnelling protocol which allows transport of both IPv4 and IPV6 packets that can also use IP-

over-GRE as an encapsulation header. Along with the data transport over GRE, there are signalling messages called Proxy Binding Update (PBU) and Proxy Binding Acknowledge (PBA), which pass over registration and attach information about the users, complementing the Layer-3 information in such a way that the other side of the tunnel is also aware of Layer-2 information parameters about the user.

This extra signalling introduced does not necessarily impact the efficiency and performance of the transport layer. As an example in Layer-2 solutions, DHCP messages traverse the entire tunnel introducing more round trip delay than a single round trip of PBU/PBA as DHCP is composed of multiple exchanges while in Layer 3 solution DHCP is only local to the user/AP environment.

L3GRE considerations:

- Provides UE connectivity/tunnelling between AP <-> TWAP at Layer-3, no UE-specific Layer-2 information is provided. Subscriber identity based functions (e.g. Billing, Lawful Intercept) relies on the correlation data provided as part of the signalling.
- UE IP version (IPv4/IPv6) is uniquely indicated in the GRE header. IPv4/IPv6 traffic would be carried in separate GRE tunnels which are identified by the state maintained on both ends of the tunnels for a subscriber session.
- Inter-AP mobility may require re-addressing of UE, and/or signalling between the AP and the TWAG (via PMIP). This signalling corresponds to an equivalent of ISW3 requirement but is indeed not following the same path as the ISW3 specification as it in many cases removes the need for ISW3 to exist in the same way it does when TWAG & TWAP are collocated in Layer-2 case.
- L3oGRE is typically associated with PMIPv6 and hence leverages the standardized PMIPv6 control plane exchanges. PMIPv6 control plane can be used to dynamically enable operation across NATs. In case a NAT operation is detected, the L3-GRE data plane packets get encapsulated in UDP to allow traversal across the NAT function. Furthermore, PMIPv6 signalling will be triggered on mobility events to enable the TWAG to be signalled with updated information, e.g. associated with UE location.
- As there is no preservation of IP/MAC binding information on the TWAG, any sort of security/anti-spoofing capability would need to exist on each AP to prevent having a rogue UE impersonate a valid UE.

L2TPv3 – protocol/encapsulation overview

L2TPv3 (RFC 3931) defines a standard method by which Layer-2 protocols could be encapsulated and tunnelled over an IP network to a remote tunnel endpoint. Version 3 improved on L2TPv2 (which supported only PPP frame encapsulation) by supporting transport of any L2 frame. It also defines support for UDP, IPv4 or IPv6 transport, allowing it to be deployed throughout a wide scope of transport networks.

The generic encapsulation is as follows:

```
+-----------------------------------------------------+
|                                                     |
|                IP Transport Header                  |
|                                                     |
+-----------------------------------------------------+
|                                                     |
|                UDP Header (Optional)                |
|                                                     |
+-----------------------------------------------------+
|                                                     |
|                   L2TPv3 Header                     |
|                                                     |
+-----------------------------------------------------+
|                                                     |
|                    UE IP Header                     |
|                                                     |
+-----------------------------------------------------+
```

Figure 4.7 L2TPv3 Encapsulation

Where the:

- IP transport header – comprises of the SA/DA of the AP/TWAG. Commonly referred to as the “outer IP”.
- UDP header – An optional shim header used to include source/destination UDP port numbers (supports NAT-traversal).
- L2TPv3 header – The L2TPv3 header itself provides support for both control plane signalling as well as data plane encapsulation. The generic encapsulation is as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|T|x|x|x|x|x|x|x|x|x|x|  Ver  |           Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Session Id                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                         64-bit  Cookie                        |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4.8 L2TPv3 Header

- UE IP header – This is the IP payload of the UE generated packet, and refers to the UE IP@ and the internet destination IP@ as the SA/DA combination.

While L2TPv3 provides a similar capability to L2oGRE, in the ability to encapsulate and translate Layer-2 based frames across an IP network, it differs in that it introduces a control plane element not present in stateless L2oGRE. This provides a performance trade-off when compared with L2oGRE, as it also introduces additional management/overhead when deploying.

Wi-Fi deployments where the AP and the TWAG/GW are separated by a NAT function are applications where L2TPv3 may be considered. L2GRE rely on GRE to encapsulate an inner IP/MAC inside another IP header. However, the L2GRE header is pure IP-in-IP, and hence it contains no source/destination port mappings and therefore cannot be effectively mapped through a NAT function. As L2TPv3 supports a UDP-based encapsulation mode, it can traverse a NAT function without issue.

Please note: AP deployments utilizing IPSec across the backhaul network can take advantage of the native support for NAT traversal within the IKEv2 protocol, This function uses a similar UDP shim header to negotiate/map inside/outside port numbers. This allows L2oGRE/IPSec deployments to be used in conjunction with NAT.

L2TPv3 considerations:

- Preserves the UE hardware information, simplifies identifying specific UE for policy enforcement, initiating Lawful Intercept (LI), anti-spoofing, etc.
- Transparent to IP version. UE IPv4/IPv6 traffic carried in the same GRE tunnel.
- Simplified inter-AP/AC mobility as an AP <-> mobility event looks to the network as a MAC address relearn on a different tunnel, rather than an IP@ change (more below).
- Supports overlapping UE L3 addressing per AP/SSID.
- Potentially introduces additional (relative heavy) control plane signalling between the AP/TWAG which could negatively impact network scaling. Note: this tunnelling mode can be made stateless in a similar mode to L2oGRE for improved scalability and reduced complexity.
- Native UDP encapsulation provides native NAT traversal support.

Network considerations

Backhaul (trusted/untrusted)

When AP deployments reside within a trusted transport environment, where operators own/maintain the infrastructure between the AP and the TWAG (GW) there may not be a requirement to protect the traffic. However, for cases where the connectivity between the trusted Wi-Fi elements (AP <-> TWAG) traverses third-party networks, additional security may be required.

IP Security (IPSec) can be utilized to secure traffic between the AP <-> TWAG. Such implementations can leverage a 3GPP-defined security gateway (SeGW/SEG) to provide the secure tunnel termination and demarcation between trust domains. In this model, the AP would encrypt L2oGRE/L3GRE/L2TPv3 traffic in an IPSec tunnel which would terminate on the SeGW; after decrypting the packet, this would forward the native tunnelled frame to the TWAG.

As discussed in the previous section, another advantage of utilizing IPSec is the inherent support for NAT traversal for instances where a NAT device resides between the AP and the TWAG.

Provisioning

When considering an AP deployment, provisioning and operations have a bearing on the tunnelling mechanisms used. Wide-spread AP deployment/turn-up, e.g., associated with autonomous residential APs, lends itself best to a light weight protocol, which requires minimal network touches to operationalize each new element. It should be understood that control plane signalling between the AP/AC/TWAG is not provisioning but just a process which takes place while subscribers attach to the network. From this sense using ETHoGRE or PMIPv6 solutions are equivalent as provisioning is about activating one or the other option. The difference is not in provisioning, however it is a valid fact that the development of PMIPv6 software stack onto an AP/CPE is more complex than layer 2 ETHoGRE bridging between two interfaces.

As well, minimizing/eliminating provisioning complexity, control plane signalling between the AP/AC/TWAG simplifies the provisioning effort required for turning up a new AP.

Inter-AP mobility

Ensuring fast handovers between APs with minimal traffic impact is key to ensuring a high quality experience for users avoiding any re-configuration of network settings on the UE when a transfer between APs is crucial.

Furthermore, adoption of EAP based authentication methods associated with Hotspot 2.0 necessarily impacts handover operation as the EAP exchange is used to negotiate keying material to secure the 802.11 air interface. In order to avoid re-authentication following an inter-AP mobility event, IEEE 802.11r can be used to deliver keying material to the new AP without necessitating a full (and lengthy) EAP exchange.

From an architecture perspective, these requirements tend to align with a more centralized model for IP address assignment/management as well as a controller for providing 802.11r key distribution functionality. Therefore within a Wi-Fi-domain/venue, placement of the UE IP@ assignment element and the first routed hop (from the UE perspective) should be carefully considered to avoid suboptimal IP@ design, unnecessary network configuration changes, degraded inter-AP mobility performance and poor QOE.

From a user-plane perspective, the inter-AP mobility model varies between tunnel mode types. Layer-2 based tunnelling models can often signal/detect a mobility event, either by the detection of movement of Layer-2 addresses across different AP tunnels (triggered by an up-link packet from the UE), or via a new AAA request from the new AP.. A straight-forward implementation of the inter-AP mobility based on Layer-3 tunnelling models could extend the duration of the mobility event due to the signalling involved. However, Inter-AP mobility for Layer-3 based tunneling typically uses access signaling to indicate the new AP that the UE is reachable without changing the underlying IP address of the UE and hence avoiding any interruption increase Finally, the user-plane aspects of inter-AP mobility need to be considered with control plane aspects, e.g., necessary for supporting mobility with Hotspot 2.0 EAP/802.1X.

For all approaches, security threats associated with inter-AP mobility need to be addressed; for example, to ensure that an existing session cannot be hijacked using a MAC spoofing attack.

