INTERDIGITAL

WHITE PAPER

Cellular-Wi-Fi Integration

A comprehensive analysis of the technology and standardization roadmap

June 2012

1 Contents

2 Introduction: From Competitive Positions to Shared Goals

Cellular and Wi-Fi® radio technologies originated and evolved from two fundamentally different objectives. The former was motivated by the desire to make telephony technology mobile, and the latter by the desire to make data communications wireless. Over time, each has trended towards the other, with wireless data a central use of cellular technology today while over-the-top services provide voice over data networks. This confluence seems headed towards a fundamentally integrated cellular and Wi-Fi landscape, but the evolutionary nature of the trend has resulted in a broad variety of approaches and solutions.

Significant advancements in data over wireless began to emerge in the early 1980s. InterDigital helped pioneer this capability, with TDMA access in a DSP-based implementation in the 1980s laying the technological blocks for the digital wireless revolution of the 1990's, followed by InterDigital's WCDMA system using CDMA in channels as wide as 20 MHz to provide high-capacity fixed wireless access. With the introduction of the ETSI's GSM system (a digital TDMA system with DSP-based devices), the vision of ubiquitous connectivity was at last beginning to appear real. By the late 1990's, ETSI and then 3GPP were already looking towards providing packet connectivity, first as the GPRS "add-on" system to GSM and then, with UMTS (a CDMA system), as a fundamental capability.

At the same time a completely different vision of wireless access emerged. This vision was based on the success of Local Area Networks – particularly Ethernet – in connecting the enterprise "intranet" into a highly capable local network. Using the "free-for-all" ISM bands, first allocated by the US FCC in 1985, the IEEE 802.11 Working Group began looking at taking the Ethernet wireless. With no reliance on expensive licensed spectrum and fewer concerns regarding QoS, Wi-Fi technology emerged as a strong consumer – and, increasingly, enterprise – wireless solution by the mid-2000s.

The initial response from the cellular community was purely defensive. Rather than embracing and integrating the new technology, 3GPP embarked on a fundamental re-architecture of its system which resulted in a completely IP-based packet-focused Evolved Packet Core (EPC). Combined with OFDM-based LTE access technology, this was supposed to be the answer to the threat posed by Wi-Fi.

The response from the Wi-Fi community to the customer demand for integration with mobile communication solutions was similarly lukewarm. With the MIP family of IP enhancement, IETF took the lead in trying to provide mobility support to IP-based systems such as Wi-Fi. However, the limited traction these protocols did find was in 3GPP where MIP and PMIP have been adopted as solutions for the EPC. Until very recently the focus of the Wi-Fi community remained on delivering access to ever-greater bandwidth (with 802.11n), while the need for QoS management and mobility was completely ignored.

That mutual defensiveness has now reversed, fuelled both by consumer demand regarding data to new device types and operator efforts to relieve network pressure. From the cellular side, small, localized cells, such as Wi-Fi AP coverage regions, are growing in importance. As an IP-based system, the EPC is well positioned for integration of multiple heterogeneous access technologies and 3GPP is now moving towards taking advantage of EPC to delivery solution for real integration of technologies such as Wi-Fi.

With ANDSF, an integrated policy-based management system for how devices access spectrum 3GPP has already taken a first step in that direction.

On the other hand, the Wi-Fi community has finally acknowledged that when using mobile devices (for example, the iPhone), consumers expect to receive the same quality of service whether they use Wi-Fi, 3G or LTE. By extension, Wi-Fi must provide operators with the tools to manage Wi-Fi networks in the same way that they can manage their own 3G or LTE networks, and the recent Hotspot 2.0 profile and the associated PassPoint certification program sees the Wi-Fi Alliance beginning to move towards delivering such "carrier-grade" Wi-Fi solutions to the market.

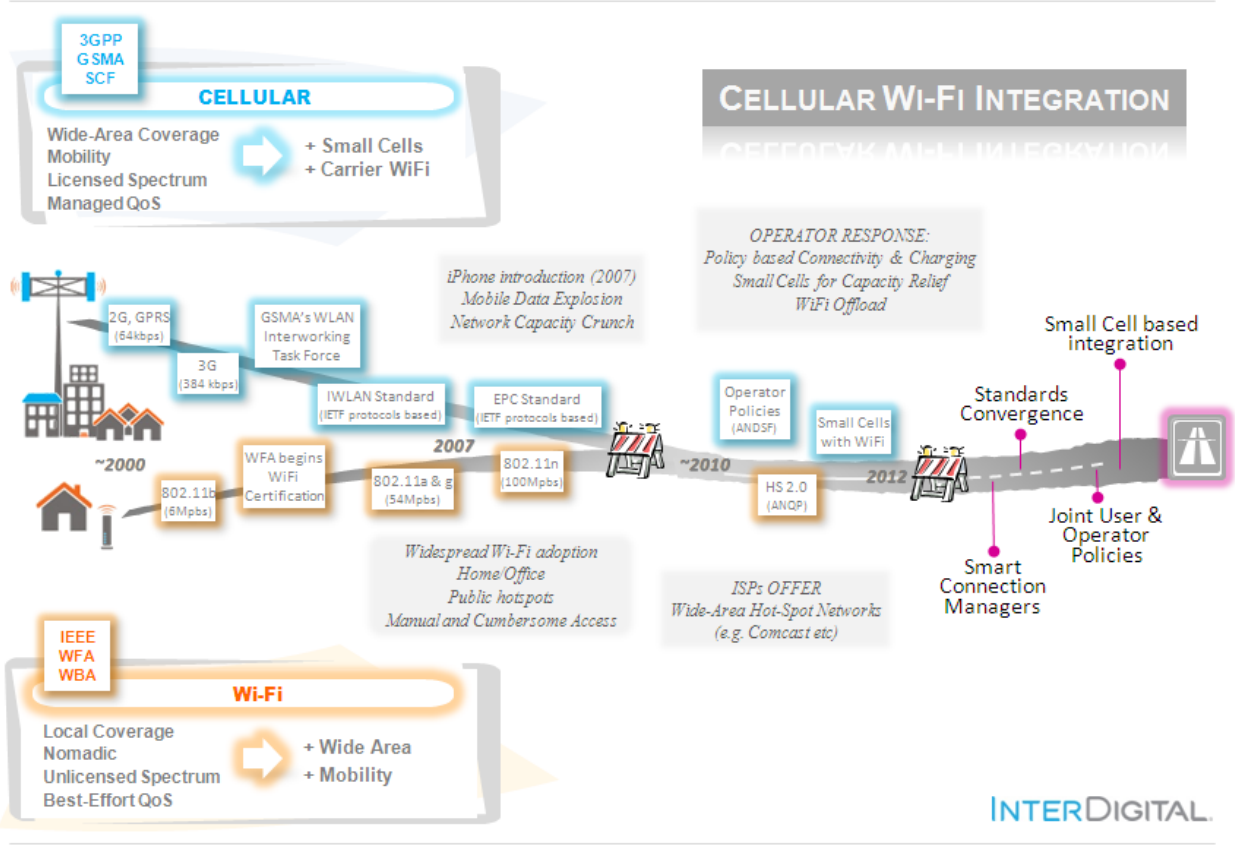


Figure-1: Chronological Developments in Cellular/Wi-Fi Integration

Finally, the trend towards true integration is beginning to come to the fore. The need is particularly acute in small cells – designed to address the high spectrum needs of local consumer and enterprise networks and Hotspots. Thus, through its work on Integrated Femto-Wi-Fi (IFW), the Small Cells Forum is already taking steps towards defining the near-future of such spectrum integration. What will this future hold? A combination of integrated small-cell solutions, smart connection management at the terminal, within a policy framework that provides management controls to both users and operators.

