Next Generation Hotspot (NGH) - based Integrated Small Cell Wi-Fi (ISW) Networks White Paper

Version 0.26
Issue date:

About the Wireless Broadband Alliance

Founded in 2003, the aim of the Wireless Broadband Alliance (WBA) is to secure an outstanding user experience through the global deployment of next generation Wi-Fi. The WBA and its industry leading members are dedicated to delivering this quality experience through technology innovation, interoperability and robust security.

Today, membership includes major fixed operators such as BT, NTT Communications, Comcast and Time Warner Cable; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Google and Intel. WBA member operators collectively serve more than 1 billion subscribers and operate more than 1 million hotspots globally. They also work with international operators to drive innovation, deliver seamless connectivity and optimize network investments.

The WBA Board includes Arqiva, AT&T, BT, Boingo, China Mobile, Cisco, Comcast, iPass, KT, NTT DOCOMO Orange and Ruckus Wireless.

More information about WBA: contactus@wballiance.com

www.wballiance.com
www.twitter.com/wballiance

About the Small Cell Forum

The Small Cell Forum, formerly known as the Femto Forum, supports the wide-scale adoption of small cells.

Small cells are low-power wireless access points that operate in licensed spectrum, are operator-managed and feature edge-based intelligence. They provide improved cellular coverage, capacity and applications for homes and enterprises as well as metropolitan and rural public spaces. They include technologies variously described as femtocells, picocells, microcells and metrocells.

The Small Cell Forum is a not-for-profit, international membership organisation, with membership open to providers of small cell technology and to operators with spectrum licences for providing mobile services.

The Forum has 137 members including 63 operators representing more than 1.71 billion mobile subscribers – 33 per cent of the global total – as well as telecoms hardware and software vendors, content providers and innovative start-ups.

The Forum has three main aims:

- To promote adoption of small cells by making available information to the industry and the general public;
- To promote the rapid creation of appropriate open standards and interoperability for small cells;
- To encourage the development of an active ecosystem of small cell providers to deliver on-going innovation of commercially and technically efficient solutions.

The Forum is technology agnostic and independent. It is not a standards setting body, but works with standards organisations and regulators worldwide to provide an aggregated view of the small cell market.

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.

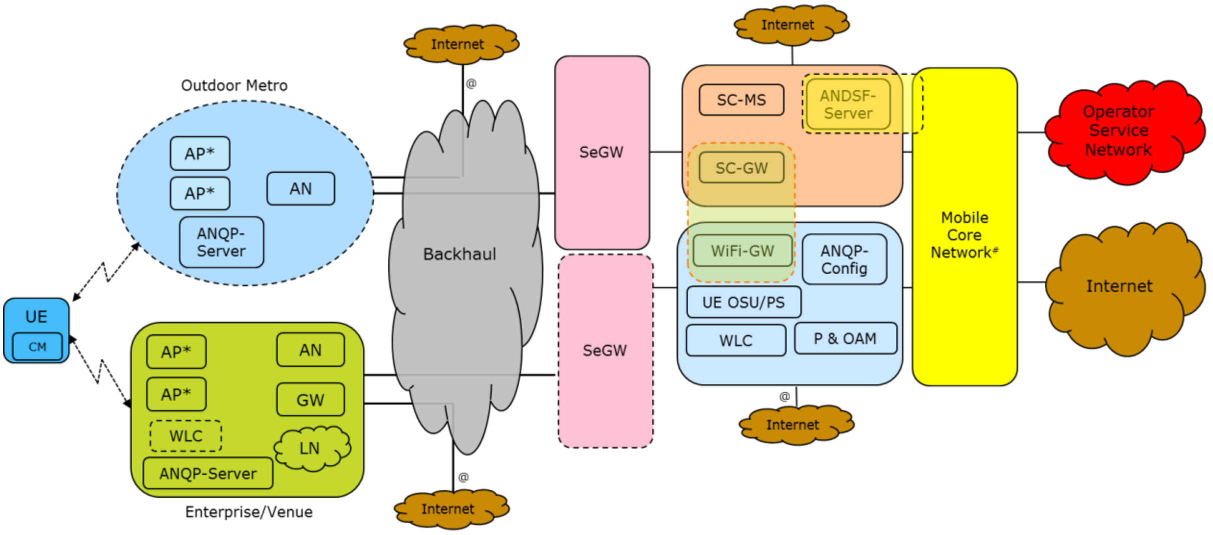
Contents

Executive Summary

This whitepaper represents the first deliverable from the collaboration between the Wireless Broadband Alliance (WBA) and Small Cell Forum (SCF) towards exploring the benefits, opportunities and challenges of the adoption of integrated networks based on Next Generation Hotspot (NGH) Wi-Fi and Small Cells technologies and standards. As a result, both organizations intend to put in place a common roadmap of joint activities to accelerate the industry adoption of this crucial technological evolution.

At a high level, this paper represents a broad view of the opportunities and challenges of integrating carrier-grade Wi-Fi, being driven by WBA's NGH initiative, and Small Cells, being driven by Small Cell Forum. It presents detailed accounts of use cases, architectures, network elements, network functions, exemplary implementations, as well as underlying standards. It also highlights a number of topics that deserve further study and some best practices. It is hoped that the SCF-WBA Task Force will initiate future projects based on these suggestions.

The paper starts by describing various Deployment Scenarios, classified according to Venue-type (Indoor/Outdoor, Enterprise/Venue), Purpose (Coverage/Capacity etc.), Business Reasons (cost savings/new services/etc.). It then proposes a high level framework for network architectures supporting integrated Small Cell and Wi-Fi (ISW) networks, shown below.



* SC or WiFi or ISW
@ Optional Breakout of Data Plane Traffic
SGW/MME/PGW; SGSN/GGSN; AAA/HSS; Billing

UE: User Equipment
AP: Access Point
AN: Aggregator Node
GW: Gateway
LN: Local Network
CM: Connection Manager

SeGW: Security Gateway
SC-GW: Small Cel Gateway
SC-MS: Small Cell Management System
WLC: WLAN Controller
WiFi-GW: WiFi Gateway
P&OAM: Wi-Fi RAN Provisioning & OAM
UE OSU/PS: Online Signup & Provisioning Servers for Wi-Fi UEs

The Architecture Framework identifies a number of domains, namely the Access Network domain, the backhaul domain, the ISW-Core Network Domain and the Mobile Operator Core Network Domain. Within each domain, a number of building blocks (or network functions) are identified, including: various types of Access Points (APs) and their characteristics; WLAN Controllers (WLC), Small Cell Gateways (SC-GW), Gateways for WLAN access to Operator Core Networks (Wi-Fi-GW for CN Integration) as well as NGH elements such as ANQP Server/Client & Mobile Operator Policy elements such as ANDSF Server/Client.

Focusing on the Integration of SC and NGH enabled Wi-Fi Networks, the paper next addresses various Integration Use Cases and Functions, such as: Intelligent Network Selection, Seamless Authentication, Simultaneous Connectivity to and Traffic Management across SC and Wi-Fi, User Mobility across an ISW (Integrated Small Cell Wi-Fi) networks, Online Sign-Up etc.

The paper further addresses network Architectures, examining first Integration Architectures, and then Trusted Wi-Fi Access Network (TWAN) architectures. It is hoped that the latter is especially useful given that there are currently no common industry-wide standards concerned with TWAN realization. The paper includes comprehensive documentation covering the broad landscape of the ISW networks. The paper identifies 6 areas deserving of further study, and potentially useful for driving the industry forward. They are:

- TWAN Architectures;
- ISW-Access Points;
- “Integrated” SON (Self Organizing Networks);
- Policy;
- Edge based Traffic Management; and
- Backhaul Sharing.

It is hoped that these topics will be pursued by the SCF-WBA Task Force as well as other similar organizations.

Finally, an annex to the paper includes a comprehensive discussion on various standards applicable to this ISW space. They include SDOs such as 3GPP, IEEE, Broadband Forum (BBF), IETF, Open Mobile Alliance (OMA) and CableLabs, as well as Industry Forums such as GSM Association (GSMA), W-Fi Alliance (WFA), WBA, SCF and Next Generation Mobile Networks (NGMN).

1. Introduction

The growth in the demand for wireless data traffic as a result of the mass adoption of mobile devices like smartphones, tablets, and gaming consoles, is putting increased pressure on mobile networks. The estimate for the evolution of the demand for data is huge, creating the need for operators to look at network densification as a core capability for serving the increased demand. In terms of densification options, Small Cells and Wi-Fi have been identified as key technologies for this purpose.

Both Small Cells and Wi-Fi technologies enable the delivery of increased capacity and coverage, including targeted network deployment to provide dark spot coverage, hot spot capacity in both indoor and urban scenarios, as well as improved quality of experience in conjunction with Macro Cell Networks (with the combination of Macro Cell and Small Cell often being referred to as HetNets).

Industry initiatives like the WBA’s Next Generation Hotspot (NGH) Program, WFA’s Passpoint Certification Program, SCF’s Integrated Small Cell Wi-Fi (ISW) Networks studies and the GSMA’s 3G Offload are examples of industry efforts to leverage Wi-Fi as a core part of the solution for the current and upcoming data demand, as well as to providing relief for the problem of spectrum congestion.

Leveraging the WBA´s track record in enhancing the Wi-Fi user experience together with insights into operator deployment and Wi-Fi rollout capabilities, together with the SCF’s track record in pioneering Small Cell technologies, standards and deployment practices, this white paper focuses on analyzing the Integrated Small Cell Wi-Fi Networks and possible streams of implementation.

The target audience for this paper includes (i) Mobile and Wi-Fi Operators, (ii) Integrated Operators, fixed and mobile, (iii) Infrastructure vendors, (iv) Mobile device vendors, (v) System Integrators and (vi) Other international organizations.

1.1 Scope and objectives of the NGH-based Integrated Small Cell Wi-Fi (ISW) Networks

At a high level, the purpose of this WBA and SCF joint whitepaper is to provide a description of the challenges of integrating licensed Small Cell Access-Points/Networks and un-licensed NGH-based Wi-Fi Access-Points/Networks, and highlighting methods by which those challenges may be overcome, including describing the various network nodes and functionalities involved, deployment aspects and typical use cases. The white paper provides recommendations and identifies gaps, thereby facilitating the promotion of the ISW-Networks by both organizations and thus lowering the barriers to adoption of ISW-Networks.

Specific objectives of this whitepaper are to (i) identify deployment solutions, (ii) overview the current use cases being considered by the industry, and (iii) discuss high level architectures for the solution.

The scope of the white paper includes:

- Small Cells: Mobile Operator owned and 3GPP defined 3G, LTE;
- Wi-Fi: (1) Mobile Operator owned and operated Wi-Fi; (2) Fixed Operator owned and operated Wi-Fi; (3) Customer/Venue-Owner owned and/or Mobile/Fixed operator Managed Wi-Fi;
- Integration: Small Cell and Wi-Fi technologies may be integrated at different levels, including: (1) SC and Wi-Fi APs Integrated in the same physical unit; (2) SC and Wi-Fi APs physically collocated (3) SC and Wi-Fi not physically collocated, but having common coverage; and
- Deployment: (1) Outdoor-Metropolitan (defined by SCF in its Release 3 as “Urban”), (2) Indoor-Enterprise, (3) Indoor-Public-Venue (e.g. Shopping Malls, Public Libraries), and (4) Open-Venues (e.g. Stadiums)

1.2 Deployment Scenarios

The deployment scenarios and aspects of ISW-Networks can be described along different dimensions.

Firstly, as alluded to in the Scope Section, the deployment scenarios for ISW-Networks may be characterized in terms of the different venue types:

Venue-based Deployment Scenarios:

(1) Outdoor-Metropolitan;

(2) Indoor-Enterprise;

(3) Indoor-Public-Venue (e.g. Shopping Malls, Public Libraries); and

(4) Open-Venues (e.g. Stadiums, Theme Parks).

Secondly, we may characterize deployments according to their purpose. The Small Cell Forum in its “Backhaul Requirements” white paper [1], classifies small cell deployment scenarios into four major categories, depending on their purpose being to enhance:

(1) Coverage (and capacity) indoors;

(2) Coverage outdoors;

(3) Capacity in (outdoor) hotspots; and

(4) Quality of Experience in (outdoor HetNets).

Similarly, Wi-Fi APs can be deployed for providing:

(1) Dark spot coverage (e.g. hotels, enterprises);

(2) Wide area coverage (e.g. campuses, communities); and

(3) Hotspot capacity (e.g. conference rooms, arenas).

Networks that integrate Wi-Fi and Cellular Networks in general, can and are expected to be deployed for providing relief from macro cell congestion, via Wi-Fi and small cell “offload” technologies. Here “offload” is used to refer to the offloading of the traffic from the macro cell and its associated RAN transport. In particular, Wi-Fi Networks integrated with Small Cell Networks can bring additional advantages of cost savings due to shared real-estate, power, backhaul and implementation as well as being able to access the increased spectrum allocated to un-licensed operation. Furthermore, new services and applications that leverage the integration of small cells and Wi-Fi are possible. These scenarios are described in the WBA whitepaper on “Cost Savings and Revenue Benefits from NGH” [2] and in the NGH whitepaper “Maintain the Profitability of Mobile Data Services” [3].

1.3 Integration Options

The following are possibilities for integrating Small Cell and Wi-Fi Networks, assuming that the small cell and Wi-Fi access are managed by a single MNO.

- Integration Option #1

  Co-location of small cell and Wi-Fi access points leveraging single site installation, i.e., using common power and backhaul facilities. In addition, the implementation of the SC and Wi-Fi Access Points may also leverage common hardware and software product features.

- Integration Option #2

  Integrated control by Mobile Core Network of access selection, authentication, and traffic management across ISWs and/or macro cells.

- Integration Option #3

  Integrated control by Intermediate Converged Small Cell Gateways supporting small cell and Wi-Fi access points performing selection, authentication and/or traffic management across one or more sites.

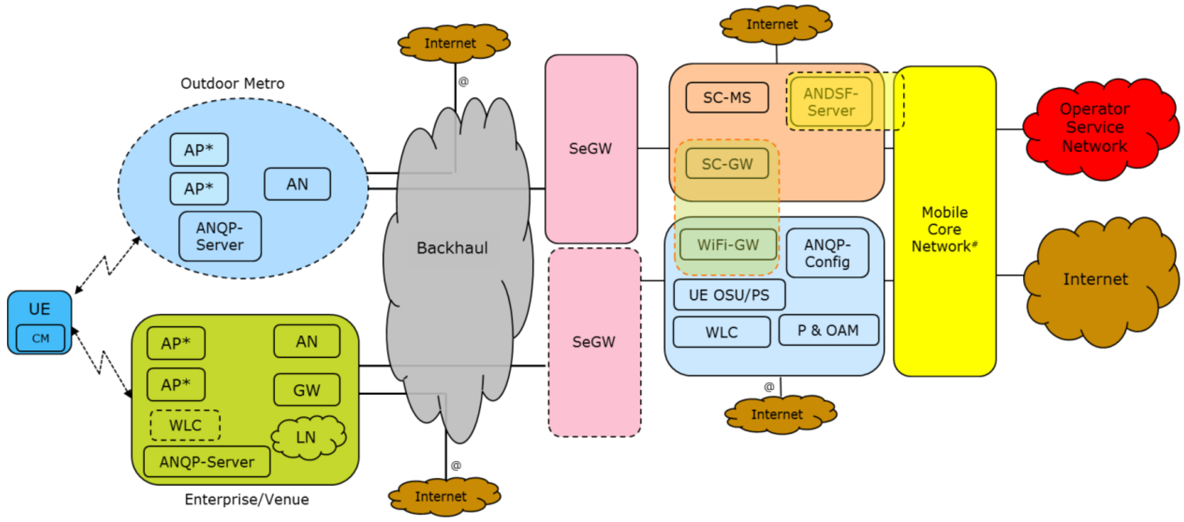
- Integration Option #4

  Integrated value-added functionality, e.g., combining small cell location analytics from licensed and un-licensed small cells, and/or local intelligence and decision-making features integrated into the ISW network.

- Integration Option #5

  Integrated Self Optimizing Networks (SON) capability that is able to optimize the combined resources of the ISW, e.g., being able to provide effective load balancing of traffic between Wi-Fi and Small Cell Access Points.

1.4 Deployment Framework



* SC or WiFi or ISW
@ Optional Breakout of Data Plane Traffic
SGW/MME/PGW; SGSN/GGSN; AAA/HSS; Billing

UE: User Equipment
AP: Access Point
AN: Aggregator Node
GW: Gateway
LN: Local Network
CM: Connection Manager

SeGW: Security Gateway
SC-GW: Small Cel Gateway
SC-MS: Small Cell Management System
WLC: WLAN Controller
WiFi-GW: WiFi Gateway
P&OAM: Wi-Fi RAN Provisioning & OAM
UE OSU/PS: Online Signup & Provisioning
Servers for Wi-Fi UEs

Figure 1: ISW Network Deployment Framework (Logical Framework)

Shown above in Figure 1 is a deployment framework for ISW-networks. Detailed architectures as well as definition of various network nodes can be developed within this framework.

From left to right in the above framework diagram:

1) Various types of User Equipment (UE) (also known as Stations/STA in Wi-Fi terminology) are used to access ISW networks. These may include SIM-based Cellular Devices; Certificate based Wi-Fi devices, etc. For UEs to work optimally in an ISW-Network environment, UEs typically have software functionalities known as Connection Managers, either natively integrated into the OS or delivered by a third party. These are used by the UE to select a Wi-Fi radio access according to a variety of criteria, e.g., user preference. Enhancements to such Connection Manager functionality are being discussed, for example, to enable the selection of the Wi-Fi network to take into account the loading conditions of the Wi-Fi network, and/or to intelligently “steer” the traffic between the licensed and un-licensed physical interfaces based on different criteria.

2) The access network portion of an ISW network would be made up of a network of APs, which is a term used generically to refer to either of the licensed Small Cell type or unlicensed Wi-Fi type or Integrated Small Cell and Wi-Fi type. APs may be deployed to provide outdoor metro coverage and capacity or deployed within a venue or Enterprise. Both deployment models may have an optional Aggregator Node (AN) function. The optional AN function concentrates the traffic from the APs to the Mobile Network and can also provide hierarchical mobility hiding, i.e., providing capabilities defined by SCF in their Enterprise Small Cell Concentrator (ESCC) function [4]. Various realizations for implementing the AN function are possible, including co-location with an access point, in a stand-alone element, or co-located with a gateway. Additionally, the Enterprise/Venue ISW-Network may also have a Gateway function to provide connectivity to an Enterprise/Venue Local Network (LN), including possibly IP-PBX functions. The data traffic from the Wi-Fi UEs may be carried back to the Mobile Core, or optionally be directly offloaded at the access network edge, taking into account any regulatory requirements that may need to be satisfied. Finally, the ISW access network may also include ANQP Server functions, which may be provided as part of the WLC or, in the case of autonomous APs, may be located in the AP. The ANQP server supports the Hotspot 2.0/NGH functions of Wi-Fi network discovery and selection.

3) The backhaul network connects the ISW access network to the Mobile and Wi-Fi Core Networks. The backhaul network itself may be realized using wired or wireless technologies. These networks may be private networks offering intrinsic security for the transport and referred to as “trusted” or public networks, which could be open and hence vulnerable to various attacks, and hence referred to as “un-trusted”.

4) The operator networks contain the essential elements for mobile communications. These will typically include perimeter security functionality, especially when providing access to ISW over untrusted backhaul networks. In such scenarios, Security Gateways may be optionally used to secure the communications between the ISW-AP and the operator network by the use of IPSec tunnels. While this method of securing the communication is standard for Small Cells (operating in the licensed spectrum), it is not mandated for Wi-Fi AP communication. Indeed, the securing of the Wi-Fi traffic may be achieved via alternate methods such as DTLS. This situation is depicted in the architecture framework, by the use of dotted lines for the SeGW between the Wi-Fi APs and the operator network. Of course, when an IPSec-SeGW is also used for Wi-Fi, it may be shared with the Small Cell AP traffic as well.

   Finally, when ISW networks are connected to the operator network via unsecure networks, such as the public Internet, the operator network is prone to various types of attacks, such as DOS attacks, etc. In order to protect the networks against such attacks, firewalls are often used.

5) The operator networks typically contain Small Cell Gateways (e.g. HNB-GW for 3G Small Cells) for providing connectivity to the Mobile Core Networks, as well as Small Cell Management Systems (e.g. HMS for 3G Small Cells) for provisioning and configuring the Small Cells. In addition, ANDSF-Servers may be used in operator networks to define policies for UEs in terms of their discovery and selection of Wi-Fi networks as well as for routing of traffic over the Wi-Fi and Cellular radio interfaces. These policies can be communicated to the UEs via 'push' or 'pull' methods.

   Similarly, operator/service-provider networks may also contain Wi-Fi related network elements, such as WLAN Controllers (for centralized control and management, including coordinated radio control features, AP provisioning, OAM functions and ANQP server functionality), as well as Wi-Fi-Gateways to connect to the Mobile Core Networks. The last of these are defined by standards bodies such as 3GPP. Finally, these operator/service provider Wi-Fi networks may also utilize centralized Online Signup and Provisioning Servers to allow users to self-provision/subscribe for service and to support operator policy within the client's Wi-Fi Connection Manager.

   As indicated in the Figure 1, the SC-GW and Wi-Fi GW may also be co-located (indicated by the dotted block covering both), in which case the SC-Wi-Fi integration functions may also be realized at the Gateway level.

6) The Small Cell Gateways and Wi-Fi Gateways provide connectivity to the Mobile Core Networks, which consist of mobility and data functions such as MME/SGW/PGW for EPC core networks (or SGSN/GGSN for UMTS Core Networks), which in turn provide connectivity to service networks such as Public Internet and/or Operator/Service-Provider Service Networks. Additionally, the Mobile Core Networks also contain Billing and User Authentication functions (via AAA servers and HSS database systems).

1.5 Emerging Frameworks

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 these are still either proprietary and/or in very early stages of standardization studies.

The architecture framework in Section 1.4 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.

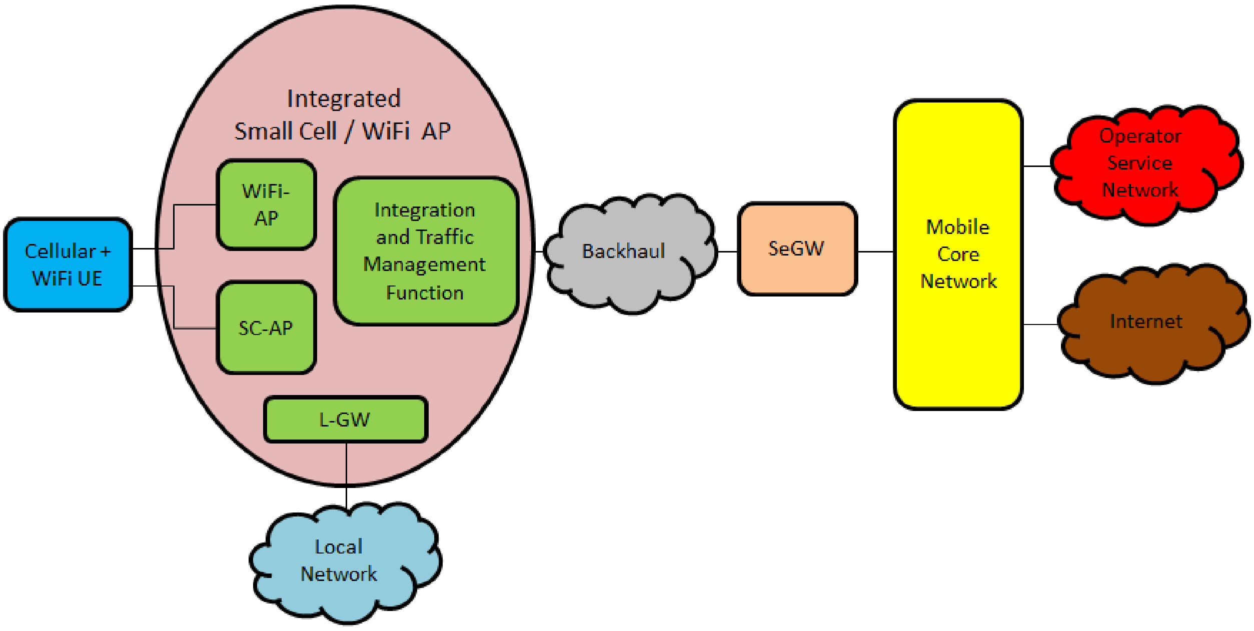


Figure 2: Integrated Small Cell / Wi-Fi Access Point

Here the Integration function resides at the edge, possibly in an integrated ISW-AP. RAN-based integration has been recently been taken up by 3GPP as a topic for a feasibility study [6]. The standardization study is in its initial stages and is expected to be completed by May 2014.

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.

2. Deployment Building Blocks

2.1 User Equipment (UE)

Currently in the industry there is no standard categorization of devices types. A common approach is to divide them by the following types:

- Mobile phone: Legacy phones with access to GSM/UMTS/LTE networks for voice and SMS usage mainly;
- PDA: Personal digital assistant, mainly used as personal companion;
- Smartphone: New generations phones that add capabilities of accessing data both from GSM/UMTS/LTE networks and Wi-Fi networks;
- Tablet: Larger size device, that addresses the data needs of end customers. Usually has Wi-Fi enabled chipsets and sometimes also cellular data chipsets;
- Laptop: full portable computer with Wi-Fi connectivity and in some cases with 3GPP as well, with ultra notebooks getting more popular due to their weight and performance; and

- Others: several handheld devices are becoming more popular and connectivity plays an important role on the user experience of these devices, like digital cameras, gaming consoles, mobile routers, for example.

