WLAN Traffic Offload in LTE

White Paper

This whitepaper provides an overview of the WLAN offload in LTE as standardized by 3GPP, as well as the enhancements for Wi-Fi standardized by IEEE and the Wi-Fi Alliance. It also describes access methods in the joint network, treats the security, and describes IP mobility. In addition network discovery and selection are explained.

White Paper

A. Schumacher / J. Schlienz

11/21/2012 - 1MA214_0e

ROHDE&SCHWARZ

Table of Contents

1 Introduction

Due to the strong increasing number of smart phones in the mobile market there is a tremendous growth for mobile data traffic. According to a forecast from Cisco [1], this traffic will grow from about 2 Exabyte per month in 2012 to more than 10 Exabyte per month in 2016, leading to a possible bottleneck in the mobile networks. In order to cope with this amount of traffic, operators are therefore under pressure to find pertinent solutions with reasonable costs.

One way is the optimization on the mobile network itself. In the 3rd Generation Partnership Project (3GPP) there are plenty of work items to improve the spectral efficiency and to improve the network architecture, for example with the introduction of *Heterogeneous Networks*, either with or without carrier aggregation. Of course, also the extension of the available frequencies is a permanent topic, allowing higher peak data rates and denser networks with reduced interferences in the cell edge.

Another way to improve data throughput is to include additional access technologies which already exist. WLAN is a promising candidate for this kind of solution, because there is a huge amount of networks already rolled out worldwide and the end devices are very price competitive. In addition, WLAN is optimized for in-building usage and is therefore best suited for a data offloading solution, because according to statistics from Ericsson [2], about 70% of the mobile data are created indoors.

WLAN is already integrated in most of the current smartphones. However, in most devices in the market today, WLAN and 3GPP technologies may be regarded as two separate devices in one box: Specific IP flows are routed over the WLAN access without traversing the 3GPP nodes. A first architecture for the integration of WLAN networks in 3GPP was defined from Release 6 on, the Interworking WLAN (I-WLAN) [3][4]. This architecture describes the interfaces between the networks, the data and control paths, and the protocols for the access and authentication. In the 3GPP Evolved Packet Core (EPC), this connection was defined from the very beginning, with two options denoting the trust relationship of a cellular network operator to the WLAN network [5].

In addition to the architecture there is the question how the data-offload is realized. Up to Release 9, the only way to offload data is using the WLAN as a foreign network with a handover on the IP level. Consequently, either the 3GPP network or the WLAN may be used for data exchange, but not both simultaneously. This is now changed from Release 10 on. In the IP Flow Mobility (IFOM) approach selected IP flows may be routed over the EPC connection, while others are routed over WLAN, depending e.g. on the availability and QoS requirements. Often only the IFOM capability is the feature which is called WLAN offload [6].

In this whitepaper the IFOM technology for the EPC is discussed. We start in chapter 2 with a short summary of the WLAN networks and explain in chapter 3 its integration into an EPC network. In chapter 4 the IP mobility is described showing the path to IFOM. In chapter 5 details about the network selection principles and operator policies are described. Finally, a short summary and outlook is provided in chapter 6.

2 Architecture of WLAN Networks

Wireless Local Area Network (WLAN) also commonly known as Wi-Fi is a wireless data communication system. It is widely used e.g. in corporate enterprises, offices, airports, stores, cafes/restaurants, and at home. Many portable computers (notebooks, tablets) and basically all smartphones are equipped with WLAN. The underlying technology is standardized by the Institute of Electrical and Electronics Engineers (IEEE) and the current specification is IEEE 802.11-2012, published in March 2012 [7]. It defines the physical layer (PHY) and medium access control (MAC).

For evolving the standard, IEEE forms task groups and enumerates them with letters. Their output is then an amendment to the base 802.11 standard. Since 1999 there are 18 amendments that were incorporated into a new revision of the whole 802.11 standard.

IEEE Std 802.11-2007 revision	
IEEE Std 802.11a™-1999	High Speed Physical Layer in the 5GHz Band
IEEE Std 802.11b™-1999	Higher-Speed Physical Layer Extension in the 2.4 GHz Band
IEEE Std 802.11d™-2001	Specification for Operation in Additional Regulatory Domains
IEEE Std 802.11g™-2003	Further Higher Data Rate Extension in the 2.4 GHz Band
IEEE Std 802.11h™-2003	Spectrum and Transmit Power Management Extensions in the 5 GHz Band in Europe
IEEE Std 802.11i™-2004	MAC Security Enhancements
IEEE Std 802.11j™-2004	4.9 GHz - 5 GHz Operation in Japan
IEEE Std 802.11e™-2005	MAC Enhancements for Quality of Service

IEEE Std 802.11-2012 revision	
IEEE Std 802.11k™-2008	Radio Resource Measurement of Wireless LANs
IEEE Std 802.11r™-2008	Fast Basic Service Set (BSS) Transition
IEEE Std 802.11y™-2008	3650–3700 MHz Operation in USA
IEEE Std 802.11w™-2009	Protected Management Frames
IEEE Std 802.11n™-2009	Enhancements for Higher Throughput
IEEE Std 802.11p™-2010	Wireless Access in Vehicular Environments
IEEE Std 802.11z™-2010	Extensions to Direct-Link Setup (DLS)
IEEE Std 802.11v™-2011	IEEE 802.11 Wireless Network Management
IEEE Std 802.11u™-2011	Interworking with External Networks
IEEE Std 802.11s™-2011	Mesh Networking

2.1 Physical Layer (PHY)

Several different implementations for operation in the 2.4 GHz ISM[1] band or the 5 GHz U-NII[2] and ISM bands are specified and used today [7]:

WLAN PHY Standards					
PHY	**Frequency Band**	**Channel Bandwidth**	**Modulation**	**Transmission Technology**	**Max. Data Rate**
802.11a (OFDM)	5 GHz	20 MHz	OFDM	SISO	54 Mb/s
802.11b (HR/DSSS)	2.4 GHz	22 MHz	DSSS/CCK	SISO	11 Mb/s
802.11g (ERP)	2.4 GHz	22 MHz	DSSS/CCK, OFDM	SISO	54 Mb/s
802.11n (HT)	2.4 / 5 GHz	20, 40 MHz	OFDM	SISO, SU-MIMO	600 Mb/s
802.11ac (VHT)	5 GHz	20, 40, 80, 80+80, 160 MHz	OFDM	SISO, SU-MIMO, MU-MIMO	6.933 Gb/s

The amendment 802.11ac (Very High Throughput) allows data rates of several Gb/s. Completion and release of this amendment is anticipated for beginning of 2013.