The Past: Cellular/Wi-Fi Integration Through ~2010

3 Wi-Fi Evolution

Initially conceived in the late 1980's as a wireless extension of Ethernet, initial WLAN installations used the then recently FCC established unlicensed frequency bands and were primarily confined to fixed enterprise deployments. With the establishment of the 802.11 Working Group by the Institute of Electrical and Electronics Engineers (IEEE)In 1991, the increasing speeds of 802.11a and 802.11b (operating on the unlicensed 5 and 2.4 GHz bands respectively), and the Wireless Ethernet Compatibility Alliance (WECA) coining the name "Wi-Fi", and initiated an industry marketing, interoperability and certification program in 1999, Wi-Fi was successfully launched as a broadly-adopted wireless standard.

Close coordination between the IEEE 802.11 Working Group and the Wi-Fi Alliance has continued to improve capabilities, and newer Wi-Fi versions like IEEE 802.11g (a 54 Mbps version of 802.11b) and IEEE 802.11n (~600 Mbps at 5GHz using a wider bandwidth and multiple antennas for transmissions and reception), coupled with backwards compatibility with the older versions of 802.11, has resulted in Wi-Fi products certified as 802.11a/b/g/n. It is important to recognize that an IEEE 802.11 device is not "Wi-Fi" unless and until it has been certified by the WFA.

Because Wi-Fi was originally conceived as a simple extension of an Ethernet cable, it's design provided for short-range, local area coverage, and did NOT address general network considerations such as radio measurements and statistics, device management, or Quality of Service (QoS) (although IEEE 802.11 did produce standards such as 802.11e for QoS, 802.11i for issues like improved security). With the relatively recent incorporation of Wi-Fi into most cell phones and adoption by many mobile operators, some of these considerations are starting to be addressed – as will be examined later in this paper in the Present Activities section.

4 Mobility Solution Toolbox from IETF

IETF (Internet Engineering Task Force) is the technical body that defines "standards" according to which the internet operates. Its "standards" are the so-called RFCs (Request for Comments), which cover various aspects of Inter-Network Transport and higher layer functionalities, in terms of a variety of protocols. For example, IETF developed the IP (Internet Protocol), which defines the structure of information packets and how they are transported between two end-to-end IP-devices across an interconnection of networks. IP protocols are designed to be agnostic to the underlying characteristics of any of the intervening networks and have provided the highway architecture for the modern internet. It is precisely this independence from the underlying network characteristics that made IP a natural choice for interworking Cellular and Wi-Fi Networks, since It is a common language that be supported by both networks.

The basic IP-protocols did not address mobility of the end-devices and these are handled in a series of Mobile-IP standards. These can be grouped in two main categories: client-based and network-based

solutions. Client-based solutions require some special functionalities in the client device, and make use of a mobility agent in the network, whereas network-based solutions rely on the network for both agent and client functionalities, thus making the mobile device agnostic to these mobility functions and therefore simpler to implement. One of the main goals of any of these mobility protocols is to provide seamless mobility as the device moves from network to network. This is essentially achieved by preserving the IP address of the mobile device via the concept of Home IP Address (which stays invariant) and associated Care-Of IP Address (which changes due to mobility). The main client-based approach used to provide seamless mobility is based on the Mobile IP (MIP) protocol [RFC 6275], which lately has been extended into the Dual-Stack Mobile IP (DSMIPv6) architecture [RFC 5555]. The main network-based approaches are based on the Proxy Mobile IP (PMIP) protocol [RFC 5213], also an extension of the MIP protocol.

4.1.1 MIP: "Mobile IP" Protocol

MIP supports uninterrupted routing of IP-packets to and from a mobile device and provides session continuity by means of a Home Agent (HA), which is an entity located at the Home Network of the mobile device (also referred to as a Mobile Node - MN) that anchors the permanent IP address assigned to the mobile device, known as Home Address (HoA). The HA keeps the device's HoA when the MN has moved from the home network, and redirects traffic to the device's current location. The HA is informed of the current location by the MN, using a temporary IP address or Care-of Address (CoA) that the MN acquires from the visited network. A bi-directional IP-tunnel between the MN and the HA is then used to redirect traffic between these nodes.

MIP, defined originally for IPv4 devices and networks, was subsequently extended to MIPv6 to be applicable to IPv6 devices and networks. DSMIPv6 is a further extension of MIPv6, where the basic mobility functionality is extended to also support dual stack IPv4/IPv6 devices and networks. Accordingly, DSMIPv6 extensions are defined to also register IPv4 addresses and transport of both IPv4 and IPv6 packets over the tunnel between the HoA and the visited network. These extensions enable the mobile device to roam between IPv4 and IPv6 access networks seamlessly, and are considered crucial as IPv4 networks and devices gradually evolve to IPv6.

4.1.2 PMIP: Proxy MIP

PMIP and its IPv6 extension, PMIPv6, are examples of Network-based IP mobility solutions, which manage the mobility of the mobile device entirely to the network. In this way, the device is not required to perform any signaling or updates, as it changes of its point-of-attachment (i.e. visited network) due to its mobility. Hence, these changes become transparent to the mobile terminal's IP protocol stack, resulting in simpler device solutions than those based on baseline MIP.

The PMIP-enabled mobile IP network architecture consists of a central entity, called Local Mobility anchor (LMA), and a number of Mobile Access Gateways (MAGs), which together define a mobility domain. The LMA plays the role of a local HA (as in DSMIP networks) and anchors the IP prefixes used by the MNs. MAGs reside close to the mobile node, usually in the Access Routers (which in turn are either collocated with the Access Points or directly connected to them).

Detection of movement of mobile devices as well as implementing associated signaling is done by the MAGs. Typically, the MAG detects mobility through standard terminal operations, such as router and neighbor discovery or by means of link-layer support, without any mobility specific support from the device. Bi-directional tunnels between the LMA and the MAGs are set up, so that the mobile device is able to keep the originally assigned IP address within the mobility domain despite any location changes. Since the LMA is aware of the actual location of the mobile device, any packets addressed to the device are tunneled to the appropriate MAG, relieving the mobile device of the need to manage the IP packet routing due to its own mobility.

4.1.3 Extensions to Mobility of Multi-connection Devices

The underlying assumption in basic MIP and all their derivatives (such as DSMIP [RFC5555], an extension of DSMIP to support simultaneous IPv4/IPv6 operation) is that a mobile device has a single Home Address and a single Care of Address (which may change due to MN mobility). However, modern devices, such as smart phones, can support multiple IP connections, for example via Cellular and Wi-Fi network interfaces. Clearly, the DSMIP cannot support mobility of such devices, and IETF standardized the basic components required to remove such limitations. These components are: multiple care-of address registration support [RFC 5648], flow bindings support [RFC 6088], and traffic selectors definition [RFC 6089].

Multiple care-of-address registration enables a device with multiple IP connections to be registered with a single Home-Address and multiple Care-of-Addresses. This allows the management of mobility of one or more network connections, by updating the corresponding care-of-addresses with the Home Agent. Flow bindings concepts enable the association (or binding) of individual IP-Flows to specific care-of-addresses (or network interfaces). IP-flows in turn are defined by the notions of traffic selectors, defined in RFC6089. These concepts extend the concept of mobility to individual IP-Flows and allow one to move IP-Flows dynamically from one network interface to another (e.g. mobility of IP-Flows from Cellular to Wi-Fi and vice versa).

In the case of network-based mobility solutions, the mobility management control is not located in the mobile device but in the network. PMIPv6 and GTP are network-based mobility protocols and they provide some basic support for handling multiple interfaces. However, they do not support mobility at an IP flow granularity. For this reason, extensions are being defined in IETF [IETF draft-ietf-netext-pmipv6-flowmob, IETF draft-ietf-netext-logical-interface-support] and the recently approved 3GPP study item on network-based flow mobility (NB-IFOM). The first extension allows a mobile device being attached to two different media access gateways (MAG) with two different interfaces (e.g. cellular and Wi-Fi) in the same PMIPv6 domain. The second extension allows a MAG to forward traffic to a mobile device, even if the IP address (e.g. IPv6 prefix) was originally delegated to the mobile via a different MAG.