Each of these types can be further categorized by the type of connectivity supported:

- Cellular only – Access to GSM/UMTS/LTE networks;
- Wi-Fi only – Access to WLAN networks;
- Cellular and Wi-Fi – Single access to either GSM/UMTS/LTE or WLAN networks; and
- Cellular and Wi-Fi – Simultaneous access to either GSM/UMTS/LTE or WLAN networks.

2.2 Access Network

As shown in Figure 1, the Access Network essentially consists of several APs. Depending upon the deployment, there may be an Aggregation Node (AN) for aggregating the small cell traffic. In other deployments the AN function may be integrated into the small cell. In case of Wi-Fi, the APs are generally assumed to be NGH capable, so that advanced Access Network Discovery is facilitated by the so-called ANQP-Server. When the APs are deployed in Indoor Enterprise/Venue environments, the Access Networks may also provide the Wi-Fi devices with direct connection to the local IP-Network. This direct connection may require the use of a local gateway function.

In this section, we shall discuss APs and ANQP Servers, while also describing key characteristics of the APs and their deployment aspects.

2.2.1 Access Point (AP)

APs in the access network portion of an ISW-network may be Wi-Fi only, 3G only, LTE only, or various integrated combinations such as Wi-Fi+3G, Wi-Fi+LTE, 3G+LTE, or Wi-Fi+3G+LTE. Each of these radios operate in a separate frequency band. For example, Wi-Fi operates predominantly in the 2.4GHz and 5GHz bands, whereas the spectrum licensed for 3G and LTE generally varies, depending on the country. When APs in the access network have integrated Wi-Fi/cellular capabilities, various levels of integration are possible, as described in section 1.3

When APs are of the integrated type, various levels of integration are possible. The simplest level of integration is one in which same physical enclosure includes separate modules and common power and backhaul services are provided to the Wi-Fi AP and Small Cell. Tighter levels of integration may include hardware integration (e.g., shared hardware for providing Wi-Fi and Small Cell functions) and/or software functional integration (e.g., common security functions) and/or logical integration (e.g., APIs between the small cell and Wi-Fi AP for sharing resource utilization information). Clearly, such features are vendor dependent at this point in time.

The Wi-Fi APs in an ISW network may be trusted or untrusted, as defined by 3GPP [7]. The provider of a trusted Wi-Fi access network has a trust relationship with the provider of the Operator/SP network, so that it can be authenticated by the Operator/SP Network and trusted communications can be established between the AP and the Operator/SP Network. In contrast, no such relationship is assumed to exist in the untrusted case. Furthermore, 3GPP’s Network Domain Security (NDS) architecture is based around a “hop-by-hop” approach [8]. This means that for the service to the trusted, the connection of the backhaul IP network also needs to be trusted. As a consequence, the presence or absence of trust has a major implication on securitization of the backhaul transport between the access network and the Operator/SP network. This backhaul transport may include integrated security techniques which provide an adequate level of protection, e.g., when the ISW Access Point includes an integrated DOCISIS 3.0 cable modem. Alternatively, when the backhaul network is determined to be unsecure, an additional layer of security can be applied. This can be achieved using various techniques, for example, by using secure tunnels such as IPSec tunnels, between the AP and the Operator/SP network, or employing transport level security such as TLS schemes between the Small Cell network elements. Finally, when the Wi-Fi access is deemed as being untrusted, the traffic needs to be protected all the way from the UE, if the device needs to connect to the operator’s core network. For example, IPSec tunnels may be used between the UE and the Operator/SP networks.

Identified Topics For Further Study: The fundamentally distinguishing aspect of optimal use for an integrated SC and Wi-Fi Access Point deserves further study. As indicated above, this includes joint software architecture (for example, SCF has alluded to defining APIs between the SC and Wi-Fi PHY/MAC HW/FW to upper layers as an extension of the popular Femto-API (or FAPI)), joint RRM, and APIs/Procedures for common use of location and possibly timing capabilities.

2.2.2 AP Characteristics

A May 2013 operator survey conducted by Infonetics, asked respondents to rate the importance of various features of Carrier Wi-Fi Access Points 0. Figure 3 shows the responses to the survey. While responses did not directly reference an ISW environment, a number of the features are directly or indirectly related to ISW deployments. Additionally, a number of the features listed apply equally to both licensed and unlicensed small cells.

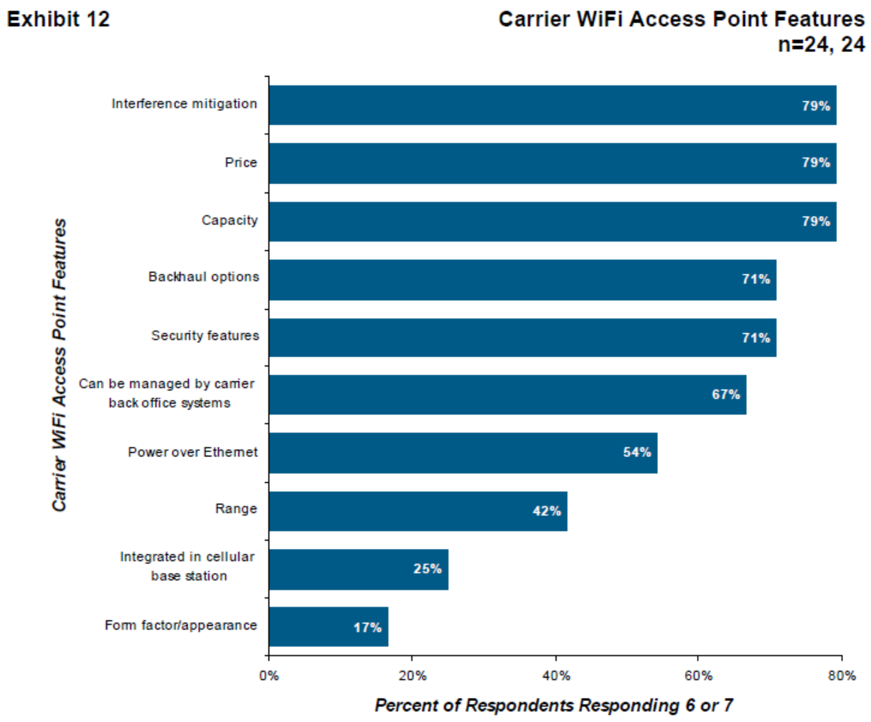


Figure 3: Carrier Wi-Fi AP Feature Priority1, 0

The two Wi-Fi AP technical capabilities rated most desirable by operators were 1) interference mitigation and Capacity, followed closely by 2) Backhaul and Security features. Interestingly, an operator poll conducted by the Small Cell Forum during 2012 [10], which asked respondents to answer “*What factor is most likely to*

[1] Reproduced with the kind permission of Infonetics

affect small cell deployment?”, yielded very similar results with the biggest challenge seen being Backhaul followed by co-existence with existing macro cells.

These ISW access network and AP characteristics are examined in the following subsections.

Spectrum Co-existence

Generalizing about the spectrum co-existence issues with ISW networks is complicated by the fact that over 40 frequency bands have been defined for operating LTE networks in different parts of the world. In terms of co-existence with globally allocated Wi-Fi spectrum in 2.4 GHz spectrum, Figure 4 illustrates the adjoining LTE frequency allocations. In particular, co-existence with high power down-link LTE transmissions in Band 40 and Band 41 is likely to require careful consideration.

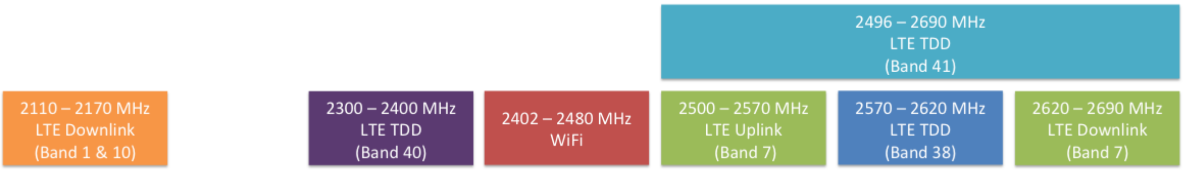


Figure 4: 2 GHz spectrum allocations for Wi-Fi and LTE

Interference Mitigation Techniques

As shown in the data included section 2.2.2, operators rank this as a top feature for both licensed and unlicensed small cell APs.

Licensed APs: The RF coordination of licensed small cell nodes with the macro layer, in both co-channel (single carrier) and multi-channel (multi-carrier) deployments, is a well-known technical challenge and the focus of much investment. Additionally, self-interference among Licensed APs must also be considered in dense deployments.

Unlicensed APs: Wi-Fi is an inherently interference prone technology as it operates in unlicensed bands. Historically the interferers tended to be other services operating in the same band (Bluetooth, Cordless Handsets, Microwave Ovens), but today the primary interferers are other Wi-Fi APs and stations operating on the same or adjacent channels. In fact, because of the pervasive deployment of enterprise and residential Wi-Fi in most urban settings, it is possible for an outdoor metro radio to “see” tens—if not hundreds—of individual WLAN networks occupying the same bands at the street level. Wi-Fi AP features that overcome and mitigate interference include:

Channel Selection: Wi-Fi operates in ~83.5MHz of spectrum in the 2.4GHz band, and more recently, in ~555MHz of spectrum in the 5GHz band. There are 3 non-overlapping 20MHz channels in the 2.4GHz band and 23 non-overlapping 20MHz channels in the 5GHz band (Note that IEEE 802.11n and IEEE 802.11ac can operate on bonded 40, 80 or even 160MHz channels). APs may possess the ability to assess the potential operating performance of each channel for each radio before assigning a channel for operation.

Channel Adaptation: The capability to determine that the current operating channel is no longer the optimal channel, and using an algorithmic determination, for the selection of a new channel for the service set. The AP may issue an IEEE 802.11h channel change notification to the associated clients advising them to switch operation to the newly selected channel.

Beamforming: Beamforming amplifies the RF signal for reception by a specific client. In an environment with a similar "noise floor", beamforming will yield a higher Signel-to-Interference Noise Ratio (SINR) at the client. There are two primary beamforming implementations, **transmit beamforming** and **adaptive antennas.** Transmit beamforming utilizes phase shifting of the same RF signal across multiple radios and antennas to amplify the signal towards a client. Adaptive antennas utilize multiple antenna elements (emitters and reflectors) that can be dynamically switched for each packet transmission so that a single radio's RF output can be focused towards a particular client. Beamforming also helps reduce interference in the neighbouring environment by focusing the RF energy towards the client and not towards other APs and stations in the area. Transmit beamforming and adaptive antennas can function additively as well.

Directional Antennas: The small cell coverage and capacity may be focused on the outdoor target area using directional antennas. This is a key capability in the outdoor urban environment where the objective is to add hotspot capacity along the busy streets and public gathering places. Typically, access nodes will need to be mounted to street furniture or the sides of buildings, and the ability to narrowly concentrate the beam down the street or to cover a sector of a city square is critical. In a dense urban environment, omni-directional antennas may result in sub-optimal coverage, creating interference and decreasing overall network capacity.

Modulation / Coding Schemes (MCS) and Rate Switching: It is important that a transmission between AP and client be performed at the highest possible data rate. This allows the stations to get on and off the air as quickly as possible, reducing the window during which interference could corrupt the packet and trigger a retransmission. APs may implement advanced rate switching algorithms that maintain the highest possible MCS rate given the client range and RF conditions.

Spatial Multiplexing: Spatial multiplexing increases the effective data rate to the client (again reducing the interference window) by sending multiple streams of data between the stations using two or more radios chains. Unlike transmit beamforming, each radio's signal is unique, which is necessary in order for the receiving station to receive and demodulate the multiple signals. For practical purposes this caveat makes spatial multiplexing and transmit beamforming mutually exclusive.

Transmit Power Control: Transmit Power Control (TPC) is used to regulate the power levels used by IEEE 802.11 radios. Originally mandated by the European Radiocommunications Committee (ERC) for use in 5 GHz, it is now commonly implemented in 2.4 GHz operation and across multiple regulatory regimes. TPC provides for the following:

- Stations can associate with an AP based on their transmit power;
- Designation of the maximum transmit power levels permitted on a channel as permitted by local regulations;
- An AP can specify the transmit power of any or all stations that are associated with the access point; and
- An AP can change transmission power on stations based on factors of the physical RF environment such as path loss.

APs with Overlapping Coverage: Wi-Fi APs that will be deployed in overlapping coverage with licensed small cell nodes, and especially those co-located with licensed nodes, may need to implement band-pass filters that attenuate signals in the operating licensed bands.

Integrated Small Cell Wi-Fi (ISW) APs: APs that will support both licensed and unlicensed radios may require additional co-existence filters for both the cellular and Wi-Fi radio chains, attenuating signals in the "foreign" band(s). Figure 4 illustrates some of the key licensed frequency bands where co-existence with Wi-Fi may be particularly challenging.

Capacity

The Small Cell Forum has recently published simulation studies that compare Wi-Fi and LTE performance [11]. The simulation studies have compared LTE and 802.11n Wi-Fi operating in 20 MHz channels, both single channel and multiple channels, and in sparse and dense deployments (2 or 4 APs). Because of the Listen-Before-Talk MAC, the overall throughput of Wi-Fi in this simulation is shown to be slightly less than can be achieved with the scheduled LTE MAC, as illustrated by these 2 AP results in Table 1.

Best Effort User Throughput (Mbps)	Power	Users per AP / Cell	Wi-Fi, 802.11n		LTE SU MIMO 2x2
			2.4 GHz	5 GHz	2.6 GHz
2 APs - Multiple Channels	21 dBm	10	9.67	9.49	12.17
2 APs - Single Channel	21 dBm	10	4.73	4.63	7.88

Table 1: Simulated user experience comparison between 802.11n and LTE (Source: SCF [11])

Note, in reality, the typical performance of the Wi-Fi and LTE portion of the ISW may be improved compared to the simulation studies of the SCF, in particular due to the use of:

- IEEE 802.11n is assumed in the simulation, compared with IEEE 802.11ac that is now being deployed. 802.11ac supports higher order modulation (256 QAM), mandates the use of aggregate frames (A-MPDUs), provides for much larger A-MPDUs, and standardizes sounding-based beamforming between AP and client. The result is that the maximum PHY rate for 1 and 2 stream 802.11ac in 20 MHz channels is 20-21% higher than for 802.11n.

- LTE Rel. 9 is assumed in the simulation, but many interesting features introduced with LTE-A (Rel.10) have been not simulated, like MU-MIMO with high-order MIMO schemes.

- 802.11ac will support Multi-User MIMO (MU-MIMO) in Wave 2 of the standard. This will allow a multi-radio AP to transmit to multiple clients simultaneously using beamforming.

- Wi-Fi Channel Bandwidths are restricted to be comparable with LTE. The case used of 20 MHz is typically only used in 2.4GHz, with 5GHz Wi-Fi installations typically using 40 or 80 MHz bandwidths. 802.11ac also supports 160 MHz channel bandwidth in Wave 2.

- LTE bandwidths are also restricted, and no carrier aggregation is assumed in order to provide a common framework, as dual carrier cells aggregate two 20MHz carriers.

- WiFi Antenna configurations are restricted to 2x2 to enable comparison with LTE, compared to the 3x3:3 and 4x4:3 that are typically deployed with 11n and 11ac.

Taking into account the above considerations, operators can be confident that Wi-Fi and LTE deliver a similar order of magnitude and ISW solutions will add capacity, specifically data capacity, to their networks. While this involves the 'densification' of the network with large numbers of licensed and unlicensed APs providing high throughput values indicated above, it is also imperative that the APs support large number of connected clients (especially mobile devices – handsets and tablets).

AP features that improve client capacity include:

Channel Selection and Adaptation: For APs the aggregate performance will be bound by the RF characteristics of the operating channel. Operating on a suboptimal channel limits overall capacity.

Small Cell Access Points typically include enhanced Self Organizing networks (SON) capabilities that are targeted at optimum network selection. Small Cell Access Points include distributed SON capabilities including “network listen” functionality to sense their environments. Channel Selection algorithms may operate autonomously, or be distributed to enable neighbouring small cell APs to share channel selection information, or be centralized where macro cellular configuration can be used to optimize channel selection.

Similarly, Wi-Fi vendors implement various techniques for channel selection in the presence of Wi-Fi and non-Wi-Fi interference. These channel selection algorithms may implement autonomously, or operate centrally to co-ordinate channel selection across the entire Wi-Fi access network.

High Data Rates: APs that can maintain higher modulation and coding rates with the same client connection parameters will provide higher overall capacity than APs using lower rate modulation and coding schemes.

ISW Access Points may include features such as transmit beamforming and adaptive antennas that can be used to provide the highest possible data rate.

Polarization Diversity: APs may implement both horizontally and vertically polarized antenna elements, utilizing this polarization diversity to enhance the signal received from mobile clients regardless of the client’s orientation.

Note, depending on the propagation environment, the channel between UE and ISW AP may be characterized as Non Line of Sight or Near Line of Sight, in which case the multi-path may enable limited polarization diversity to be realized with a single polarized antenna.

The IEEE 802.11 High Throughput Task Group found the gain from antenna polarization diversity to be on the order of 7-15 dB for Line of Sight environments and 3-5 dB for Non Line of Sight environments [12].

Backhaul Options

Backhaul options ranked near the top of operators’ priorities for both licensed and unlicensed small cell APs. At a high level, this can be seen as the flexibility for the AP to support various types of backhaul transport (fibre, copper, licensed or unlicensed wireless). [1] provides a comprehensive review of alternative technologies that can be used to backhaul ISW APs. Included in this analysis is the use of Wi-Fi mesh to backhaul Small Cell traffic, leveraging the fact that many outdoor Wi-Fi APs support integrated mesh backhaul, where a Wi-Fi radio link is used to backhaul the access traffic via another Wi-Fi node. It should be noted however, that one of the services that may be required to be supported by the backhaul network relates to synchronization distribution. As described in [1], the operation of meshed Wi-Fi backhaul links may limit the ability to deliver synchronization services to ISW APs. In such cases, alternative techniques may need to be used for providing synchronization services, e.g., using collocated GPS equipment.

Where ISW includes co-located unlicensed and licensed nodes, a unified backhaul supporting the control and data plane communication for both cellular and Wi-Fi radio access networks across a common backhaul link may be deployed. In this case, features may be required to enable the efficient sharing of the backhaul resource between the different licensed and un-licensed radios implemented in the combined ISW AP.

Identified Topics For Further Study: There are many aspects of shared backhaul between Licensed Small Cells and Wi-Fi APs. Examples includes, framing aspects, bandwidth sharing, COS support, etc.

Powering Options

Whilst most indoor APs provide the ability to be powered via their backhaul Ethernet interface, there does need to be careful consideration of the power consumed by the ISW APs. The standardized power over Ethernet profiles include:

- IEEE 802.3af that can deliver 15.5 watts of DC power to an attached device; and
- IEEE 802.3at that can deliver 25.5 watts of DC power to an attached device.

Support for higher powers over Ethernet currently requires the use of pre-standard implementations.

Alternative power options are available, e.g., where the ISW Access Point is backhauled over cable MSO services. CableLabs has defined the mechanical and power specifications for the deployment of an “Integrated Wi-Fi Pico” (IWP) Access Point [13]. The IWP specification indicates how the combined AP may be powered from CATV Plant Power, in which case the combined power consumption of the ISW AP should be less than 100 watts.

RF Coverage

Metro small cell networks, both licensed and unlicensed, are usually going to be deployed to provide capacity, or ‘densification’, to the existing macro cellular network. It’s important to keep this in mind as the design principles can be very different when the success of the deployment is based on the aggregate data capacity of the network and not on the extent of geographical coverage. For instance, when designing for capacity, RF barriers such as building exteriors or stadia section dividers can be leveraged to allow APs to operate in closer proximity to one another, increasing the overall capacity of the network. Another aspect related to such deployments is that lower operating power per small cell may increase the network’s capacity by supporting a larger number of APs in the same geographical area.

However, the RF coverage will depend on the transmitted RF power from the Access Point. From a regulatory perspective, the Wi-Fi portion and Cellular potion of any ISW Access Point may be subject to different restrictions. For example, the Wi-Fi regulations will vary on a region-by-region basis:

- In the United States, the Wi-Fi products must meet certain requirements, such as operation under 1-watt transmitter output power; and

- European countries and others covered by ETSI regulations place limit on the power output and EIRP. These regulations specify a maximum EIRP of 0.1-watt at 2.4 GHz.

From a licensed radio perspective, most of the countries have adopted the ICNIRP (International Commission on Non-Ionized Radiation Protection) levels as the norm. Using such a precautionary principle, some countries apply more stringent rules based on the ICNIRP recommendation.

Obviously, if the ISW deployment is required to offer similar coverage from both licensed and un-licensed radios, then consideration needs to be given to the effective regulations that may limit transmitter powers and/or EIRP levels.

2.2.3 Network Discovery

The Access Network Query Protocol (ANQP) is a query protocol used by Wi-Fi stations to discover information about the network prior to making a connection determination. ANQP can be used to discover detailed network information – beyond the limited information elements contained in beacons and probe responses. ANQP is the protocol upon which Hotspot 2.0/Passpoint™ and Next Generation Hotspot are built, and support for it is mandatory in those programs. Most of the ANQP information elements are specified in the foundational IEEE 802.11u specification, as illustrated in Figure 5, however a few ANQP elements have been added during development of the Wi-Fi Alliance’s Hotspot 2.0 Technical Specification.

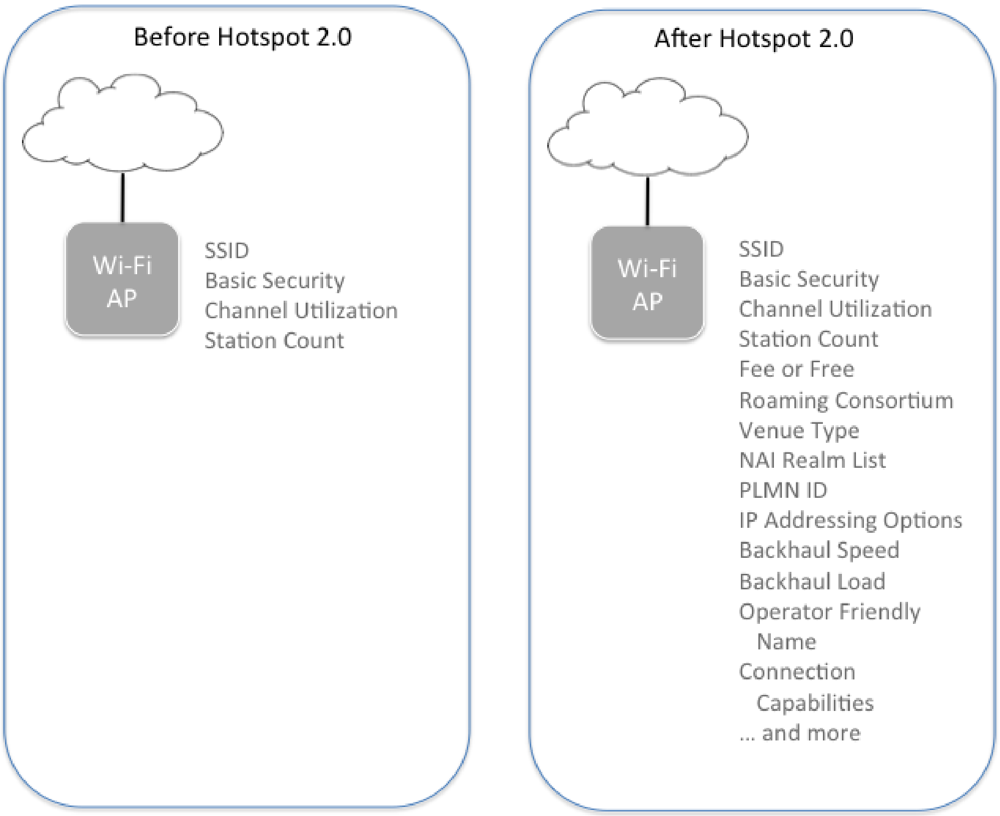


Figure 5: Example ANQP Information Elements

The ANQP Server is a functional element in the Wi-Fi RAN that responds to the ANQP queries initiated over the air by client devices. While neither the IEEE 802.11u nor Hotspot 2.0 specifications mandate the location of the ANQP Server, it is commonly implemented either directly on the Wi-Fi AP or on the Wi-Fi controller with the configuration of the ANQP/Hotspot 2.0 parameters performed via the UI of the centralized Wi-Fi controller.

Small Cell Network Discovery

Licensed small cells leverage conventional macro-cellular techniques for network discovery. Each small cell broadcasts one or more PLMN identities. The UE compares the received PLMN identity with that recovered from its own identity (IMSI) as well as possible preference lists and forbidden lists stored in its SIM card.

The definition of small cells has further enhanced the procedure with the definition of a Closed Subscriber Group (CSG). The CSG is provisioned in the UE and broadcast by the small cell and enables the UE to determine whether it is permitted to select a closed small cell which is then restricted to CSG-members only.

Typically CSG based access control will be deployed in residential small cell deployments but can be used to provide differentiated services in enterprise deployments.

Wi-Fi AP Discovery Process

The discovery of NGH-enabled Wi-Fi-APs is facilitated by two aspects of the NGH-technology. The first is the discovery information that is embedded into the beacon signals and the second is through an ANQP query process between the UE and the AP.

Normally, the UE's Wi-Fi radio wakes up periodically and scans for beacon signals. An NGH-enabled AP Beacon consists of the following discovery information elements:

- Internetworking element (identifying the AP as 802.11u capable);
- Network Type (SPs use this type fields to identify their hotspots);
- Internet Access bit;
- ASRA bit (indicates AP using Web-authentication or supports online sign-up); and
- Roaming consortium element (advertising hotspot owner Organizationally Unique Identifier (OUI) + top 2 roaming partner's OUIs).