2.2 Medium Access Control (MAC)

The physical medium access is controlled by the protocol named Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). This also implies that the MAC has to acknowledge correctly received data packets. Further functionality includes the data fragmentation and reassembly, data security, authentication/de-authentication, association/disassociation, and the periodical transmission of beacon frames. Additional functions for transmit power control, Quality-of-Service (QoS) traffic scheduling, and radio measurements are also incorporated into the MAC layer.

There are three frame types for communication on MAC-level:

- **Management Frames**
  beacon, probe request/response, association request/response, re-association request/response, authentication, de-authentication, disassociation, announcement traffic indication message (ATIM), action.
- **Control Frames**
  acknowledge (ACK), block ACK request, block ACK, request to send (RTS), clear to send (CTS), power save (PS) poll.
- **Data Frames**
  data, null (no data), several for contention free (CF) and QoS prioritized communication.

---

[1] Industrial, Scientific, and Medical band: 2.400 - 2.500 GHz, 5.725 - 5.875 GHz

[2] Unlicensed National Information Infrastructure band: 5.150 - 5.350 GHz and 5.470 - 5.825 GHz

2.3 Network Architecture

The IEEE 802.11 architecture consists of several components. Every addressable device with WLAN functionality is a Station (STA). There are special STA entities that have additional functionality and are connected to a Distribution System (DS). Such an entity is named Access Point (AP). See Figure 2-1 for an illustration.

An AP with one or several connected STAs forms a Basic Service Set (BSS). The BSS is the basic building block of a WLAN and corresponds to a cell in e.g. LTE. The STAs that are member of a certain BSS are not static. I.e. a device (e.g. STA 3) could move away from its associated AP 1 and/or come closer to the neighboring AP 2 and associate with it, thus becoming a member of BSS 2.

Several APs can be connected together with the DS. This allows e.g. STA 1 in BSS 1 to communicate with STA 6 in BSS 2. Such a group of elements is then called Extended Service Set (ESS).

There is another basic type of connection, namely when STAs directly connect with each other and no AP is involved. Such a network is an Independent Basic Service Set (IBSS) or also known as ad-hoc network. This network topology is possible, because in WLAN the communication is symmetrical on the physical layer, i.e. there is no distinction between uplink (UL) and downlink (DL).

Hotspots always consist of an AP and usually are connected to a router and the Internet, therefore they are a BSS or in case of a larger venue, an ESS.

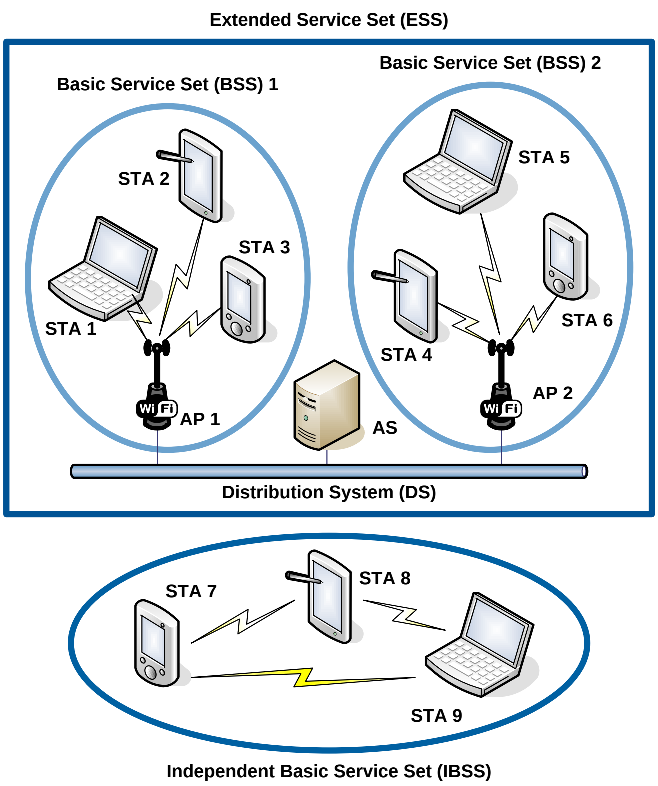

Figure 2-1: Components of the WLAN Architecture

The standard 802.11-2012 also defines the Robust Security Network Association (RSNA) as part of the architecture. It was added through the 802.11i amendment and improves the security with the following features:

- Enhanced authentication mechanisms for STAs
- Key management algorithms
- Cryptographic key establishment
- Enhanced data cryptographic encapsulation mechanisms
- Fast basic service set (BSS) transition (FT) mechanism
- Enhanced cryptographic encapsulation mechanisms for robust management frames

In order to use these features, external components may be necessary. One is an IEEE 802.1X port access entity (PAE) implemented in every STA. Another is the Authentication Server (AS) that can authenticate elements of an RSNA and also uses IEEE 802.1X.

2.4 IEEE 802.11u

The IEEE 802.11u [8] is an amendment to the 802.11 standard and is titled "Interworking with External Networks". It was published in February 2011 and was incorporated into the 802.11-2012 specification version. According to [7] the amendment "*defines functions and procedures aiding network discovery and selection by STAs, information transfer from external networks using QoS mapping, and a general mechanism for the provision of emergency services.*"

The main extensions to the MAC layer are: the Generic Advertisement Service (GAS) that enables a communication of a STA with an AP before an actual association; additional information elements (IEs) for the Beacon frame and other management frame types; a QoS mapping of external QoS control parameters to the QoS parameters of 802.11; a MAC Service Data Unit (MSDU) rate limiting function to enforce the resource utilization limit if indicated by the destination STA; support of emergency services, i.e. allow a STA without proper security credentials to still place an emergency call.

There are no changes to the PHY layer and therefore the same hardware can be used.