Depending on the implementation choice of vendors, the logical ISW3 interface may not exist when the TWAG and TWAP are collocated within the same system/platform. However, when the ISW3 does not collapse, from an inter-AP mobility perspective, ISW3 may be necessary to signal information required to be populated on the TWAG northbound interface (towards the EPC). One example is the updated TWAN identifier information that can be used to signal the updated Wi-Fi AP MAC address (BSSID). For L3GRE deployments, PMIPv6 signalling can be used to signal such information directly between the WLAN and the TWAG, thus avoiding ISW3 requirements.

Regardless of the tunnelling method, inter-AP mobility can be accelerated by avoiding full re-authentication/re-association every time a UE moves between APs via IEEE 802.11 pairwise master key (PMK) caching or 802.11r or opportunistic key caching (OKC).

Inter-AC mobility

For deployments utilizing a Wi-Fi access controller (AC) in the data plane (between AP and TWAG), an additional element of complexity can be introduced when a UE moves between two APs which are homed into two different ACs. In these cases, the AC may aggregate/terminate AP tunnels into a single tunnel back to the TWAG. The mobility model again depends on the tunnelling mode between the AP and the AC.

If the AP<->AC/AC<->TWAG tunnelling is L2-based (L2oGRE/L2TPv3), the mobility model is similar to the L2-based inter-AP model discussed above. In the case where a TWAG is present and is the first L3 hop, it will manage the mobility between the ACs similar to the AP<->TWAG model. If no TWAG is present, the ACs are responsible for IP@ assignment and mobility management while inter-AC synchronization of per-UE keying information and session data is required to reduce handover latency.

Also it is important to note that the lack of AC in the autonomous mode deployment introduces extra complexity for providing fast handoffs because the key distribution across APs for fast rekeying capabilities is generally associated with an AC.

Evolution of tunnelling from a 3GPP perspective (virtual MAC)

In Release 12, 3GPP has standardized an evolved architecture for enabling UEs to improve integration with EPC services over a trusted Wi-Fi architecture via SaMOG (S2a over GTP). Specifically, the enhanced functionality, termed multi-connection mode (MCM), enables a UE to support connections to different EPC services (APNs).

MCM requires UE/TWAG support of the WLAN control plane (WLCP) protocol – which the UE uses to request connections to a specific APN(s) from the TWAG. Traffic for each of these separate APN connections are delineated by a virtual MAC (vMAC) address per APN. The destination vMAC address is the virtual MAC address associated with the specific APN connection. The TWAG provides this destination vMAC@ during the WLCP signalling phase, and the UE will send all traffic for a specific APN to this destination vMAC. Upon receiving these frames from the UE, the TWAG is able to route traffic to the specific S2a bearer to the correct PDN GW.

Since this method of access requires transporting Layer-2 addressing/frames between the UE and the TWAG, tunnelling encapsulations which natively support carrying Layer-2 frames are best suited for future proofing AP <-> TWAG connectivity.

1.11.2 ISW1-interface: AP/TWAG & WLC/TWAG data plane

The ISW1 interface defines the data plane connectivity between either the AP or the WLC into the TWAG. This connection could be using any of the protocols defined in section 5.1.

The two most used protocols are ETHoGRE and PMIPv6. The reason why those are the most predominant ones is because of their scalability, compared to other protocols.

Though the same protocols can be used either from an AP to a TWAG or from a WLC to a TWAG, the above considerations in terms of scale vary. As well as being able to accommodate NAT traversal, it may be an issue for supporting direct AP to TWAG connectivity, but may be less of a concern for WLC to TWAG connectivity. Indeed a WLC is already an AP aggregator, therefore the number of tunnels required between a WLC and a TWAG is significantly reduced by a scale of the number of APs that can be connected to a single WLC.

The parameters that drive any deployment are the scalability of respective platforms, the performance and a seamless user experience. The security concerns related to a service provider, such as identity management of a subscriber, ensure the integrity of a user's session and the performance. In order to account for these requirements, the TWAG must implement a state machine to manage the lifecycle of a user's session, transitioning him from his initial connection through the various roams he may occur up to the session termination. Various user state parameters need to be provided to the TWAG either natively by the transport tunnel or though some out of band signalling. This statement is what differs between L2oGRE and L3GRE (PMIPv6) options which can be used.

It is important to state that even though there are differences between both options, when implemented correctly they end up delivering the same level of services to an end-user. However the way the TWAG ends up interacting with either the WLC or the AP differs, and one cannot exclude the interaction between the TWAG and the TWAP.

The two following call flows will be used to explain the differences, however no recommendation is given between the two; a fine analysis of the deployment scenarios must be first investigated to decide on one or the other.

In the case of L2oGRE, the diagram is the following:

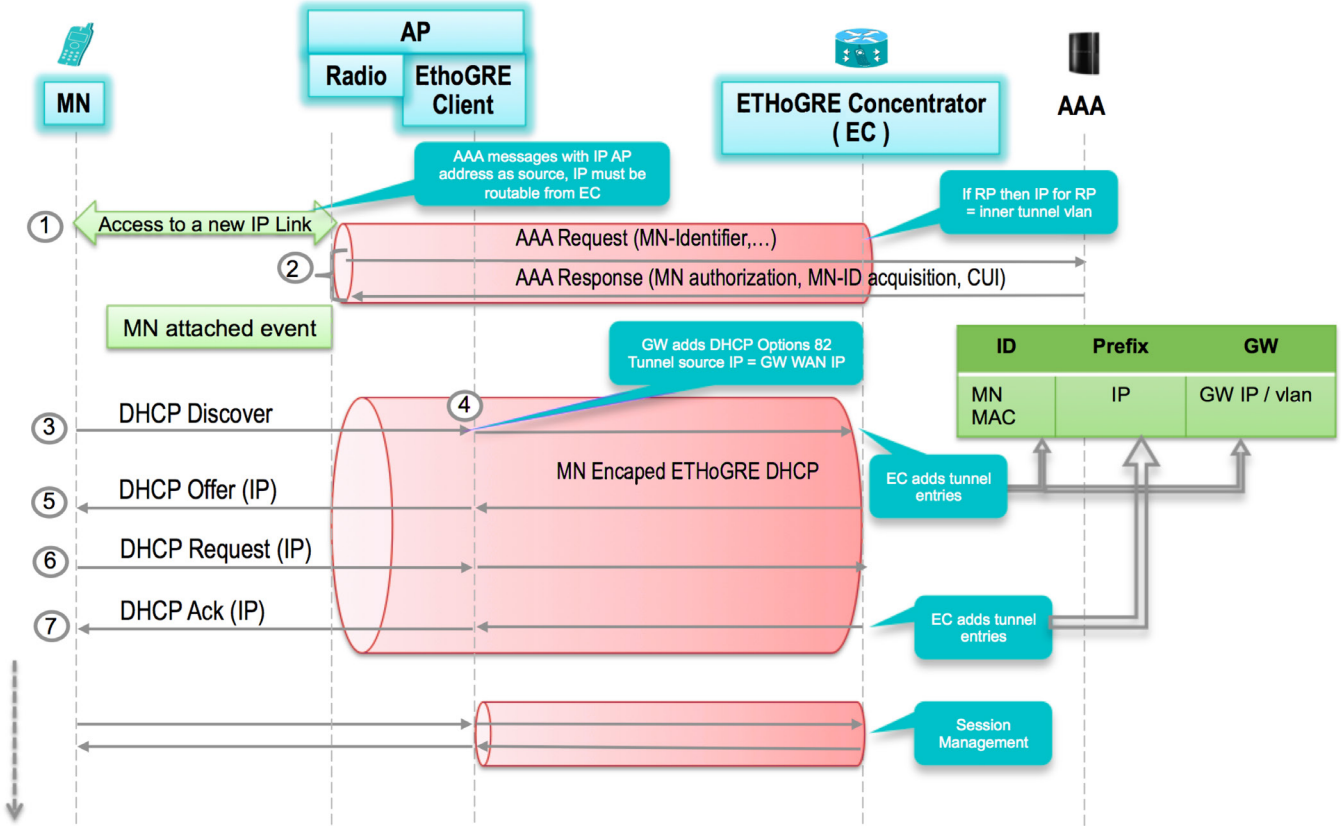


Figure 4.9 **Initial L2oGRE tunnel establishment for DHCPv4**

In the case of PMIPv6, the diagram is the following:

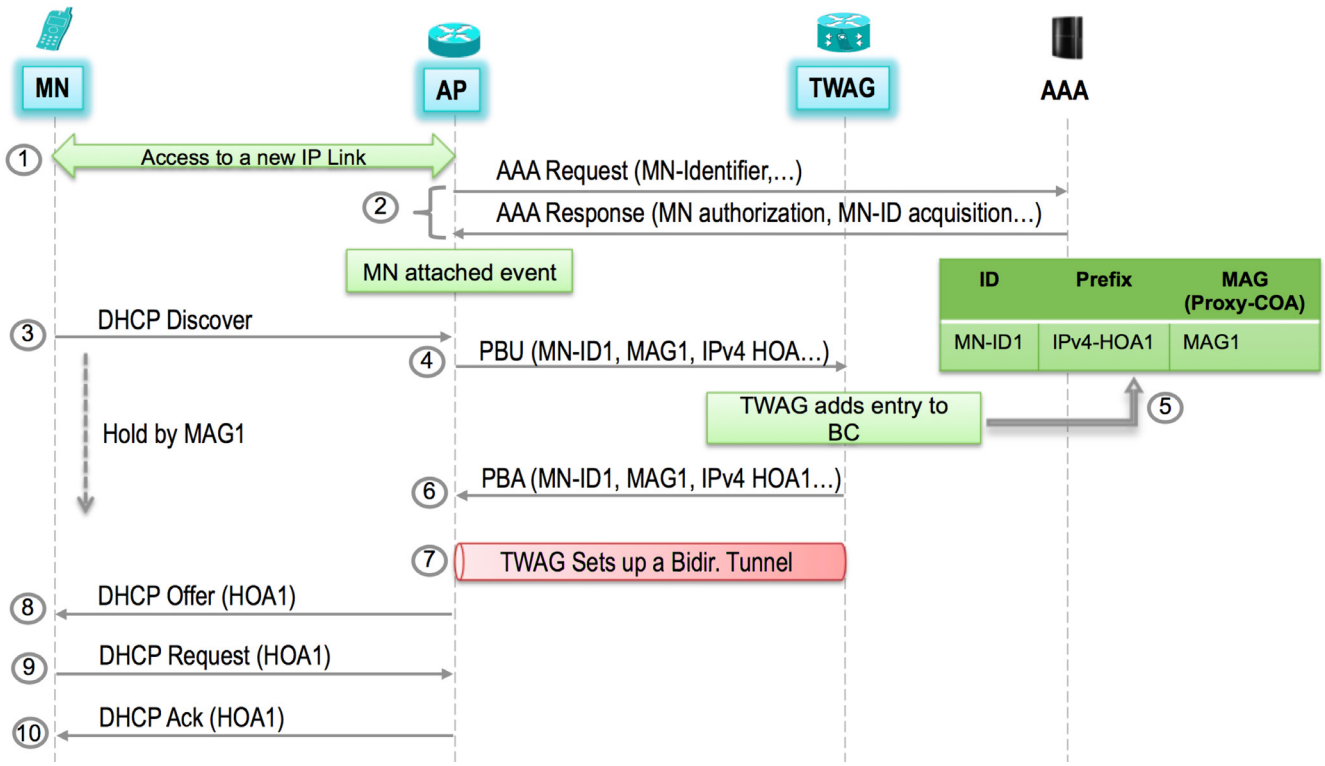


Figure 4.10 Initial L3oGRE tunnel establishment using DHCPv4

Architecturally, the fundamental differences between L2GRE and L3GRE include:

- Termination of the Layer-2 link which takes place at the AP level in the case of PMIPv6 (L3GRE) compared with L2GRE where the Layer-2 link is transported up to the TWAG.
- Control plane definition which is typically integrated into the L3GRE approach, using PMIPv6 signalling versus L2GRE which typically utilizes DHCP and/or RADIUS signalling

This difference induces some key implementation aspects which will be detailed hereafter for the understanding of the ISW1 interface.

In both cases every time a user attaches to an AP an authentication process takes place towards the AAA serving as TWAP. This allows the AAA to authenticate and authorise the user or not, based on identity and security policies. This TWAP then has a correlation capability between the user's MAC address and his identity.

The ISW3 interface in the case of ETHoGRE is key for the TWAG to know what policies to enforce for incoming traffic over the ISW1 tunnel as it only receives the user's MAC address and no other information related to this user over ISW1. The TWAP uses ISW3 to provide the TWAG with the corresponding parameters related to a MAC address. Note that the existence of the ISW3 interface assumes that the TWAG/TWAP functions are instantiated on two separate platforms. In many implementations, the ISW3 interface does not exist as the TWAG/TWAP functions co-reside on the same platform (refer to section 5.6).

In the case of PMIPv6 (L3GRE) the ISW3 interface is not necessary as in the case of L2GRE. The out of band PMIPv6 signalling from the AP to the TWAG is used to pass all necessary information the TWAG needs to handle the user's session. As an example the MAC address, even though not present in the L3 GRE encapsulated packets, is passed along the PMIPv6 proxy binding update, with an initial message from an AP to the TWAG and populated by the information the AP received in the RADIUS response from the TWAP.

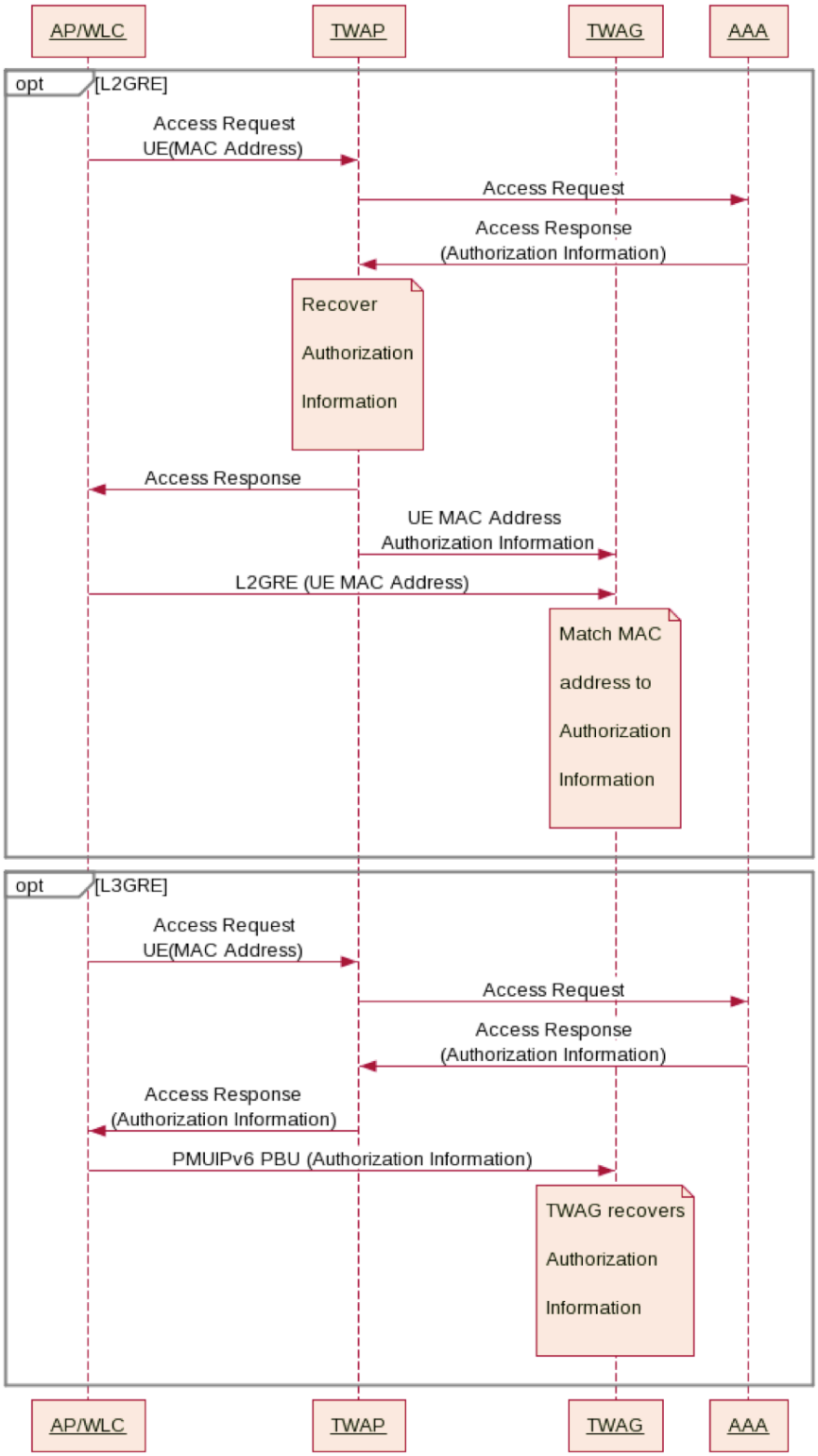


Figure 4.11 Comparing L2LRE and L3GRE handling of authorization information

Another noticeable difference lies in the handling of IP address assignment. In the case of ETHoGRE, a user's DHCP request is sent up to the TWAG. For an initial request 4 (DHCP), messages are necessary to be exchanged

with the TWAG to assign an IP address. A user will need to wait for the completion of this exchange, including the two round trip time delay between the AP and the TWAG; this is generally more centrally located in a network deployment. In case of PMIPv6 the four DHCP exchanges are local between the user and the AP and only a single round trip time delay is necessary between the AP and the TWAG.

For a user session, terminating a TWAG using ETHoGRE cannot result in knowing whether a user has left the radio coverage of an AP unless this information is relayed over ISW3 to the TWAG by the TWAP, which itself would identify this through some radius accounting originating from the AP towards the TWAP. In the case of PMIPv6, the information can be relayed directly from the AP to the TWAG using the out of band signalling mechanism.

The above examples were meant to highlight that even though the two models have different ways to manage a user's session, both need to correlate equivalent data between an AP, a TWAP and a TWAG. The control channels differ but in the end similar user session management functions are delivered. There are currently multiple network deployments utilising one or the other model.