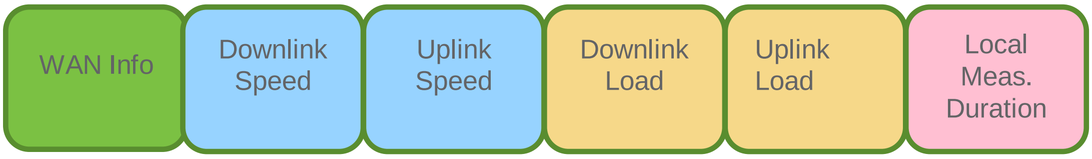
If the UE recognizes the recovered OUI, then it attempts association using security credentials corresponding to that OUI. If UE doesn't recognize OUI, then it initiates the ANQP-procedure and transmits a native-GAS query to retrieve:

- Roaming consortium list (remainder of OUIs that didn't fit in beacon element); and
- NAI Realm List (Realms are for hotspot operator or its roaming partners. List also provides supported EAP types).

The ANQP process also allows the device to query the AP and obtain WAN metrics. WAN metrics refer to quantitative metrics regarding the Wide Area Network that is used to connect the Wi-Fi AP to the SP/Operator's Service Networks. The main objective of the WAN metrics is to contribute to the decision process of selecting the best network to connect the end user when performing a query.

Note, the inclusion of WAN metrics in HS2.0 enhances the already available information that describes the channel utilization and device counts in legacy Wi-Fi equipment.

Technically, WAN Metrics provide information about the WAN link connecting an IEEE access network and the Internet. Transmission characteristics such as the speed of the WAN connection to the Internet are included. In particular, WFA specifies the WAN metrics as show in Table2 [14]:



WAN Info	Downlink Speed	Uplink Speed	Downlink Load	Uplink Load	Local Meas. Duration

Table 2: HS 2.0 Technical specification of the WAN metrics

If hotspot supports online sign-up (ASRA=1), then the UE checks if the Mobility Services Advertisement Protocol (MSAP) is supported at hotspot. If it is, then the UE can sign-up for service. If not, then mobile searches for another hotspot or remains on the cellular network.

2.2.4 AP deployments

Deployment of Licensed Small Cell-APs and Unlicensed Wi-Fi-APs share common challenges and requirements. Since the deployment of Wi-Fi-APs has an established history, we document various aspects of Wi-Fi-AP deployments, recognizing that most of the ideas also apply to Small Cell as well as ISW APs.

Currently in the Wi-Fi industry it is widely accepted that AP locations should fall into the following categories:

- Public;
- Private; and
- Hybrid (Community and/or enterprise).

For each of these categories the APs can be considered indoor (located inside a specific venue, propriety of someone) or outdoor (located in a public place accessible to any person).

Wi-Fi APs: Identifying Venue Deployments

For public APs, the industry is moving towards the adoption of a common standard that is aligned with IEEE 802.11u, base for the WBA WRIX-L (Wireless Roaming Intermediary Exchange for Location) [15]. This standard is also based on the International Building Code's Use and Occupancy Classifications, 0

Currently, venues are organized into the following Groups along with the corresponding Group Codes, 0

1	Assembly
2	Business
3	Educational
4	Factory and Industrial
5	Institutional
6	Mercantile
7	Residential
8	Storage
9	Utility and Miscellaneous
10	Vehicular
11	Outdoor
12 – 255	Reserved

Table 3: WRIX-L Venue Group Code & Venue Group Description, based on IEEE Std 802.11-20120

For each of these Groups, a number of Venue Types are assigned in 0. For example, the table below illustrates the Venue Type assignments for the Business and Mercantile Venue Groups:

0	Unspecified Business	0	Unspecified Mercantile
1	Doctor or Dentist office	1	Retail Store
2	Bank	2	Grocery Market
3	Fire Station	3	Automotive Service Station
4	Police Station	4	Shopping Mall
6	Post Office	5	Gas Station
7	Professional Office	6-255	Reserved
8	Research and Development Facility		
9	Attorney Office		
10-255	Reserved		

Table 4: WRIX-L Venue Type and codes, based on IEEE Std 802.11-20120

It is important for costumer care and billing purposes that the usage of this standard becomes a common practice adopted by operators. WBA WRIX-L is already aligned with this standard, and its members are already implementing it.

Note, GSMA Transferred Accounts Procedure (TAP) Records have been enhanced to carry information related to Wi-Fi accounting [18]. These records include the serving location description that must be present when reporting Wi-Fi usage when it contains a text description of the Wi-Fi Hot Spot or location, for example “London City Airport”.

ISW APs: Metro Deployments

With licensed small cells, AP placement usually begins with a decision about the small cell layer’s role relative to the macro layer; e.g. should the small cells be placed near the edge of the macro coverage so as to provide the most spectral efficiency, or should the small cells be placed as close to the demand as possible regardless of the macro layout.

On the other hand, Unlicensed Wi-Fi APs can be deployed as close to the demand as possible because there are no macro integration issues and the transmit power will tend to be lower than for licensed metro small cells (see section 2.2.2.9).

Demand Location: Outdoor metro demand is defined by the urban streetscape and involves corridors and pockets of heavy use. Tools are emerging to map this demand based upon such factors as social media use correlated with geo-tags. For example, Figure 5 illustrates the ‘heat map’ of the traffic in a downtown area highlighting that demand is very non-uniform. This aligns with various studies, e.g., [19] that observe that both population density and mobile telephony traffic are approximately log-normally distributed.

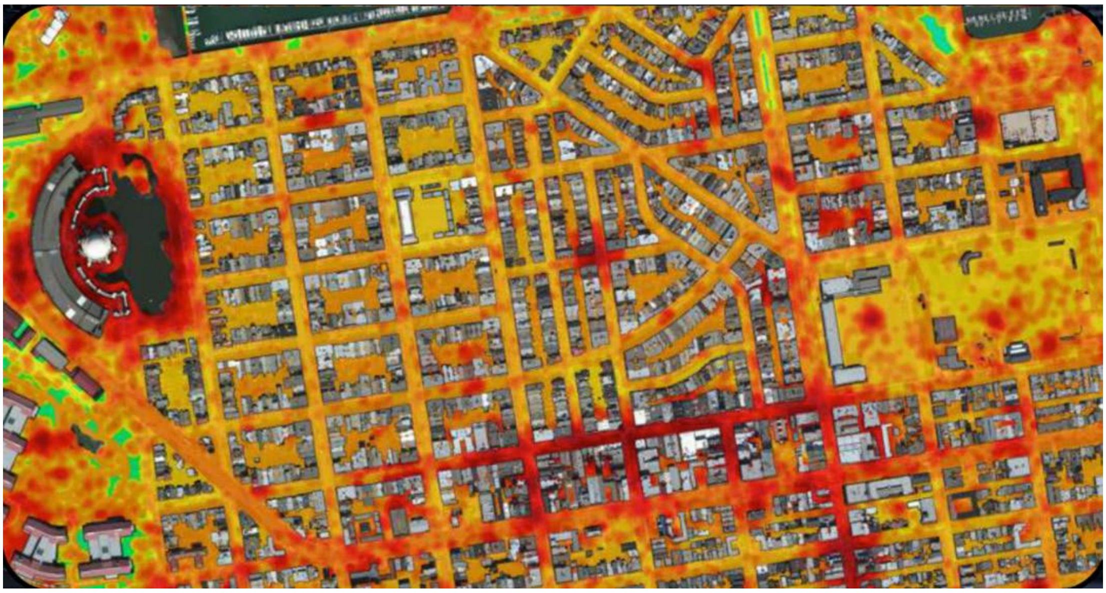


Figure 6: Outdoor Demand Example 2**Erro! A origem da referência não foi encontrada.**

Once the areas of greatest demand have been identified the AP location process moves to questions of site acquisition possibilities, backhaul options and aesthetics.

Site Acquisition: Described with terms like "land rush" or "the search for the Golden Lamppost", there is increasing evidence that in many urban environments there is an urgency to acquire the rights to prime AP locations that are proximate to the demand and afford good backhaul options. Fixed operators (especially the MSOs and Loop Cos) are also seeking to leverage their existing fibre or hybrid fibre-coax (HFC) assets by attaching APs directly to their plant, especially where that is aerially mounted. On the other side of the discussion will be the owners of the rooftops, walls and storefronts or the entity that controls access to the street furniture (e.g., local municipality).

Backhaul: Does the site provide easy access to fibre backhaul? If not, is there a LOS or NLOS path from the site that can be used for wireless backhaul? What is the average and peak demand expected for this site, and does the backhaul support that load?

Aesthetics: While AP aesthetics were not a primary concern of operators based on the Infonetics survey, 0, it may be a significant issue for many municipalities and venue owners. There is a growing focus on APs that are unobtrusive and meld easily into the environment in which they are deployed. Many APs are now available in a variety of different colours or can be painted to match their surroundings. APs with integrated antennas may also be preferred to those with multiple external antennas.

2.3 Core Network

By the term 'Core Network', we refer to the network elements that support the Access Network, provide network services and connectivity to service networks such as the Internet and Operator/SP Service Networks.

Referring to the Architecture Framework shown in Figure 1, we first focus on the Wi-Fi Network and discuss the key core network element, namely Wi-Fi Access Controller (AC). It must be noted that, although we

[2] Reproduced with the kind permission of Keima Wireless.

discuss the AC as a Core Network element, sometimes the Wi-Fi AC may be premised-based, especially where the venue has large number of APs deployed at the premise. Following this, we shift our focus to Small Cell Networks and elaborate on the SC Gateways.

Next we address the Integration of the Wi-Fi and Small Cell Networks and describe the key aspects of the WLAN Gateways, as well as ANDSF Servers which play a key role in the discovery, selection of and routing across the Wi-Fi and Small Cell APs.

2.3.1 Wi-Fi Network Architectures

In service provider networks, Wi-Fi APs are almost always deployed in conjunction with a Wi-Fi Controller (see Section 2.3.4). The two primary deployment models are local controller and centralized controller. Furthermore, the controller may process both the Control/Management Plane and Data Plane traffics or only the Control/Management Plane traffic.

Local Controller Architecture: Wi-Fi Controllers are deployed at the venue/Enterprise or at the metro level to provide management of the APs within a single Wi-Fi RAN. The number of APs managed by the local controller is typically in the tens or hundreds.

Centralized Controller Architecture: Wi-Fi Controllers are centralized at the operator's data center and provide management of the APs across a large number of Wi-Fi RANs administered by that operator, its subsidiaries, or wholesale partners. The number of APs managed by a centralized controller can scale to tens of thousands.

Figures 7 and 8 below illustrate these concepts, where it is assumed that both the Control Plane and Data Plane traffics are processed by the controller.

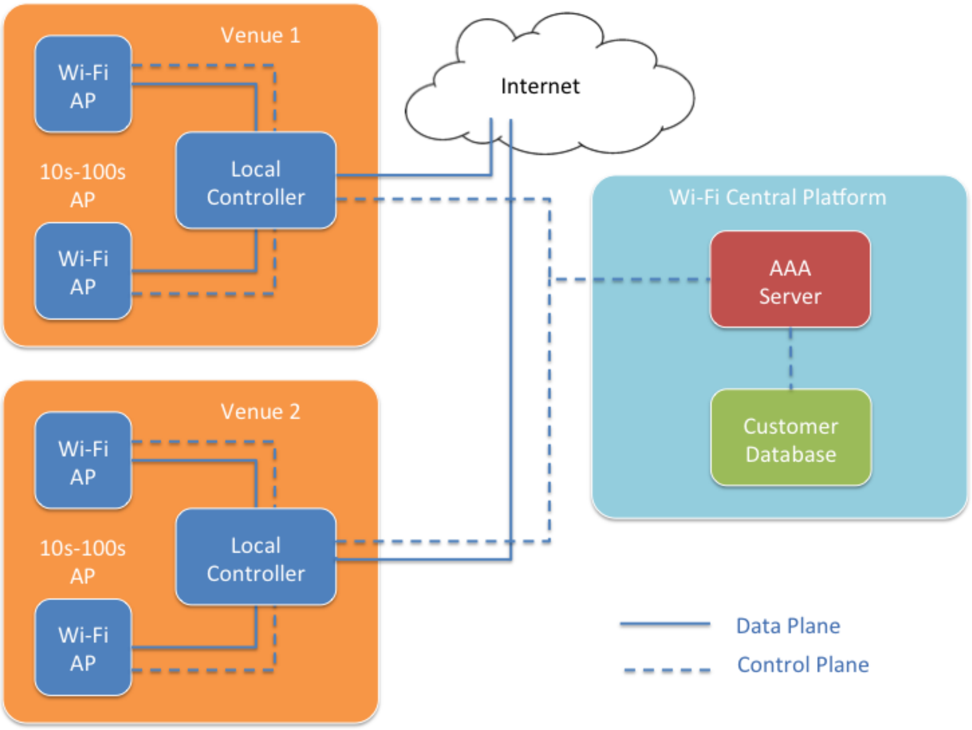


Figure 7: Local Control Wi-Fi Architecture

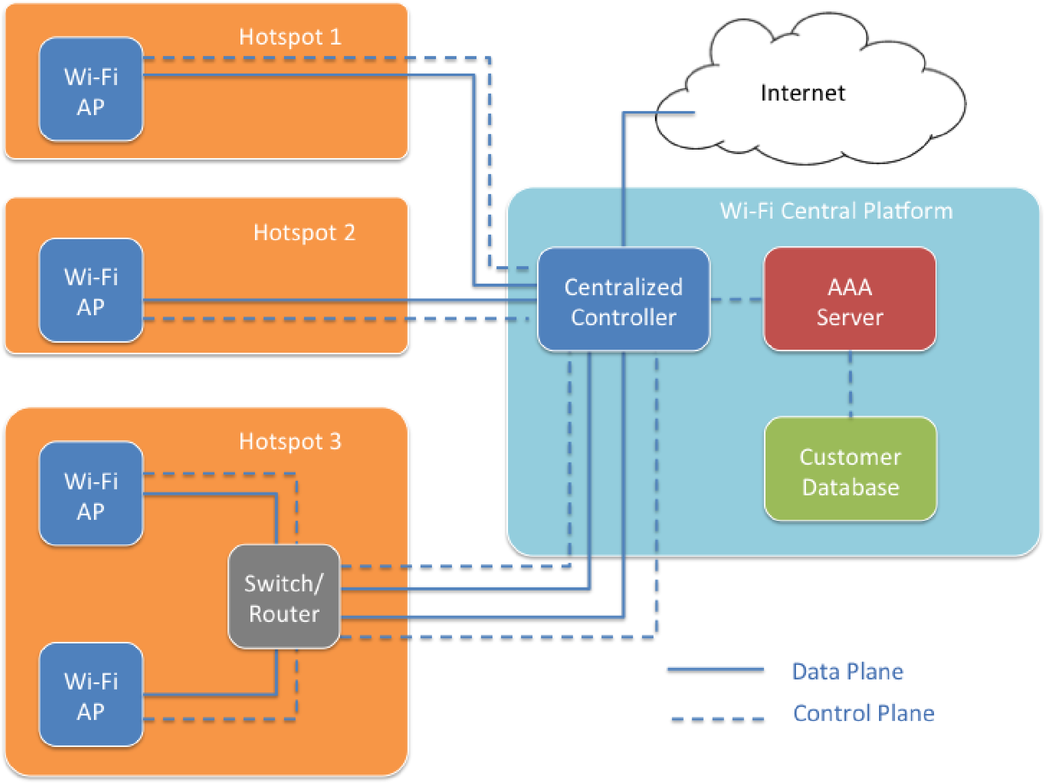


Figure 8: Centralized Controller Wi-Fi Architecture

Wi-Fi Access Controller

The Wi-Fi Controller provides centralized configuration, management and co-ordination of the Wi-Fi APs in the operator's network. When APs are added to the network they can learn of the controller(s) via a number of different discovery mechanisms and then request to register with the controller as a managed node. The configuration of the APs, Wireless LANs (WLANs), authentication and security services are all performed on the controller with the requisite information being disseminated to the affected APs. Controllers are also utilized to perform centralized co-ordination of the APs and overall RF configuration/optimization, with examples including channel assessment/assignment, client load-balancing, roaming facilitation, etc. Controllers, also provide the Wi-Fi RAN's centralized connection to external management systems, adjunct servers (e.g., AAA), and Wi-Fi Access Gateways.

There are three communication planes implemented in the Wi-Fi Controller and/or AP. The Management Plane is used to provide administrative access to the controller and also supports communication with external Network Management Systems. It provides functionality to support firmware management, gathering statistics, logging and debugging. The Control Plane is used for registration, configuration and monitoring functions and is implemented on both the controller and APs. The Data Plane is used for forwarding client data traffic to and from the Wi-Fi access network. In a *centralized forwarding* architecture the data plane is implemented on both the controller and APs and the controller plays a central role in data plane forwarding, while in a *distributed forwarding* architecture the data plane is only implemented on the AP and the controller does not participate in data plane forwarding. In the former case of centralized forwarding, the controller will also typically manage inter-AP mobility, thereby masking the mobility management of a device as it roams between different Wi-Fi Access Points from upper layers and achieving a hierarchical mobility management solution.

Vendors have based their controller to AP communications upon protocols such as CAPWAP [21], SSH [22], and GRE [23]. Whereas the baseline CAPWAP protocol was multi-vendor interoperable, implementations have typically used vendor proprietary extensions to extended the original protocol to support enhanced control and data plane requirements and features. This has resulted in a situation where there are no common interoperable controls or data plane protocols to provide standardized communication and services between the controller and APs.

In a Carrier Wi-Fi environment the critical characteristics of the control and data planes include:

- **Security** – The communication between the controller and the AP should be encrypted using a robust security mechanism. This is an absolute requirement for the control and management planes, while it may be optional for the data plane.
- **Scalability** – With operators looking at deployments in the tens of thousands of APs, the control and data planes must be able to scale, with the controller(s) being the consolidation point. Vendors have many approaches to this challenge, in terms of the protocol implementation and the controller architecture.
- **Reliability** – Protocol and controller architecture are critical to ensure there are no disruptions in services. Again, there are various vendor-specific implementations at both the protocol and controller level.

In contrast to the proprietary nature of the control and data plane protocols, the northbound management plane from the controller utilizes standard protocols, such as SNMP, SYSLOG, FTP, etc., in order to ensure interoperability with third party management systems and adjunct servers.

Controllers may have dedicated hardware interfaces to support these various communication planes or consolidate them over a single interface. In an operator environment, controllers are almost always deployed in a redundancy configuration which might be an active-standby pair or a cluster of controllers with active-active failover.

An Infonetics Carrier Wi-Fi survey from May 2013, 0, asked operators to rank controller features. As Figure 9 below shows, advanced RF coordination and scalability were considered to be the two most important capabilities in this survey.

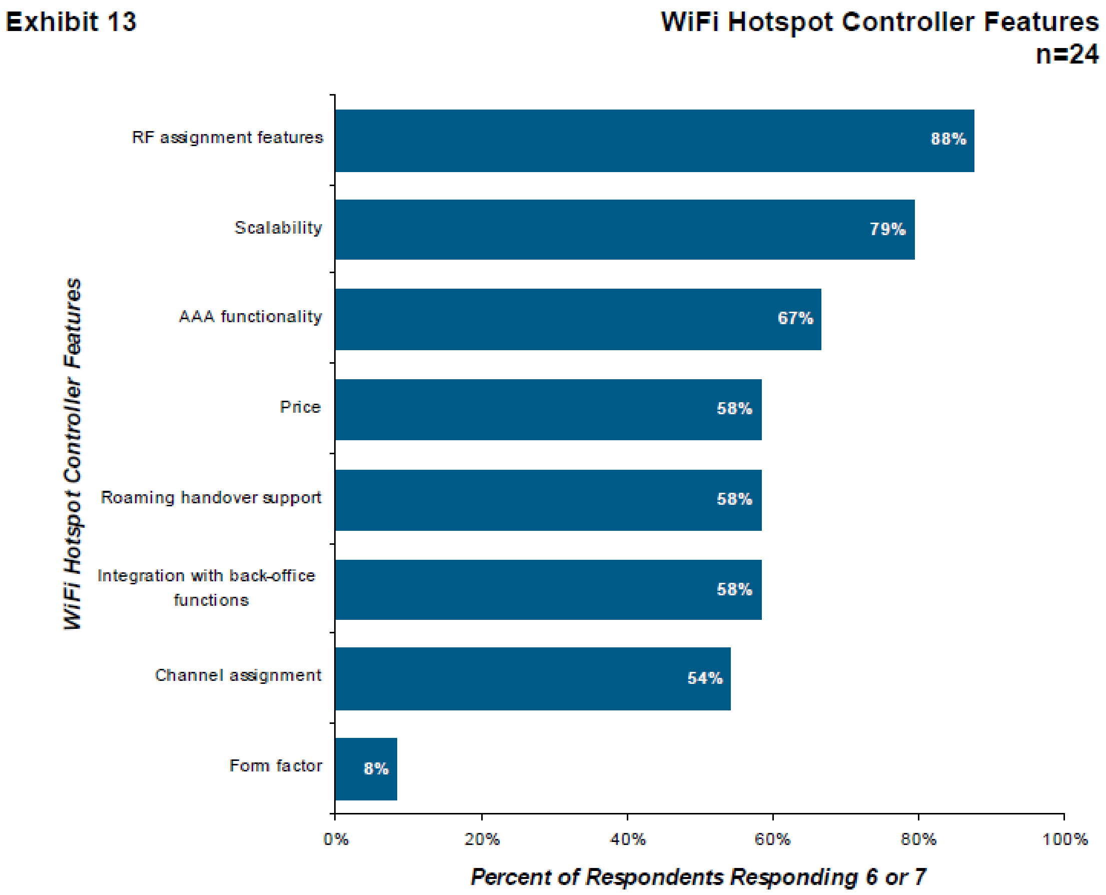


Figure 9: Carrier Wi-Fi Controller Feature Priority[3], 0

Identified Topics For Further Study: The Wi-Fi-Network architectures have been generally vendor specific implementations, based on proprietary interfaces and/or proprietary extensions to standardized interfaces. Examples include the interface between the Wi-Fi AP to Controller. As Carrier Wi-Fi is gaining momentum, and also integration with Cellular Core Networks is being increasingly considered/deployed, it may be useful for the industry to establish standards and/or best practices/recommendations for such Wi-Fi-network aspects. Additional topics include Inter-AP, Intra/Inter-Controller Mobility Management.

[3] Reproduced with the kind permission of Infonetics.

2.3.2 Small Cell AP Network Architecture

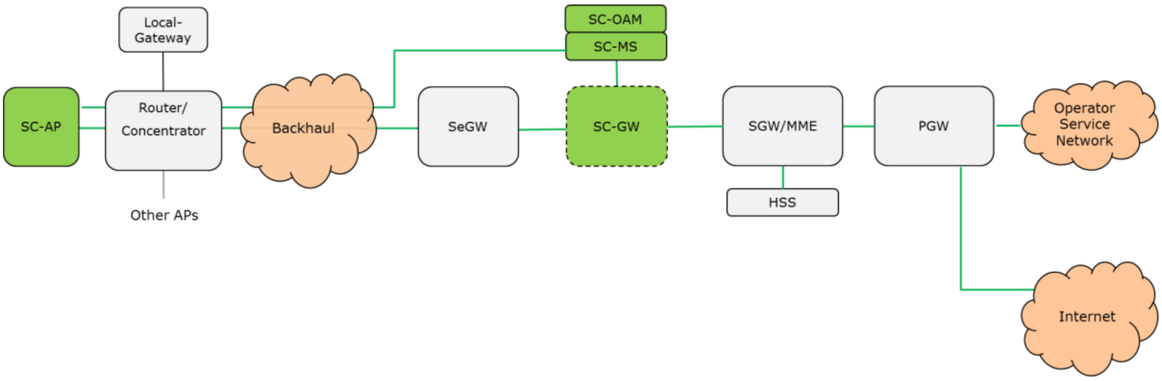


Figure 10: Small Cell Network (3GPP Representation)

Figure 10 shown above is a simplified diagram of a Small Cell Network, as defined by 3GPP standards. The SC-AP may be 3G or LTE AP and, although not defined by 3GPP, several of such APs are sometimes aggregated by a premise based Concentrator (or Aggregation Node – AN). The premises may also have a Local Gateway to connect to Local IP Networks. The SC-APs connect to the Operator Core Network via a routed backhaul network. Due to the varied locations of SC-APs, the backhaul technology and backhaul networks also vary significantly. For example, the backhaul network may be a wired network, such as DSL, HFC, Fiber, or wireless network operating in licensed or unlicensed frequency bands. Furthermore, the wireless technology may be LOS (Line of Sight) type of Non-LOS type.

Of particular importance to note is the fact that the backhaul network may often be an open IP network, such as the Internet, so that communications between the SC-AP and the Core Network must be securitized. In 3GPP this is referred to as Network Domain Security for IP network layer security (NDS/IP) [8]. Protection is achieved by employing a Security Gateway (SeGW) at the ingress of the Operator Core Network and employing encrypted IPSec tunnels between the SC-AP and the SeGW.

The User data and control traffic further traverses the Small Cell Gateway and onto the well-known Mobile Operator Core Network elements, namely SGW/MME and PGW (the Evolved Packet Core – EPC) for LTE and SGSN/GGSN (the Mobile Packet Core – MPC) for 3G. While the data and control plane traffic traverses through the SeGW, the provisioning and management of the SC-APs is often achieved via a separate channel using Transport Layer Security (TLS) and using TR-069/TR-196 protocols [24, 25]. Alternately, it may also be transported within the IPSec tunnel.

Small Cell Gateways

In general networking terms, a gateway is an internetworking system capable of joining together two networks that use different base protocols. A Small Cell Gateway is based on current 3GPP standards for providing secure access to the EPC, concentrating the signaling to the EPC/MPC, or offloading user plane traffic from the EPC/MPC.