4.2 Extensible Authentication Protocols (EAP)

Extensible Authentication Protocol (EAP) is a simple authentication protocol defined in [RFC 3748] which is designed to provide a generic framework for user authentication in a network within IP-Networks. A key aspect of EAP is that it itself does not define how authentication is done – rather it defines a

framework which can be used to define a specific authentication protocol. Such protocols are referred to as EAP methods and in most cases the protocol involves authentication with a remote server.

Examples of such EAP methods include EAP-SIM [RFC 4186] and EAP-AKA [RFC 4187, RFC 5448], which are used for authenticating cellular subscribers over Wi-Fi networks. Specifically, these use the SIM or USIM credentials of cellular subscribers for authentication. These protocols also provide for mutual authentication, meaning that UE is authenticated to the mobile network, but, at the same time, the UE is able to verify the identity of the network as well.

As an example, a Wi-Fi network performing EAP-SIM authentication would consist of a Wi-Fi Access Point (AP) to which the UE is attached. The AP is also connected to an AAA-server, which in turn is connected to a mobile operator's HLR/HSS for the purpose of authenticating the user. The AP asks the UE to identify itself via EAP message exchange. On hearing back from the UE, the AP passes on the UE responses to the AAA Server via RADIUS messages, which are further passed on to HLR/HSS. Upon successful authentication, the HLR/HSS informs the AAA Server, which in turn communicates the results to the AP and eventually to the UE.

5 3GPP Efforts to Integrate Wi-Fi

5.1 Beginnings: GSM Association's WLAN Interworking Task Force

Taking note of the standardization of Wi-Fi by IEEE and the increasing uptake of Wi-Fi technology by the market, mobile operators and vendors in GSMA undertook the step of studying the potential integration of Wi-Fi as an alternate radio access method to the core network and services of mobile operators. A task force was created, called the "WLAN Interworking Task Force" which studied the topic between 2002 and 2004. The group investigated various use cases and defined six different levels of interworking between the Wi-Fi and cellular networks.

The simplest interworking scenario was what may be termed as "loose interworking" and consisted of common authentication, access control and billing. Such a combined network would allow a cellular operator to offer Wi-Fi access services to their subscribers, authenticate them using standard cellular methods (i.e. based on SIM cards in the cell phones), verify the service level subscriptions and bill them as needed. The main technical contribution here was the recommendation to use the EAP-SIM protocol over the Wi-Fi networks to authenticate cellular subscribers with SIM-based Wi-Fi enabled handsets.

Progressively tighter levels of interworking were defined in terms of increasingly seamless and integrated access to cellular networks and services. For example, in the loose interworking scenario, the subscriber can access the cellular operator's core network and service network, but some services may not be accessible over the Wi-Fi radio. This limitation is removed in the second level of interworking. The second level of interworking allows "Service Continuity", meaning that all the services that a subscriber has subscribed to must be accessible by the subscriber via the Wi-Fi network. This would include voice-mail, texting, mobile TV, and any other services offered by the cellular operator.

A limitation of the second level of interworking is that while all services may be accessed via the Wi-Fi network, an ongoing session that a user has established over the cellular radio may not, due to user mobility, seamlessly handover to a Wi-Fi network. In other words, the ongoing cellular radio session would be torn down and a new Wi-Fi session would have to be established. This would seriously impact the quality of the user experience. This limitation is removed in the third level of tighter interworking, which calls for so-called "session continuity". This would make the experience of a user moving between Wi-Fi Networks and Cellular Networks as seamless as if he or she were still connected to the cellular network.

Shown below is a figure from GSMA PRD (Permanent Reference Document) SE.27, illustrating various integration scenarios, as understood at the time.

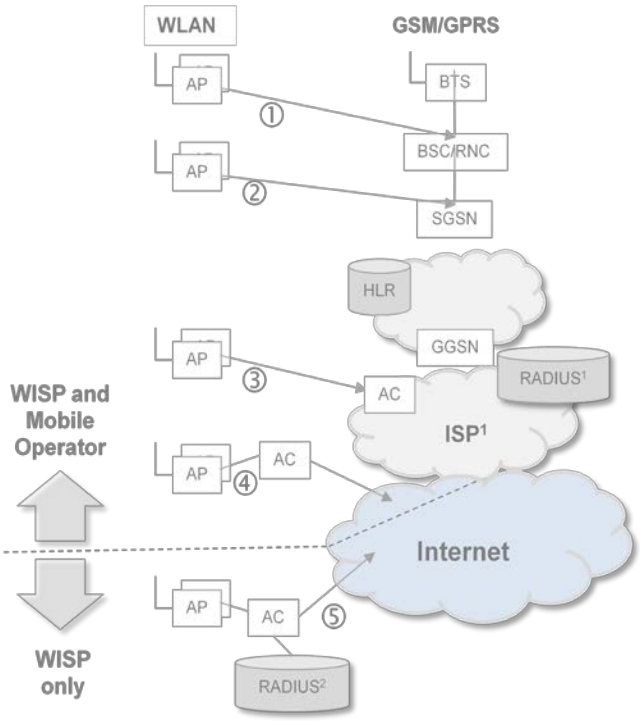


Figure-2: Various Possible Levels of Cellular Wi-Fi Integration

GSMA's WLAN Task Force completed the study in a comprehensive manner and identified the need for standardization within 3GPP. This resulted in the development of a number of standards, based essentially on the loose integration of Wi-Fi networks with the 3GPP core network and can be viewed as an evolution of integration scenario #3 in the above figure. The detailed integration solutions depend upon whether the core network is a UMTS Core network or Enhanced Packet Core (EPC) network. The former set of standards is referred to as IWLAN (Integrated/Interworked WLAN) standards and the latter as EPC standards.

5.2 Integrated Wireless LAN (IWLAN) Standards

The IWLAN standardization work commenced with an initial feasibility study, which included some of the findings of the GSMA's WLAN Task Force. It resulted in a 3GPP Technical Report, TR 23.234, latest version of which is v10.0.0, produced in 2011. The report essentially identifies a number of interworking scenarios, numbered 1 through 6 as follows:

Scenario 1 - Common Billing and Customer Care

Scenario 2 - 3GPP system based Access Control and Charging

Scenario 3: Access to 3GPP system PS based services

Scenario 4: Service Continuity

Scenario 5: Seamless services

Scenario 6: Access to 3GPP CS Services

The last scenario has not been pursued in standardization, but the others led to a number of 3GPP specifications, listed below:

TS 23.234: Scenarios 1 and 2: Common Billing, Access Control and Charging and Access to PS Services.

TS 23.327: Scenarios 4 and 5: Service Continuity and Seamless Services – Single Radio Case and Mobility

TS 23.261: Scenarios 4 and 5: Service Continuity and Seamless Services – Dual Radio Case and Flow Mobility

TS 23.234 provides a solution for Interworking Scenarios 1 and 2. The figure below is a simplified version of a figure from 23.234, wherein the 3GPP AAA server performs the necessary user authentication and authorization for both WLAN access and 3GPP services. Two different types of IP-Access Services are provided to the user, namely "3GPP IP access" and "Direct IP access". The former refers to access to 3GPP packet data services, such as MMS, mobile video, etc. as well as internet services, whereas the latter refers to direct access to internet or intranets.