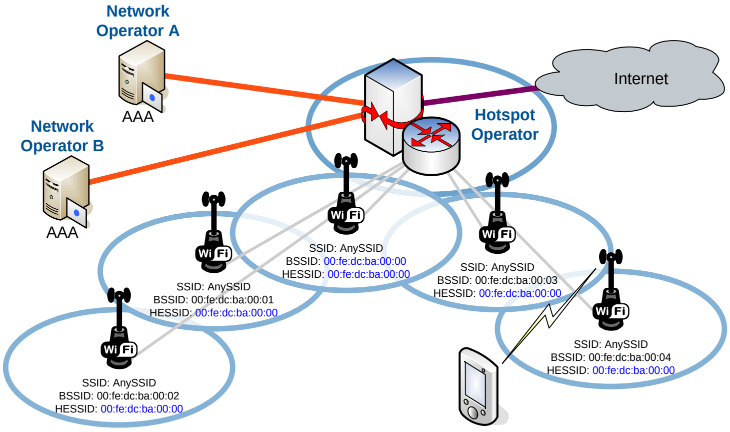

Figure 2-2: Several 802.11u APs forming a homogeneous ESS

Venues where WLAN access is provided often have several APs linked together in an ESS, what is also called a Homogeneous ESS. 802.11u adds the Interworking IE that also contains a Homogeneous ESS identifier (HESSID) that allows the STAs to identify which APs belong to the same ESS. An example is shown in Figure 2-2 where all the APs indicate that they belong together by using the BSS identifier (BSSID) of one of them as HESSID.

2.5 Security

In WLAN, authentication and data encryption is integrated together. For authentication there are two methods, open system authentication and secure authentication. The open system authentication which is part of Wired Equivalent Privacy (WEP) does not require credentials to access a network. Therefore, no authentication is done and any STA can connect. WEP keys may be used for data encryption, but this method does not provide security anymore. Since 2006 all new Wi-Fi devices have to provide Wi-Fi Protected Access 2 (WPA2) for secure authentication and data encryption.

It is also possible to use another authentication method with the help of the Extensible Authentication Protocol (EAP) and WPA2 provides the data encryption.

2.5.1 Data Encryption over the WLAN Air Interface

The Wired Equivalent Privacy (WEP) protocol was the first security feature introduced for WLAN for both authentication and data encryption. It relies on a four step challenge-response handshake. Technically, it requires the knowledge of a shared key (40, later 104 bits) that is used for an RC4 symmetric encryption. However, with today's available processing power and certain software tools, it is possible to decipher the shared key and thus cannot be regarded anymore as secure.

In order to improve the security, the Wi-Fi Protected Access (WPA) was introduced as an interim solution. It offers two modes: Preshared Key (PSK) and Enterprise. WPA-PSK wraps another layer around WEP adding three new elements: a Message Integrity Code (MIC) that is a keyed hash value of the payload, a per packet key mixing function using the Temporal Key Integrity Protocol (TKIP), resulting in an effective full 128-bit dynamic key, and a packet sequencing number also derived from the TKIP, that is added into the MPDU before the legacy WEP encryption. The enterprise mode uses an 802.1X based protocol and offers a higher security, because it does not rely on a shared secret.

Today's state of the art security is the Wi-Fi Protected Access 2 (WPA2), which is specified in the 802.11i amendment, finally ratified in June 2004. It is based on a 128 bit Advanced Encryption Standard (AES) block cipher algorithm and uses the new architecture called Robust Security Network (RSN). It is suitable for small home networks (WPA2-Personal) as well as large corporate networks (WPA2-Enterprise). An RSN Association (RSNA) consists of three entities: *Supplicant* e.g. a WLAN STA, *Authenticator* e.g. a WLAN AP, and *Authentication Server* often a Remote Authentication Dial-In User Service (RADIUS) server. How a WPA2 authentication works is briefly shown in Figure 2-3.

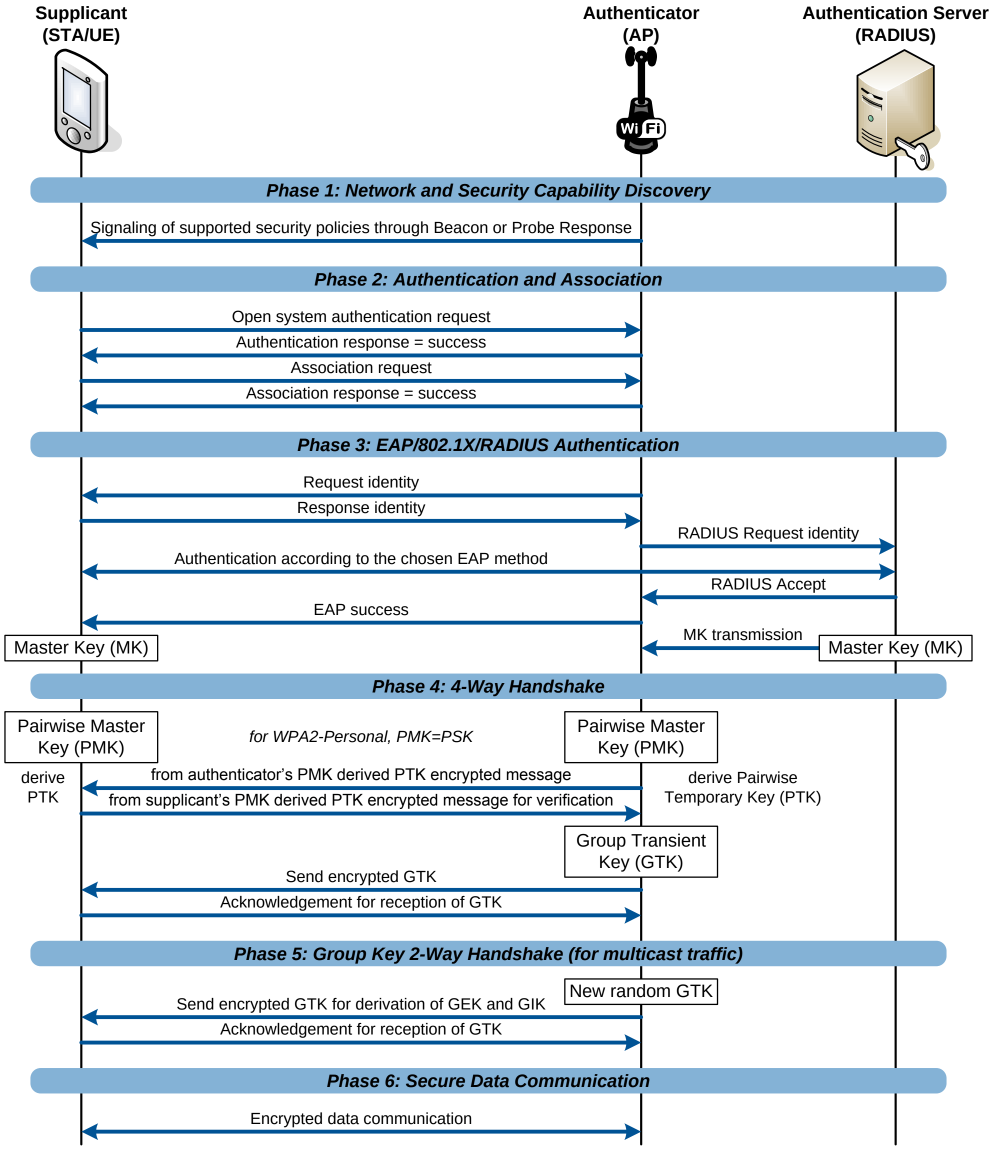

Figure 2-3: WPA2 Authentication Procedure

For secure communication, data integrity and data confidentiality is provided with Counter Mode Cipher-Block Chaining Message Authentication Code Protocol (CCMP) and optionally with TKIP. CCMP utilizes the AES block cipher algorithm with 128 bit key and block length. This encryption ensures certification by the Federal Information Processing Standards (FIPS) for use in non-military government agencies.