We use the term “Small Cells Gateway” to refer to a gateway that sits between the Small Cell RAN and the EPC/MPC, aggregating a bunch of Small Cells. This is similar in functionality to an ‘Home eNodeB Gateway’ or “Home NodeB Gateway”. However, whereas that term is restricted to residential deployments, the Small Cell deployments are broader, including small cells of all sizes (residential femtocell, enterprise small cells, urban microcell, and metrocell). Furthermore, while Small Cell Gateways are defined for both 3G and LTE Small Cells, hereafter we shall, for simplicity, restrict the discussion to only LTE Small Cells. One key difference to keep in mind is that 3G Small Cell Gateways (known as HNB GW in 3GPP terminology) are mandatory unlike their LTE counterparts. Furthermore, 3G Small Cell Gateways aggregate both data and control plane traffics, whereas LTE Small Cell Gateways have an option to aggregate both data and control plane traffics or only control plane traffic.

LTE Small Cell Gateways

The 3GPP "Stage 2" normative specifications for eNode Bs (eNBs) and Home eNode Bs (HeNBs) are standardized in TS 36.300 [26]. Figure 11 illustrates the EPC connections with eNB, HeNB, and the optional HeNB Gateway (HeNB GW). It also shows an example of a HeNB operating in Local IP Access (LIPA) mode with a co-located Local Gateway (LGW). In this case, the S1 interface is proxied through the HeNB GW while a logical S5 interface exists directly between the L-GW and the remote S-GW, e.g to support termination of LIPA users on the L-GW when they are accessing via the macro network.

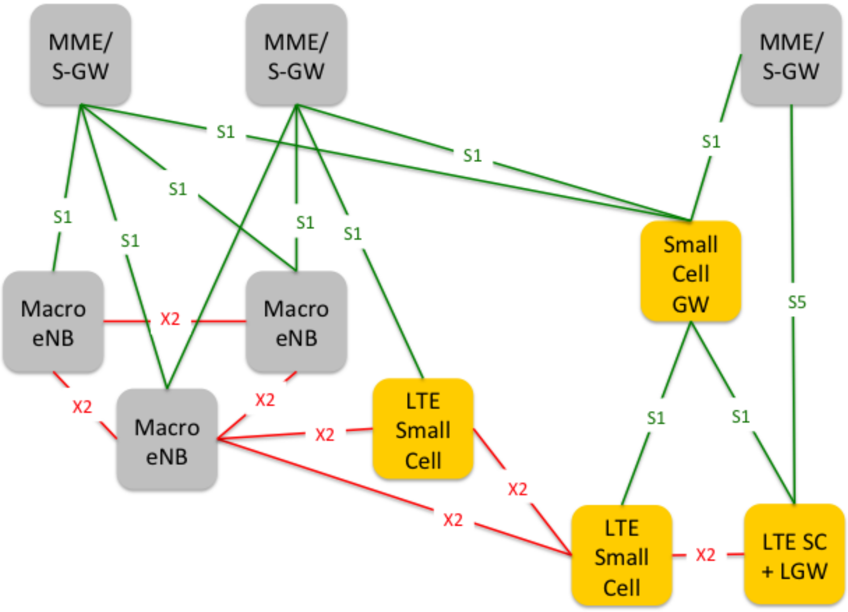


Figure 11 - Overall E-UTRAN Architecture with deployed HeNB GW

Location in the Network

An LTE small cell gateway can be located based on the deployment requirements. For example, it could be: (1) Co-located with the 3G small cell gateway; (2) Co-located with the SeGW; (3) Co-located with Core Network; or (4) separately deployed. Based on the location in the network (closer to the RAN, or deeper in the core), scaling aspects would vary.

Functionalities of an LTE SC Gateway

Due to the advantageous positioning of an LTE SC Gateway, a number of useful features can be implemented in it. Some of these are mandated by the 3GPP standards, while others are vendor dependent. They are listed below:

- Aggregate only to control plane (S1-MME) or in both control and user planes (S1-MME as well as S1-U)

- Provide Logical Link management across different MME/S-GW

- S1 mobility optimizations: There may be excessive mobility signalling events in the core network due to mobility between small cells. These mobility events can be hidden from the core network by terminating the S1 handover related signalling messages at the gateway and then implementing a NAT like function to route the GTP-U packets to the relevant eNodeB. [4] Provides more detail of how an intermediate gateway can provide hierarchical mobility hiding in an LTE small cell environment.

- From the MME perspective, the SC Gateway simulates a macro eNodeB on behalf of all the small cells aggregated by it. This means that the MME doesn't have visibilities of the Small Cell identities, and instead needs to provide mobility, e.g., hand-in support, based on the Tracking Area Identity used by the small cell system. As with the macro, the MME will be responsible for any paging functions.

  Note, unlike the 3G Small Cell Gateway which has visibility of the user's permanent IMSI identity over HNBAP and RANAP and which can therefore use such to perform various optimizations, the LTE Small Cell Gateway only has visibility of a user's temporary identity whenever the user attaches to the network. This may prevent the LTE Small Cell gateway from performing some of the optimizations available in 3G.

- S1 load balancing and overload handling: Handle S1 signalling overload conditions and protect the core network from S1 signalling storms.

- S1 Firewall: Validate GTP-U packets to ensure they correspond to an established bearer.

- S1 Analytics: Monitor S1 signalling messages and build a database of useful data.

  Note, as per the discussion above, the LTE Small Cell Gateway may only have visibility of temporary user identities and so may be less able to provide user tracking functionality compared to a 3G Small Cell Gateway.

- RAN Congestion determination: Using monitoring tools between the LTE Small Cell and the Gateway to determine whether such links are congested.

- Charging data collection function, e.g., in case of LIPA/SIPTO functionality is co-located with the Small Cell Gateway.

* Monitor Network Performance metrics, such as: (1) Bearer setup delay; (2) User packet processing delay; (3) Latency, Jitter, packet loss; (4) Number of handover requests, preparation, execution, success, failures, cancellations, ping pong; (5) Number of Registrations, TAU; etc.

Product Aspects

Since the small cells gateway is a core network element, a hot standby model of high availability should be supported. For example, “1:1 or N:K hot standby redundancy support” or “Active/Standby model or Active/Active model”

Note: Since the routing of messages between the MME and LTE Small Cell gateway is based on Tracking Area, careful consideration may need to be given to the aspects of redundancy/high availability of the small cell gateway as it relates to TA routing decisions by the macro MME.

2.3.3 WLAN Gateways for Core Network Integration

3GPP introduced interworking standards between 3GPP and WLAN access networks as part of their Release 6 specifications in 2005 [27]. One of the goals was to facilitate 3GPP subscriber access to network services via WLAN, e.g., when there is no cellular coverage or when it is desirable to offload multi-RAT users from the macrocellular network.

Two new network gateways were introduced to enable WLAN access to 3GPP-based packet switched (PS) services, namely the Wireless Access Gateway (WAG) and the Packet Data Gateway (PDG).

In the I-WLAN architecture, the WLAN access network (WLAN AN) was always considered "untrusted" from the perspective of the core network. In order to allow secure access by WLAN users into the core network, the I-WLAN standards specified a mechanism for establishing an IPSec tunnel between the UE and the PDG located at the edge of the core network.

In Release 8, an enhanced architecture for enabling 3GPP-WLAN mobility was introduced. The mobility solution was based on IETF Dual Stack Mobile IPv6 (DSMIPv6) [28]. With this solution, a host-based client communicates with a Home Agent (HA) in the core network to exchange connectivity information related to the WLAN access via "binding updates". The DSMIPv6 signalling is enhanced to support the cellular use case, e.g., enabling the UE to signal which APN it is requesting access to. Furthermore, 3GPP enhanced the system architecture to support IP Flow Mobility (IFOM) between DSMIPv6 UEs that are connected simultaneously to the same PDN connection over Wi-Fi and Cellular [29]. In particular, the UE can provide the HA with routing rules defining the policy for the HA to determine whether downlink packets should be routed via the cellular or Wi-Fi networks.

3GPP Release 8 also defined the new "all-IP" Evolved Packet Core (EPC) network. The Release 8 EPC architecture and protocols addressed generic "non-3GPP" accesses which were originally designed to enable cdma2000 and WiMAX access networks to interface to a converged core network [7]. The EPC defined a new PS core network architecture which included an "evolved" PDG (ePDG) for supporting "untrusted" non-3GPP access such as unsecure WLANs. However, it also addressed "trusted" non-3GPP networks which we will explore further for the specific case of "trusted WLAN". [7] Defines integration with "trusted non-3GPP networks", originally using IETF network-based Proxy Mobile IPv6 protocols (PMIPv6), and has recently added support for the GPRS Tunnelling Protocol (GTPv2) for supporting trusted Wi-Fi networks. In Figure 12, these network-based protocols can be used for "untrusted" access over the S2b interface, or "trusted" access over the S2a interface.

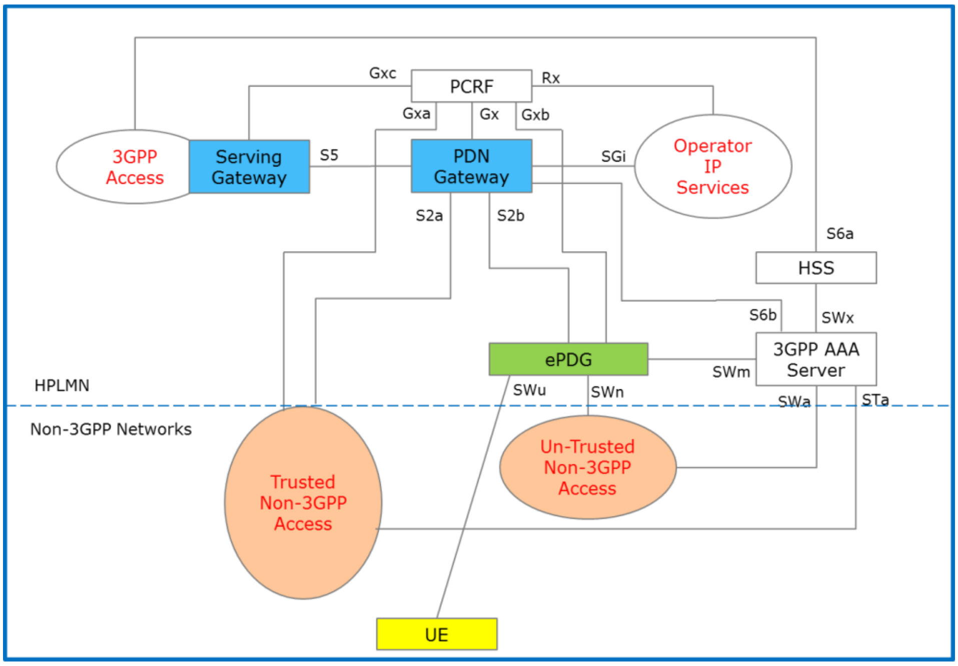


Figure 12: Non-roaming Mobility Architecture for S2a/b EPC

The 3GPP Release 11 work item for “S2a Mobility based on GTP” (SaMOG) focused on supporting GTPv2 on the S2a interface to the PDN Gateway (PGW) for “Trusted WLAN Access Networks” (TWANs). Although technical report TR 23.852 [30] considers the detailed functional split within a TWAN as out of scope for 3GPP, the following functions were assumed in the TWAN as depicted in Figure 13.

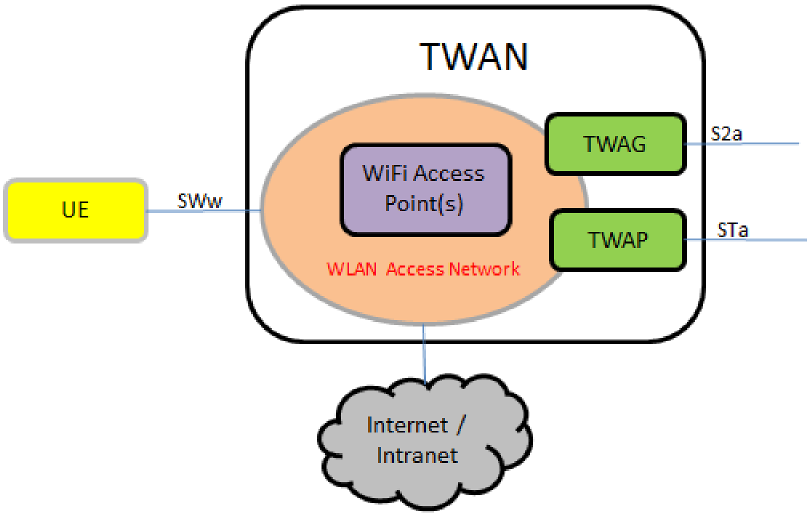


Figure 13: Trusted WLAN Access Network functional split

The Trusted WLAN AAA Proxy (TWAP) function includes [30]:

(1) Relaying the AAA information between the WLAN Access Network and the 3GPP AAA Server or Proxy in case of roaming;

(2) Establishing the binding of UE IMSI with UE MAC address on the WLAN Access Network into a (IMSI, MAC) tuple via snooping on the AAA protocol carrying EAP-AKA exchange;

(3) Detecting L2 Attach/Detach of UE to the WLAN Access Network via snooping on the AAA protocol for EAP-Success/Accounting-Request messages respectively;

(4) Informing the Trusted WLAN Access Gateway of WLAN Attach and Detach events for UE with (MAC, IMSI) tuple;

(5) Protocol conversion to Diameter protocol for STa, when needed; and

(6) Transfer necessary information for suitable per-UE L2 encapsulation between the Trusted WLAN Access Network and the Trusted WLAN Access Gateway.

The Trusted WLAN Access Gateway (TWAG) function includes [30]:

(1) For IP version 4: Default IPv4 Router and DHCP server according to IETF RFC 2131 [31]. (The TWAG allocates to the UE the IPv4 address that is signalled to the UE by the PDN GW);

(2) For IP version 6: Default IPv6 Router according to IETF RFC 4861 [32];

(3) Enforces routing of packets between the UE MAC address and the S2a tunnel for that UE; and

(4) Enforce per-UE L2 encapsulation of traffic to/from the UE.

As an informative example of a TWAN integrated with a small cell (e.g., femtocell / H(e)NB), [30] provided the following discussion in Appendix A of the technical report:

"For the Femto, the network will perform authentication and integrity checking through AAA before the femto can be connect to the EPC. In addition, the IPSec function in Femto can be used to build a secure transmission tunnel through the backhaul to the EPC. Therefore, the WLAN module integrated with the Femto box can leverage the authentication, integrity checking and the IPSec function to build a trusted WLAN access for connectivity to the EPC."

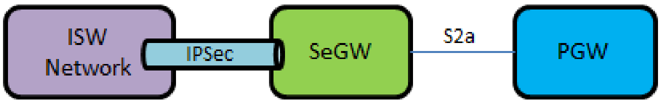


Figure 14: WLAN Integrated with Femto Accessing EPC through S2a

Identified Topics For Further Study: It must be noted that the 3GPP document does not go deeper into this idea and this represents a potential gap and an opportunity to study further. For example, the details of sharing an IPSec between the various Small Cell and Wi-Fi are worth exploring further. In particular, the IPSec tunnel used for the stand alone Small Cell is typically configured in "remote access" mode whereby only a single IP address is allocated to the Small Cell. In the above figure, no consideration is given to the changes in IPSec Tunnel configuration to support possible multiple inner IP addresses on the converged ISW Access Point.

Although the 3GPP Evolved Packet Core (EPC) supports small cell access via low powered eNodeB (eNB), Home eNode B (HeNB), and WLAN technologies, current 3GPP standards still do not exploit all potential synergies between eNB, HeNB and Wi-Fi accesses. As previously stated, the geographic coverage of Wi-Fi and Small Cells can be comparable. Although HeNB Gateways are standardized as deployment options for HeNBs, the aggregation and scalability benefits are not obviously available for small cell eNB deployment. Also, the standards do not explicitly consider network optimizations for co-located 3G/4G/Wi-Fi small cells. Finally, although current 3GPP “HetNet” activities consider interactions between 3G/4G small cells and macro cells, they do not address interaction Wi-Fi access points.

2.3.4 ANDSF Server for Wi-Fi Discovery, Selection & Routing

The Access Network Discovery and Selection Function (ANDSF) server is a functional element part of the 3GPP Mobile Evolved Packet Core Network capable of providing ANDSF policy to the 3GPP UE. The ANDSF policy is composed of a set of rules for indicating to the 3GPP UE criteria for selection of network and for steering of traffic when various networks are available, such as WLAN and 3GPP.

The ANDSF server has been introduced in 3GPP Rel-8 (see [7] and [33]) and it has been further enhanced in each subsequent Release. The ANDSF server is able to provide a 3GPP UE the ANDSF policy in pull mode, i.e. when interrogated by 3GPP UE, and in push mode, i.e. providing policy to the 3GPP UE when needed. The communication between the 3GPP UE and the ANDSF uses OMA DM as defined in OMA-ERELD-DM-V1_2 [34] with the management object as specified in 3GPP TS 24.312 [35]. In roaming scenario the ANDSF server can be deployed in both Home and Visited networks. In such a scenario, the 3GPP UE can receive policy from both networks and, based on indicated policy or configuration, the UE can give precedence to policy provided by Home or Visited network.

3. ISW-Network Functions & Use Cases

This section describes the key functions and procedures supported by the various building blocks described in Chapter 2, which are necessary to implement the various ISW use cases.

3.1 Intelligent Discovery & Selection

Unlike the macro cells, Small Cells as well as Wi-Fi Hot Spots have much smaller foot print and are, in general, deployed on an as needed basis, and therefore not necessarily contiguous in their coverage over large geographic areas. This makes the discovery of such small cells/Wi-Fi hotspots a challenge, requiring intelligent network assisted discovery solutions.

Similarly, when a UE is covered by both small cell and Wi-Fi hotspots, the selection of the most suitable radio becomes an interesting challenge. For example, the selection may depend upon several factors, including user preferences, operator policies, network conditions, device conditions, application needs, quality of service, security, cost etc. As such, an intelligent selection of network and steering of appropriate data flows across the different radio technologies is an important problem that the industry is focused on solving. In this section, we describe the current state of the technology for such intelligent network discovery, selection and routing.

3.1.1 Cellular Network and Cell Selection

Small Cell Discovery and Selection are generally realized using existing Cell Selection/Reselection methods usually employed in the macro-cellular networks, with some modifications and extensions made in a small cell environment. Normally, the UE searches for physical cell ID (e.g., LTE PCI) for cell reselection.

When small cells are deployed in the shared-carrier and open-access mode in an outdoor environment, the technique of Cell-Range-Extension (CRE) may be used to “attract” UEs to the small cell. In this technique, the UE camps on the small cell even though the macro-cell signal is stronger than the small cell signal (but within a limit defined by the CRE parameter).

When small cells are deployed in dedicated-carrier and open-access mode, the UE may need measurement gaps for small cell discovery. Possible solutions include UE autonomous search/background scan, network based finger printing to detect UE proximity to inter-frequency small cells, etc.

When small cells are deployed in the closed-access mode (for example, residential Femto cells), the UE can perform autonomous search for CSG cells and also prioritize discovered CSG cells in case of inter-frequency cell reselection.

Furthermore, from a UE perspective, as small cells get deployed, it can be advantageous if the 3GPP network implements mobility state determination by which the UE counts the number of cell reselections within a defined period. If this is above a defined threshold, then the UE switches to operating in a high mobility state. In such a state, the UE alters its reselection timers and hysteresis parameters to effectively avoid camping on the small cell layer. Using such techniques, the cell type (either macro or small cell) can be used as a factor in a UE’s decision on cell reselection.

Automatic cellular PLMN selection is based on a list of PLMN-IDs that are included in the system information broadcast from the cell site together with a prioritized list of preferred PLMN-IDs stored in the user’s SIM card. The SIM card includes an operator controlled PLMN selector list that may contain a list of preferred PLMNs in priority order. The list is also able to include access technology associated with an entry in the list, e.g., E-UTRAN, UTRAN or GERAN. When the user is roaming in a visited network, the user’s handset will periodically search for its home PLMN, with a default 60 minute repetition.

3.1.2 Wi-Fi Network Selection

The Wi-Fi network discovery and selection is normally divided in three steps:

(1) Device configuration
Devices need to be configured in order to discover Wi-Fi networks. The configuration can be accomplished statically or dynamically. The configuration information contains operator policy and user preferences that will be used for the network selection.

(2) Device network discovery
Network discovery is a process executed by the device that is using the configuration information to look for the Wi-Fi networks to which the device can associate. The device looks for Wi-Fi networks using scanning mechanisms to discover relevant network information.

(3) Device network selection
After the device discovers the Wi-Fi networks it will associate and authenticate to a network based on the operator’s and user’s policies.

The content of the Technical Specification for WFA Hotspot 2.0 [14] is designed to address the following four system solution requirement areas:

(1) Discovery: the mobile device is scanning for networks with which to associate and for related information useful for network selection. The mobile device is not associated to the Wi-Fi access network it's scanning (however, it might be associated to a different Wi-Fi access network). The mobile device also uses operator policy and user preferences in the network selection process.

(2) Registration: the mobile device is in the process of setting up a new account with a SP or hotspot provider. If the mobile device already has valid credentials for a given Wi-Fi access network, registration is not performed.

(3) Provisioning: the Wi-Fi infrastructure is establishing credential information and optionally providing network-selection policy information to the mobile device. If the mobile device already has valid credentials for a given Wi-Fi access network, provisioning is not performed.

(4) Access: the mobile device successfully associates and authenticates with the Wi-Fi access network and can access the services for which the user has subscribed.

Also, provisioning (both subscription and policy provisioning) must be available via the Wi-Fi access network. This is necessary when cellular data connectivity is not available (e.g. the subscriber does not have international roaming available on their mobile subscription) or when the device is a Wi-Fi only device (e.g., tablet).

In addition, for Hotspot 2.0 compliant networks it is essential that roaming elements are defined to identify the roaming partners during the process of network discovery; as an example, the availability of NAI Realms Lists or PLMN Lists are to be used by terminals.

The ANDSF policy has the scope to provide to 3GPP UE information and criteria for selection of network and traffic steering between 3GPP radio and Non-GPP access, mainly WLAN. The support of ANDSF policies is an optional feature. Additionally, the 3GPP UE may take a decision also using other local information which is left to implementation.

The ANDSF policy is defined by 3GPP TS 23.402 [7], TS 24.302 [33] and TS 24.312[35]. However in Rel-12 a broad work of extension of policy is underway, aiming to clarify the usage, solve some identified gaps and take into account applicability of WFA HS2.0 Rel 2.

The ANDSF policy are generally constituted by a indication of preferred access, a priority valued and a set of validity conditions, e.g. validity area, time of the day, etc. 3GPP Rel-11 ANDSF includes the policies listed below:

- Access Network Discovery Information policy indicates which is the preferable access technology type (WLAN, WiMAX, 3GPP) or radio access network identifiers (e.g. SSID and/or REALM for WLAN);
- Inter-System Mobility Policy (ISMP) indicates when inter-system mobility is allowed or restricted (e.g. WLAN is preferred, WLAN is forbidden) and which is the preferable access technology or network for EPC routed traffic (e.g. SSID #1 is preferable to SSID#2); and
- Inter-System Routing Policy (ISRP) indicates when access network/type for IP Flow based or APN is restricted (e.g. WLAN is preferred, WLAN is forbidden for APN#A) and which is the preferable access technology/access network for APN/IP flow (e.g. all traffic for a given APN on WLAN SSID #1, IP Flow for HTTP on WLAN, all IP flow for IMS on 3GPP).

  The ISRP policy covers several scenarios: IP Flow mobility (IFOM), the feature for moving IP flows belonging to the same PDN connection between different access when the UE is simultaneously connected to 3GPP and Non-3GPP access (see Figure **15**); Multi Access PDN Connectivity (MAPCON), the support of different simultaneous active PDN connections through different access networks (see Figure **16**); Non-seamless WLAN offload (NSWO), the capability to send the traffic directly to internet/server without traversing EPC (see Figure **17**).

Note, the IFOM operation assumes that the APN can be signaled over the Wi-Fi access network and hence operation of such policies may be limited to those access techniques that enable APNs to be supported over the Wi-Fi access network, e.g., signaled using IKEv2 to an ePDG or Binding Update to a DSMPv6 Home Agent.