1.11.3 ISW1b-Interface: AP-WLC data plane

Most deployments of carrier Wi-Fi networks today are deployed using access points which are managed by WLAN controllers. The protocol serving this purpose is defined by the IETF under RFC5415 and is known as control and provisioning of wireless access points (CAPWAP).

The CAPWAP protocol is defined to be independent of Layer-2 (L2) technology. CAPWAP assumes a network configuration consisting of multiple wireless termination points (WTP) communicating via the internet protocol (IP) to an access controller (AC). WTPs are viewed as remote radio frequency (RF) interfaces controlled by the AC. The CAPWAP protocol supports two modes of operation: split and local MAC (medium access control). In Split MAC mode, all L2 wireless data and management frames are encapsulated via the CAPWAP protocol and exchanged between the AC and the WTP.

The goals for the CAPWAP protocol are listed below:

a. To centralize the authentication and policy enforcement functions for a wireless network. The AC may also provide centralized bridging, forwarding, and encryption of user traffic. Centralization of these functions will enable reduced cost and higher efficiency by applying the capabilities of network processing silicon to the wireless network, as in wired LANs.
b. To enable shifting of the higher-level protocol processing from the WTP. This leaves the time-critical applications of wireless control and access in the WTP, making efficient use of the computing power available in WTPs, which are subject to severe cost pressure.
c. To provide an extensible protocol that is not bound to a specific wireless technology. Extensibility is provided via a generic encapsulation and transport mechanism, enabling the CAPWAP protocol to be applied to many access point types in the future, via a specific wireless binding. The CAPWAP protocol concerns itself solely with the interface between the WTP and the AC. Inter-AC and station-to-AC communication are strictly outside the scope of this document.

Though many vendors support CAPWAP access points and access controllers, each vendor implements its own CAPWAP extensions and proprietary features.

1.11.4 ISW2-Interface: AP/TWAP & WLC/TWAP control plane

The ISW2 interface is identical to the 3GPP Ta reference point (see section 3.1.1). However, 3GPP considers the specification of this interface to be out of its scope. There are multiple options currently seen in the industry:

- IPv4: no encapsulation is used
- GRE (L3GRE): IP packets are encapsulated in GRE tunnels, which may or may not use keying

- L2GRE (EoGRE): Layer2 over GRE (Ethernet over GRE), where the entire Ethernet frame is encapsulated in the GRE tunnel.
- QinQ (IEEE 802.1Q): stacked VLANs can also be used to encapsulate the packets.

In any case, all packets (radius, EAP, DHCP) for the ISW2 interface are encapsulated by one of the options above. When L2 GRE is used, the addressing elements of the protocol stack are used in the following fashion:

Layer	Addressing contents for uplink packets
Inner IP	Source IP: UE Destination IP: Outbound packet destination
VLAN (Optional)	
Ethernet	Source MAC: UE Destination MAC: TWAP
GRE Header	
Outer IP	Source IP: Wi-FI AP (or WLC) Destination IP: TWAP (GRE termination)
VLAN (Optional)	
Ethernet	Source MAC: Wi-Fi AP (or WLC) Destination MAC: IP Next hop device

Table 4.2 L2GRE addressing

1.11.5 ISW2b-interface: AP-WLC control plane

If the architecture includes a WLC, then the ISW2b interface becomes relevant.

The standard CAPWAP protocol is defined with IETF RFC5415. The main function of the CAPWAP protocol is to control and provision wireless (Wi-Fi in this case) access points.

When CAPWAP is used, all the protocols discussed in section 5.4 above are encapsulated within the CAPWAP protocol. In addition, the CAPWAP protocol is used by the WLC to establish sessions to each AP and to control them. CAPWAP defines messages and procedures for both control and user plane packets. CAPWAP control messages are encrypted using DTLS, while this is optional for the data plane.

The CAPWAP protocol contains control messages and procedures for:

- Access points discovering WLC
- DTLS session establishment
- AP configuration and provisioning
- Station (client) control from the WLC
- Keep alive procedures

1.11.6 ISW3-interface: TWAP-TWAG

When TWAG/TWAP components are realized separately and interconnected by ISW3 interface, the TWAP could serve multiple TWAG elements. However, for L2GRE implementations, signalling will be required between the two elements for the TWAG to be signalled the UE-specific policy (e.g., associated with QoS, accounting/billing, mobility, security). In such cases, all information the TWAP receives over the STa interface would need to be shared with the TWAG (e.g. UE-MAC, IP-address, attached-SSID, subscriber policy, billing requirements, incoming tunnel-ID, AP-ID). For L2GRE implementations, this information needs to be exchanged quite frequently (e.g. each attach/detach/profile update/mobility event) and depending on deployment scenario, may drive a very high amount of transactions/second. Since the data exchanged is used to directly manipulate a subscriber's data plane session, ensuring the data integrity of all parameters associated with the session is critical. However, to date, there has been little interest in defining a specific interface (ISW3) between these two elements.

While the TWAG and TWAP functions are logically separate, many implementations collapse the two functions on to the same platform. Functionally, a TWAG provides the instantiation of the individual user data plane sessions which includes ensuring forwarding rules, quality-of-service settings, accounting policies, etc. are applied on the traffic flow. Having the same element authenticate the user, receive the user policy/service configuration via AAA, instantiate the user and act as the policy enforcement point removes the complexity associated with configuring, maintaining and synchronizing multiple elements. It also eliminates additional signalling overhead between the TWAG/TWAP during session establishment, interim updates and session termination.

Whereas combining the TWAG and the TWAP eliminates inter element messaging defined by ISW3, it may remove the opportunity to individually scale the control and data plane functionalities. The lack of standardisation of ISW3 results in the requirement to use the same vendor for the TWAP and the TWAG, as proprietary synchronisation is required between the two in order to ensure the security aspects of mobility detection and many other features. Future efforts towards standardization of ISW3 could benefit the application of SDN/NFV techniques to TWAN.

5. Deployment consideration of TWANs

1.12 Closed/open access

In theory, “trusted” Wi-Fi deployments utilize closed-SSIDs and rely on 802.1x/EAP based authentication, e.g., using SIM-based authentication. However, in practice, commercial Wi-Fi deployments often offer Wi-Fi services to non-native users by way of an open, untrusted-SSID. As such, supporting both closed/open-SSIDs on the same Wi-Fi infrastructure is very common.

As previously mentioned, native users can connect to a closed-SSID via their existing SIM-based credentials (using EAP-AKA/AKA’/SIM methods). As these users are tied to an existing 3GPP AAA/HSS infrastructure, access can be managed via an existing data plan, or can be provided as complementary, “sticky” type service.

Open-SSID access is delivered differently from closed-SSID access in that network configuration is provided before the UE is actually authenticated/authorized.

For venue/open type applications, where Wi-Fi access is provided to all attendees (through either pay-per-use, or conditional free access), operators must allow an unknown user on to the network and direct them to a portal for registration, and optionally payment. As the open-SSID case involves attaching users to the network before authenticating them, often devices connect automatically to an open-SSID even though the user is not actually active. Though inactive, these users are consuming network resources and reducing overall network capacity. The TWAG/TWAP should have the intelligence to identify these users and handle them appropriately until they are active/registered.

Wi-Fi APs support the ability to host both SSID types simultaneously, and TWAG/TWAP implementations require same flexibility on the same platform.

1.13 RADIUS proxy

3GPP networks have heavily adopted DIAMETER for AAA functions throughout the mobile network, whereas other network types have relied on RADIUS for AAA functions. Wi-Fi access for closed SSID networks has typically relied on RADIUS to carry EAP-AKA/SIM credentials between the AP/WLC and the AAA server.

In many cases, AAA servers are capable of handling either RADIUS or DIAMETER AAA messages. Most Wi-Fi APs today authenticate UEs via RADIUS, so on a Wi-Fi network with a AAA server which supports RADIUS, the TWAP can provide a simple RADIUS-proxy function. For Wi-Fi APs supporting DIAMETER authentication, the TWAP can provide a DIAMETER proxy function. An interesting situation occurs when an AP supports RADIUS-based authentication, and the 3GPP AAA server supports DIAMETER. In this situation, RADIUS/DIAMETER translation is typically required by the TWAP such that RADIUS messages received from the AP are translated to DIAMETER, ensuring correct AVP translation.

1.14 Encryption

The security gateway (SeWG) is a function on the border of the IP security domains and can be used for securing IP interfaces when being transported over untrusted networks. The small cell network is architected to support multiple tunnelling protocols described in the sections above, hence authentication, integrity, confidentiality and overall security should be utilized to best fit the deployment architecture including remote security gateway access requirements.

When the small cell components are not closely integrated or need to deploy over untrusted networks, IP security (IPsec) and transport layer security (TLS) can be implemented and can be used to secure data and control traffic.

The following sections describe IPSec and TLS/DTLS (datagram TLS) security protocols for integrated small cell networks.

1.14.1 IPSec security

When IPSec security protocol is utilized, it shall only support encapsulating security payload (ESP) protocol. IPSec ESP protocol provides traffic encapsulation and tunnelling for transmission to and from a gateway with forwarding capabilities.

The IPSec protocol requires that both integrity protection/message authentication and anti-replay protection are always used.