Two additional features were also added with 802.11i, the key-caching and a pre-authentication. Caching together with a session timeout allows a station to faster reconnect if it returns to the same AP. Pre-authentication enables faster roaming because APs can send authentication messages between them. For example, if someone with a Wi-Fi device walks through an airport, he or she does not need to authenticate to every AP, the network can handle that.

2.5.2 Secure Authentication

The Extensible Authentication Protocol (EAP) is defined in [9] and provides a simple and generic framework for authentication in IP networks. It does not define the authentication itself. Currently, there are over 40 EAP methods defined such as EAP-TLS, EAP-TTLS, EAP-SIM, and EAP-AKA.

User Equipment (UE) based on GSM or 3GPP standards have a (Universal) Subscriber Identification Module (U)SIM with which they are authenticated with the Mobile Network Operator (MNO). In order to prevent redundant provisioning and to reuse the billing infrastructure, it is beneficial to use the UE's authentication method even at the Wi-Fi hotspot. Therefore, a hotspot AP should support EAP-SIM (2G/GSM), EAP-AKA (3G/WCDMA), and EAP-AKA' (4G/LTE).

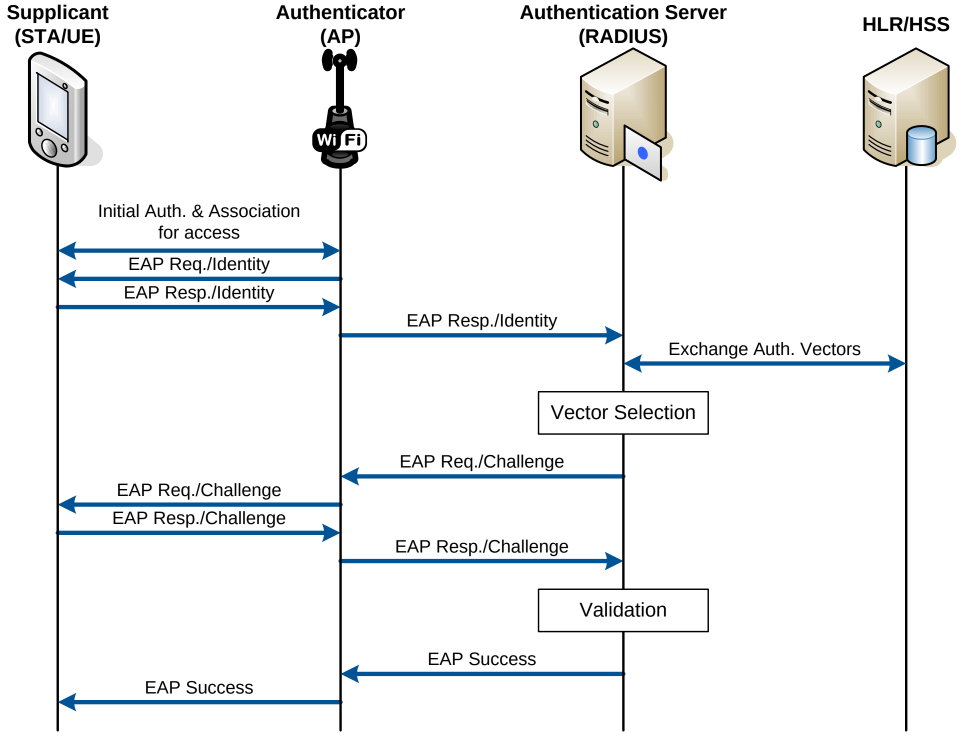

Figure 2-4: EAP Authentication

An EAP authentication is exemplarily shown in Figure 2-4. A user's UE that wants to connect to an MNO's Wi-Fi hotspot will use the EAP method for e.g. an EAP-AKA' authentication. The UE sends its unique identity to the AP which communicates with a RADIUS server. This server then checks with the MNO's Home Subscriber Server (HSS) if this UE is allowed to connect. Then, the RADIUS server does the mutual authentication via the AP with the UE, and in the successful case, the RADIUS server signals to the AP that the UE is authenticated and allowed to connect.

2.6 Wi-Fi Alliance

The Wi-Fi Alliance® is a global non-profit organization. Their goal is to promote and market Wi-Fi worldwide, encourage manufacturers to adhere to the 802.11 technology standards, and test and certify these products for interoperability. The term *Wi-Fi* stands for *Wireless Fidelity*, analogous to high fidelity (*Hi-Fi*) for audio equipment.

In March 2000, the Wi-Fi CERTIFIED™ program was launched to provide a widely-recognized designation of interoperability and quality. A product is only allowed to carry the Wi-Fi CERTIFIED logo after it passes rigorous interoperability certification tests. Users can then be sure that these products work with each other and deliver the best user experience.

Within the Wi-Fi Alliance there are task groups that define minimum feature requirements and test specifications. The members of this industry association and the task groups are mostly manufacturers devoted to wireless communication.

2.6.1 Hotspot 2.0 / Passpoint

In 2010 the Wi-Fi Alliance started a task group named “Hotspot 2.0”. The aim was to define functions and services from the standards that fully support service provider business objectives and improve the end-user hotspot experience. Using a hotspot should be as simple and secure as using the cellular network.