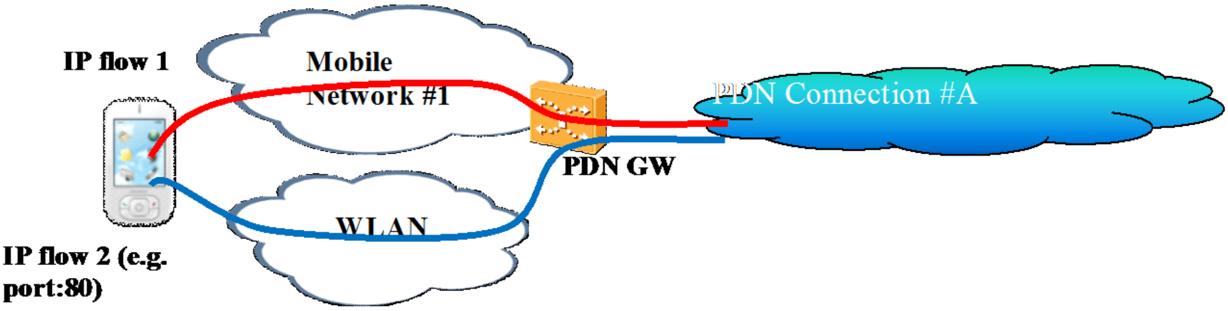


Figure 15: IP Flow Mobility (IFOM) Scenario

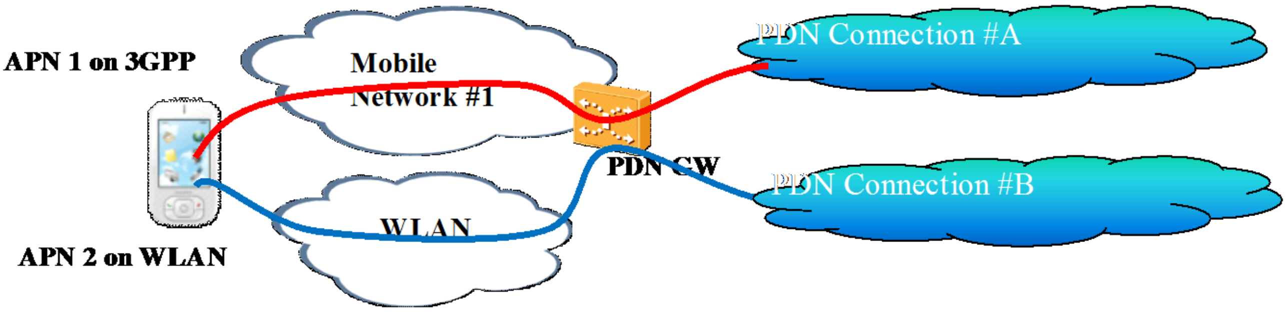


Figure 16: Multi Access PDN Connectivity (MAPCOM) Scenario

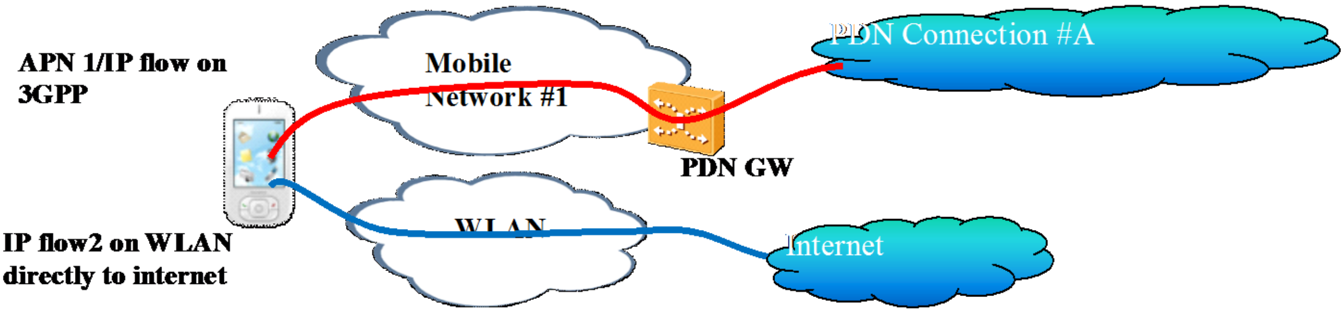


Figure 17: Non-Seamless WLAN Offload (NSWO) Scenario

In 3GPP Rel-12 the Inter-APN routing policy has been introduced to allow the operator to define a set of rules that determine which traffic should be routed across different PDN Connections and which traffic should be NSWO. This policy allows binding a service to a specific PDN connection.

3GPP also studied the relationship between Rel-11 ANDSF policies and WFA HS2.0 Rel 2 specification to identify gaps and harmonisation. The result of the analysis is that two new policies, the WLAN Selection policy and the Preferred Service policy, have been defined. The WLAN Selection Policy (WLANSP) is a set of rules that determine how the UE selects and reselects a WLAN access network. Importantly, the Policy includes elements defined by the HS2.0 Policy node, enabling these HS2.0 policies to be incorporated into the updates ANDSF-based policy. The Preferred Service Policy List (PSPL) contains a prioritized list of service providers preferred by the UE's 3GPP home operator for WLAN roaming.

In summary, the ANDSF policies are used by UE under the following circumstances:

- The UE uses Access Network Discovery Information policy when it selects the network to perform attachment;
- The UE uses ISMP when it can route IP traffic over a single radio at a given time and for EPC routed traffic (not for IFOM capable UE). In this case the ISRP rule shall be ignored;
- The UE uses ISRP when it can route IP traffic for same PDN connection simultaneously over a 3GPP and Wi-Fi radio at a given time. In this case the ISMP rule shall be ignored;
- The UE uses IARP when it can be connected simultaneously over a 3GPP and Wi-Fi radio for different PDN Connection at a given time. In this case the ISRP rule shall be ignored; and
- The UE uses WLANSP policy in conjunction with PSPL policy to identify the most preferred Wi-Fi network.

3.2 Seamless Authentication

Traditionally, cellular networks and Wi-Fi networks used different authentication methods. For example, cellular networks used SIM-based GSM/UMTS authentication methods, whereas Wi-Fi networks used username-password/WiSPr based authentication methods. When Cellular (or Small Cell) and Wi-Fi Networks are interconnected or integrated, it makes sense to develop common authentication methods that work on both networks. This has been achieved by leveraging EAP (the Extensible Authentication Protocol) which is a ‘framework’ for authentication by any underlying authentication ‘procedure/algorithm’. EAP was originally developed within the 802.1X framework for Ethernet port-based security and authentication, and later extended to provide corporate WLAN authentication within the WPA2-Enterprise framework. If the underlying authentication procedure is SIM-based, then the overall authentication scheme is called EAP-SIM (as specified in RFC 4186 [36]). Similarly, if the underlying authentication procedure is USIM-based, then the overall authentication scheme is called EAP-AKA (as specified in RFC 4187 [37]). Other schemes such as EAP,-TLS and EAP-TTLS,, etc are also defined.

As mentioned above, EAP is not an authentication algorithm in itself and is therefore very simple, consisting of just a few messages. Furthermore, these messages can be transported over any data link layer protocol, such as Ethernet, PPP, IEEE 802.11 Frames etc.

The EAP framework essentially consists of 3 entities, namely the Supplicant (contained in the UE), the Authenticator (implemented in the AP/WLC), and an Authentication Server (AAA Server). The EAP procedure consists of a few simple steps, as illustrated in Figure 18. Using Wi-Fi radio and IEEE 802.11 Frames, the UE’s EAP supplicant communicates with the Wi-Fi AP using EAPOL (EAP over LAN) authentication messages. The AP (or WLC), which contains an EAP Authenticator, conveys these messages to the EAP Authentication Server, using the RADIUS protocol. The EAP Server exchanges EAP messages with the UE Supplicant, authenticating the user and in the process generating the Pairwise Master Keys (PMK) that are subsequently used to generate keying material to encrypt the Wi-Fi radio interface.

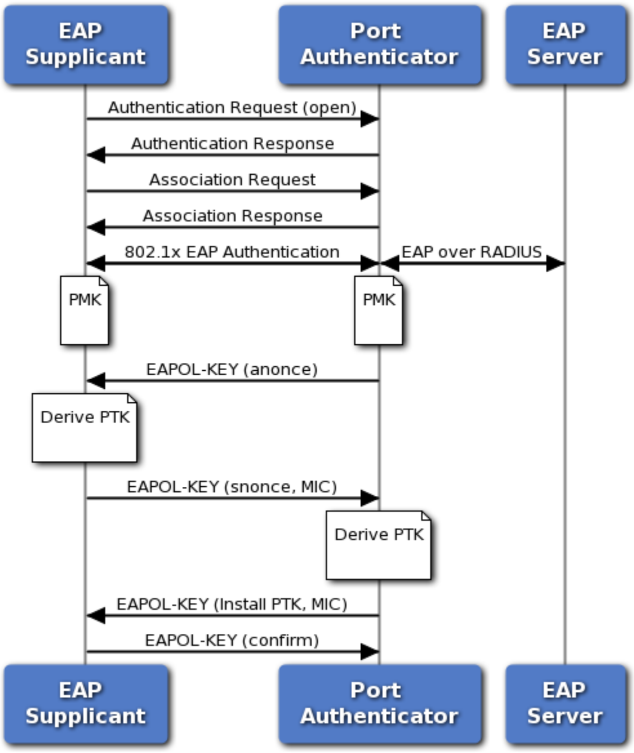


Figure 18: EAP Exchange

For example, consider a UE with Cellular and Wi-Fi radios and a SIM card containing the user credentials. The UE is in the coverage of a Wi-Fi-AP and would like to use its SIM credentials for being authenticated by the Wi-Fi Network, for Internet access. The UEs EAP supplicant exchanges EAP-SIM messages with the EAP Authentication Server. The Authentication Server in turn communicates with the 3GPP Network's HLR or HSS systems which completes the UE's authentication using the existing 3GPP authentication procedures/algorithms, as illustrated in . Figure **19**. It may be noted that when a Wi-Fi controller is used in the ISW Network, the EAP Authenticator will typically be located in the Wi-Fi Access Controller instead of being in the AP itself. This allows the keying material to be stored centrally and be re-used as the UE changes Wi-Fi access points.

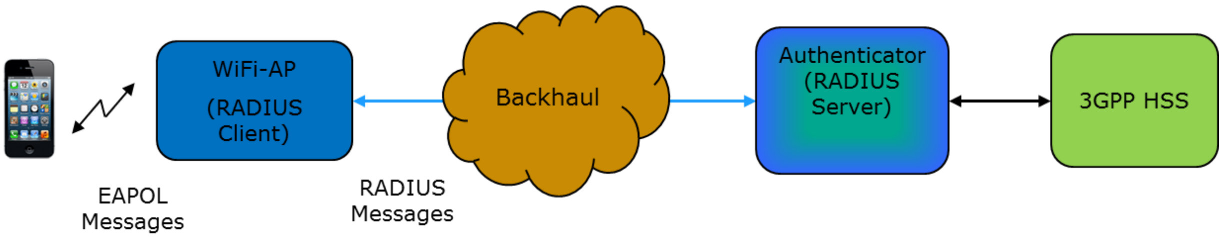


Figure 19: EAP Framework

It can now be appreciated that the EAP-SIM and related procedures do not involve user intervention and are therefore deemed 'seamless' procedures. In the following, a brief description is given for various EAP methods.

The key authentication methods to be supported for public Wi-Fi networks are the following: EAP-SIM, EAP-AKA, EAP-AKA', EAP-TLS and EAP-TTLS. To ensure that mobile devices will always have an authentication method in common with Wi-Fi and SP infrastructure, all Hotspot 2.0 equipment is mandated to support EAP-SIM, EAP-AKA, EAP-TLS and EAP-TTLS/MSCHAPv2 authentication methods.

The expected user experience by using these seamless authentication methods should be the following: (1) User arrives to a Wi-Fi hotspots with a switched-on Passpoint certified device; (2) Device automatically selects the Wi-Fi network and submits credential for authentication, (3) 'home' provider authenticates user and sends access accept message back to the Wi-Fi network; (4) User has network access.

> Note, since the device and network both likely support multiple different EAP methods, there needs to be an agreed approach as to the negotiation of which EAP method to use. This is realized by the Supplicant selecting the format of its EAP-Identity such that it can be used to indicate a preference for a particular EAP method. For example, permanent EAP-SIM identities are specified to start a leading "1" and permanent EAP-AKA identities are specified to start with a leading "0", enabling the EAP Server to deduce which method it should select.

EAP-SIM

EAP-SIM is an EAP method for authentication and session key distribution using the Global System for Mobile Communications (GSM) Subscriber Identity Module (SIM) and is specified in [36, 38]. The EAP-SIM method re-uses the GSM authentication and key agreement, enabling multiple SIM authentication exchanges to be combined to create authentication session keys for the Wi-Fi Access Network. The method also includes network authentication (previously missing for the original GSM standard), privacy support, result indications, and a fast re-authentication procedure. For generation of the Wi-Fi keying material, the GSM A3 and A8 algorithms are used. These are located on the GSM SIM card and also in the Authentication Centre in the mobile core network. The definition of these algorithms is operator-dependent and therefore not standardized.

EAP-AKA

The EAP-AKA mechanism is an EAP method for authentication and session key distribution that uses the Authentication and Key Agreement (AKA) mechanism and is specified [37, 38]. AKA is used in Universal Mobile Telecommunications System (UMTS) and LTE Access Networks as well as in CDMA2000. It is based on symmetric keys. AKA is typically implemented in a Subscriber Identity Module (SIM) or UMTS Subscriber Identity Module (USIM). Similar to EAP-SIM, EAP-AKA provides security features such as mutual authentication, user privacy support and replay protection.

EAP-AKA'

EAP-AKA' is a small revision to EAP-AKA method and is specified in [39, 40]. The change is a new key derivation function that binds the keys derived within the method to the name of the access network. In addition, EAP-AKA' employs SHA-256 instead of SHA-1. EAP-AKA' is the only EAP method agreed by 3GPP for *trusted* non-3GPP access to the EPC, as specified in TS 33.402 [40]. Trusted non-3GPP access simplifies the EPC system architecture, where the user plane does not need to be routed via an ePDG (see [7]).

> Note, the original Hotspot 2.0 release 1.0 specification mandated the support of EAP-AKA and not EAP-AKA' by compliant terminals and networks. This has been addressed in release 2.0 which now mandates EAP-SIM, EAP-AKA and EA-AKA' support.

EAP-TLS and EAP-TTLS

Because of the use of high entropy secrets and secure tamper resistant storage, there is strong preference for a device having SIM/USIM credentials to be always authenticated using the SIM/USIM. However, if the terminal is a tablet or laptop computer and does not have a SIM credential, then EAP-AKA/EAP-SIM authentication will not be possible and hence the alternative Hotspot 2.0 EAP methods, namely EAP-TTLS and EAP-TLS can be used. Equally, a smartphone supporting EAP-SIM/EAP-AKA may be attempting to access a visited Next Generation Hotspot (NGH) network that does not have a roaming agreement with their home network. In some cases this may require the user to set up a new account, separate from his home subscription, with the visited network.

WISPr v1.0

To maintain a seamless user experience for subscribers who do not have EAP capable devices and/or those roaming into non-EAP capable networks, Wi-Fi operators and device manufacturers may continue to support the WISPr v1.0 specification for username/password based authentication. It is the responsibility of the Home Service Provider to determine the credential construct and manage the user experience where WISPr v1.0 authentication is required.

Sessions established using WISPr based username and password authentication are vulnerable to session hijacking using a simple MAC spoofing attack. This may mean that MNOs will be unwilling to permit users authenticated using non-EAP method to access the 3GPP core network.

3.3 ISW-Connectivity Use Cases

Use cases for ISW network access may involve the following criteria:

1. User Requirements and Preferences
    a. Type of service requested by user, e.g. voice, streaming video, web access, etc.
    b. Type of service continuity expected when moving across network access points, e.g. with IP address preservation between Wi-Fi access points, with specific limits on session interruption time, with IP address preservation between SC and Wi-Fi access points, etc.
2. Network Conditions
    a. Network capacity, load and congestion status
3. Operator Policies
    a. Service subscription and priorities
    b. Relative cost of production
    c. Inter Operator Tariffing
4. User Policies
    a. Charging and billing concerns

Based on the above criteria, the following ISW connectivity options can be envisioned for a particular user based on UL/DL traffic and/or user plane/control plane considerations:

1. All connections through common ISW access
    a. UL and/or DL user plane and/or control plane data via small cell and/or Wi-Fi hotspot
2. Simultaneous connection(s) across multiple ISW accesses
    a. UL and/or DL user plane and/or control plane data via two or more ISWs
3. Simultaneous connection(s) across ISW and standalone small/macro cell and/or Wi-Fi hotspot
    a. UL and/or DL user plane and/or control plane data via ISW and standalone small/macro cell and/or Wi-Fi

    Note, the earlier co-operation between the WBA and GSMA has highlighted issues related to (1) around disabling cellular interfaces when the user entered Wi-Fi coverage [41]. In particular, such a configuration can lead to significant increases in signalling load on the cellular interface, e.g., as charging records are closed as soon as the user enters Wi-Fi coverage.

    Note, in terms of the cellular interface and option (3), there is currently no standardized technique by which a UE can know that it is attached to a small cell or a macro cell.

    Note, these options may require enhanced functionality to be implemented on the UE, e.g., to allow the policy to be enforced for socket binding decisions.

3.4 ISW Traffic Management

Below we describe some 3GPP-defined traffic management solutions for interworking between cellular and Wi-Fi access networks. In general, these techniques are also applicable for integrated small cell and Wi-Fi networks.

We note that, depending upon the application, "seamless" session continuity across access networks may require preservation of the terminal's IP address. Lack of support for IP address preservation techniques may lead to "non-seamless" transitions between access networks which may be acceptable in some cases.

Furthermore, the support for IP address preservation is complicated by the definition of Access Point Names (APNs) on the cellular network. APNs enable multiple IP addresses to be supported by the UE, including support for overlapping IP addresses, whereby it is assumed the APN is used within the terminal to be able to distinguish between different flows. Currently, the only standardized techniques for signalling APN information of Wi-Fi networks are by using I-WLAN's (e)PDG which uses IKEv2 to signal APN information, or by using S2c Home Agent which uses DSMIPv6 to signal APN information.

3.4.1 Use Case 1: Handover between cellular and WLAN

This use case is only applicable when the Mobile Network Operator (MNO) supports access to Mobile Core Network (MCN) services via both cellular and WLAN access networks. Per current 3GPP standards, handover between cellular and WLAN is always UE initiated. When the UE detects a preferred access, e.g., based on received ANDSF Inter System Mobility Policy (ISMP), the UE provides a "handover" indication in the attach request over the preferred access. This handover indication enables the PGW to maintain the IP address for the UE and act as a mobility anchor between the two access networks thereby allowing for a *seamless* handover. For the case of handover, all IP flows belonging to the same PDN connection are moved from the source access system to the target access system.

3GPP TS 23.402 [7] supports two mechanisms for mobility between cellular and WLAN, namely "host based mobility" (HBM) and "network based mobility" (NBM). HBM specifies the use of DSMIPv6 between the UE and the MCN, whereas NBM specifies the use of GTPv2 or PMIPv6 protocols between the access networks (cellular and WLAN) and the MCN.

Because the UE may not be able to provide any APN information over the Wi-Fi network (e.g., in the case of NBM), then it may be ambiguous as to which session the handover indication refers to. In such circumstances, one approach is to assume that the Wi-Fi access corresponds to the default-APN. This may be problematic, e.g., if operators have chosen to configure the IMS-APN as the default APN.

> Note, the current Gx based interface to the PCRF supports [42] Host Based Mobility and not Network Based Mobility.

3.4.2 Use Case 2a: Non-Seamless WLAN Offload (NSWO)

To alleviate congestion in both the licensed cellular spectrum and in the mobile core network (MCN), operators may use NSWO to permit dual-mode subscribers to use WLAN when available for direct Internet or local IP network services. The MCN bypass is typically done via a local breakout in the WLAN access network. The traffic to be offloaded may be identified in the UE via pre-configuration or may be provisioned via policy updates such as those defined for ANDSF Inter System Routing Policy (ISRP) for Non-Seamless WLAN Offload (NSWO).

> Note, the MCN is typically responsible for providing certain regulatory services including intercept, and these will still likely be required to be applied to NSWO traffic.

Non-Seamless WLAN Offload (NSWO) provides traffic management *without IP address preservation* between cellular and WLAN accesses. For NSWO traffic, the UE IP address assigned by the WLAN is not managed by the

MCN, hence, there is no IP address preservation and any transition between access networks will be "non-seamless".

Discovery and selection of preferred WLAN access points for NSWO may be facilitated by pre-configured operator policies, user preferences, ANDSF policy updates, or Hotspot 2.0 mechanisms. Depending on the service being provided, the application being used, and the tolerance of the user, the non-seamless transition may or may not be perceptible. For instance, the transition might not be noticeable if it occurs while the user is reading an email or a web page. Also, the buffering capability of a device may hide the transition during adaptive bit rate video streaming. However, real-time conversational services would most certainly be impacted, e.g., if required to onload back to the cellular network.

3.4.3 Use Case 2b: Cellular Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO)

To reduce MCN traffic while still using cellular access technologies, 3GPP has standardized two approaches for MCN offload, namely, Local IP Access (LIPA) and Selected IP Traffic Offload (SIPTO).

LIPA was standardized in 3GPP Release 10 and specifically enables a UE to communicate with IP devices on a local network via a Home eNodeB "small cell". LIPA uses a Local Gateway (L-GW) that may be co-located with the HeNB. A UE may request a LIPA PDN connection and the network may then select the L-GW associated with the HeNB if the user subscription allows it. (SCF has analysed the use of LIPA within Enterprise 3G and LTE Small Cell deployments in their document [4]).

SIPTO was initially standardized in Release 10 for the case where MCN gateways (SGW and PGW) are selected based on their proximity to the UE. By selecting gateways closer to the UE, traffic delay can be reduced and the MCN may experience less congestion. This technique is usually referred to a "SIPTO above the RAN" because the offload takes place within the MCN.

SIPTO was subsequently expanded in Release 12 to address SIPTO "at the Local Network" (SIPTO @LN). This approach uses L-GW functionality such as that defined for LIPA and enables the UE to access the Internet directly from the local IP network. Two flavours have been standardized. One case involves co-location of the L-GW with the (H)eNB. The second case involves a standalone L-GW (separate from the HeNB) and requires co-location with an SGW function in the local network.

Operation of SIPTO and/or LIPA may impact regulatory obligations as discussed in [4].

3.4.4 Use Case 3: Multiple Access PDN Connectivity (MAPCON)

For DSMIPv6 enabled terminals capable of concurrent MCN access via cellular and WLAN (i.e., "multiple access"), another option is to enable access to services from different PDNs via the two access networks, i.e., effectively using two different APNs. In this case, the user is assigned two different IP addresses for exclusive use in the two different PDNs. Although both IP addresses may be assigned by MCN network elements, the two addresses are managed separately and there is no IP address preservation (i.e., similar to the case of a cellular UE with simultaneous access to two independent APNs). In this case the transition of PDN services across access networks is not applicable.

A use case for MAPCON-enabled terminals and networks is one where the operator uses ANDSF ISRP policies to guide VoIP sessions over the cellular interface to an IMS PDN, while guiding email sessions over the WLAN to a corporate PDN through the MCN.

3.4.5 Use Case 4: IP Flow Mobility (IFOM)

For DSMIPv6 terminals capable of simultaneously accessing *the same PDN* via both cellular and WLAN access, 3GPP enables the capability to dynamically move IP flows from one access to the other, e.g., based on ANDSF ISRP, user preferences, or local conditions in the UE. This is referred to as "IP flow mobility" (IFOM) [29].

3GPP Release 10 has provided a standard IFOM solution based on extensions to DSMIPv6 whereby the PGW Home Agent (HA) acts as the anchor point for the IP flows. When a UE configures different IP addresses on multiple accesses, it can register these addresses with the HA as Care-of-Addresses (CoAs) using multiple bindings as specified by the DSMIP extensions in IETF RFC 5648 [43].

For this use case, VoIP traffic may initially be routed over the cellular access in order to provide lower latency and better reliability over the licensed spectrum, while other non-voice traffic, e.g., IMS-video, can be routed over the WLAN (with both services provided via the same PDN). If the cellular access subsequently becomes congested, the VoIP flow can be moved *seamlessly* to the WLAN access.

3.4.6 Use Case 5: Multipath TCP connection (MPTCP)

Whereas 3GPP has defined DSMIPv6/S2c to effectively support simultaneous multi-path communications over two Care-of-Addresses, there are alternative protocols that can be used to effectively bond multiple IP streams over different access networks together.

One alternative is through the use of Multi-Path TCP (MPTCP) which has been developed by the IETF MPTCP group, 0. In this approach, both the UE and the application provider (i.e., both sides of TCP peers) support Multipath TCP. One TCP connection is composed of multiple sub-TCP flows. There are three modes of operation of MPTCP, “full mode” which has both paths active, backup mode (e.g., where Wi-Fi is preferred while sub flows are open on 3G as a backup) and single path mode (one path only). Hence, one TCP-based application can run across multiple connections, e.g., both WLAN and the cellular network. The TCP flows can be dynamically created or removed and the new IP addresses of the UE can be acknowledged by the service provider side. This results in the seamless mobility for the TCP connection. .

3.4.7 Traffic Manager Function

By Traffic Manager, we refer to a network functional entity that coordinates the traffic management use cases described above. A natural place for the traffic manager is in the PGW node of the EPC, but interesting alternate possibilities exist, as described in a SCF white paper on ISW Networks [5].

Scenario 1: The traffic manager is part of EPC

In this scenario the traffic manager is part of PGW/HA, as shown in Figure 20. The traffic manager moves the IP flows seamlessly between Wi-Fi access point and 3GPP based Small Cell for terminals capable of simultaneously accessing the same PDN via both cellular and Wi-Fi access. Thus, based on UE requests (e.g., based on RFC 6089 [45]), the traffic manager can offload the traffic from licensed 3GPP spectrum to unlicensed Wi-Fi spectrum. The traffic manager can also distribute the IP flows based on the policy and traffic category. For terminals capable of accessing a PDN via only one radio access, the traffic manager moves all the IP flows belonging to the same PDN connection when there is handover between cellular and Wi-Fi. In this scenario, the S2c-over-S2a and S2c-over-S2b interfaces are used for trusted Wi-Fi access and untrusted Wi-Fi access respectively. Figure 20 only depicts the case where S2a is used between the WiFi AP and the PGW/HA; however, S2b and S2c based implementation are also possible. The UE IP’s address is preserved by the PGW/HA during the handover.

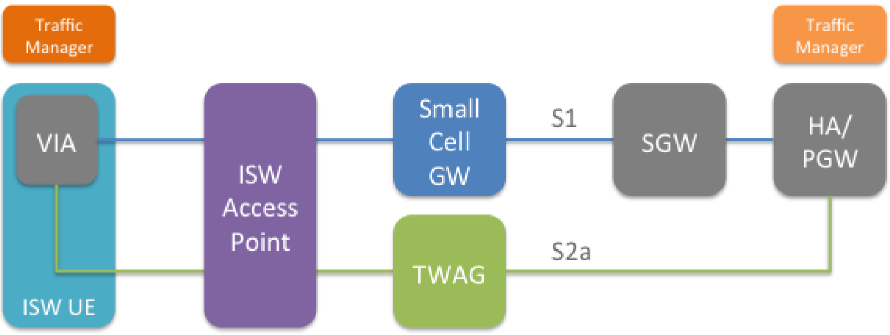


Figure 20: PGW-based Traffic Manager

A typical realization of a traffic manager may include the following functions: (1) Handover and Flow Mobility protocols; (2) possibly Deep Packet Inspection (for network controlled traffic management use cases); (4) Virtual Interface Adaptor (VIA) functionality for making changes from established socket interfaces; and (4) possible interfaces to Operator Policy Servers, such as ANDSF Server. Figure 21 below illustrates the concepts. It is to be noted that Traffic Managers are not standardized and tend to be vendor and operator defined.