The security services to be supported by IPSec shall provide:

- data origin authentication, mutual authentication
- data integrity
- confidentiality
- anti-replay protection

The network security key management functions should be supported by the internet key exchange V1 (IKEv1) (RFC-2407, RFC-2408 and RFC-2409) or internet key exchange V2 (IKEv2) (RFC-5996). The main purpose of IKEv1 and IKEv2 is to negotiate, establish and maintain security associations between parties so that they can establish secure connections.

Since security gateways are an integral part of the network architecture, tunnel mode shall be supported to allow the gateway to encapsulate and de-capsulate embedded payloads.

Only the ESP authentication algorithms mentioned in RFC 4835 shall be used. ESP shall always be used to provide integrity, data origin authentication, and anti-replay services, thus the NULL authentication algorithm is explicitly not allowed for use.

These requirements imply that the network elements must have a capability to generate random data. RFC-1750 gives guidelines for hardware and software pseudorandom number generators. Details of the IKE profiles and procedures are included in Annex-2.

1.14.2 TLS/DTLS Security

TLS and DTLS security are similar to one another. DTLS protocol is based on TLS (starting with TLS rel 1.1). Hence all security requirements defined in this profile apply to both TLS and DTLS protocols. The advantage of using DTLS and TLS is NAT traversal.

The DTLS protocol is designed to use UDP while TLS protocol is designed to use TCP.

DTLS/TLS security shall support with the following restrictions and extensions:

- SSL 3.0 as specified in RFC 6101 shall not be used as it is outdated
- At least TLS 1.1 as specified in RFC 4346 shall be supported
- TLS 1.2 as specified in RFC 5246 should be supported
- The highest TLS version supported on both endpoints shall be used
- The rules on allowed and mandatory cipher suites given in TLS 1.2 (RFC 5246) shall be followed. In addition, the mandatory cipher suite of TLS 1.1 (RFC 4346) shall be supported.
- The cipher suite TLS_RSA_WITH_AES_128_CBC_SHA256 should be supported. Cipher suites with NULL integrity protection (or HASH) shall not be used.
- When DTLS is used, it is mandatory that cipher suites with RC4 shall not be used. For TLS, it is recommended that cipher suites with RC4 should not be used.
- For TLS clients, TLS_RSA_WITH_NULL_SHA shall be supported and TLS_RSA_WITH_NULL_SHA256 should be supported. For TLS servers, if TLS cipher suites without

encryption are implemented, TLS_RSA_WITH_NULL_SHA shall be supported and TLS_RSA_WITH_NULL_SHA256 should be supported.

- For TLS compression, CompressionMethod.null as specified in TLS 1.2 is mandatory to support. Further compression methods as specified in RFC 3749 are optional to support.
- The key exchange method shall not be anonymous. Hence the cipher suites starting with "TLS_DH_anon_WITH_" as defined in TLS 1.2 are not allowed for protection of a connection.
- If TLS Extensions are used in conjunction with TLS, then for TLS 1.2 RFC 6066 shall apply, and for TLS versions lower than TLS 1.2 RFC 4366 shall apply.
- If pre-shared key (PSK) cipher suites are used in TLS, then RFC 4279 shall apply. The same rules as for RSA-based cipher suites shall apply, i.e. for all cipher suites "TLS_RSA_WITH_" is replaced by "TLS_PSK_WITH_".
- TLS session resumption based on RFC 5246 or RFC 5077 should be supported in TLS client and server.
- TLS servers and TLS clients shall support RFC 5746. The server shall accept client-initiated renegotiation only if secured according to RFC 5746.

1.14.3 Side-by-side comparative view of security protocols

Security features	IPSec, IKEv1, IKEv2	TLS, DTLS
Key management	ISAKMP, Diffie-Hellman key exchange	Diffie-Hellman key exchange, authenticated D-H
Authentication	Mutual authentication, using PSK, digital certificate, and EAP, XAUTH	Server to client: via X.509 certificate, PSK, client authentication is optional.
Integrity	Yes (see above list)	Yes (see above list)
Confidentiality/encryption	Yes (see above list)	Yes (see above list)
Anti-replay protection	Yes	Yes
Re-authentication	Yes	Optional

Table 5.1 Security protocol comparison

1.14.4 Computation resources to support cryptographic functions

Cryptographic operations, such as encryption, hashing, public/private key operations, and symmetric key generations, may require intensive CPU-based computation. It is recommended that such operations be modelled and tested to determine a baseline for the physical design, resource allocation and performance needed to support traffic by the small cell hardware. To strengthen security and accelerate performance, it is feasible that sensitive storage of cryptographic key, digital certificate and computation leverage hardware or firmware to alleviate bottle neck for such processing at the host OS level.

1.14.5 Security between ISW1 and ISW2 interfaces

Security protection should be implemented and is recommended for the interface between the Wi-Fi access point and the TWAG, similarly, between the Wi-Fi access point and the Wi-Fi controller, as well as between the Wi-Fi controller and the TWAG. The security protection should be assessed in light of the deployment configuration and device capability to determine which interface segment is vulnerable and requires protection.

It is feasible not to securely protect traffic on the ISW1, ISW1b or ISW2b interfaces if a deployment is securely guarded in a protected facility.

1.14.6 Deployment security between AP, WLC and TWAG

Implementation of security among the Wi-Fi access point, the Wi-Fi controller, the TWAP and the TWAG components to protect critical traffic is strongly recommended.

Traditionally, the control traffic within the small cell should always be protected with packet encryption or physical layer access protection or both, while data traffic between the access point, the controller and the TWAG is optional or can be protected with physical access protection if they are within close proximity.

When the Wi-Fi access points, the Wi-Fi controller and the TWAG are dispersed over a long haul or connected via a public IP network, it is strongly recommended that IP security be implemented using either IPSec or DTLS protocol to secure data transmission.

1.15 End-to-end QoS

An earlier SCF document, [53], discusses how QoS is provided for cellular EPS and GPRS connections. End-to-End QoS treatment can generally be provided to non-LIPA connections that use a cellular RAT to connect to the mobile core network. Currently, no standardized policy engine exists in the local network to facilitate providing QoS to LIPA connections.

Limited QoS mechanisms are in place for TWAN connections. As shown in Figure 4-2, the TWAN data plane connection is composed of the following segments:

a. The S2a interface between TWAG & PGW.
b. The TWAN internal interfaces ISW1/ISW1a between the AP & TWAG
c. The Wi-Fi radio interface between the UE & AP

Providing E2E QoS within the TWAN entails specifying QoS-markers on each of these interfaces and mapping QoS markings between the interfaces. Mapping between QoS markings on the 3 links can be achieved via operator defined tables.

QoS is established on the S2a interface when the TWAG obtains a bearer's QoS profile from the PCRF during the gateway control session establishment Procedure, [7]. The QoS profile that is obtained during gateway control session establishment can be used by the TWAG to determine how to mark uplink packets that are routed towards the P-GW. The TWAG may also use the QoS profile or the packet markings that were applied at the P-GW to determine how to treat downlink packets.

The TWAN internal interfaces, ISW1/1a, are typically over an IP-network, and use a tunnelling protocol (i.e. L2GRE/L3GRE/L2TP). QoS over the IP layer can be achieved via DSCP markings. Whether DSCP markings are respected by the routers in the IP network is a decision that is left to the TWAN operator.

Providing QoS on the 802.11 radio link is out of 3GPP's work scope. IEEE 802.11e has standardized mechanisms for providing QoS in WLANs. IEEE 802.11e introduced MAC enhancements for QoS prioritization in WLANs where transmission opportunities (TXOPs) are determined based on traffic priority. There are no known deployments of interworking between the 802.11e WLAN QoS with the 3GPP EPS QoS, and currently there are no standardized methods that allow the TWAN or EPS to provide the UE with QoS rules so that the UE can prioritize uplink Wi-Fi packets. EAP signalling between the UE and TWAN could be enhanced to provide QoS rules to the UE when the UE attaches or ANDSF signalling between the UE and ANDSF server could be enhanced to provide QoS rules when the UE obtains traffic offload rules the solution can rely on application level signalling to signal the UE with QoS related bearer requirements.

1.16 Legal interception

With respect to legal interception (LI) requirements, three different traffic routing scenarios need to be considered in the ISWN.

a. Traffic that is part of a PDN connection (3GPP or non-3GPP access) that is terminated at the P-GW.
b. 3GPP traffic that is locally offloaded by a local gateway (L-GW).
c. Non-3GPP traffic that is locally offloaded by the TWAN, i.e. non-seamless WLAN offloading (NSWO).

The scenarios above may be further complicated by the fact that the user may be mobile.

The LI requirements for traffic that is part of a PDN connection (3GPP or non-3GPP access) can be fulfilled by the PDN-GW as described in 3GPP TS 33.107 [54].The LI architecture for traffic that is offloaded via an L-GW is currently marked as an item for "For Further Study" (FFS) in 3GPP TS 33.107. This topic is currently being studied within the Small Cell Forum's NET and REG working groups and 3GPP's SA3 working group.

The LI requirements associated with NSWO traffic have received less attention; however, the requirements on such traffic may be similar to that of 3GPP traffic that is locally offloaded by an L-GW. The fact that NSWO traffic does not traverse the EPC suggests that an IAP in the TWAN may be needed.