As of June 2012, the Wi-Fi Alliance® is testing mobile devices and infrastructure equipment for its Wi-Fi CERTIFIED Passpoint™ program. Passpoint mobile devices can automatically discover and connect to Wi-Fi networks powered by Passpoint-certified access points, delivering the true mobile broadband experience that users want and supporting service provider business objectives. The specification behind Passpoint was defined by service provider and equipment maker members of the Wi-Fi Alliance to address critical business needs for mobile data, streamlined access and subscriber loyalty. In addition to making it easy for end users to connect, hotspots equipped with Passpoint-certified equipment automatically enable enterprise-grade WPA2™ security. The Passpoint certification program is based on technology defined in the Wi-Fi Alliance Hotspot 2.0 Specification; a planned update to the program will add support for operator policy in network selection and capability for on-the-spot provisioning of new accounts. [10]

3 WLAN Access to the 3GPP Network

There are two different ways for a WLAN network to connect to the EPC, either as a non-trusted or as a trusted access. The name *trusted* means that there is a secure communication between the WLAN network and the EPC for both authentication and data protection. The trust relationship is the same for the complete network even if it supports access to multiple Packet Data Networks (PDNs). In order to use the trusted access, the EPC operator should have either control over the WLAN network or a trusted relationship to its owner. Consequently the trust relationship is essentially a business decision and is not related to the access network itself.

3.1 Non-Trusted Access

The network architecture of the non-trusted EPC access is shown in Figure 3-1. It is the evolution of the WLAN access to the 3GPP UMTS in Release 6, called I-WLAN [3], where the access to the 3GPP network was over the Packet Data Gateway (PDG) network node to the GGSN, the 3G counterpart of the PDN GW.

The I-WLAN architecture was adapted to the EPC in Release 8 with an evolved PDG (ePDG) connected to the PDN GW. The ePDG is under full control of the EPC network operator and interfaces to the WLAN via the SWn interface. It is an enhancement of the PDG adapted to the EPC with new functionalities defined, e.g. for IP mobility. Both, network based and client based IP mobility architectures are supported which shows up in using the S2b or S2c interface between the ePDG and the PDN GW, respectively.

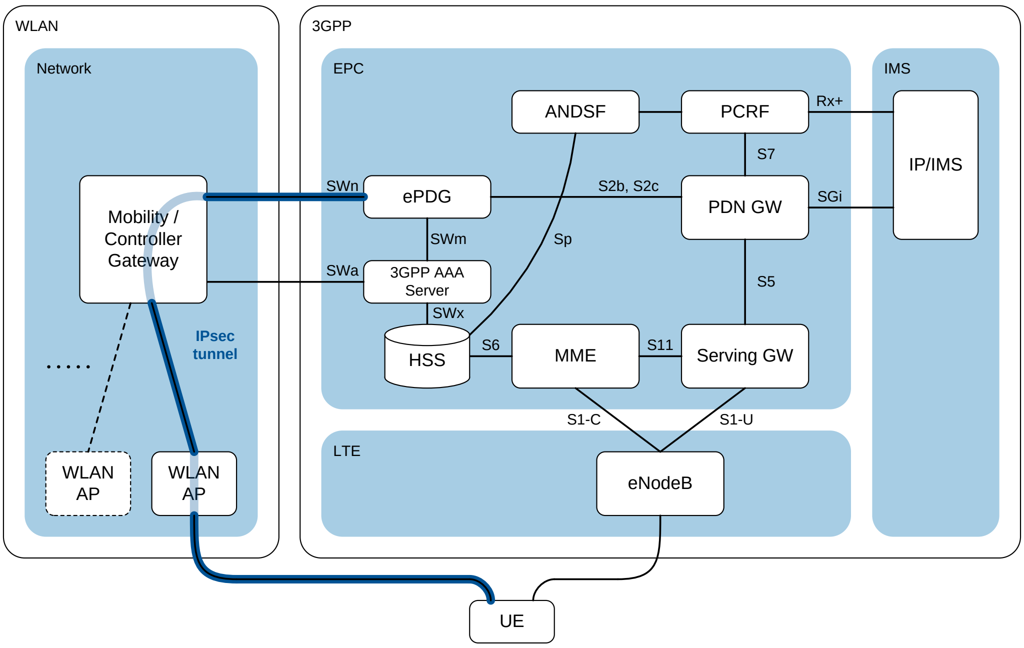

Figure 3-1: WLAN network integrated into the EPC as an untrusted access (non-roaming architecture)

For access authentication the WLAN gateway interacts with the EPC over the SWa interface to the 3GPP Authentication, Authorization, and Accounting (AAA) server, or to the 3GPP AAA Proxy in the roaming case.

In order to get connection with the EPC, the UE has first to authenticate with the AAA (Proxy) server. In a next step, a secure data tunnel (IPSec) between the UE and the ePDG has to be established in order to set up a data path. Here, the ePDG acts as an authenticator and gets the required AAA related parameters from the AAA server (proxy) via the SWm interface. In this part, Internet Key Exchange Version 2 (IKEv2) signaling between the UE and the ePDG is used. When client based mobility (see chapter 4.1) is applied, an additional IPSec tunnel between the UE and the PDN GW has to be established.

3.2 Trusted Access

The trusted WLAN access to the EPC is only defined from 3GPP Release 11 on. From an architectural point of view, the main difference to the non-trusted access is the missing ePDG. Instead, the non-3GPP network interacts directly with the EPC (Figure 3-2).

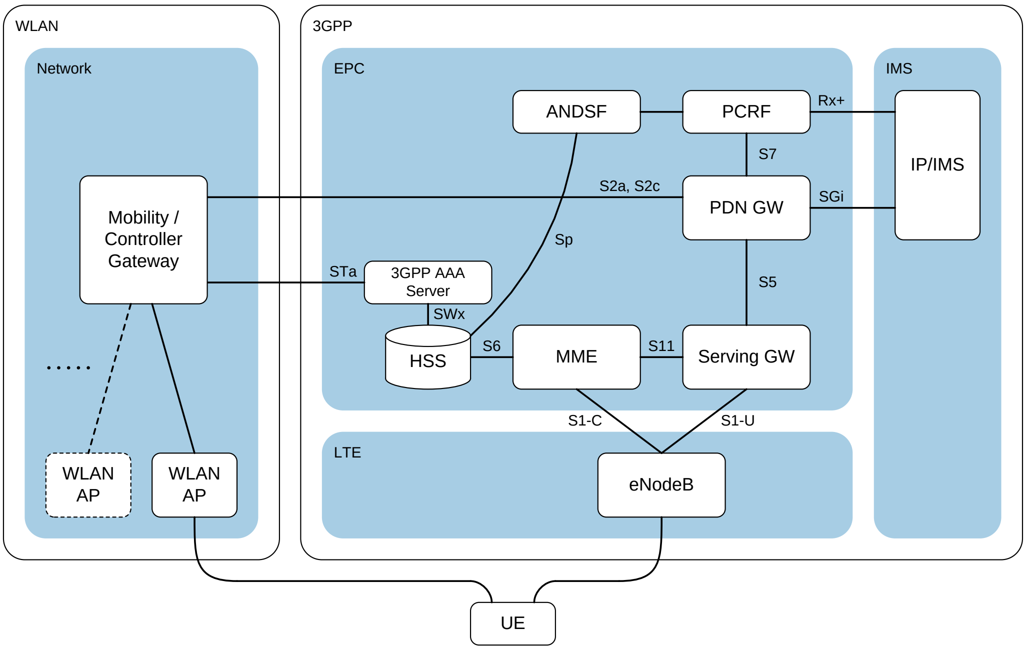

Figure 3-2: WLAN network integrated into the EPC as a trusted access (non-roaming architecture)