> Note, 3GPP does not currently support network controlled/pushed IP Flow Mobility signalling, instead specifying these to be always triggered by the client using RFC 6089 extensions [45].

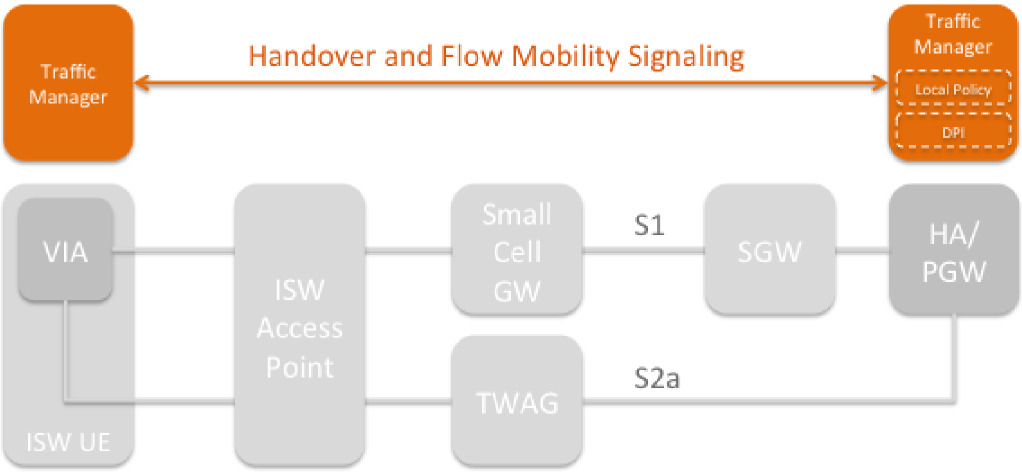


Figure 21: Exemplary Functional Architecture of a Traffic Manager

Alternative Scenarios

Alternative scenarios may be considered with the traffic manager function being co-located with the Small Cell GW or with the ISW Access Point. Such scenarios will require the traffic manager to be able to associate a session established over the Wi-Fi network with a session established over the Small Cell Network, e.g., by making use of a common IMSI based permanent user identity over both Wi-Fi and Small Cell networks.

A recent white paper from SCF identifies the benefits of providing joint radio resource management for a multi-mode (3G/LTE) Small Cell [46]. Such an approach can be enhanced to examine the case of the multi-technology LTE/Wi-Fi ISW Access Point. However, such enhancements need to recognize, that whilst there is convergence in the network controlled handover approaches in the original 3G/LTE study, the ISW approach may need to take into account the different approaches to handover from LTE and Wi-Fi, with the latter being primarily triggered by the UE.

In one alternative the Traffic Manager is realized at the SC-GW and TWAG/TWAP level, whereas in another alternative, it is realized at the ISW-AP. Figure 22 and Figure 23 below illustrate these concepts, neither of which are standards based. These figures show the scenario where the S2a interface is used for the Wi-Fi access, however similar architectures are possible with the S2b and S2c interfaces. Note that placing the Traffic Manager at the SC-GW and TWAG/TWAP level or ISW-AP level does not preclude the presence of a traffic manager function in the PGW that routes traffic over the S1 and/or the interfaces between the WLAN AP and PDN GW.

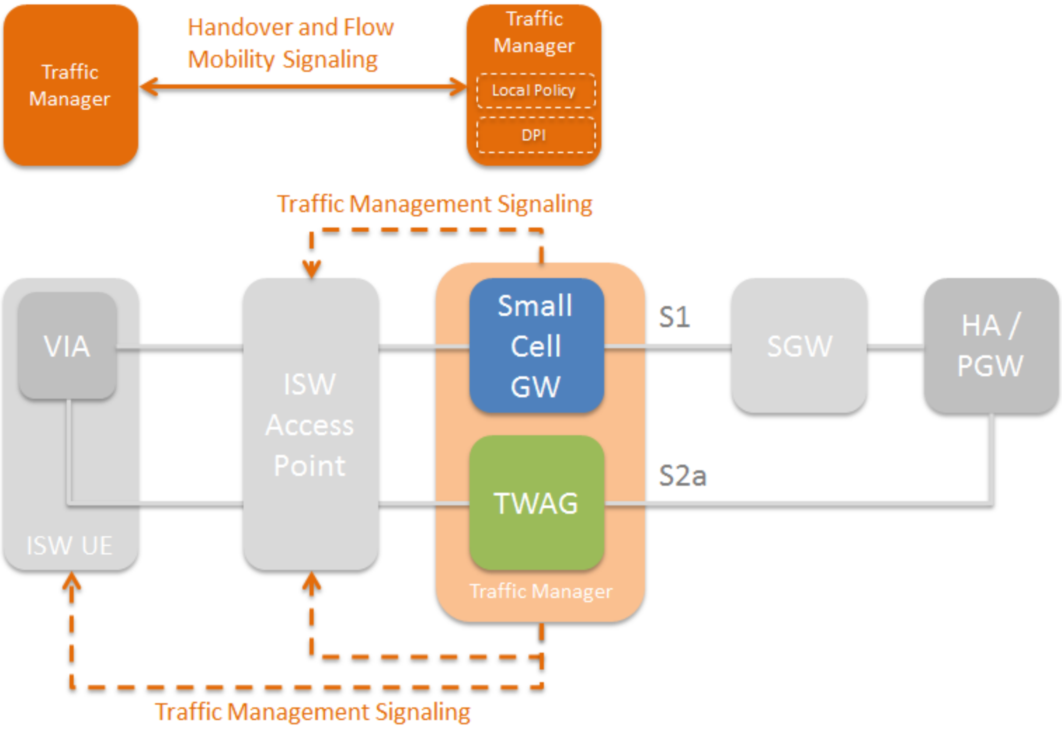


Figure 22: Gateway-based Traffic Manager

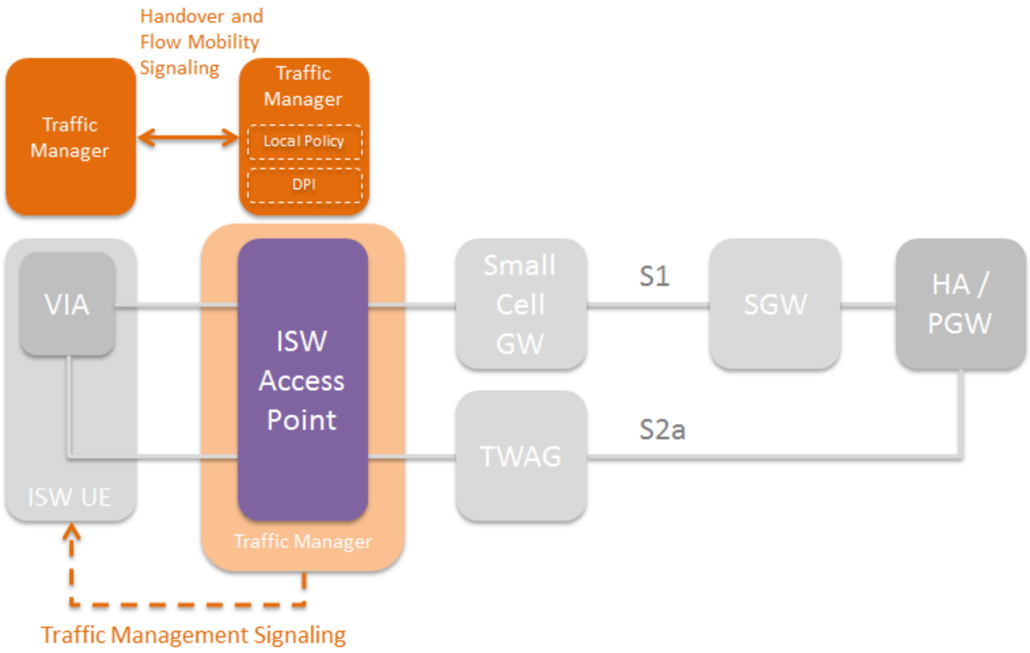


Figure 23: AP-Based Traffic Manager

Identified Topics For Further Study: It may be of value to consider alternate ISW-architectures, due to their potential benefits of reduced core network signalling and distribution of functions. Examples include architectures where the Traffic Management function is located in either the GWs or APs.

3.5 ISW User Mobility Management

Whereas the previous section dealt with movement of user traffic across different radio interfaces, this section deals with the mobility of the users between APs of varying capabilities.

UE moves from an ISW-AP (source) to another ISW-AP (target)

This scenario leverages standard access network procedures.

- UE has bearers established with both LTE and Wi-Fi accesses.
- The common RRM or traffic manager decides to move the UE with all bearers to the target base station
- The common RRM or traffic manager signals the source ISW Access Point to effect the handover of both LTE and Wi-Fi connections
- Handover of LTE bearers happens using LTE signalling as defined in 23.401 [47]
- Handover of Wi-Fi bearers shall happen according to the WLAN specifications.

  Note, the UE may have to be triggered to initiate setting up the Wi-Fi bearers in the target base station, e.g., by using a BSS transition procedure

- The S1 and S2a sessions are re-established from the target ISW Access Point
- The services are restored normally in target base station

UE moves from source SW-AP to target Wi-Fi-AP

- UE has bearers established with both LTE and Wi-Fi accesses.
- The common RRM or traffic manager decides to move the UE with all bearers to the target (Wi-Fi only) base station
- The common RRM or traffic manager signals the source ISW Access Point to effect the handover of the Wi-Fi connections
- Handover of Wi-Fi bearers shall happen according to the WLAN specifications.

  Note, the UE may have to be triggered to initiate setting up the Wi-Fi bearers in the target base station, e.g., by using a BSS transition procedures

- The S2a session is re-established from the target ISW Access Point

- S2c procedures are used to ensure that the services are restored normally in target base station with IP Flows that were being transported over LTE now being transported over Wi-Fi.

UE moves from source 3G SC-AP to target LTE SC-AP

In case of single mode UMTS base station handover to single mode LTE handover, per specification definition today the core network elements of both UMTS and LTE network will have to be involved. The procedure is defined in 23.401 [47].

UE moves from source ISW-AP to target LTE SC-AP

In case a UE that has PS bearers with both Wi-Fi and LTE Core network and it needs to be handed over to a LTE only base station, the Wi-Fi bearers will be released and S2c procedures used to carry the flows previously carried over the Wi-Fi bearer over the LTE bearer in the target Small Cell.

UE moves from source Wi-Fi-AP to target ISW-AP

This scenario shall follow the Wi-Fi specification to move the Wi-Fi bearers to target Wi-Fi-SC base station.

UE moves from source SC-AP to target ISW-AP

This scenario shall follow the 3GPP TS 23.401 [47] for moving from source LTE small cell to target Wi-Fi-SC base station.

3.6 Online Signup, Policy, and Subscription Remediation services for Wi-Fi

As mentioned in Section 3.1, the Wi-Fi Alliance's Hotspot 2.0 program addresses the issues of registration and provisioning. Specifically, the upcoming Release 2 specification will introduce new capabilities and functional entities to support Wi-Fi client account registration, credential provisioning and subscription management. Hotspot 2.0 Release 2 will serve as the technical foundation for the WBA's NGH Phase 2 Step 2 trials.

Online Sign-Up (OSU) provides the capability for a hotspot operator to advertise to Wi-Fi clients that they may sign up for service (from this operator and/or roaming partners). This allows a previously unprovisioned/uncredentialed client to register for and receive service on demand. The availability of one or more OSU providers is advertised to clients via enhancements to ANQP and Hotspot 2.0 information elements, meaning that the device does not need to be associated to the Hotspot 2.0 WLAN in order to receive the OSU information. The available OSU providers are presented to the user as a text list, icons, or combination of icon with text description. When the user selects a specific OSU provider, this triggers the Wi-Fi connection manager to associate to a provided OSU WLAN and then opens a browser session to a provided OSU URL. The user then provides the necessary registration information and is provisioned with either a username/password or certificate credential and any associated policy or parameters for use with that credential.

Release 2 implements new Wi-Fi security features to ensure that the OSU process is secured and the client can authenticate the validity of the OSU server. One use case for Online SignUp would be to add a Wi-Fi only device to a mobile subscription, issuing a TLS or TTLS credential to the device and associating it with the existing subscription.

In addition to the credential itself, Passpoint Release 2 can also be utilized by the credential issuer to provision policy and subscription parameters regarding the credential. Some examples of the kinds of parameters that can be provisioned include:

- Preferred Roaming Partners (based on Hotspot 2.0 Domain Name);
- SSID Blacklist (do not use this credential on the listed WLANs);
- Usage Limits (time or data based);
- Minimum Backhaul Requirements;
- Required Protocol Tuple Connectivity; and
- Subscription Expiration.

The Release 2 specification also includes mechanisms for the credential issuer to inform the client of any needed remediation, which triggers a client connection to the Policy Server or Subscription Remediation Server. Release 2 utilizes the Open Mobile Alliance Device Management (OMA DM) framework or SOAM/XML to signal the credential and associated parameters to the device. A new OMA DM Management Object (MO) is defined for this purpose. Communication of the MO contents from the server to the client is performed using HTTPS with either SOAP XML or OMA-DM formatting.

4. Architectures

Having introduced the Architecture Framework in Section 1, described the main building blocks in Section 2 and network level functions and use cases in Section 3, we now devote this section to develop more detailed end-to-end network and system architectures. It must be noted that some of these architectural designs are standardized by 3GPP, whereas others are example options provided by vendors and/or proposed for deployment by Operators. We shall strive to make these distinctions clear within the section.

4.1 Cellular and Wi-Fi Network Integration Architectures

This section describes architectures where the cellular and Wi-Fi integration takes place in the MCN 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. These were depicted earlier in Section 2.3.3 and reproduced here for convenience.

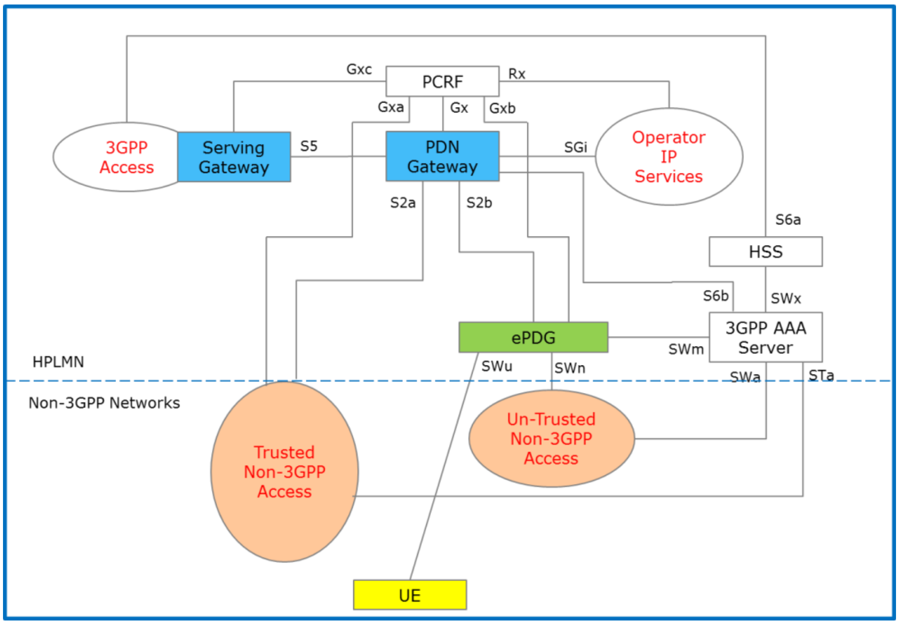


Figure 24: Cellular & WiFi Integration: Network-based (S2a/b) Mobility Architecture

With the evolution of 3GPP's packet core network capabilities, operators are now able to integrate trusted non-3GPP radio access technologies into a converged Evolved Packet Core (EPC) function [7]. Originally defined for integrating wide area non-3GPP radio access networks based on cdma2000 and WiMAX, these same core capabilities can be used to enable Service Provider Wi-Fi solutions to be integrated with standardized EPC functionality. Using such an approach, operators are able to leverage existing policy, charging and regulatory capabilities defined for cellular access and re-apply those to users accessing the network using trusted Wi-Fi based access networks.

Compared with the end-to-end definition of 3GPP based access networks, 3GPP remains less prescriptive in terms of how non-3GPP Access Networks are realized. The generic architecture then defines a Trusted WLAN Access Network that integrates a Trusted WLAN AAA Proxy and a Trusted WLAN Access Gateway. The TWAP supports DIAMETER based STa interface towards the 3GPP AAA server for authentication of the user. The TWAG supports GTPv2/PMIPv6 based S2a interface for user plane tunnelling and user plane tunnel management functionality between the TWAN and 3GPP PDG Gateway. The TWAN can manage roaming and non-roaming use cases.

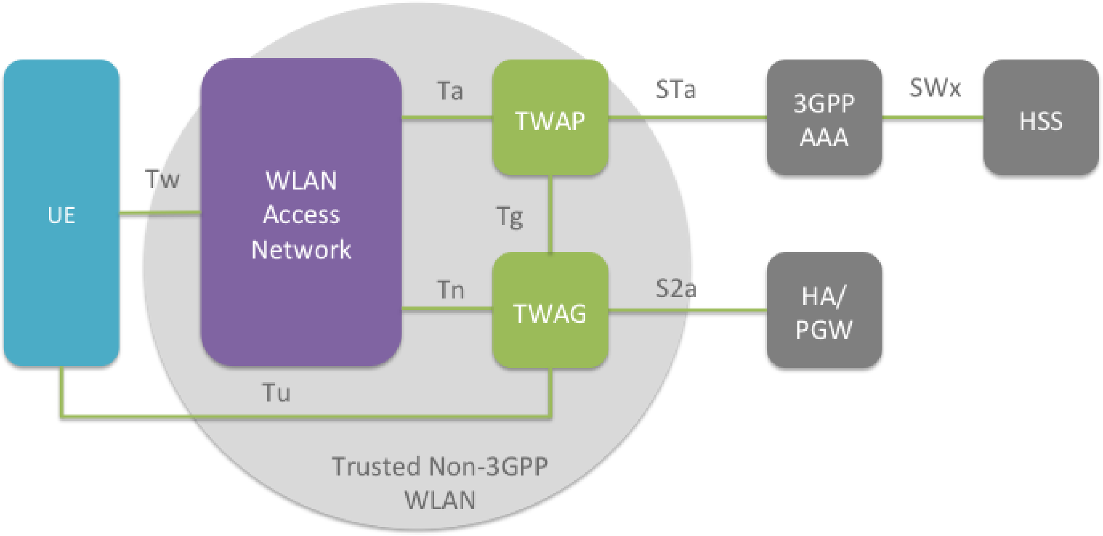


Figure 24: Trusted WLAN (TWLAN) Network Architecture

4.1.1 Small Cell and Wi-Fi Network Integration Architecture

While the architecture in Figure 25 above applies to general integration of Cellular and Wi-Fi Networks, the following Figure 26 focus 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 MCN. 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 MCN.

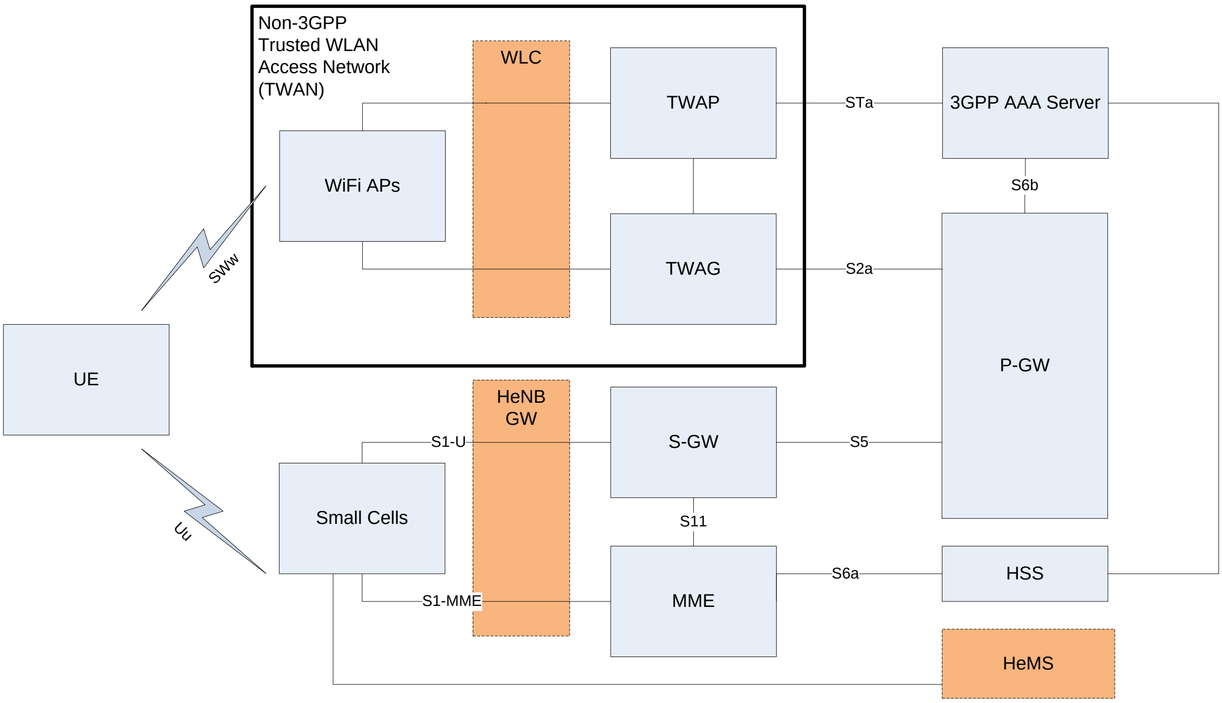


Figure 25: Multi-access TWAN and multi-access small cell network

Figure 27 below illustrates the optimized case where the Small Cell and Wi-Fi are integrated into a single Access Node. Such implementations have the advantages of sharing of hardware, software, power, backhaul, secure housing etc.

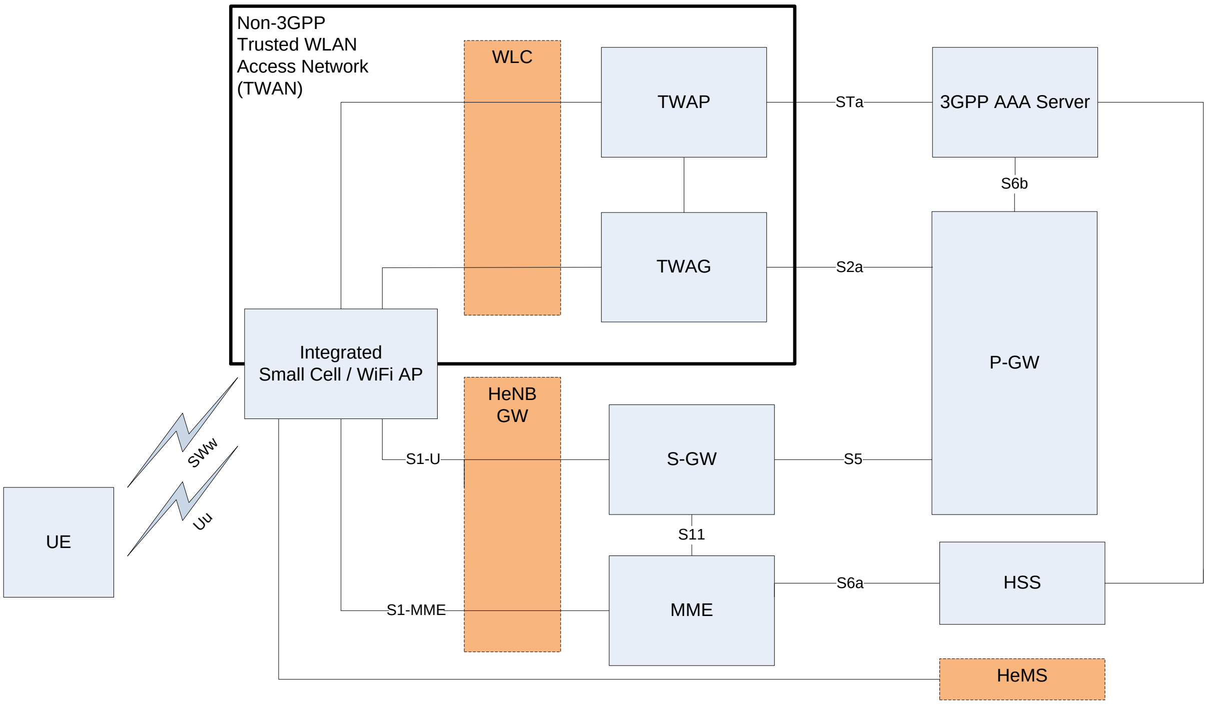


Figure 26: Integrated Small Cell / Wi-Fi AP

4.2 Trusted WLAN Access Network (TWAN) Architectures

The aim of this section is to provide details regarding the different options available about 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.

4.2.1 TWAN Forwarding Models (Control and Data Plane)

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 un-licensed 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 25 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 using alternative vendor-specific protocols. In whichever case, the control plane but should be secured using robust encryption.

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 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 52: WLAN Configuration Options

4.2.2 TWAN Integration Options

When the WLAN configuration examples are considered, at least 6 different options for realizing TWAG and TWAP functionality can be considered as illustrated in Figure 28 below, showing options for integrating WLC Centralized Forwarding, WLC Distributed Forwarding, and Autonomous AP deployments.