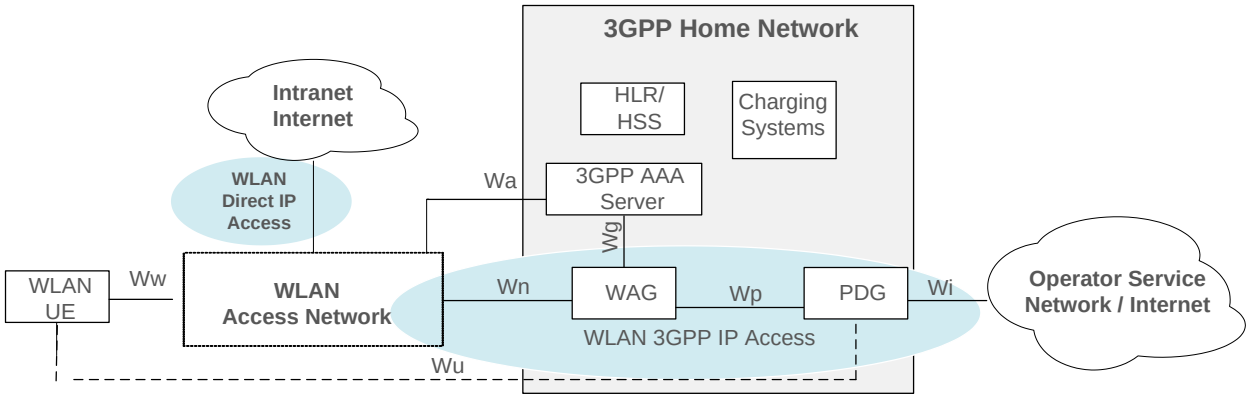


Figure 3: IWLAN Architecture for Seamless Access Control

One of the main goals of the IWLAN solutions was to achieve authentication without manual user intervention, such as entering a username-password, as is common is many Wi-Fi networks. This is made possible by developing authentication protocols based on the use of SIM cards, which are already provisioned in the 3GPP handsets. In addition to providing authentication in a manner transparent to the user, SIM based authentication methods are also familiar to 3GPP operators and provide the same level of security as 3GPP devices. Since the SIM based authentication is now done via WLAN networks, which are essentially IP Networks, the basic 3GPP authentication protocols are modified and are known as EAP-SIM, EAP-AKA and EAP-AKA' protocols, which were standardized by the IETF. IP Networks also use certificate-based authentication methods, which are also standardized as EAP-TLS and EAP-TTLS protocols for WLAN based authentication. Regarding IP access services, the 3GPP-IP-access is provided by two functional entities called WAG and PDG. As the name indicates, the PDG is a gateway to a specific Packet Data Network, such as the internet or an operator service network. Clearly, the 3GPP network may support multiple PDNs and hence multiple PDGs, for different types of services. The WAG implements a typical gateway function on the user side, by connecting the user to one of the possibly several PDGs. It also acts as a firewall and implements operator policies, which are downloaded from the 3GPP AAA servers.

Finally, WAG performs charging related functions, as set by the operator, and communicates with the 3GPP charging systems, of which there are two types, namely offline (for post-paid customers) and online (for pre-paid customers and for checking spending limits).

While the solutions presented in TS 23.234 allow WLAN UEs to access 3GPP core networks and services, the radio connection cannot be dynamically switched between Wi-Fi and 3GPP access networks. These solutions are standardized in TS 23.327, which describes mobility between Interworking WLAN Networks and 3GPP networks.

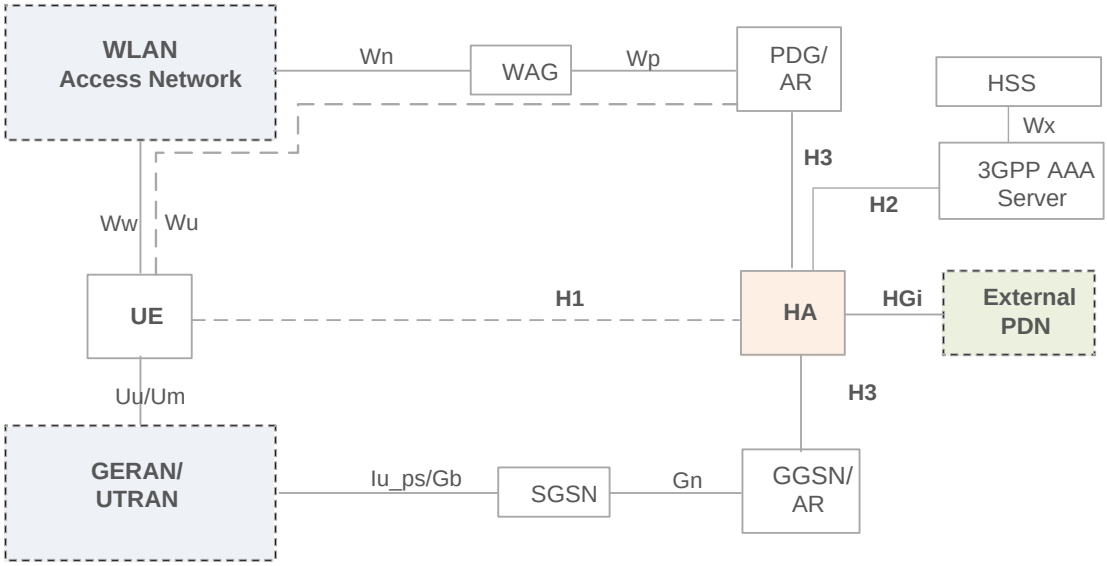


Figure 4: IWLAN Architecture for Seamless Mobility

The mobility function is essentially based on an IP-level mobility management protocol called DSMIPv6, which is standardized by IETF. This protocol is implemented in an entity called HA (Home Agent) in the core network of the home 3GPP network and in a peer entity called DSMIPv6 client in the UE. The UE has a single IP address (for the purposes of mobility management), which is called Home Address (HoA) and a Care-of-Address (CoA) which changes as the UE attachment is changed between IWLAN and 3GPP radio interfaces. Changes in CoA address are synchronized between the UE and the HA by exchanging the so-called "Binding Updates" messages. These are sent over the logical interface H1 shown in the above figure. It is supported over the chain of physical interfaces Uu/Um, Iu_ps/Gb, Gn and H3 when connected over the 3GPP access network and over Ww, Wn, Wp and H3 when connected over the WLAN Access Network.

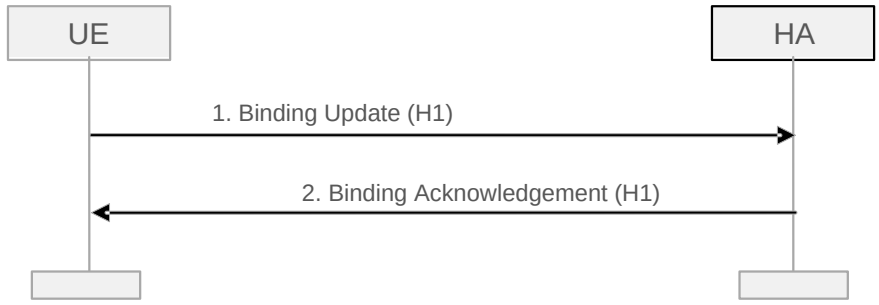


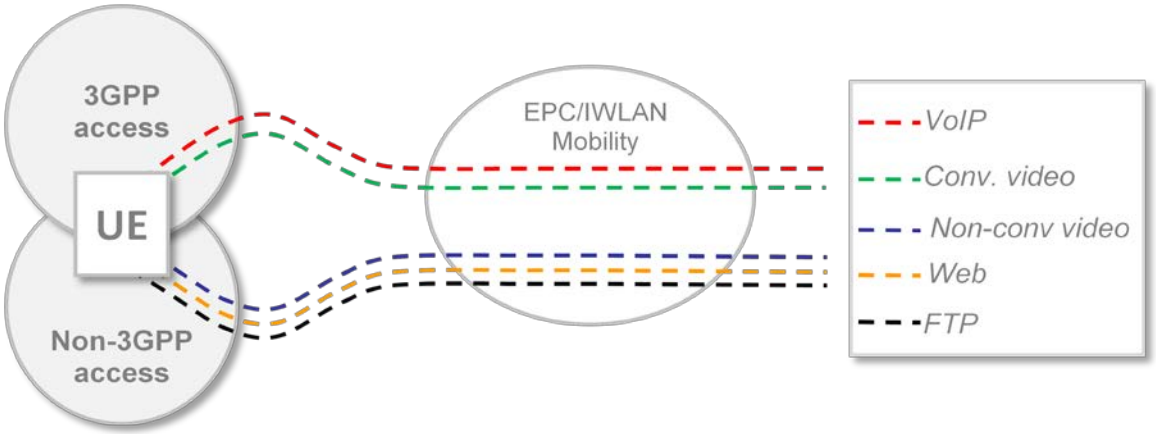
Figure 5: Basic Concept of Mobile IP

DSMIPv6 mobility protocols allow handover from 3GPP access to WLAN access or vice versa. However, in the current version of the standards, only the UE can initiate such a handover procedure. This is based partly on the rationale that the UE has a better knowledge of the WLAN radio networks. However, there are some initiatives in the 3GPP standards organization currently that are seeking to standardize network-initiated handovers as well, since the network has a more comprehensive knowledge of the network congestion state. Although the HA function is shown as a separate function in the above figure, it is often collocated with the GGSN.