The PDN GW is connected over the S2a or S2c interface, depending on the IP mobility. Due to the trust relationship, there is no need to set up an additional IPSec tunnel between the UE and the EPC network, apart from the one used in case of client based IP mobility. Connection to the AAA server is done over the STa interface. Whereas it is optional in the non-trusted architecture to require a 3GPP based authentication, it is mandatory in the trusted one.

In both architectures, the trusted and the non-trusted, this authentication is independent of the WLAN technology and is instead based on the EAP-AKA' protocol. Authentication is based on USIM credentials which are obtained by the 3GPP AAA server over the SWx interface from the HSS, together with additional subscriber information needed.

4 IP Mobility

IP mobility takes care of routing data packets to the intended receiver when moving to a foreign network. A central point is to keep the IP address of a UE fixed so that there is no need for layers above the IP layer to adapt to the network change. Consequently, upper layer connections can continue without notification about the receiver's mobility.

Generally, IP mobility support can be realized with two different approaches:

- Client based IP mobility
- Network based IP mobility

This distinction does not depend on the underlying Radio Access Technology (RAT); it is completely realized in the IP protocol stack.

4.1 Client Based IP Mobility

In the client based mobility of IPv6 the UE carries the mobility extensions in its own IP protocol stack. Central to this approach is to split the IP address into the home address (HoA), which is the permanent IP address obtained from the home network, and the care of address (CoA), which corresponds to a temporal IP address and is obtained from the visited network.

The administration of these addresses is done in a Home Agent (HA) (Figure 4-1). As long as the UE is in the home network, the HA routes the data packets directly to the UE using the HoA. When the UE changes the network, it informs the HA with a Proxy Binding Update (PBU) message about its new IP address, which is stored by the HA in the binding cache. This is essentially a lookup table which is queried for each incoming packet. If there is a CoA entry for this UE in the binding cache, the packet is instead forwarded to its CoA. As an optimization it is also possible to route IP traffic between a Correspondent Node (CN) and the UE directly, in this case a binding cache has additionally to be established in the CN itself.

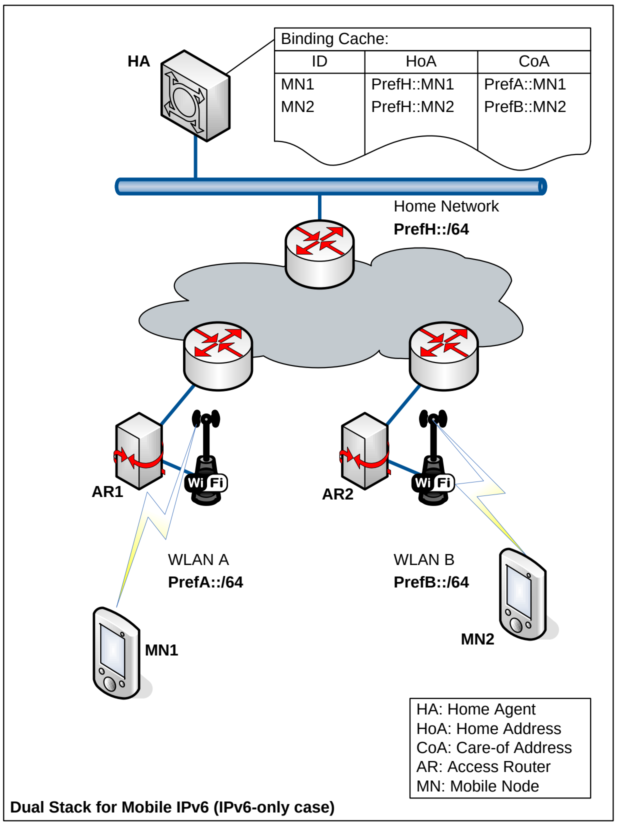

Figure 4-1: Client based mobility. The HA keeps the information about the client's location and routes the incoming data packets to the client in the visited network.

In an extension [11] mixed networks with both, IPv4 and IPv6 are supported with the Dual Stack Mobile IPv6 protocol (DSMIPv6). This is essential to integrate most existing networks built on IPv4 into the new networks, which will be more and more equipped with IPv6 technology. For a client based mobility EPC access with WLAN, DSMIPv6 is mandatory.

With this approach it is possible to offload data traffic from an LTE network to the WLAN connection. However, this works only for a complete offload, i.e. it is either possible to communicate over the LTE connection or over the WLAN connection, but not over both (Figure 4-2). The reason is that in this architecture the WLAN network is considered as a foreign network, to which all the data packets are forwarded when there is a corresponding entry in the binding cache of the HA.

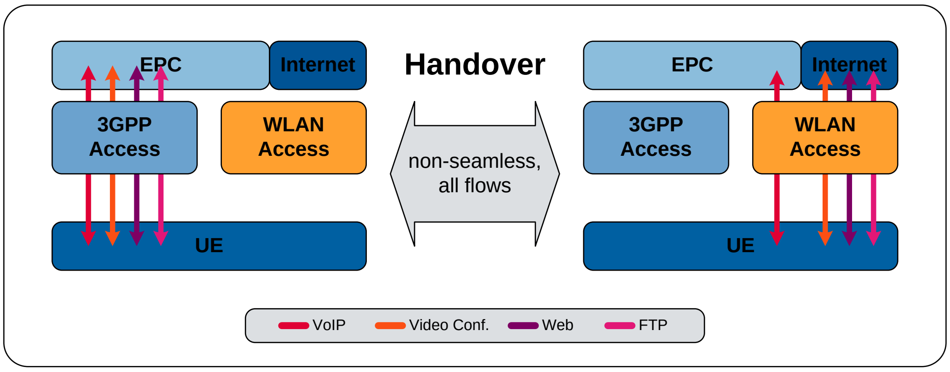

Figure 4-2: Complete WLAN offload using IP mobility

4.1.1 IP Flow Mobility (IFOM)

For a more efficient WLAN data offload there is the requirement to send different data flows to different CoAs. This is not possible in the current architecture, because there is only support for one CoA in the binding cache. So, a new extension for the network mobility has been designed (Figure 4-3)[12], called IFOM.