The intercept requirements for traffic that is locally offloaded, by an L-GW or a TWAG, may also depend on whether the traffic stays in the local network or is routed by the local network towards the Internet.

Table 5.2 summarizes the traffic scenarios that require particular consideration with respect to LI.

Traffic type	Access GW	IAP	Note
3GPP	P-GW	S-GW / P-GW	Standard 3GPP PDN connection via a small cell.
Non-3GPP	P-GW	P-GW	Standard non-3GPP PDN connection via a small cell.
3GPP	L-GW	FFS	LI solutions are FFS in 3GPP TS 33.107.
Non-3GPP	TWAG	FFS	An LI solution for NSWO (TWAG) traffic may be based on an IAP in the TWAG.
Carrier Wi-Fi	WLAN GW	WLAN GW	Standard carrier Wi-Fi connection via a WLAN GW (i.e. the Wi-Fi access infrastructure anchor)

Table 5.2 Legal intercept scenarios

1.17 Coexistence with Hotspot 2.0

Wi-Fi Hotspot 2.0 technology can enable seamless discovery, authentication and connection to a Wi-Fi network similar to the way a mobile device discovers, authenticates and connects to a regular cellular network. The TWAN architecture can be extended to accommodate both existing Wi-Fi and new Hotspot 2.0 technologies.

The Hotspot 2.0's underlying IEEE 802.11U protocol supports access network query protocol (ANQP) which enables mobile devices to discover, query, identify, and automatically authenticate to such a network. The Hotspot 2.0 specification [55] also supports standards such as HTTPS, OMA DM, and SOAP protocols to facilitate provisioning of mobile devices with policy and credential to enable seamless user experience.

The existing TWAN network architecture depicted in Figure 2.3 is flexible to potentially accommodate Wi-Fi Hotspot 2.0 extension.

1.17.1 Joint architectures

The TWAN network needs access to the AAA service to authenticate Hotspot 2.0 users. It can leverage the same in-network AAA server or utilize an AAA proxy to forward authentication traffic to the AAA server in the network.

Additional functions proposed for the TWAN extension to support Hotspot 2.0 Rel 2 capabilities, with backward compatibility for Hotspot 2.0 Rel 1, are:

a. ANQP
b. Policy
c. Remediation
d. Online sign up
e. Certificate authority
f. AAA / AAA proxy

The proposed extension to the TWAN architecture to accommodate Wi-Fi Hotspot 2.0 is depicted in Figure 5.1.

The proposed architecture has the flexibility to implement and deploy new Hotspot 2.0 functions in the small cell unit, or in the network core, or partially in either locations.

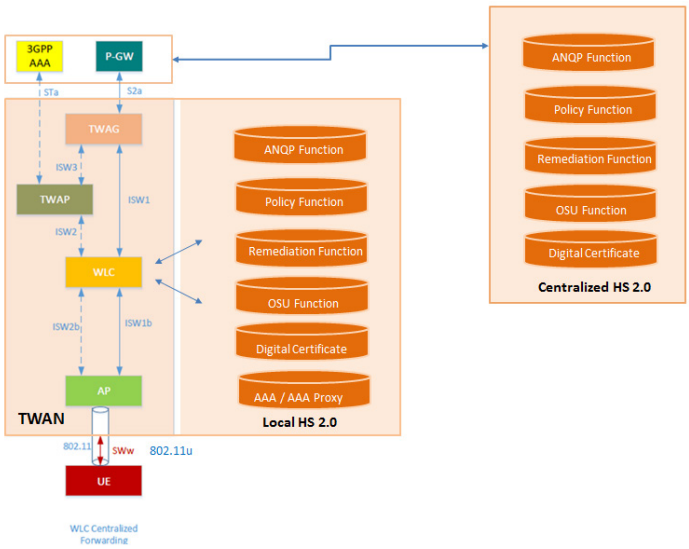


Figure 5.1 TWAN with Hotspot 2.0 support

A key improvement of using Hotspot 2.0 technology in the small cell architecture providing trusted Wi-Fi access is enablement and simplification of mobile policy provisioning for newer mobile devices equipped with Wi-Fi Alliance Passpoint compliant chipset and/or client agent.

1.17.2 Use cases and deployment options

- Use case 1: Hotspot 2.0 functions partially deployed in small cell network by a mobile operator. A local ANQP server is integrated in the small cell's Wi-Fi controller while other Hotspot 2.0 functional servers are deployed in the network. The mobile operator supports its subscribers and deploys Wi-Fi controllers without requiring the use of an external ANQP server.
- Use case 2: All server Hotspot 2.0 functions in network. Similar to the use case #1 with the exception that all functional servers are deployed in the network to optimize management and the Wi-Fi controller can access an external ANQP server.
- Use case 3: All server Hotspot 2.0 functions in the small cell. The policy, remediation and on-line signup, and local AAA server are provided by an enterprise or small Wi-Fi venue to allow visitors to access Wi-Fi for short duration.

The following table captures these aspects:

Hotspot 2.0 capabilities	Small cell extension	Centralized / network extension
ANQP server	Yes (*)	Yes (**)
Policy/credential server	Yes (*)	Yes (**)
Remediation server	Yes (*)	Yes (**)
Online signup server	Yes (*)	Yes (**)
Digital certificate / CA	centralized or public CA	centralized or public CA
AAA/AAA proxy server	proxy AAA, or local AAA	network AAA

Table 7-1 Comparison of deployment options

* - local deployment in small cell if there is no centralized deployment
** - centralized deployment to optimize instances of remote small cells/Wi-Fi HS 2.0

1.17.3 User authentication

The small, cell-trusted Wi-Fi architecture should support existing and upcoming Wi-Fi technologies, including multiple access control and authentication methods:

a. Existing Trusted Wi-Fi

- Wi-Fi access is based on Wi-Fi SSID identification with EAP-SIM/EAP-AKA/EAP-AKA' authentications.
- This method expects the handset or its software agent to configure a Wi-Fi profile in the mobile handset to utilize 802.1X/EAP when it comes in range of a specific SSID to exchange EAP based authentication.
- The handset and the Wi-Fi access point needs to support 802.11i security protocol.

b. Trusted Wi-Fi and Hotspot 2.0 Rel 1:

- The above capabilities, plus Wi-Fi Alliance Passpoint Release 1 compliant access using ANQP with EAP-SIM/EAP-AKA/EAP-TTLS/EAP-TLS authentications.
- Mobile devices or client agent should have advance access to a policy file populated with credentials manually created or downloaded in the mobile handset to utilize ANQP and 802.1X/EAP authentication protocols when the device comes in range of Hotspot 2.0 access point.
- In MNO-deployed small cells, EAP-TTLS/EAP-TLS authentications may be optionally provided to support subscriber or roaming devices without SIM/USIM credential.
- The handset and the Wi-Fi access point need to continue to support 802.11i security protocol.

c. Trusted Wi-Fi and Hotspot 2.0 Rel 1 and Rel 2:

- The above capabilities, plus Wi-Fi Alliance Passpoint Release 2 compliant access using ANQP with EAP-SIM/EAP-AKA/EAP-TTLS/EAP-TLS authentications, as well as SSID based connection with HTTPS/OMA/SOAP protocol to facilitate mobile policy provisioning and remediation.
- Mobile devices may redirect the user to sign up for a policy and credential for use in subsequent authentications.

1.18 Carrier Wi-Fi and business/enterprise Wi-Fi

The non-3GPP Wi-Fi access architecture defined in the small cell architecture allows secure tunnelling of control and user data traffic over the TWAP and TWAG paths to communicate with the AAA and the P-GW functions. This architecture provides trusted non-3GPP access via home network routing.

Carrier Wi-Fi can be deployed by a mobile operator to provide Wi-Fi access to its subscribers or partners' roaming subscribers. Venue Wi-Fi can be deployed by a commercial retailer or enterprise to provide Wi-Fi access to its customers and employees; this may not be tied to the same carrier Wi-Fi network, but can physically coexist.

There are relevant business use cases for a mobile operator with a TWAN deployment to support both carrier and Venue Wi-Fi accesses. As a result, user traffic can be directed in either of the following paths:

a. home network routing to access operator IP services, or
b. local break-out routing (or non-seamless offload) to support non-critical IP services as well as to alleviate network congestion.

The local break-out or venue Wi-Fi traffic should be supported in scenarios where local services are only available in the vicinity of TWAN unit deployment. Some example use cases are:

- direct access to location specific services, e.g., at an airport where services are available in the flight terminals, or
- captive audience access to local video clips at a sports arena, e.g., used as sponsored content before providing free internet access to users, or
- Wi-Fi intranet access by an enterprise, such as inside a public safety agency's building, serviced by a mobile operator. Its users can roam in and out of the macro cellular network, small cell network, and the TWAN's Wi-Fi network with Hotspot 2.0 policy, credential and authentication.

As Wi-Fi access becomes strategic for mobile operators and service providers, there are several viable Wi-Fi development options using conventional Wi-Fi or Hotspot 2 technology. The TWAN architecture should be able to support such deployments.