5.3 Enhanced Packet Core (EPC) Standards

The above solutions have two basic limitations. The first limitation is that the HA is not connected to policy and QoS management entities in the core network, such as PCRF. This prevents advanced policy and QoS based management of the IWLAN-3GPP mobility. These limitations are removed in the case of integration of WLAN into EPC core networks, which is described in the next section.

The second limitation is that the above solutions restrict the UE to have only a single radio connection at any given time, namely either to the WLAN or 3GPP radio interface. Modern smart phones allow simultaneous connectivity to both radio interfaces, which raises the possibility of managing 3GPP and WLAN interworking at an individual IP-Flow level. That is, it should be possible to support certain IP-Flows on the 3GPP radio interface and certain others on the WLAN radio interface, based on criteria such as QoS requirements, user subscription, type of user equipment, etc. Furthermore, it could also enable dynamic switching of individual IP-Flows from one radio interface to another. The figures below illustrate the situation.



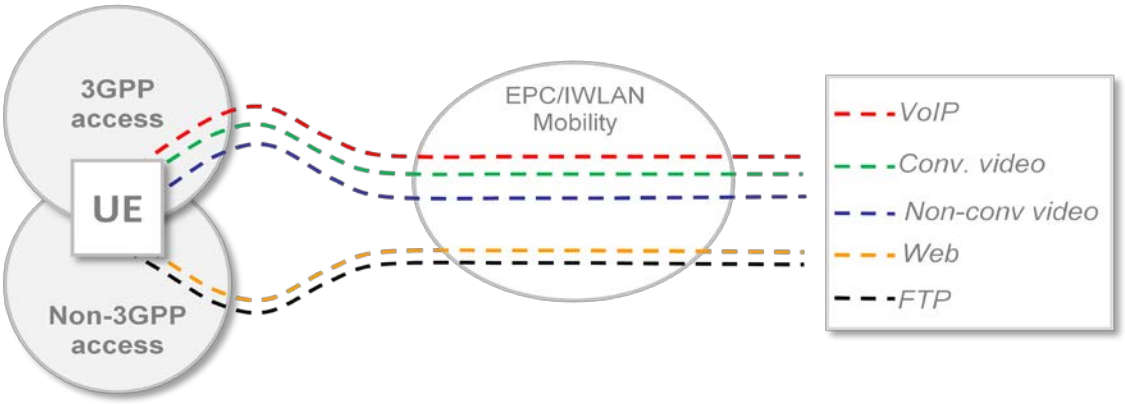


Figure 6: Dynamically Moving IP-Flows Between 3GPP and non-3GPP Radio Access Networks

The EPC standards for 3GPP and Non-3GPP interworking introduce a new class of non-3GPP access networks, namely Trusted Non-3GPP Networks, with the word "trust" referring to trust by the operator (and not necessarily by the user). Accordingly, Trusted Wi-Fi Networks imply that the Trusted Wi-Fi access points are deployed and managed by the Operator, so that UE can connect to the Wi-Fi Network directly using the radio interface without requiring any additional security measures. In contrast, Un-trusted Wi-Fi Networks do not have any trust relationship to the operators, so that the operators require that the UE establish a secure tunnel (i.e. IPSec tunnel) to a trusted node in the operator core network. Typically, such a node is a PDG in UMTS core networks (as in IWLAN architectures) and ePDG in EPC core networks. Shown below are two simplified architectures of an EPC core network with 3GPP as well as Trusted and Un-Trusted non-3GPP Access. Other architectures are also possible and are documented comprehensively in TS 23.401 and TS 23.402.

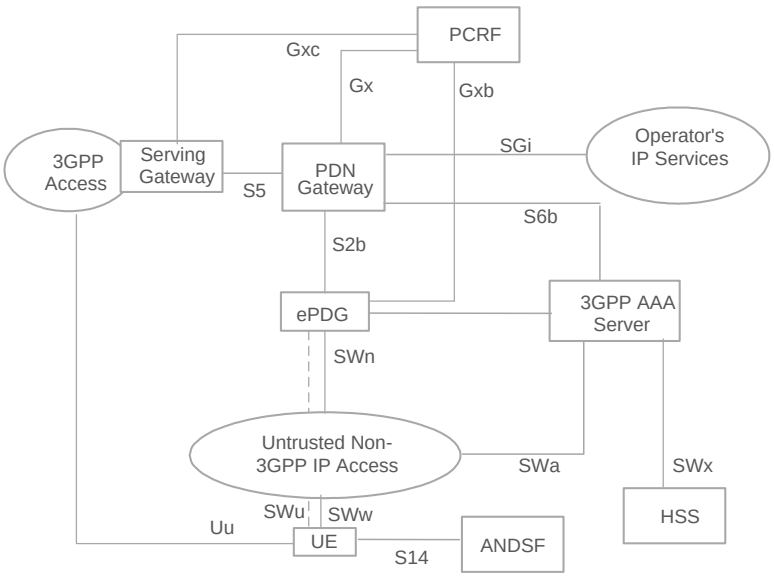


Figure 7: EPC Architecture for Access via Untrusted WLAN

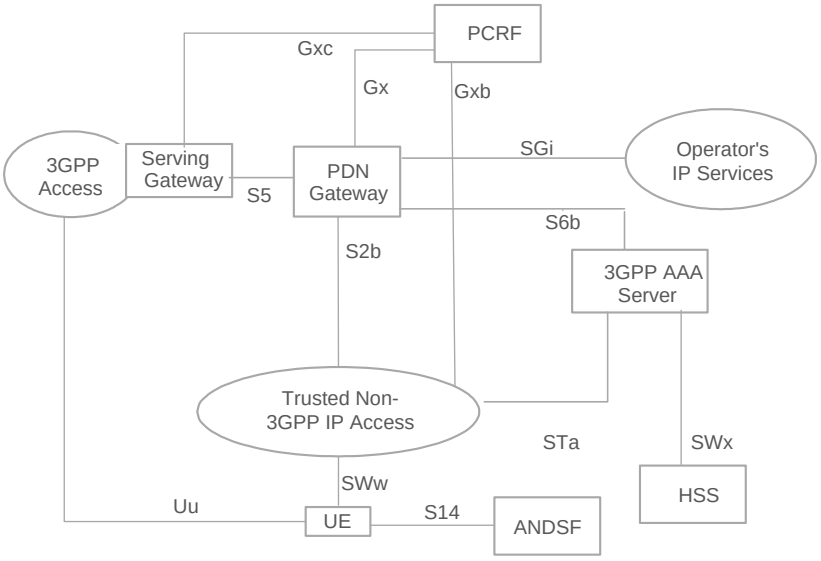


Figure 8: EPC Architecture for Access via Trusted WLAN

Note that here the PGW includes a HA functionality and that PCRF is connected to various gateway functions, each of which has a PCRF or its functional equivalent to enforce the operator policies.