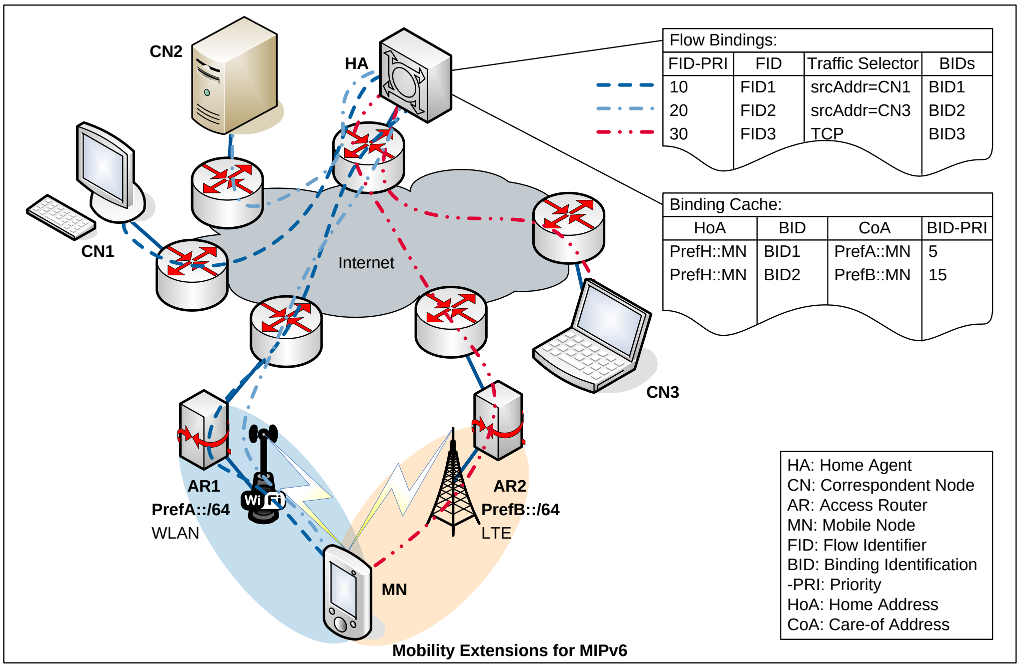

Figure 4-3: IFOM Extension to the client based mobility. There are several entries in the binding cache now possible, each one connected to a characterized traffic flow.

Central to this approach is a new table, the *Flow Bindings*. This is a table with one entry for each flow, which is characterized in the *Traffic Selector* field by the source or destination address, transport protocol or other fields in the IP and higher layer headers[13]. Each flow points to one entry in the *Binding Cache* using the BID field, which identifies one of several CoAs assigned to the UE. Both lists are ordered with respect to the priorities (FID-PRI and BID-PRI), which are assigned to each mobile separately. A lower number means a higher priority.

For each incoming data packet, its flow is identified with the highest priority matching entry from the top of the Traffic Selector field. Using the corresponding BID, the CoA and so the technology to be used is identified using the BID entry in the Binding Cache. If either the data packet does not fit to any traffic selector or if the corresponding entry in the Binding Cache does not exist, the CoA with the highest priority is used.

In the example of Figure 4-3, two entries in the Binding Cache are defined for the UE under consideration: BID1 to route the packets over the WLAN interface, and BID2 to route them over LTE. Here, routing over WLAN has higher priority than routing over LTE. If an incoming packet comes from CN1, it is routed over the WLAN interface, if it comes from CN3, it is routed over LTE. Data packets sent with the TCP protocol and neither from CN1 nor CN3 are also routed over WLAN, because they point to BID3 which is not defined (yet) in the Binding Cache and so uses the Binding Cache entry with the highest priority. The same is also true for any other packets.

Using these IFOM extensions, the offloading of different data flows described in Figure 4-4 can be realized: Depending on the availability and quality of the access technologies, different flows can be offloaded to WLAN while keeping the LTE connection running. In this example, the (real time) video stream is kept on LTE, while the VoIP, Web and FTP connections are offloaded to WLAN.

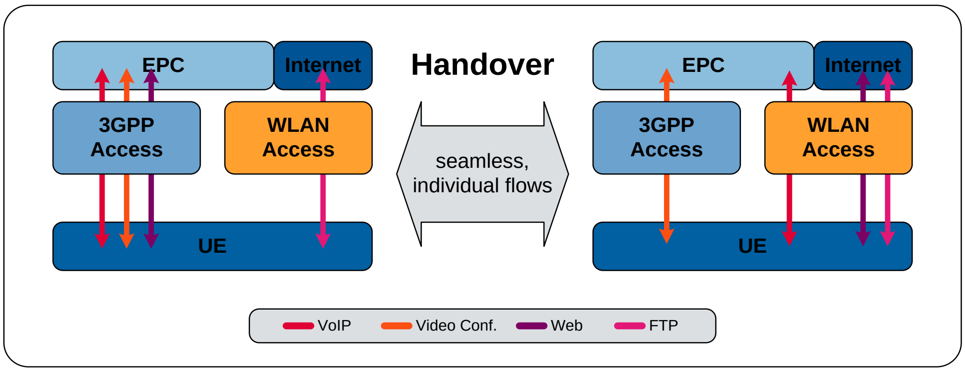

Figure 4-4: WLAN Offloading of different data flows using IFOM

4.2 Network Based IP Mobility

A completely different approach to take care of the user mobility is the network based mobility. Contrary to the client based IP mobility, the network takes all necessary steps to route the data packets to the intended receiver. From this follows that there is no need for the client to do any signaling on network change, this is all done by the network itself. There are two approaches for the network based IP mobility, the PMIPv6 and the GTP.

4.2.1 Proxy Mobile IP Version 6 (PMIPv6)

The Proxy Mobile IP protocol (PMIPv6) is specified by the IETF in [14]. Routing is based on two additional entities, the local mobility anchor (LMA), which works in a similar way as the HA in the client based mobility approach, and the mobile access gateway (MAG), which implements the necessary mobility functions in the visited network (Figure 4-5). When the UE changes the network, the MAG is contacted by the new base station and informs the LMA about the change of location.