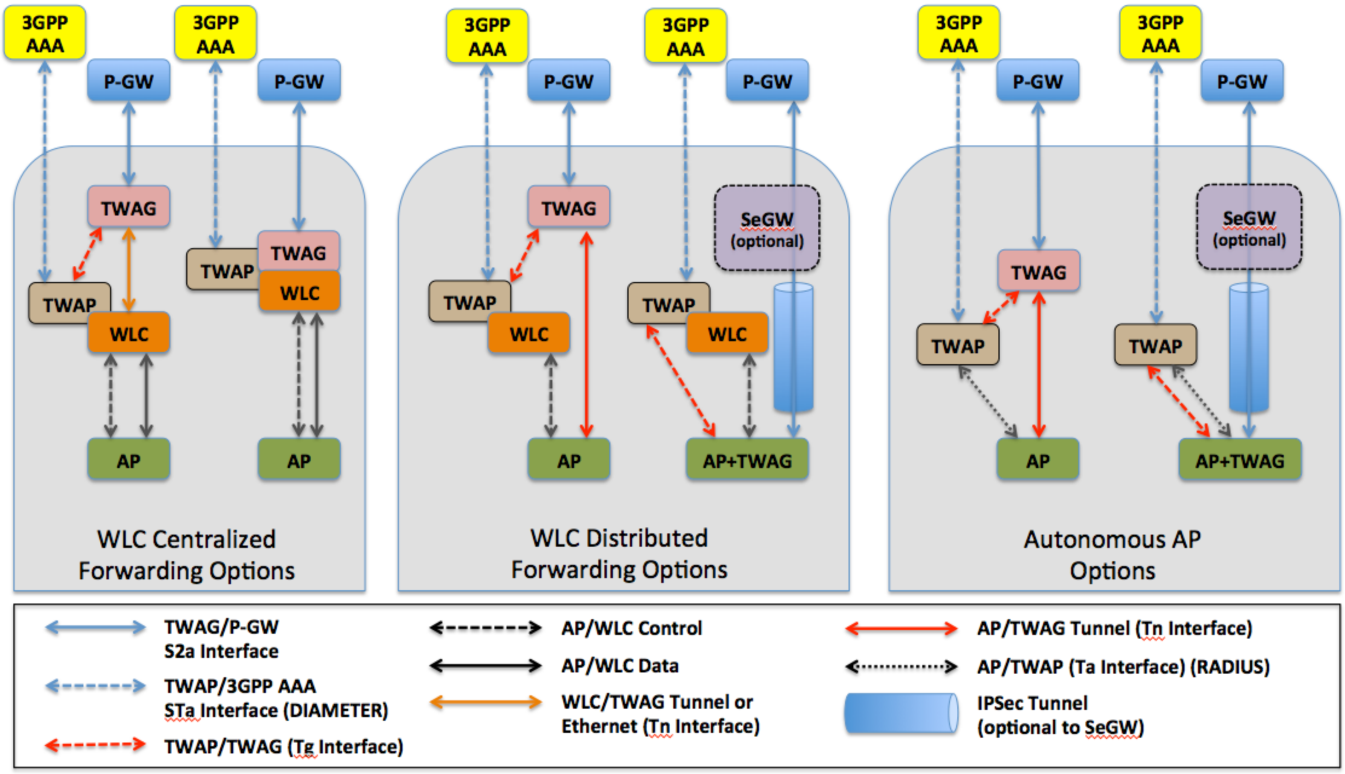

3GPP AAA
P-GW
TWAG
TWAP
WLC
AP
WLC Centralized Forwarding Options
SeGW (optional)
AP+TWAG
WLC Distributed Forwarding Options
Autonomous AP Options
TWAG/P-GW S2a Interface
TWAP/3GPP AAA STa Interface (DIAMETER)
TWAP/TWAG (Tg Interface)
AP/WLC Control
AP/WLC Data
WLC/TWAG Tunnel or Ethernet (Tn Interface)
AP/TWAG Tunnel (Tn Interface)
AP/TWAP (Ta Interface) (RADIUS)
IPSec Tunnel (optional to SeGW)

Figure 27: TWAN Integration Options

In all of these various models, the TWAG function (whether implemented as a standalone gateway or integrated into the WLC or AP) is responsible for mapping the UE data plane session into an S2a connection to the P-GW.

For the AP to WLC control and data plane connectivity there are a number of common protocol implementations, as shown in Table 6:

Control Plane	**Data Plane**
CAPWAP-Control RFC 5415 [21]	CAPWAP-Data
SSH	GRE
SLAPP RFC 5413 [49]	802.1Q VLAN Tagging

Table 6: Examples of protocols for AP to WLC control and data plane connectivity

In the model utilizing WLC centralized forwarding and a separate TWAG (the left most model shown in Figure 28 above), the data plane connection between the WLC and TWAG may be implemented as a direct L2 Ethernet connection or via a tunnelling protocol. In the models showing a direct data plane connection from an AP with tunnel support to the TWAG, tunnelling protocols such as L3-GRE, L2-GRE can be utilized. .

Figure 28 above also shows various implementations of the TWAP functional entity within the TWAN. In the WLC models, there is an implied connection from the WLC to the TWAP (either an external standalone system or an embedded service on the WLC). The WLC communicates with the TWAP, typically using the RADIUS protocol, in order to forward the UE authentication requests to the 3GPP AAA which then forwards the requests to an authentication peer like HSS. In the case of Autonomous APs, the AP would have a direct RADIUS connection to a standalone TWAP. The TWAP interfaces to the 3GPP AAA server in the EPC over the STa reference point using the DIAMETER protocol.

There is also a Tg logical interface between the TWAP and TWAG. This is used to communicate the UE's authentication state and S2a tunnel management information between the TWAP and TWAG.

It is worth noting that the BroadBand Forum WT-229 [50] working text proposes the implementation of a TWAG function on the Broadband Network Gateway (BNG). Where a BNG is used in the access network, it could be integrated with the TWAG to fulfil the role of standalone TWAG in any of the models shown in the figure above. Alternative access networks may look to offer enhanced capabilities by integrating TWAG into alternative legacy elements, e.g., TWAG integrated into CMTS for HFC based access networks.

4.3 Example Architectures

4.3.1 Nanocell System Architecture (China Mobile)

Some architectures of Small Cell and Wi-Fi integration are explored in this section. One of the architecture is called as "Nanocell", which integrate both Cellular and Wi-Fi in the single box/unit, sharing the same power supplier, the same backhaul but provides both cellular and operator owned Wi-Fi services

Nanocell integrates the functionalities of Smallcell with WLAN. The cellular and Wi-Fi in Nanocell provide the same service as macro cellular cell and operator deployed public Wi-Fi access. Therefore, the basic requirement is that the Nanocell can access both cellular core network (i.e., EPC for LTE case) and Wi-Fi (i.e., WLAN access controller and authentication system).

Note: the cellular part of Nanocell could be 2G/3G/LTE. This section explores the LTE case for illustration.

The Nanocell architecture is shown in Figure 29 below. There are three parts shown in the architecture: (a) EPC Core Network, (b) WLAN Access Control; (c) Newly added entities related with Nanocell. The LTE part of the Nanocell follows H(e)NB architecture defined in 3GPP. The Nanocell WLAN part is the same as the WLAN architecture, in which the Nanocell is connected to the authentication system through the backhaul network and the interfaces with AC, Portal and AAA. In this way, both Web portal authentication and automatic authentication mechanisms such as EAP-SIM/AKA/PEAP can be supported.

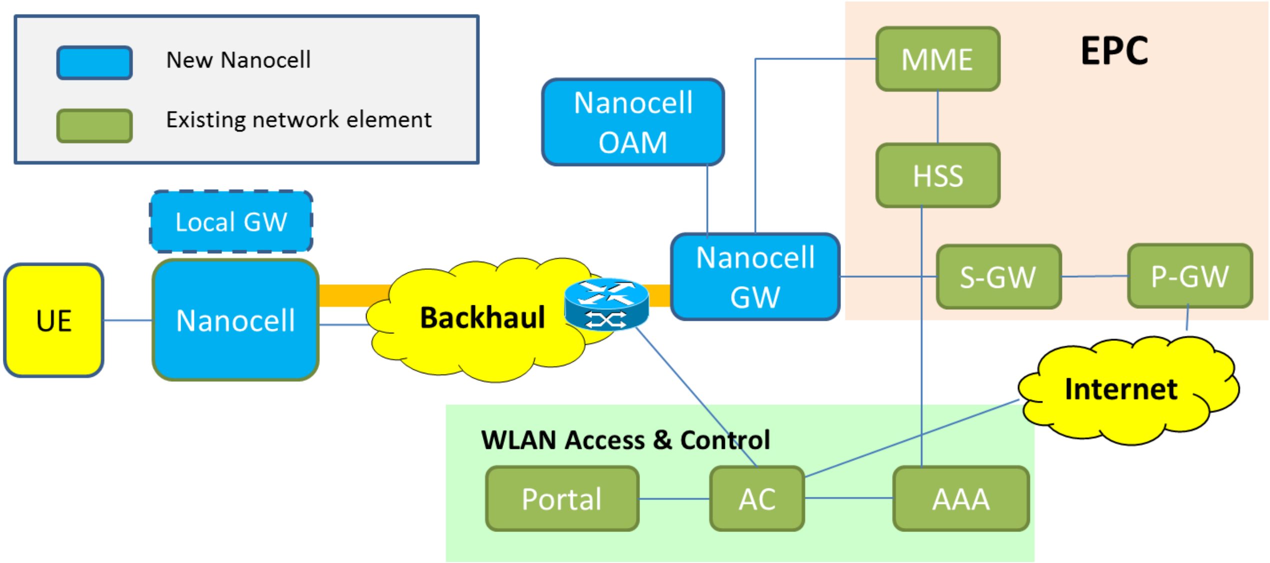


Figure 28: Nanocell System Architectur

The Nanocell related entities are introduced as below.

1) **Nanocell**. It is used to provide cellular access for terminals using the Uu interface. It also provides WLAN IEEE 802.11 access module.

2) **Nanocell Gateway**. It is used to provide mutual authentication with the Nanocell. And it protects S1 interface and the messages between Nanocell and the network management system using IPsec. When the number of Nanocell is large, it can be configured to aggregate the S1 signal interface to reduce the impact to the MME.

3) **Nanocell OAM**. It is used to manage the Nanocell and Nanocell gateway, configure the parameters of Nanocell and conduct performance management.

4) **Backhaul Network**. To provide flexible ways of access, both wired and wireless backhaul should be considered to convey the Wi-Fi and LTE signalling/data traffic.

5) **Local Gateway**. It is an optional function. It is used to route the data packets via the local network to the local IP services. This can provide local IP access and also alleviate the traffic load on backhaul and the core network.

6) **Interface between Nanocell and AC**. To support multi-vendor environment, the Nanocell shall use the 'core' CAPWAP protocol [21, 51] to between its Wi-Fi part and AC.

4.3.2 Small Cell- Wi-Fi System Architecture (AT&T)

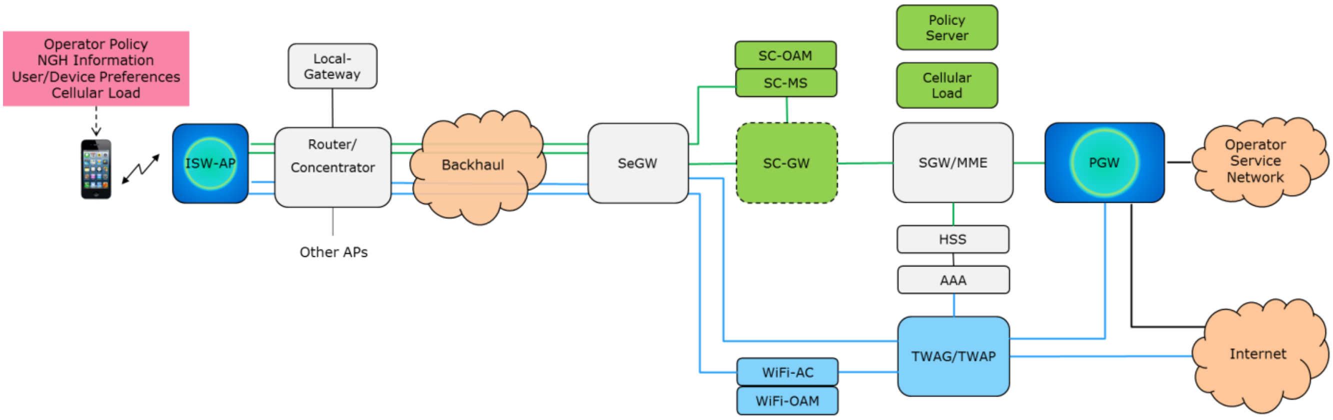


Figure 29: ISW Network Architecture

The ISW Network architecture illustrated in Figure 30 consists of one or more ISW-APs connected to the Operator Core Network over a possibly insecure Backhaul Network using a SeGW. The ISW-APs may be aggregated via local Concentrator function and connected to a Local Gateway to access local IP networks and services. Communication over the backhaul may be secured by encrypted IPSec tunnels, which may be a single tunnel or one for each technology (3G, LTE and Wi-Fi). The Small Cell and Wi-Fi user data and control traffic traverse to the SGW/MME and TWAG/TWAP respectively, with the Small Cell traffic possibly passing through a SC-GW in case of LTE Small Cells.

The Small Cell and Wi-Fi APs are respectively provisioned, controlled and managed by SC-Management System and Wi-Fi Access Controllers respectively. Performance Management etc are handled by their respective OAM systems, as shown. The communication channels are routed via encrypted IPSec tunnels between the ISW-AP and the SeGW (or may alternately be secured via Transport Layer security methods).

Users are authenticated via the HSS and AAA for Small Cell and Wi-Fi attached users respectively. The Small Cell and Wi-Fi traffics converge at the PGW, which manages seamless IP-address-preserving mobility of the UE between the two accesses. Note that Small Cell nodes and interfaces are colored in green, whereas blue color is used for Wi-Fi. Since the two technologies converge at the ISW-AP and PGW, these nodes are shown in dual color.

Selection of Small Cell and Wi-Fi accesses is managed by an Operator Policy Server (ANDSF based) and Cellular Load function on the network side. Correspondingly, the UE can perform intelligent selection of networks based on Operator Policies, User and Device Preferences as well as Load conditions of Cellular/SC and Wi-Fi networks. Some or all of these may be communicated to the UE statically, or semi-statically or dynamically using techniques that are under development within the standardization bodies and vendor community.

5. Standards

This section serves to as a reference for standards addressed elsewhere in this document. More importantly, it serves to identify and clarify the following:

- Role of Standards Organizations and Industry Forums that contribute to ISW integration.
- Catalog of major standards, protocols, and best-practice documentation that guide ISW networking.
- Briefing on those standards and documents that most directly address ISW networking
- Identification of “Gaps” – areas of interoperability not yet standardized

5.1 Standards “Gaps”

The following areas have been identified which remain in need of standardization or definition for implementation.

5.1.1 Trusted Wi-Fi Network Reference Architectures

Documentation of common architectures in terms of AP, AC, and OAMP systems. This should include Radio Resource Management (RRM), Mobility, and client-side 3GPP-defined TWAG/TWAP interfaces.

5.1.2 Unified, Functional Standardization for Integrated SC-Wi-Fi APs

Standardization should be expanded to include: Shared backhaul optimizations, shared geo-location information, enhanced discovery, security, and the extension of SC-AP interfaces to carry Wi-Fi information

5.1.3 Integrated Policy Framework for SC and Wi-Fi Networks

Unified SLA and other policy framework definitions across both SC and Wi-Fi networks, potentially to include backhaul network policies allowing uniform management of subscribers regardless of air interface connection.

5.1.4 Interoperability Specification for AP-AC Connectivity

Interoperability definition to include architecture, protocol selection including configuration parameters, and best practices for connecting multi-vendor AP and AC environments.

5.1.5 Unified Self-Organizing Network (SON) Definitions for ISW APs

Self-Organizing Network (SON) interface protocols have not yet converged around interoperable standards for licensed-frequency small cells, let alone for multi-radio network elements. As SON standards develop for 3GPP networks, WLAN integration should be included across all major areas of SON, including: Automated Neighbor Relations (ANR), Self-configuration, Self-optimization, and Self-healing.

SON Energy Efficiency developments should also consider joint management of SC and Wi-Fi elements.

5.2 Standards Organizations and related Working Groups Targeting ISW Networking

5.2.1 3rd Generation Partnership Program (3GPP)

3GPP addresses multiple ISW networking interfaces and related protocols. 3GPP specifications are released in 3 Stages:

> “Stage 1" refers to the service description from a service-user’s point of view

> "Stage 2" is a logical analysis, breaking the problem down into functional elements and the information flows amongst them across reference points between functional entities

> "Stage 3" is the concrete implementation of the protocols appearing at physical interfaces between physical elements onto which the functional elements have been mapped

Services and Systems Aspects (SA):

- **SA - WG1, Services**
  Stage 1. SA WG1 Service and feature requirements applicable to mobile and fixed communications technology for mobile network, IMS and fixed-mobile convergence when mobile is involved.

- **SA - WG2, Architecture**
  Stage 2 of the 3GPP network. SA WG2 identifies the main functions and entities of the network, how these entities are linked to each other and the information they exchange.

- **SA - WG3, Security**
  Stage 2 and stage 3 - Security and privacy in 3GPP systems, determining the security and privacy requirements, and specifying the security architectures and protocols.

- **SA - WG5, Telecom Management**
  Stage 2 and Stage 3 - SA WG5 will specify the requirements, architecture and solutions for provisioning and management of the network (RAN, CN, IMS) and its services

Core Network and Terminals (CT):

- **CT - WG1, Services**
  Stage 3. Responsible for definition of protocols and related functions involving directly the UE

- **CT – WG3, Internetworking with External Networks**
  Stage 3. Specifies the bearer capabilities for circuit and packet switched data services, the necessary interworking functions towards both, the user equipment in the UMTS PLMN, and the terminal equipment in the external network. CT is also responsible of end to end QoS for mobile network.

- **CT – WG4, MAP / CAMEL / GTP / BCH / SS/ TrFO / IMS / GUP / WLAN**
  Stage 2 and Stage 3 aspects within the Core Network focusing on Supplementary Services, Basic Call Processing, Mobility Management within the Core Network, Bearer Independent Architecture, GPRS between network entities, Transcoder Free Operation, CAMEL, Generic User Profile, Wireless LAN - UMTS interworking and descriptions of IP Multimedia Subsystem. CT WG4 is also responsible as a "protocol steward" for the some IP related protocols (this involves analyzing, validating, extending if necessary, clarifying how they are used, specifying packages and parameter values).

Radio Access network (RAN):

- RAN – WG2, Radio Layer 2 & 3 specs

5.2.2 Broadband Forum (BBF)

BBF develops multi-service broadband packet networking specifications addressing interoperability, architecture and management. BBF also defines best practices for network service implementation. ISW contributions include extension of existing AP OAMP definitions, SLA/management parameter definitions, and ISW internetworking specifications.

5.2.3 Institute of Electrical and Electronics Engineers (IEEE)

IEEE is the home of Wi-Fi (802.11) technical definitions within the 802 Ethernet Standards. 802.11 standards are often referenced in WLAN operation and management for ISW.

5.2.4 Internet Engineering Task Force (IETF)

The IETF focuses on defining interface protocols for internet-related architectures.
Multiple ISW protocols, such as those used for authentication methods now common to SC and WLAN UE, are defined in IETF.

5.2.5 Open Mobile Alliance (OMA)

Based on our review, some OMA specifications (i.e., device provisioning, management, connection manager, etc.) would need to be modified in order to efficiently support ISW cell service.

5.2.6 CableLabs (CL)

MSO-member driven organization that researches new broadband technologies, authors specifications, and performs vendor certification/qualification. CableLabs worked on the specifications for Wi-Fi integration with existing CableLabs-defined architectures. CL also created the specification that describes an integrated Wi-Fi and Pico cell.

5.3 Industry Associations involved in ISW Networking

5.3.1 GSM Association (GSMA).

GSMA has recently focused on the support of Wi-Fi network access. GSMA has independently, and jointly with WBA, worked on the specifications and white papers to identify related issues and specify requirements.

5.3.2 Small Cell Forum (SCF)

The Small Cell Forum is a co-author of this document and has released several other documents that discuss Integrated Small Cell / Wi-Fi Networks.

- SCF White Paper, "Wireless in the home & office: the need for both 3G femtocells and Wi-Fi access points", Release-1, Doc No. SCF-007, 2013, http://www.scf.io/en/documents/007_Wireless_in_the_home__office_the_need_for_both_3G_femtocells_and_Wi-Fi_access_points.php

- SCF White Paper, “Integrated femto-Wi-Fi networks”, Release-1, Doc No. SCF-033, 2013, http://www.scf.io/en/documents/033_Integrated_femto-Wi-Fi_networks.php

5.3.3 Wireless Broadband Alliance (WBA)

WBA addresses multiple aspects of Wi-Fi technology and W-Fi integration into the network, including:

- Making Wi-Fi easy to use for customers using different devices;
- Creating specification and guidelines for Wi-Fi Internetworking and Roaming; and
- Facilitating Wi-Fi interoperability with other technologies.

The WBA and its members are committed to helping Wi-Fi fulfil that potential. The WBA is achieving this through the development of specifications, guidelines, resources and collaborative work that will help make the Wi-Fi experience easier, more secure and available to more people. This means a focus on three key areas.

1. **Wi-Fi for today:** WBA creates specifications and guidelines to make Wi-Fi interworking and roaming more efficient and reliable for operators and service providers, including interoperability with all major wireless technologies
2. **Wi-Fi for tomorrow:** As LTE rollout continues, interoperability efforts are also moving beyond 3G and towards the cellular technologies of the future. At the same time our own Next Generation Hotspot Initiative is promising new levels of access, security and robustness to Wi-Fi operators and users.
3. **Wi-Fi for all:** Roaming, outreach and collaboration across technologies are key parts of our work. Our Roaming Workgroup and Global Wi-Fi Roaming Initiative encourage and aid the development of roaming specifications and guidelines, embracing Wi-Fi and non-Wi-Fi players and partners.

5.3.4 Wi-Fi Alliance (WFA)

WFA is an established organization that develops certification programs for Wi-Fi products. Most recently, the HotSpot 2.0 standards, which are the basis for WBA’s NGH program, have been developed by WFA.

5.3.5 Next Generation Mobile Networks (NGMN)

The vision of the NGMN Alliance is to expand the communications experience by providing a truly integrated and cohesively managed delivery platform that brings affordable mobile broadband services to the end user with a particular focus on LTE and LTE-Advanced.

The mission of the NGMN Alliance is:

- Expand/evolve the mobile broadband experience, with a focus on LTE, LTE-A, and future enhancements,
- Establish clear functionality and performance targets as well as fundamental requirements for deployment and operations,
- Cost-optimization: provide guidance to equipment developers and standards bodies
- Implementation NGMN recommendations / liaise with SDOs and industry organisations,
- Provide an information exchange forum on critical and immediate concerns
- Address spectrum requirements and support a transparent and predictable IPR regime.

NGMN – “Small Cells Work Program”

The objective of project Small Cells is to define scenarios, use cases, system architecture and functional requirements for the fast and efficient introduction and operations of Small Cells. The work-streams of the project activity will deal in particular with the aspects of Wi-Fi integration, cost efficient deployment, operational issues, multi-vendor deployment and backhauling for Small Cells. This project is sub-divided into three work-streams:

1. Work-stream #1: Use cases and scenarios, including Wi-Fi
2. Work-stream #2: Multi-vendor deployment
3. Work-stream #3: Backhaul - Analysis of backhauling solutions and related requirements and use cases:

5.3.6 4G-Americas

4G Americas has analyzed the issue around intelligent Network Selection from a client perspective and produced a comprehensive set of recommendations on some of the main client related aspects of integration between Wi-Fi and Cellular networks [52]

Note: A detailed list of various standards bodies and relevant documents is presented in the Annex.

6. Conclusions

At a high level, this paper represents a broad view of the opportunities and challenges of integrating carrier-grade Wi-Fi being driven by WBA's NGH initiative and Small Cells being driven by Small Cell Forum. It presents detailed accounts of use cases, architectures, network elements, network functions, exemplary implementations, as well as underlying standards. It also highlighted a number of topics that deserve further study and some best practices. It is hoped that the SCF-WBA Task Force would seriously consider future projects based on these suggestions.

The paper starts by describing various Deployment Scenarios, classified according to Venue-type (Indoor/Outdoor, Enterprise/Venue, Purpose (Coverage/Capacity, etc), Business Reasons (cost savings/new services/etc). It then proposes a high level framework for network architectures for integrated Small Cell and Wi-Fi (ISW) networks, shown in Figure-1.

The Architecture Framework identifies a number of domains, namely the Access Network domain, the backhaul domain, the ISW-Core Network Domain and the Mobile Operator Core Network Domain. Within each domain, a number of building blocks (or network elements) are identified, including: various types of Access Points (APs) and their characteristics; WLAN Controllers (WLC), Small Cell Gateways (SC-GW), Gateways for WLAN access to Operator Core Networks (Wi-Fi-GW for CN Integration) as well as NGH elements such as ANQP Server/Client and Mobile Operator Policy elements such as ANDSF Server/Client.

Focusing on the Integration of SC and NGH enabled Wi-Fi Networks, the paper next addresses various Integration Use Cases and Functions, such as: Intelligent Network Selection, Seamless Authentication, Simultaneous Connectivity to and Traffic Management across SC and Wi-Fi, User Mobility across in ISW (Integrated Small Cell Wi-Fi) networks, Online Sign-Up etc.

The paper further addresses network Architectures, first on Integration Architectures, and then on Trusted Wi-Fi Access Network (TWAN) architectures. It is hoped that the latter is especially useful given that there are no common industry-wide standards.