Shown also is the ANDSF functionality, which is a critical one for Cellular-Wi-Fi interworking from an operator policy point of view. Currently, most smartphones choose and camp on to Wi-Fi networks based on explicit user preferences or preconfigured preferences, already stored in the UE. It was clear that if operators were to offer Wi-Fi access as an integral part of the access offerings, they needed to be able to install operator policies on the UE and also be able to change them dynamically, as the conditions may change. To achieve this, the framework of ANDSF was standardized. It essentially consists of an ANDSF server in the operator network, which stores the operator policies regarding discovery and selection of Wi-Fi access. For example, it contains discovery information of Wi-Fi hotspots based on the location of a UE. Regarding selection of Wi-Fi Hotspots, the policies may specify that certain Wi-Fi hotspots are preferred at certain locations and/or certain times of day, or for certain types of applications, such as mobile video etc. These operator policies can be transferred to the UE via the S14 interface using communication procedures based on device management procedures, originally developed by the OMA organization.

Interworking between 3GPP and non-3GPP networks essentially consists of mobility of IP-Flows between the 3GPP and non-3GPP networks. A number of cases of such mobility can be distinguished depending on the following aspects: (1) mobility is on a per IP-Flow basis or per all IP-Flows associated with a PDN connection; (2) mobility is Seamless or Non-Seamless, with Seamlessness defined as preservation of the IP-address of the UE during the mobility process. Different combinations of these two fundamental aspects result in a number of scenarios, such as Wi-Fi offload, referring to mobility of IP-Flow(s) from

3GPP to Wi-Fi networks, and handovers, referring to mobility of all IP-Flows associated with a PDN connection etc.

The 3GPP standard TS 23.401 describes Seamless and Non-Seamless Handover solutions between 3GPP and Non-3GPP access networks, wherein GTP is used as the protocol for the Handover over the interfaces S2a, S2b and S5. Similarly, TS 23.402 documents similar solutions for the cases where PMIP and DSMIP are used for mobility.

Finally, TS 23.261 describes the solutions for Seamless IP-Flow Mobility using DSMIP protocols. As mentioned below, this allows for selective assignment of different IP-Flows to different access networks and includes Seamless Wi-Fi Offload as a special case.

In all cases listed above, the mobility is triggered by the UE and not by the network. Efforts are also being made to standardize network-triggered mobility procedures, since the network is often more knowledgeable about the overall network usage and congestion state than the UE.

The Present: 2011-2012

6 Hotbed of Cellular/Wi-Fi Integration Activities

Following a decade of somewhat independent technological and market developments in Wi-Fi & cellular worlds and the limited deployment of cellular-Wi-Fi integration standards of 3GPP, 2011-2012 has seen a feverish level of activity in this area. In this section, we attempt to describe some of the major activities that are ongoing and try to show their inter-relations and inter-dependencies. We shall describe the activities in terms of those of various industry forums and various technology developments.

6.1 Industry Forums

6.1.1 WFA: Hotspot 2.0

As mentioned earlier, WFA is the organization that certifies Wi-Fi devices that are based on certain WFA defined profiles. These profiles are based on standards set by IEEE 802.11 groups.

As Wi-Fi devices are being used increasingly in a mobile environment for accessing mobile data (e.g. tablets, smart phones etc), and there is a proliferation of number of Wi-Fi access points, WFA recognized the need to extend the capabilities of the previous Wi-Fi networks to improve the mobility experience in such networks. This need is articulated as a series of problems.

Discovery of Wi-Fi Hotspots needed to be simplified, especially when there are a large number of them. Furthermore, it is also important for the UE to know the properties of each Hotspot, in terms of who the owner/operator is, what the service capabilities are etc. This came to be characterized as the Hotspot Discovery problem.

Having discovered a Hotspot and its characteristics, there was a need to select one of the possibly many Hotspots that the UE may have discovered. This selection procedure requires the standardization of operator policies, user preferences etc. This problem is the Selection Policy problem.

Having selected a Hotspot, there was a need to simplify the authentication and access to the Hotspot. The older methods of manual entry of username and password are too cumbersome and there was a need to authenticate using user and device credentials stored in the UE. This is the seamless and transparent authentication problem. It was also important to extend the seamless authentication to include roaming between different operators. Finally, WFA also recognized that it was important for the UE to authenticate the AP, since it is possible that the AP is a rogue AP.

These and similar additional concerns were addressed by WFA in its Hotspot 2.0 program, which culminated in the PassPoint certification. The Hotspot 2.0 “profile” combines seamless (U)SIM-base authentication with a network discovery protocol defined in the 802.11u amendment to the 802.11 standards and management features of the 802.11v amendment. Later in this paper, we shall overview the specific techniques employed by Hotspot 2.0 for discovery (ANQP) and seamless authentication

(EAP-SIM/AKA). Moreover, we shall also discuss the relationship between ANQP and 3GPP's network discovery and access policy mechanism (ANDSF).

6.1.2 Small Cell Forum: Integrated Small Cell – Wi-Fi Networks

Small Cells are considered by many the real long-term solution to the capacity crunch experienced by mobile networks caused by the mobile data explosion. One reason for this viewpoint is that the traditional approaches of improving spectral efficiency and allocating additional spectrum are believed to be approaching their practical limits. A hopeful solution is believed to be in new network architectures, made up of Small Cells with various cellular technologies (i.e. 3G and 4G) as well as Wi-Fi.

The industry forum that is devoted to the study and promotion of Small Cell technologies is the Small Cell Forum. Formerly known as the Femto Forum, the Small Cell Forum was originally focused on developing and promoting the Small Cell / Femto Technologies that use licensed spectrum alone for communication. As the role played by Wi-Fi became increasingly more important, the Small Cell Forum undertook the study of radio level coexistence between collocated Femto and Wi-Fi APs. In fact, the Femto vendors soon began to consider implementing the Femto and Wi-Fi APs in the same equipment as a single unit, and this led the Small Cell Forum to create a work item to investigate the networks that integrate the Small Cells (including both 3G and LTE) and Wi-Fi technologies. The work item resulted in a comprehensive white paper that provided the complete framework, including various deployment and operational scenarios, user and operator benefits and various technical aspects. The latter included discussions on architectures, techniques to optimally use the Femto and Wi-Fi radios, policy and provisioning solutions etc. The Small Cell Forum is continuing work in this area, while also interacting with other industry bodies, especially those dealing with Wi-Fi.

6.1.3 3GPP and IETF Standards

As described earlier, 3GPP has done pioneering work in studying the integration of cellular and Wi-Fi technologies and developing appropriate standards. While most of the solutions are in place, there are several new specific work items that are being studied in various groups, especially the SA (System Architecture) area. One of the ongoing studies addresses the case where the Wi-Fi APs are trusted entities, in contrast to the traditional assumption made by 3GPP that Wi-Fi APs are untrusted. In a sense, these result in certain architectural simplifications and standards are being enhanced to cover these architectures. This study item is called SaMOG.

Another example is the completion of some cases of mobility solutions for Wi-Fi – cellular integration. They include certain cases of network based IP Flow Mobility that are being studied in a work item called MAPIM.

There are additional work items such as OPIIS, which looks into operator policies for IP Interface selection; WORM for including both 3G and 4G in Wi-Fi offloading scenarios; enhancements to ANDSF policy solutions; P4C (formerly called BBAI) for interworking with broadband backhaul networks etc.

As mentioned earlier in the paper, IETF mobility standards are ideal as interworking solutions between Cellular and Wi-Fi, since the IETF solutions are IP-layer based, a common language supported by both

networks. IETF is continuing to advance these technologies, an example of which is the Distributed Mobility Management (DMM). This is an architectural enhancement for the PMIP based mobility solutions, where there are multiple LMAs and mobility between these is managed in a distributed manner.

6.2 Technology Developments

6.2.1 Discovery of Wi-Fi Hotspots

Discovery of Wi-Fi Hotspots by a UE is not trivial because often there are many Hotspots at a given UE location, each provided by a different person or entity, with some being open for public access and others being secured private Hotspots, with some having a roaming relationship with the UE's mobile operator, etc. Furthermore, Hotspots, by definition, do not generally provide contiguous coverage over a wide area, so that it is not feasible for the network to provide such information to the UE on a regular basis. To address this problem, both 3GPP and IEEE/WFA have developed solutions for Wi-Fi Hotspot discovery. The 3GPP approach to addressing this problem is centered on the Access Network Discovery and Selection Function (ANDSF), c.f. 3GPP TS 24.302 and TS 24.312. The ANDSF server is typically a remote server which must be accessed using IP-based access. The ANDSF provides the Wi-Fi Hotspot discovery information to UEs in the form of OMA DM Management Objects (MOs) and uses the OMA DM protocol to deliver the information. The MOs provide a list of Wi-Fi Hotspots near the location of the UE, which location may be defined in terms of Cellular Location Area or Cell ID etc. As the UE moves around, the MO needs to be synchronized to obtain the latest relevant information.