Moreover, WBA has developed the carrier Wi-Fi guidelines, which bring together nearly 20 large operators and vendors to participate in creating its definition. The WBA guidelines state that the following standardized carrier-grade Wi-Fi capabilities are needed to ensure networks can scale to meet the requirements of the industry:

- Consistent user experience
- Network discovery and access
- Authentication and security
- Service experience
- Fully integrated end-to-end network
- Network architecture
- End-to-end service provisioning
- Network management
- Network quality
- Network security
- Network manageability

For further information please consult the WBA carrier Wi-Fi guidelines [56].

6. Conclusions

It is now well-recognized that the data explosion the industry is currently experiencing, and that which is forecasted to continue to grow in the years to come, poses unprecedented challenges on wireless networks. No single network solution will be able to meet these challenges and the overall solution is widely believed to be a heterogeneous network comprising of multi-layered networks (macro-micro-pico-femto-small cell networks), networks for indoor & outdoor scenarios and networks operating in a broad range of spectral bands (including licensed, unlicensed & shared bands, as well as sub-6GHz and above-6GHz bands). Of chief importance among these is the integration of existing & evolving networks operating in the licensed and unlicensed bands, as well as developing new networks that seamlessly leverage licensed, unlicensed and shared spectral bands, with acceptable paradigms to coexist with legacy networks.

Integration of cellular and Wi-Fi Networks has been an area of study for over a decade, and yet has not been an easy problem to solve. While the benefits are easy to comprehend at a high level, there have been several hard challenges affecting several layers:

- The business models and players for cellular and Wi-Fi traditionally have been different.
- There are also profound differences in the services and user expectations for Cellular and Wi-Fi
- Deployment and Operational aspects also exhibit several fundamental differences for the Operators.
- At the network architecture level, there are key differences, such as the more centralized nature of Cellular Networks as opposed to the flatter & distributed nature of the Wi-Fi networks.

Recognizing such fundamental differences between the Cellular and Wi-Fi worlds, Small Cell Forum and Wireless Broadband Alliance came together to jointly engage the two technical and business communities in developing a common understanding of the challenges and solutions, in developing consensus positions and promoting agreed solution options. This white paper is the second achievement in our joint efforts, with the first being the formation & fostering of a working-level joint task force (JTF) of various stake-holders and the production of a comprehensive framework for the business and technical aspects of Small-Cell & Wi-Fi integration.

The current white paper focused on an architectural ‘gap’ that existed within the Cellular & Wi-Fi integration architectures, namely the internal architecture and external interfaces of the Trusted WLAN (TWAN). This piece of the end-to-end architecture was considered out of scope for all SDOs, including 3GPP, IEEE etc, and yet formed a key part of the overall architecture.

The SCF-WBA JTF successfully addressed this gap and has documented in this white paper a practically useful subset of architecture options, while providing an unbiased comparative assessment. It is hoped that the white paper will bring clarity of the options both to the operators considering the deployments, as well as to the vendors who are building equipment to drive these deployments.

The saga of cellular & Wi-Fi integration continues and, since the kick-off of the present white paper, we have witnessed several new developments, such as Wi-Fi Calling (based on 3GPP’s Untrusted Wi-Fi architecture), RAN-based Wi-Fi integration (e.g. 3GPP’s LWA initiative) and operation of LTE in unlicensed bands (e.g. 3GPP’s LTE-LAA). The SCF-WBA JTF will continue to track these developments and strive to provide clarity and guidance to the industry to make the vision of truly seamlessly integrated small cells and Wi-Fi a reality in the near future.

Annexes

A. IKE profiles & procedures

A.1 IPSec IKEv1 profile

With regard to the use of ISAKMP security associations for IKEv1 in the network domain security IP-networks the following is noted:

- Recommendation for network domain security IP networks requires support for ISAKMP SAs with pre-shared keys.

A.2 For IKEv1 phase-1 (ISAKMP SA):

- The use of pre-shared secrets for authentication shall be supported
- Only main mode shall be used
- IP addresses and fully qualified domain names (FQDN) shabe supported for identification
- Support of 3DES in CBC mode shall be mandatory for confidentiality
- Support of AES in CBC mode (RFC-3602 [29]) shall be mandatory for confidentiality
- Support of SHA-1 shall be mandatory for integrity/message authentication
- Support of Diffie-Hellman group 2 shall be mandatory for Diffie-Hellman exchange.

Phase-1 IKEv1 SAs shall be persistent with respect to the IPsec SAs which derive from it. That is, IKEv1 SAs shall have a lifetime for at least the same duration as does the derived IPsec SAs.

The IPsec SAs should be re-keyed proactively, i.e. a new SA should be established before the old SA expires. The elapsed time between the new SA establishment and the cancellation of the old SA shall be sufficient to avoid losing any data which is being transmitted within the old SA.

A.3 For IKEv1 phase-2 (IPsec SA):

- Perfect forward secrecy is optional
- Only IP addresses or subnet identity types shall be mandatory address types
- Support of notifications shall be mandatory
- Support of Diffie-Hellman group 2 shall be mandatory for Diffie-Hellman exchange

A.4 Key Length and support of AES transform:

Since the AES-CBC allows variable key lengths, the key length attribute must be specified in both a Phase 1 exchange (RFC 2409) and a Phase 2 exchange (RFC 2407). It is noted that the key length for use with the present implementation shall be at the minimum 128 bits.

A.5 IPsec IKEv2 profile

The internet key exchange protocol IKEv2 shall be supported for negotiation of IPsec SAs. The following additional requirements apply.

A.6 For IKE_SA_INIT exchange:

The following algorithms are listed with their names according to RFC 4307.

Following algorithms shall be supported:

- Confidentiality: ENCR_3DES
- Confidentiality: ENCR_AES_CBC with 128-bit key length
- Pseudo-random function: PRF_HMAC_SHA1
- Integrity: AUTH_HMAC_SHA1_96
- Diffie-Hellman group 2 (1024-bit MODP)
- Diffie-Hellman group 14 (2048-bit MODP)

For security reasons, the use of Diffie-Hellman group 2 (1024-bit MODP) is not recommended. If a larger group is available, it should be used.

The following algorithms should be supported if possible:

- Pseudo-random function: PRF_AES128_CBC
- Integrity: AUTH_AES_XCBC_96.

A.7 For IKE_AUTH exchange:

- The use of pre-shared secrets for authentication shall be supported
- IP addresses and Fully Qualified Domain Names (FQDN) shall be supported for identification
- Re-keying of IPsec SAs and IKE SAs shall be supported as specified in RFC 5996
- In addition to the requirements defined in RFC 5996, rekeying shall not lead to a noticeable degradation of service

A.8 For the CREATE_CHILD_SA exchange:

- Perfect forward secrecy is optional.

A.9 For Reauthentication:

- Reauthentication of IKE SAs
- A network element (SeGW) shall proactively initiate reauthentication of IKE SAs, and creation of its child SAs, i.e. the new SAs shall be established before the old ones expire
- A network element (SeGW) shall destroy an IKE SA and its Child SAs when the authentication lifetime of the IKE SA expires

A.10 MOBIKE with Multi-Homing

IKEv2 provides additional support for multi-homing and mobility security. MOBIKE protocol allows the IP addresses associated with IKEv2 and tunnel mode IPsec security associations to change. A secure session on one end of the network could use MOBIKE to keep the connection with the security gateway active while switching from one IP address to another. Similarly, a multi-homed host could use MOBIKE to move the traffic to a different interface if, for instance, the one currently being used stops working or the assigned IP address changes overtime.

References

[1] SCF049, “Backhaul Technologies for Small Cells”, Small Cell Forum,

[2] Cost savings and revenue benefits from Next Generation Hotspot (NGH) Wi-Fi, WBA White paper, September 2013

[3] Maintaining the Profitability of Mobile Data Services, WBA White paper, October 2012

[4] SCF067, “Enterprise Small Cell Architectures”, Small Cell Forum,

[5] SCF033, “Integrated femto-Wi-Fi Networks”, Small Cell Forum

[6] RP-132086, “Study on Multi-RAT joint coordination”, 3GPP http://www.3gpp.org/ftp/tsg_ran/TSG_RAN/TSGR_62/Docs/RP-132086.zip

[7] 3GPP TS 23.402, “Architecture enhancements for non-3GPP accesses”.