Next, the paper includes a comprehensive discussion on various standards applicable to this ISW space. They include SDOs such as 3GPP, IEEE, BBF, IETF, OMA and Cable Labs, as well as Industry Forums such as GSMA, WFA, WBA, SCF & NGMN.

Last but not least, as a result comprehensively documenting the broad landscape of the ISW networks, the paper identified 6 areas deserving of further study, and potentially useful for driving the industry forward. They are captured below and it is hoped that these topics would be pursued by the SCF-WBA Task Force as well as other similar organizations.

6.1 Recommendations For Further Study

ISW-AP:
The fundamentally distinguishing aspect of optimal use of an integrated SC and Wi-Fi deserves further study. As described in this paper, this includes joint software architecture (for example, SCF has alluded to defining APIs between the SC & Wi-Fi PHY/MAC HW/FW to upper layers as an extension of the popular Femto-API (or FAPI)), joint RRM, and APIs/Procedures for common use of location and possibly timing capabilities.

Shared Backhaul:
There are many aspects of shared backhaul between Licensed Small Cells and Wi-Fi APs, which deserves further exploration. Examples include framing aspects, bandwidth sharing, COS support, etc.

TWAN Architectures:
The Wi-Fi-Network architectures have been generally vendor specific implementations, based on proprietary interfaces and/or proprietary extensions to standardized interfaces. Examples include the interface between the Wi-Fi AP to Controller. As Carrier Wi-Fi is gaining momentum, and also integration with Cellular Core Networks is being increasingly considered/deployed, it may be useful for the industry to establish standards and/or best practices/recommendations for such Wi-Fi-network aspects. Additional topics include Inter-AP, Intra/Inter-Controller Mobility Management.

GW/AP based ISW Traffic Management:
It may be of value to consider ISW-architectures where the Traffic Management function is located in either the GWs or APs, due to their potential benefits of reduced core network signalling and distribution of functions.

Integrated Policy Framework for SC and Wi-Fi Networks:
Unified SLA and other policy framework definitions across both SC and Wi-Fi networks, potentially to include backhaul network policies allowing uniform management of subscribers regardless of air interface connection.

Unified Self-Organizing Network [SON] Definitions for ISW APs:
Self-Organizing Network [SON] interface protocols have not yet converged around interoperable standards for licensed-frequency small cells, let alone for multi-radio network elements. As SON standards develop for 3GPP networks, WLAN integration should be included across all major areas of SON, including: Automated Neighbor Relations [ANR], Self-configuration, Self-optimization, and Self-healing.

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 Whitepaper, September 2013

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

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

[5] SCF033, “Integrated femto-WiFi 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 WiFi 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] BroadbandForum TR-069, “CPE WAN Management Protocol (CWMP)”

[25] BroadbandForum 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

Annex: ISW Standards Organizations – Standards & Documentation References

Stds. Org. / Working Group Spec./Doc	Title	*Status*	Scope / Notes
3GPP (TSG SA)			
SA WG1 -Service & Systems Aspects			
TS 22.234	**Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking**	*Rel.8- Rel.11*	Definition of interworking WLAN with 3G GPRS network (I-WLAN)
TS 22.278	**Requirements on 3GService requirements for the Evolved Packet System (EPS)**	*Rel.12*	Definition of requirement for 4G 3GPP EPS network. Include the requirements for the support of Non-3GPP systems, e.g. 3GPP2, WLAN, fixed network
NOTE: the study documents (TR) superseded by normative specifications are not included. Only TR's not yet transformed (as of Sep'13) in finalized normative specification are listed here.			
SA WG2 - Architecture			
TS 23.234	**3GPP system to Wireless Local Area Network (WLAN) interworking; System description**	*Rel.8- Rel.11*	Reference architecture, reference points, functionalities for I-WLAN with 3G GPRS for fulfill requirements defined in TS 22.234 (I-WLAN)
TS 23.327	**Mobility between 3GPP-Wireless Local Area Network (WLAN) interworking and 3GPP systems**	*Rel.8- Rel.11*	DSMIPv6 mobility for I-WLAN based on TS 23.234 (I-WLAN)
TS 23.402	**Architecture enhancements for non-3GPP accesses**	*Rel.12*	Ref Architecture and functionalities for supporting the Non-3GPP system in 3GPP EPS. 3GPP-WLAN seamless and non-seamless handover via PMIPv6 (s2a, s2b), DSMIPv6 (s2c) and GTP (s2a, s2b), network selection policy (ANDSF) (3GPP EPS)
TS 23.261	**IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2**	*Rel.10- Rel.11*	Definition of IP flow mobility for S2c DSMIPv6 (3GPP EPS)
TR 23.852	**Study on S2a Mobility based on GTP & WLAN access to EPC**	*Rel.11*	Study for support Trusted WLAN (s2a)
TR 23.890	**Offloading to WLAN in 3GPP RAT mobility**	*Rel.12 (d)*	
TS 23.203	**Policy and charging control architecture**	*Rel.12*	Policy and charging control for 3GPP mobile network. Annex P referes to interworking with BBF policy framework defined in BBF TR-134. New annex for the covergence scenario supporting BBF access (limited to Non-Seamless WLAN offload traffic from 3GPP and fixed device) based on TR 23.896 (3GPP EPS)

	TS 23.139	**3GPP system - fixed broadband access network interworking;**	*Rel.12*	Reference architecture, reference point, requirement and procedure for interworking with fixed Broadband network. Consider the 3GPP UE connected to WLAN/RG in S2a, s2b and S2c scenario and connected to H(e)Nb via BBF network. (3GPP EPS)
	TR 23.896	**Technical Report on Support for fixed broadband access networks convergence**	*Rel.12*	Study for Fixed Mobile convergent scenario, where the 3GPP PCC is connected directly to the BNG for QoS and charging control. In this release the scope is limited to Non-Seamless WLAN offload traffic from 3GPP and fixed device (3GPP EPS)
ref.	***TR 23.865***	***WLAN network selection for 3GPP terminals***		*Study for enhancement of ANDSF policy taking into account WFA HS2.0 Rel.2.0. Identify possible conflict and propose resolution (3GPP EPS)*
SA WG3 - Security				
	TS 33.234	**Wireless Local Area Network (WLAN) interworking security**	*Rel.11*	security architecture; Definition of authentication procedure and protocol EAP-SIM, EAP-AKA and security for interworking WLAN based on 23.234. (I-WLAN)
	TS 33.402	**Security aspects of non-3GPP accesses**	*Rel.11*	Definition of authentication procedures and protocols EAP-AKA', DSMIPv6 bootstrapping (s2c) with AKA authentication, SWu IPsec tunnel establishment between UE and ePDG with AKA authentication (s2b). Definition of trusted/untrusted. (3GPP EPS)
SA WG5 - Telecom Mgmt				
	TS 32.107	**Telecommunication management; Fixed Mobile Convergence (FMC) Federated Network Information Model (FNIM)**	*Rel.11*	Telecommunication management; Fixed Mobile Convergence (FMC) Federated Network Information Model (FNIM)
	TS 32.252	**Wireless Local Area Network (WLAN) charging**	*Rel.6 - Rel.11*	Charging for I-WLAN architecture based on TS 23.234 (I-WLAN)
	TR 32.841	**Study on WLAN Management**	*Rel.12 (d)*	
	NOTE: TS for covergent charging not yet included			
3GPP (RAN)	RAN WG2			
	TR 37.834	**Study on WLAN/3GPP Radio Interworking**	*Rel.12*	study
3GPP (CT)				
CT WG1				
	TS 24.234	**WLAN User Equipment (WLAN UE) to network protocols (Stage 3)**	*Rel.6- Rel.11*	Stage 3 document for TS 23.234 (I.WLAN)

TS 24.327	**Mobility between 3GPP Wireless Local Area Network (WLAN) interworking (I-WLAN) and 3GPP systems; General Packet Radio System (GPRS) and 3GPP I-WLAN aspects; Stage 3**	*Rel.8-Rel.11*	Stage 3 document for TS 23.237 (I.WLAN)
TS 24.235	**3GPP System to Wireless Local Area Network (WLAN) interworking Management Object (MO)**	*Rel.10-Rel.11*	This document defines the 3GPP System to Wireless Local Area Network interworking Management Object (MO) for I-WLAN PLMN selection as specified in 3GPP TS 24.234 . (I-WLAN)
TS 24.302	**Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3**	*Rel.8-Rel.12*	Stage 3 document for TS 23.402 (3GPP EPS)
TS 24.303	**Mobility management based on Dual-Stack Mobile IPv6; Stage 3**	*Rel.8-Rel.11*	Define the DSMIPv6 protocol for s2c reference point (3GPP EPS)
TS 24.304	**Mobility management based on Mobile IPv4; User Equipment (UE) - foreign agent interface; Stage 3**	*Rel.8-Rel.11*	Stage 3 aspects of mobility management for User Equipment (UE) using IETF Mobile IPv4 foreign agent mode to access the Evolved Packet Core Network (EPC)
TS 24.312	**Access Network Discovery and Selection Function (ANDSF) Management Object (MO)**	*Rel.8-Rel.12*	This document define the ANDSF Management Object (MO) as specified in TS 23.402 (3GPP EPS)
TS 24.139	**3GPP system - fixed broadband access network interworking; Stage 3**	*Rel.11*	Stage 3 document for TS 23.139 (3GPP EPS)

CT WG3 - Interworking with external network

TS 29.212	**Policy and Charging Control (PCC); Reference points**	*Rel.11*	Define the PCC functionalities and protocol for reference point Gx and Gxx. From Rel.11 included extension for supporting BBF interworking as specified in TS 23.139 and TS 23.203
TS 29.212	**Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping**	*Rel.11*	Define the PCC functionalities. From Rel.11 included extension for supporting BBF interworking as specified in TS 23.139 and TS 23.203
TS 29.215	**Policy and Charging Control (PCC) over S9 reference point; Stage 3**	*Rel.11*	Define the protocol for reference point S9 in PCC. From Rel.11 included the definition of protocol for S9a for supporting BBF interworking as specified in TS 23.139 and TS 23.203

CT WG4 - MAP / CAMEL / GTP / BCH / SS / TrFO / IMS / GUP / WLAN

TS 29.234	**3GPP system to Wireless Local Area Network (WLAN) interworking; Stage 3**	*Rel.6-Rel.11*	Defined procedure and protocol for reference point defined in TS 23.234 (I-WLAN)
TS 29.273	**Evolved Packet System (EPS); 3GPP EPS AAA interfaces**	*Rel.8-Rel.12*	Defined procedure and protocol for Reference points SWa,STa,SWd, SWx,S6b, H2, SWm defined in tS 23.402 (3GPP EPS)

TS 29.274	**3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3**	*Rel.11*	Defined the GTPv2 protocol. Rel.11 includes extension for usage in s2a and s2b reference points . (3GPP EPS)
TS 29.275	**Proxy Mobile IPv6 (PMIPv6) based Mobility and Tunnelling protocols; Stage 3**	*Rel.8-Rel.11*	The present document specifies the stage 3 of the PMIPv6 Based Mobility and Tunnelling Protocols used over the PMIP-based S2a, S2b, reference points defined in 3GPP TS 23.402, and are thus applicable to the Serving GW, PDN Gateway, ePDG, and Trusted Non-3GPP Access. (3GPP EPS)
TS 29.279	**Mobile IPv4 (MIPv4) based mobility protocols; Stage 3**	*Rel.8-Rel.11*	The document specifies the stage 3 of the MIPv4 Based Mobility Protocol used over the S2a reference point defined in 3GPP TS 23.402. (3GPP EPS)
TS 29.282	**Mobile IPv6 vendor specific option format and usage within 3GPP**	*Rel.8-Rel.11*	The document specifies 3GPP vendor specific option for PMIPv6 protocol
TS 29.139	**3GPP system - fixed broadband access network interworking; Home (e)Node B - security gateway interface**	*Rel.11*	Stage 3 document for TS 23.139 (3GPP EPS)
TS 29.839	**3GPP system - fixed broadband access network interworking; Home (e)Node B - security gateway interface**	*Rel.11*	Stage 3 document for TS 23.139 (3GPP EPS)

Broadband Forum [BBF]

TR-058	**"Multi-service Architecture and Framework Requirements"**		support for TS 23.890
TR-064			CWMP (CPE WAN Mgmt Prot.)
TR-101	**Migration to Ethernet-based DSL Aggregation**		support for TS 23.890
TR-196 Iss.2	**Femto Access Point Service Data Model**	*Nov'11*	defines 3G and LTE Femto data model which contains necessary RF parameters, Device Param., Time and location params., QoS and Policy param's and transport (IPsec) param's.
TR-203	**Interworking between Next Generation Fixed and 3GPP Wireless Networks**	*Aug'12*	
TR-262	**Femto Component Objects**	*Nov.11*	
WT-291	**Nodal Requirements for Interworking between Next Generation Fixed and 3GPP Wireless Access**	*Wip*	(w/ 3GPP) developing architecture and solutions for the interworking between wireline and wireless networks. **WT-203** defines the architectural framework for interworking, high level requirements for interworking solutions and a set use cases that the solution should support. **WT-291** builds on the work done in WT-203 and provides the nodal requirements for solutions

			associated with WT-203 architecture and use cases.
WT-300		*Wip*	
WT-321	**Public Wi-Fi Access**	*Wip*	
TR-134	**Policy Control Framework**	*Wip*	Definition of BBF Policy framework for supporting dynamic QoS in broadband network
IEEE 802.11			
802.11u	**802.11u**	*Feb'11*	802.11u targets Network Discovery & Selection for non-authorized clients on local WLAN. It includes: Access Network Query Protocol [ANQP] (with HS operator's domain, roaming partners; credentials/EAP methods supported; IP address type avail.; and other metadata); emergency calling; emergency alerts
GSMA			
TSG - Terminal Steering Group			
TS.22	**Recommendations for minimal Wi-Fi capabilities of terminals**	*PRD*	Consolidates terminal requirements and existing Wi-Fi experiences from various operators. Designed as tool to help operators align their Wi-Fi requirements. GSMA Is finalizing Ver.2 and will start work on Ver.3 soon.
White Paper	**Wi-Fi Offload Whitepaper - Version 1.0**	*WP - Apr'10*	GSMA Wi-Fi Offload initiative and is intended to facilitate development of an ecosystem for the availability of Wi-Fi Offload. Focused to deliver services to customers whether they are in or out of 3GPP network coverage; also to help reduce the 3GPP network load.
GSMA/WBA Task Force			
White Paper	**Wi-Fi Roaming White Paper - Version 1.0**	*Dec'12*	GSMA and WBA approved the formation of a joint taskforce on Wi-Fi Roaming, with the intention to bring together the Wi-Fi and 3G/4G ecosystems in a collaborative effort. Focus on authentication, settlement and billing, data offload, network access selection, terminal aspects, etc.

White Papers	GSMA/WBA Roaming Task Force white papers	*WP - Jun'13*	GSMA/WBA Roaming TF produced a few white papers that targeted to support interworking (seamless authentication, service continuity, etc.) of Wi-Fi technology with 3GPP EPC. The white papers identified the open issues/requirements that need to address in other standards organizations and forums,
IETF			
RFC	AP-AC Interface standardization (extension of CAPWAP)		
RFC 4187	Extensible Auth. Protocol Method for 3rd Gen. Aut & Key Agreement [EAP-AKA]		
RFC 4186	Extensible Auth. Protocol Method for GSM SIMs [EAP-SIM]		
RFC 2475	Architecture for Differentiated Services		
RFC 5448	Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')		
RFC 5247	Extensible Authentication Protocol (EAP) Key Management Framework		
RFC 3748	Extensible Authentication Protocol (EAP)		
Open Mobile Alliance			
Device Provisioning and Management			
Client Provision-ing V1.1	1) Enabler Release definition for Client Provisioning - OMA-ERELD-ClinetProvisioning-V1 2) Provisioning Arch'r. Overview - OMA-ERELD-ClinetProvisioning V1 3) Provisioning Bootstrap - OMA-WAP-TS-ProvBoot-1 4) Provisioning Content - OMA-WAP-TS-ProvCont-V1 5)Provisioning Smart Card Spec. - OMA-WAP-TS-ProvSC-V1 6) Provisioning User Agent Behav'r - OMA-WAP-TS-ProvUAB-V1	*Jul'09*	**FOR INFORMATION (some of the listed specifications will be needed to support ISW cell services)**: OMA Client Provisioning V1.1 is a backwards compatible extension of the client provisioning functionality included in WAP 2.0. This version has added support for direct access (and WAP Proxy support) and application access provisioning.
OMA Device Mgmt V2.0	1) Enabler Release Definition for Device Mgmt - OMA-ERELD--DM-V2 2) Device Mgmt Requirements for DM2.0 Enabler - OMA-RD-DM-V2 3) Device Mgmt Architecture for DM 2.0 Enabler - OMA-AD-DM-V2	*May'12*	**FOR INFORMATION (some of the listed specifications will be needed to support ISW cell services):** These set of the specifications describes the Device Management that allows network operators, service providers or corporate information management departments to carry out the procedures of configuring devices on behalf of the end user (customer).

Open CM API Req'ts	**Enabler Release Definition for Open Connection Manager API - OMA-ERELD-OpenCMAPI-V1_1**	*Mar'13*	**This specification probably needs to be modified in order for the connection manager to support the ISW cell services.** The focus of the OpenCMAPI enabler is the standardization of new functional APIs essential for applications to develop connection manager user interface and to extend applications and services with information related to the connection.
CableLabs			
IWP	**Integrated Wi-Fi/Pico cell Platform Specification -** **WR-SP-IWP-I01-120724**	*Jul'12*	Defines a new small cell platform, the Integrated Wi-Fi/Picocell (IWP). The IWP hosts both Wi-Fi and cellular Picocell radios in a modular chassis which is designed for use in MSO networks. The IWP allows MSOs to offer Cable Operator managed Wi-Fi and MNO-managed cellular Picocell services from a single platform.
IWP	**Wi-Fi Roaming Architecture and Interfaces Specification -** **WR-SP-Wi-Fi-ROAM-I02-120216**	*Feb'12*	Focus of this document is roaming among MSO Wi-Fi networks; however, the model presented here may also be applied to non-MSO Wi-Fi networks as well. Attention is placed on the internetwork interfaces and functional requirements needed among cable operators for roaming, while allowing operators flexibility on implementations internal to their network. Requirements are applicable to Wi-Fi clients, Wi-Fi gateways (GWs), and network systems.
IWP	**Wi-Fi Requirements for Cable Modem Gateways -** **WR-SP-Wi-Fi-GW-I02-120216**	*Feb'12*	Identifies the essential capabilities for a cable modem with Wi-Fi functionality to comply with cable operator Wi-Fi roaming requirements. Requirements are targeted at deployment scenarios that integrate an [802.11n] air interface with a [MULPI3.0] cable modem. This specification includes functional requirements for device management.
IWP	**Wi-Fi Provisioning Framework Specification -** **WR-SP-Wi-Fi-MGMT-I03-120216 (February 16, 2012)**	*Feb'12*	**D**etails the management requirements for the Wireless Fidelity (Wi-Fi) air interface and roaming requirements defined in Wi-Fi requirements for Cable Modem Gateways specification [Wi-Fi-GW] and WR Roaming Architecture and Interfaces Specification [Wi-Fi-ROAM]. The purpose of this specification is to define object models and over the wire interface definitions to support the management functions of the Wi-Fi requirements.

ISW Industry Forums – Standards & Documentation References

Small Cell Forum

ISW	**NGH-based Integrated Small Cell Wi-Fi (ISW) Metro Networks**		This paper
	"Wireless in the home & office: the need for both 3G femtocells and Wi-Fi access points", Release-1, Doc No. SCF-007, 2013.	*2011*	Makes a business case for need for both Small Cells and Wi-Fi
	"Integrated femto-Wi-Fi networks", Release-1, Doc No. SCF-033, 2013,	*2012*	First comprehensive paper in the Industry about various aspects of integrating small cells and Wi-Fi technologies.
Wireless Broadband Alliance [WBA]			
	NGH-based Integrated Small Cell Wi-Fi (ISW) Metro Networks	*Wip*	This paper
	Wireless Roaming Intermediary eXchange (WRIX – i, l, d & f)	*May'13*	Set of standard service specifications to facilitate commercial roaming between operators, which can be deployed by Visited Network Providers (VNPs) and Home Service Providers (HSPs) either in-house or through an intermediary WRIX service provider. Includes: WRIX-i (Interconnect), WRIX-l (Location) WRIX-d (Data Clearing) and WRIX-f (Financial Settlement)
	Wi-Fi Roaming Guidelines	*Dec'12*	This document examines the commercial and technical aspects of how to make Wi-Fi roaming – the automatic provisioning of connectivity to end-users across different service providers' Wi-Fi networks
	WIPSr 2.0	*Mar'10*	WISPr 2.0 is the specification of client software to public WLAN network interface. The WISP 2.0 is designed for "non" IEEE 802.1x networks as it requires IP communication with the AGW prior to the authentication of the user. WISPr offers authentication services based on layer 3 networking. It is designed as a front-end to authentication protocols such as Radius, Diameter and the WBA WRIX specification
Trial	**NGH Trials**	*Ongoing*	"Real world" end-to-end testing of Passpoint™ networks, including roaming
Compliancy Program	**Interoperability Compliancy Program (ICP)**	*Ongoing*	WBA operator members use a tool called Wi-Fi Roaming Compliancy Check to promote their compliancy and roaming capabilities in the community
Wi-Fi Alliance			
	HotSpot 2.0 Technical Specification, v1.0.0	*Jun'12*	Technical specification for Wi-Fi CERTIFIED Passpoint™ Release 1: Network discovery and selection; Seamless network access (EAP); Secure authentication and connectivity (WPA2)

	HotSpot 2.0 Technical Specification, Release 2	*Mar'14*	Technical specification for Wi-Fi CERTIFIED Passpoint™ Release 2: Network discovery and selection; Seamless network access (EAP); Secure authentication and connectivity (WPA2); Immediate account provisioning; Operator policy (e.g. Wi-Fi network selection & sub-specific policy)
	Wi-Fi CERTIFIED Passpoint™ (R1) Operator Best Practices for AAA Interface Deployment V1.0.0	*Dec'12*	Identifies a set of AAA attributes recommended for Wi-Fi access points and AAA infrastructure, as well as best practices for operator configuration and deployment of Wi-Fi CERTIFIED Passpoint™ (Release 1) equipment and supporting AAA infrastructure
	Wi-Fi CERTIFIED Passpoint™ (Release 1) Deployment Guidelines V1.0.0	*Oct'12*	Guidelines and recommended best practices for deployment of features in the Wi-Fi CERTIFIED Passpoint™ certification program
Certification Programs	**Wi-Fi CERTIFIED Passpoint™,** **Standard IEEE a/b/g/n/ac plus optional 11n and optional 11ac,** **WPA, WPA2 and PMF,** **EAP and Vendor-specific EAP**	*Wip*	Certification programs for Wi-Fi equipment offered by the WFA. There are many more, these are some which are likely to be of interest to ISW network providers

NGMN

N-P-Small Cells	**Project Small Cell has the following work streams:** **- Work-stream #1: Use cases and scenarios, including Wi-Fi** **- Work-stream #2: Multi-vendor deployment** **- Work-stream #3: Backhaul**	*Wip*	The objective of project Small Cells is to define scenarios, use cases, system architecture and functional requirements for the fast and efficient introduction and operations of Small Cells. The work-streams of the project activity will deal in particular with the aspects of Wi-Fi integration, cost efficient deployment, operational issues, multi-vendor deployment and backhauling for Small Cells.

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
APN	Access Point Name
CAPWAP	Control And Provisioning of Wireless Access Points
CSG	Closed Subscriber Group
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
GGSN	Gateway GPRS Support Node
GRE	Generic Routing Encapsulation
GTP	GPRS Tunneling Protocol
HLR	Home Location Register
HMS	Home NodeB Management System
HNB	Home NodeB
HSS	Home Subscriber Server
IFOM	IP flow mobility
IMSI	International Mobile Subscriber Identity
ISMP	Inter-system mobility policy
ISRP	Inter System Routing Policy
ISW	Integrated Small Cell Wi-Fi
LIPA	Local IP Access
LMD	Local Measurement Duration
LOS	Line of Sight
LTE	Long Term Evolution
MAPCOM	Multi-Access PDN Connectivity
MME	Mobility Management Entity
MNE	Mobile Network. Emulator
NDS	Network Domain Security
NGH	Next Generation Hotspot
NLOS	Non-line of Sight
NSWO	Non Seamless WLAN Offload
OAM	Operation Administration & Maintenance
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
RRM	Radio Resource Management
SaMOG	S2a Mobility Mobility Based on GTP & WLAN access to EPC

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
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
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
John Smith (Member editorial team)	Cisco Systems
Mark Grayson (Member editorial team)	Cisco Systems
Marco Spini (Member editorial team)	Huawei
Necati Canpolat	Intel Corporation
Balaji Raghothaman	InterDigital
John Tomici	InterDigital
Li Qing	InterDigital
Mike Starsinic (Member editorial team)	InterDigital
Tony Chiang	Mediatek
David Chen	NSN
Mariusz Skrocki	Orange France
Nigel Bird	Orange France
Stefano Faccin	Qualcomm
Stuart Strickland	Qualcomm
Debjani De	Radisys
Renuka Bhalerao	Radisys
Upendra Ram Praturi	Radysis
Khasim Shaheed	Radysis
Carolyn Heide (Member editorial team)	Ruckus Wireless
Dave Wright (Member editorial team)	Ruckus Wireless
Rajesh	Ruckus Wireless
Steve Hratko	Ruckus Wireless
Prabhakar Chitrapu (Project lead)	SCF & AT&T
Dzung Tran	SmithMicro
Vaia Sdralia	Stoke
Qiang Zang	TWC
Bruno Tomas	WBA
Tiago Rodrigues (Project Lead)	WBA