However, the Wi-Fi discovery information included in ANDSF is limited to just the SSID (or BSSID) – essentially the name that the network advertizes over the air. It does not provide any information that would be required to access and authenticate to the network. This function is provided by the IEEE's 802.11 Group through the ANQP protocol, which is part of the 802.11u amendment – and also part of Wi-Fi Alliance's Hotspot 2.0 profile.

According to this technology, a Hotspot 2.0 capable Wi-Fi AP includes in the beacon signals (which are constantly broadcast by the AP for user devices to listen to before accessing the AP) information indicating that it is a Hotspot-capable AP. Upon detecting this, a user device may engage in a query and response exchange with the AP before the user device is authenticated by the AP and/or the network behind it. This unique feature speeds up the discovery process, especially when there are a large number of APs to discover.

The query and response protocol is called Access Network Query Protocol (ANQP) and is used by a mobile device to discover a range of information, including the Hotspot operator's domain name (a globally unique, machine-searchable data element); roaming partners accessible via the Hotspot along with their credential type and EAP method supported for authentication; IP address type availability (for example, IPv4, IPv6); and other metadata useful in a mobile device's network selection process.

Unfortunately, ANDSF and ANQP are not fully compatible with each other, although some efforts are being made by the industry towards that goal.

6.2.2 Operator Policies for Selection and Use of Wi-Fi Hotspots

The ANDSF framework developed by 3GPP also enables the operator to specify policies as to how to prioritize, select and use the discovered Wi-Fi Hotspots. For example, these policies may be based on the UE's location as well as other variables, such as time-of-day, subscription level, types of application etc. Such policies are collectively referred to as ISMP (Inter System Mobility Policy) and are again codified in the ANDSF MO, which is maintained by the UE and synchronized with the Operator's ANDSF Server either regularly or based on some triggers.

Modern UEs, such as smartphones, are expected to be simultaneously connected to the networks via cellular as well as Wi-Fi radio access. In such cases, it is possible to use Wi-Fi for certain applications (or IP-Flows) and the cellular for other applications. The operator can define such policies also, which are collectively referred to as ISRP (Inter System Routing Policy). These are also codified in the ANDSF MO.

Figure 9, which we copied from Figure 4.2.1 in the 3GPP specification TS 24.312 , shows the structure of an ANDSF MO, where the Discovery Information, ISMP (labeled only as Policy in the drawing) and the ISRP are indicated. These are dependent on the UE location, which is also shown in the MO structure.

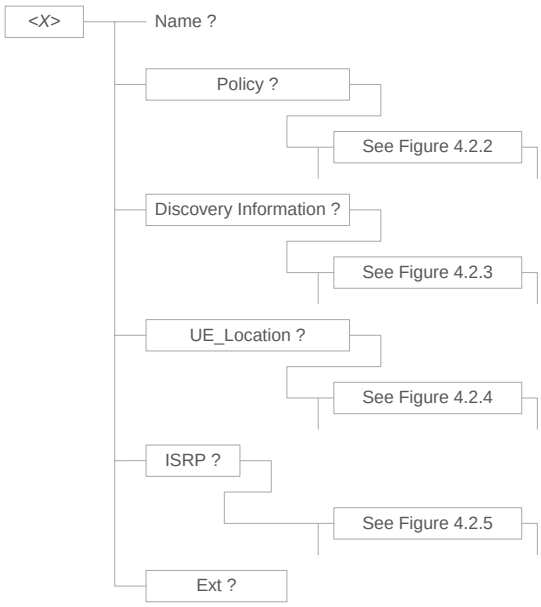


Figure 9. Structure of ANDSF Management Object (Figure 4.2.1 in 3GPP TS 24.312)

6.2.3 Connection Managers

Most of the advanced features that we have described rely on certain key capabilities at the mobile device. One of these capabilities is commonly known as the Connection Manager (CM). The CM is the software that is in charge of managing the network connections of the device, taking into account user

preferences, operator preferences, network conditions, etc. Although CMs have typically been a proprietary and/or customized technology, due to the needs to provide a uniform user experience and a coherent management platform for operators, new standardization initiatives have been created.

Some of these initiatives come from the Open Mobile Alliance (OMA) and IETF, which have started some work under the Connection Management Access Point Interface (OMA-CMAPI) and IETF Multiple Interfaces Working Group (MIF) umbrellas. The work in these working groups is aimed at providing additional and common functionalities to applications, users, and network operators to manage the network connections of the mobile device in a coherent manner, taking into account the different network types, network discovery and selection services (e.g. ANDSF and WFA Hotspot 2.0), service handling, power management, contacts handling, security authentication and authorization such as Single Sign-On (SSO), location management, etc.

6.2.4 Mobile Network Offloading (LIPA, SIPTO)

At a high level, Cellular Wi-Fi Integration may be seen as a technique for managing data traffic in a mobile operator networks in a smart manner. For example, the traffic would be dynamically routed to use the optimal radio interface to suit the particular application and user at hand, taking into account also connectivity cost, reliability security, network congestion etc.

In such a perspective, cellular/Wi-Fi integration is but one technique of such intelligent traffic management, which may be referred to as Radio Interface Offloading. The other technique would be Network Offloading, referring to intelligent routing of traffic within the backend networks. We shall briefly describe some developments in this interesting arena.

The problem addressed by IP offload is that by default all IP traffic generated by a mobile device (or sent to a mobile device) is routed to and through the mobile core network. There are good reasons for this: i) it is necessary to ensure full mobility support; ii) it allows the operator to manage both the user's QoE and how its network is used; iii) it is necessary to access operator service. However, there may be certain drawbacks in such routing for certain types of traffic. For example, local traffic (i.e. traffic destined to local IP networks) and traffic from public internet (e.g. YouTube traffic, as opposed to Operator service traffic) need not traverse the operator core network. In fact, such routing may introduce additional latencies to local traffic, affecting the user experience. For internet traffic, such routing would unnecessarily load the operator network, which can be avoided. SIPTO and LIPA are two solutions that 3GPP is standardizing for these problems.

The first of these solutions is Selected IP Traffic Offload (SIPTO). Based on network-specified policies, SIPTO supports offload of IP traffic directly to the internet and away from the mobile core network. The upside to the operator is lower load on its network, however there is a significant price to pay – mobility support for SIPTO traffic can be rather limited, and offloaded traffic cannot access operator services. Thus, the operator must be careful in selecting which traffic to offload.

For example, offloading a web browsing session is generally considered safe. Any interruptions due to mobility will often go unnoticed because the duty cycle of activity for web browsing is usually low and HTTP initiates a new session for each search. On the other hand, voice call, even when handled as VoIP, should generally be routed through the core network to provide seamless mobility.

Implementation of SIPTO requires a special functionality (in a separate node or integrated with an existing node) to be placed between the Radio Access Network (RAN) and the Core Network (CN) to accomplish this. Traffic selection for offload is based on operator policies – which must strike the right balance for offload decisions – and traffic may be segregated based on 5-tuple IP filters.

Like SIPTO, Local IP Access (LIPA) is designed to optimized IP traffic management. LIPA focuses on IP traffic destined to a local IP Network and is designed to route such traffic locally instead of through the mobile core network. As with SIPTO, the price is limited mobility support for the locally routed traffic; also, just like with SIPTO, policy-driven 5-tuple based routing is used to select which traffic is routed locally.