[8] 3GPP TS 33.210, “Network Domain Security (NDS): IP Network Layer Security”

[9] Richard Webb, Carrier Wi-Fi Offload and Hotspot Strategies and Vendor Leadership: Global Service Provider Survey, Infonetics Research, May 21, 2013

[10] Small Cell Forum, Small cell market status – Informa, June 2012

[11] SCF063, “Small Cell and Wi-Fi Coverage Study”, Small Cell Forum

[12] IEEE “TGn Channel Models”, 802.11-03/940r4 Sec 4.8

[13] “Integrated Wi-Fi/Picocell Platform Specification” , WR-SP-IWP-I01-120724, Cable Labs, http://www.cablelabs.com/wp-content/uploads/specdocs/WR-SP-IWP-I01-120724.pdf

[14] WFA, Hotspot 2.0 Technical Specification v1.0.0, https://www.wi-fi.org/hotspot-20-technical-specification-v100

[15] WBA, WRIX-L – Location Feed Format & File Exchange Standard v1.2 (January 2013)

[16] International Building Code. International Code Council. 2006. ISBN 1-58001-251-5

[17] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2012, IEEE, March 29, 2012

[18]: GSMA, TAP3.12 *GSM* PRD TD.57 v30.02 *Transferred Account Procedure* (*TAP*) *3.12*

[19] Klas Johansson, “Cost-Effective Deployment Strategies for Heterogeneous Networks”, KTH Communication Systems, 2007

[20] Heterogeneous Network Design – Evaluating Cell Spectral Efficiency, Keima Wireless, Mobile World Congress, February 2013

[21] RFC 5415, “Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Specification”, IETF, March 2009

[22] RFC 4251-3, “The Secure Shell (SSH) Protocol Architecture”, January 2006

[23] RFC 2784, “Generic Routing Encapsulation (GRE)”, March 2000

[24] Broadband Forum 2 words? TR-069, “CPE WAN Management Protocol (CWMP)”

[25] Broadband Forum 2 words? TR-196, “Femto Access Point Service Data Model”

[26] 3GPP TS 36.300, “Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2”

[27] 3GPP TS 23.234, “3GPP system to Wireless Local Area Network (WLAN) interworking; System description”

[28] RFC 5555, “Mobile IPv6 Support for Dual Stack Hosts and Routers”, June 2009

[29] 3GPP 23.261, “IP flow mobility and seamless Wireless Local Area Network (WLAN) offload”

[30] 3GPP TR 23.852, “Study on S2a Mobility based on GPRS Tunnelling Protocol (GTP) and Wireless Local Area Network (WLAN) access to the Enhanced Packet Core (EPC) network (SaMOG)”

[31] RFC 2131, “Dynamic Host Configuration Protocol”, IETF, March 1997

[32] RFC 4861, “Neighbor Discovery for IP version 6 (IPv6), IETF, Sept. 2007

[33] 3GPP TS 24.302, “Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks”

[34] OMA, “Enabler Release Definition for OMA Device Management”, OMA-ERELD-DM-V1_2

[35] 3GPP TS 24.312, “Access Network Discovery and Selection Function (ANDSF) Management Object (MO)”

[36] RFC 4186, “Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)”, January 2006

[37] RFC 4187, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”, January 2006

[38] 3GPP TS 33.234, “3G security; Wireless Local Area Network (WLAN) interworking security”

[39] RFC 5448, “Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')”, May 2009

[40] 3GPP TS 33.402, “3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses”

[41] GSMA WBA Wi-Fi Roaming Joint Taskforce White Paper

[42] 3GPP TS 29.212, “Policy and Charging Control (PCC)”

[43] IETF RFC 5648, “Multiple Care-of Addresses Registration”, October 2009

[44] RFC 6182, Architectural Guidelines for Multipath TCP Development, IETF, March 2011

[45] RFC 6089, “Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support”, IETF, January 2011

[46] SCF073, “Multi-Technology Small Cells” Small Cell Forum

[47] 3GPP TS 23.401, “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access”

[48] IETF RFC 6085, “Address Mapping of IPv6 Multicast Packets on Ethernet”, January 2011

[49] IETF RFC 5413, “SLAPP: Secure Light Access Point Protocol”, February 2010

[50] Broadband Forum WT-229 “Nodal Requirements for Interworking between Next Generation Fixed and 3GPP Wireless Access”

[51] CAPWAP Multi-Vendor Interoperability IETF Draft: http://tools.ietf.org/html/draft-ietf-opsawg-capwap-hybridmac-01

[52] 4G Americas, “Integration of Cellular and Wi-Fi Networks”, September 2013

[53] SCF & WBA, SCF-089, “NGH-based Integrated Small Cell Wi-Fi”, Feb 2014.

[54] 3GPP Technical Specification "3G security; Lawful interception architecture and functions (Release 13)", TS 33.107 V13.1.0 (2015-12)

[55] Hotspot 2.0 (Release 1) Technical Specification Package v1.0.0: https://www.wi-fi.org/file/hotspot-20-release-1-technical-specification-package-v100

[56] WBA Carrier Wi-Fi Guidelines: http://www.wballiance.com/wba/wp-content/plugins/download-monitor/download.php?id=80

Acronyms and Abbreviations

Abbreviation	Description
AAA	Authentication, Authorization and Accounting
AKA	Authentication and Key Agreement
AN	Aggregator Node
ANDSF	Access Network Discovery and Selection Function
ANQP	Access Network Querying Protocol
AP	Access Point
APN	Access Point Name
CAPWAP	Control And Provisioning of Wireless Access Points
CSG	Closed Subscriber Group
DHCP	Dynamic Host Configuration Protocol
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EoGRE	Ethernet over GRE
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
GGSN	Gateway GPRS Support Node
GRE	Generic Routing Encapsulation
GTP	GPRS Tunnelling Protocol
GW	Gateway
HLR	Home Location Register
HMS	Home NodeB Management System
HNB	Home NodeB
HSS	Home Subscriber Server
ID	Identity
IFOM	IP flow mobility
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISMP	Inter-system mobility policy
ISRP	Inter System Routing Policy
ISW	Integrated Small Cell Wi-Fi
L2GRE	Layer 2 over GRE
L2oGRE	Layer 2 over GRE
L3GRE	Layer 3 over GRE
L3oGRE	Layer 3 over GRE
LIPA	Local IP Access
LMD	Local Measurement Duration
LOS	Line of Sight
LTE	Long-Term Evolution
MAC	Medium Access Control
MAPCOM	Multi-Access PDN Connectivity
MCN	Mobile Core Network
MME	Mobility Management Entity
MNE	Mobile Network. Emulator
MSO	Multiple-System Operator
NAT	Network Address Translation
NDS	Network Domain Security
NGH	Next Generation Hotspot
NLOS	Non-line of Sight
NSWO	Non Seamless WLAN Offload
OAM	Operation Administration & Maintenance

Abbreviation	Description
OMA	Open Mobile Alliance
OSU	On-Line Signup
OUI	Organizationally Unique Identifiers
PDN-GW	Packet Data Network Gateway
PDN	Packet Data Network
PGW	PDN Gateway
PLMN	Public Land Mobile Network
PMIP	Proxy Mobile IP
PMK	Pairwise Master Key
RADIUS	Remote Authentication Dial-In User Service
RRM	Radio Resource Management
SaMOG	S2a Mobility Based on GTP & WLAN access to EPC
SA/DA	Source Address/Destination Address
SCF	Small Cell Forum
SC-GW	Small Cell Gateway
SDO	Standards Development Organization
SeGW	Security Gateway
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SIPTO	Selected IP Traffic Offload
SLAAC	Stateless Auto Configuration
SON	Self-Organizing/Optimizing Networks
SSH	Secure Shell
SSID	Service Set Identity
TAP	Transferred Accounts Procedure
TWAG	Trusted Wireless Access Gateway
TWAN	Trusted Wireless Access Network
TWAP	Trusted WLAN AAA Proxy
UE	User Equipment
VLAN	Virtual Local Area Network
WBA	Wireless Broadband Alliance
WCS	Wireless Communications Service
WLC	Wireless LAN Controller
WRIX	Wireless Roaming Intermediary eXchange

Participant List

Name	Company
Husnain Bajwa	Aruba Networks
John Mann	AT&T
James Teborek	Broadcom
Vojislav Vucetic	Broadcom
Sami Susiaho	BSkyB
Simon Ringland	BT Openzone
Steve Dyett	BT Openzone
Tao Sun	China Mobile
Zhou Naibao	China Mobile
Gaetan Feige	Cisco Systems
John Smith	Cisco Systems
Mark Grayson	Cisco Systems
Marco Spini	Huawei
Necati Canpolat	Intel Corporation
Balaji Raghothaman	InterDigital
John Tomici	InterDigital
Li Qing	InterDigital
Mike Starsinic	InterDigital
Pierre Lynch	Ixia
Tony Chiang	Mediatek
Jan Straznicky	Nokia
David Chen	Nokia
Mariusz Skrocki	Orange France
Nigel Bird	Orange France
Stefano Faccin	Qualcomm
Stuart Strickland	Qualcomm
Debjani De	Radisys
Renuka Bhalerao	Radisys
Upenra Praturi	Radysis
Carolyn Heide	Ruckus Wireless
Dave Wright	Ruckus Wireless
Steve Hratko	Ruckus Wireless
Prabhakar Chitrapu	SCF & AT&T
Dzung Tran	SmithMicro
Vaia Sdralia	Stoke
Qiang Zang	TWC
Bruno Tomas	WBA
Tiago Rodrigues	WBA

Editorial Team

Name		Company
Prabhakar Chitrapu	Chief Editor & Project Lead	SCF and AT&T
Tiago Rodrigues	Chief Editor & Project Lead	WBA
Bruno Tomas	Chief Editor & Project Lead	WBA
Jan Straznicky	Editorial team member	Nokia
John Smith	Editorial team member	Cisco Systems
Mark Grayson	Editorial team member	Cisco Systems
Gaetan Feige	Editorial team member	Cisco Systems
Pierre Lynch	Editorial team member	Ixia
Marco Spini	Editorial team member	Huawei
Mike Starsinic	Editorial team member	InterDigital
Carolyn Heide	Editorial team member	Ruckus Wireless
Dave Wright	Editorial team member	Ruckus Wireless
Dzung Tran	Editorial team member	SmithMicro