The Future: 2013 and Beyond

7 Grand Convergence for a Bright Future

Building on ten years of growing interdevelopment, the future of cellular/Wi-Fi integration is being accelerated and brought to the forefront. A significant part of that is the impact of increasing data use, resulting in network congestion on the operator side and cost/usage issues on the user side. Infonetics Research reported in May 2012 that two thirds of wireless carriers had already deployed Wi-Fi ranging from 20,000 to over 150,000 access points in public spaces, and that nearly all carriers planned to increase the number of Wi-Fi access points by 2013 (*Carrier Wi-Fi Offload and Hotspot Strategies: Global Service Provider Survey*, May 10, 2012). From the consumer side, increased capabilities and new applications are often driving demand for data that outstrips most data plans.

What might this future look like? Our vision is for an integrated solution that addresses the issue at both the network and the terminal unit ends. Starting with the device, a smart connection manager will fully automate spectrum access to the point where the users will no longer have to think about what cellular operator, what WiFi SSID, what Bluetooth connection they needs to use. They will simply start their apps or make a call or configure a background task such as health monitoring. Perhaps they will specify an app's priority, how much they are willing to pay for it or the access right. The smart connection manager will take this information, examine the available connectivity options together with access policies provided by the operator, and allocate the "right bandwidth" for the right application.

Is this vision far off? Not at all: solutions such as InterDigital's Smart Access Manager (SAM) are already providing per-application bandwidth management across Wi-Fi and cellular networks. In InterDigital's case, we combine user preferences and operator's ANDSF policies and use EAP-based techniques to automate access to wireless networks. As the operators move ahead with true WiFi integration, SAM is well positioned to provide support for features that will take advantage of such integration, such as IP Flow Mobility and bandwidth aggregation. Moreover, as WFA, 3GPP, the Wireless Broadband Alliance and the GSM Association work towards integrating policy management solutions offered by ANDSF and Hotspot 2.0 (through ANQP), the decision-making capabilities of SAM will become ever more sophisticated.

From an operator's point of view, the Integrated Small Cell, such as the IFW solution being put forward by the Small Cells Forum, will become an ever-important component of the spectrum management puzzle. From loosely integrated solutions, such as InterDigital's Converged Gateway, a tightly integrated approach is likely to emerge. This tightly integrated spectrum access solution will combine dynamic spectrum access across spectra as diverse as TV bands in sub-1 GHz band to millimeter wave spectrum in the 60 GHz range and will include all the bands traditionally used by cellular and WiFi systems. Beyond just an integrated spectrum access solution, the integrated small cell will deliver to its "owner" or "user" a true sense of ownership of the spectrum in their home, shop or office. To do so, it

will become a local policy integration and enforcement point. It will likely host operator policies (ANDSF- and PCRF-based) specific to its location, as well as the evolved Hotspot policy solution. It will combine these with emerging complex regulatory policies, such as TV White Space access policies and the policies of the small cell owner. Finally, Small Cells will evolve from isolated islands in a sea of lower-rate cellular coverage towards integrated networks. Using emerging techniques such as IETF's Distributed Mobility Management (DMM), these will provide efficient and high rate mobility solutions over localized regions, such as city downtowns, neighborhoods and college campuses.

Readers interested in video content related to InterDigital's efforts at multi-network aggregation and device management are invited to view the company's Youtube videos on our Bandwidth Management (http://www.youtube.com/watch?v=1sLjEuQkIQ8) and Spectrum Management (http://www.youtube.com/watch?v=DW7GP1wjbGw) solutions.

Appendix: Acronyms

3G	3rd Genration	LIPA	Local IP Access
3GPP	3rd Generation Partnership Program	LMA	Local Mobility Anchor
AAA	Authentication, Authorization and Accounting	LTE	Long Term Evolution
ANDSF	Access Network Discovery and Selection Function	M2M	Machine to Machine
ANQP	Access Network Query Protocol	MAPIM	Multi Access PDN Connectivity and IP Flow Mobility
AP	Access Point	MAG	Media Access Gateway
AR	Access Router	MIF	Multiple Interface
BBAI	Broadband Interworking	MIP	Mobile IP Protocol
BSSID	Basic Service Set Identifier	MIPv6	Mobile IP version 6
BTS	Basestation Transceiver Subsysten	MME	Mobility Management Entity
CDMA	Code Division Multiple Access	MMS	Multimedia Message Service
CM	Connection Manager	MN	Mobile Node
CMAPI	Connection Management Access Point Interface	MO	Management Object
CN	Core Network	NCR	National Cash Register
CS	Circuit Switched	OFDM	Orthogonal Frequency Division Multiplex
DM	Device Management	OMA	Open Mobile Alliance
DMM	Distributed Mobility Management	PCRF	Policy and Charging Rules Function
DSMIP	Dual Stack MIP	PDG	Packet Data Gateway
DSMIPv6	DSMIP version 6	PDN	Packet Data Network
DSP	Digital Signal Processor	PGW	PDN Gateway
CoA	Care-of-Address	PMIP	Proxy MIP
EAP	Extensible Authentication Protocol	PMIPv6	PMIP version 6
EAP-AKA	EAP-Authentication and Key Agreement	PRD	Permanent Reference Document

eNodeB	Evolved NodeB	PS	Packet Switched
ePDG	Evolved Packet Data Gateway	QoS	Quality of Service
EPC	Evolved Packet Core	RADIUS	Remote Authentication Dial In User Service
ETSI	European Telecommunications Standards Institute	RAN	Radio Access Network
FCC	Federal Communications Commission	RFC	Request for Comments
GERAN	GPRS & EDGE Radio Access Network	RNC	Radio Network Controller
GGSN	Gateway GPRS Support Node	SA	System Architecture
GPRS	General Packet Radio Service	SAM	Smart Access Manager
GSM	Global System for Mobile Communications	SC	Small Cell
GSMA	GSM Association	SCF	Small Cell Forum
GTP	GPRS Tunneling Protocol	SGSN	Serving GPRS Support Node
HA	Home Agent	SGW	Serving Gateway
HLR	Home Location Register	SIM	Subscriber Identity Module
HeNB	Home eNodeB	SIPTO	Selected IP Traffic Offload
HNB	Home NodeB	SSID	Service Set Identifier
HO	Handover	SSO	Single Sign On
HoA	Home Address	TDMA	Time Division Multiple Access
HSS	Home Subscriber Server	TR	Technical Report
IEEE	Institute of Electrical and Electronic Engineers	TS	Technical Specification
IETF	Internet Engineering Task Force	TLS	Transport Layer Security
IFOM	IP Flow Mobility	TTLS	Tunneled Transport Layer Security
IFW	Integrated Femto Wi-Fi	UE	User Equipment
IoT	Internet of Things	UMTS	Universal Mobile Telecommunication System
IP	Internet Protocol	UTRAN	UMTS Terrestrial Radio Access Network
IPv4	IP version 4	USIM	Universal SIM
IPv6	IP version 6	WAG	WLAN Access Gateway
ISM	Instrumentation, Scientific and Medical	WCDMA	Wideband Code Division Multiple Access
ISMP	Inter System Mobility Policy	WECA	Wireless Ethernet Compatibility Alliance
ISRP	Inter System Routing Policy	WG	Working Group
IT	Information Technology	WFA	Wi-Fi Alliance
IWLAN	Integrated Wireless Local Area Network	WLAN	Wireless Local Area Network
L-GW	Local Gateway	Wi-Fi	Wireless Fidelity
LHN	Local Home Network		

About InterDigital®

InterDigital develops fundamental wireless technologies that are at the core of mobile devices, networks, and services worldwide. As a long-standing contributor to the evolution of the wireless industry, we solve many of the industry's most critical and complex technical challenges years ahead of market deployment. Our advanced solutions support more efficient wireless networks, a richer multimedia experience, and new mobile broadband capabilities. Accordingly, we have established licenses and strategic relationships with many of the world's leading wireless companies.

InterDigital, Inc.
781 Third Avenue
King of Prussia, PA 19406 USA

www.interdigital.com