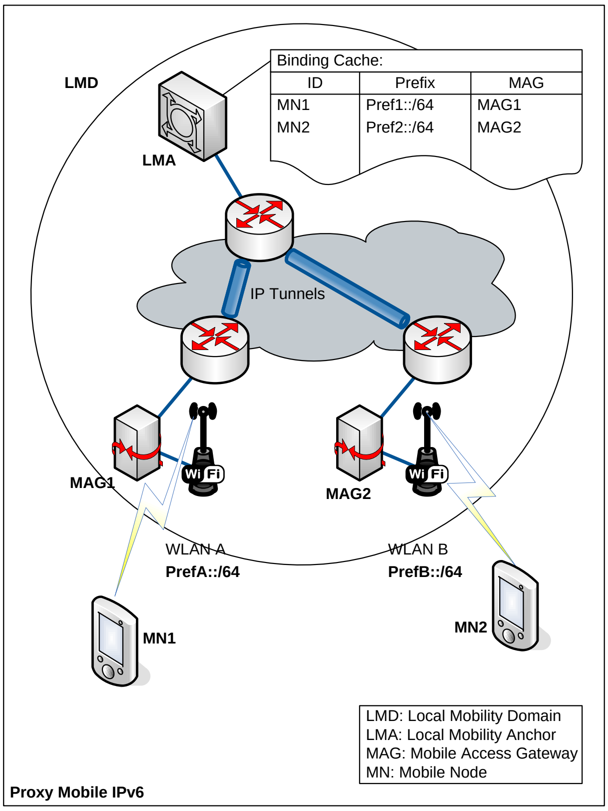

Figure 4-5: PMIP: All location information necessary to forward data packets are administrated in the network using the LMA and the MAGs.

Similar to the client based mobility this architecture has to be extended in order to implement the IFOM capabilities [12]: Moving selected flows from one access technology to another, and consequently, installing the required filters for flow routing. The corresponding working group in the IETF [15] has not finalized this project yet, however key concepts can already be read off.

In order to send and receive data packets from and to any of its interfaces, the IETF has decided to adapt the logical interface (LIF) [12]. This is a software entity which hides the physical interface to the IP layer (Figure 4-6). This means that the mobile IP stack binds its sessions to the LIF and has not to worry about the access technology to be used. So, for the UE there is only one single interface to the IP and its layers above.

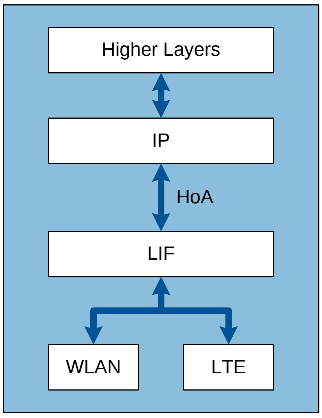

Figure 4-6: Logical Interface (LIF) to connect the IP layer with the physical interfaces.

The LIF controls the flow mobility in the UE. It is part of the connection manager in the operating system and has no impact on the IP stack. It represents a kind of virtual interface which hides all flow mobility movements to the higher layers.

A second aspect to introduce flow mobility to PMIPv6 consists in providing signaling extensions to the MAG. This is necessary because the MAG will only forward traffic from and to a UE if the prefix has been delegated to the UE by this MAG. However, in IP flow mobility, this delegation might have been done by a different MAG before the flow handover. Signaling between the LMA and the target MAG solves this issue.

4.2.2 GPRS Tunneling Protocol (GTP)

The GTP was developed by the 3GPP in order to carry packet service in GSM, UMTS and LTE networks and is used there on several interfaces. It was originally tailored for 3GPP networks only and can also be applied for access of different technologies. Like PMIP it provides network based IP mobility with session continuity, so the network takes care about changes in location or network access and does all the signaling so that the UE can communicate with the same IP address.

In GTP, control and user plane are carried over UDP [16] (Figure 4-7).

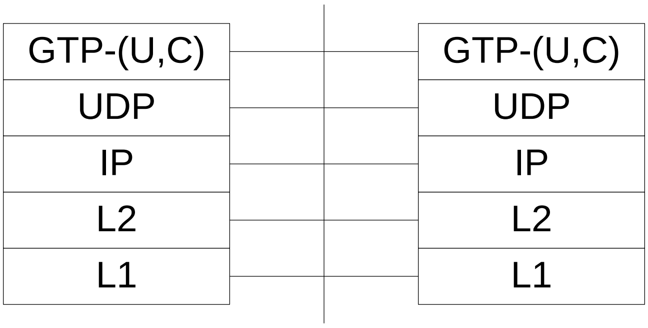

Figure 4-7: Protocol stack of a GTP tunnel

Tunnels are created between entities of interest in the network. For the case of WLAN offloading for example, data packets for a UE are first routed to the PDN-GW, and then routed through this tunnel to the peer in the WLAN network. The IP address of the PDN-GW remains the same, no matter to which peer the PDN-GW builds the GTP tunnel. This way, the same IP address is assigned to the UE, no matter in which network it is at the moment.

In contrast to PMIP, where a connection is based on a PDN and a UE, the GTP is based on a bearer, so several tunnels may be used in a connection. In addition, several bearers may be contained in a GTP tunnel and are then handled together. So, for a complete characterization of a GTP tunnel, the Tunnel Endpoint Identifiers (TEIDs) are needed in addition to their respective IP addresses in order to distinguish different tunnels between the same nodes [17].

Finally, note that like in PMIPv6, also the GTP solutions would rely on the above mentioned LIF concept [12]. It can be used there without any modifications.

4.3 Realization in the EPC

Network mobility is supported in the EPC with the approaches presented in the preceding sections. Historically, 3GPP has developed and specified the network based mobility protocol GTP. With LTE, also the PMIPv6 and the client based mobility according to [11] were introduced as an alternative. Note that if the client based IP Mobility is used, the interfaces S2c in Figure 3-1 and Figure 3-2 are used instead of S2a and S2b, respectively.

The HA or LMA in the 3GPP EPC are located in the PDN-GW for both, the trusted and the non-trusted access. This is in contrast to the location of the MAG: in the trusted access it is located in the WLAN network, in the non-trusted access in the ePDG. Consequently, the connection between the LMA and the MAG can always be regarded as trusted, because the ePDG is under control of the EPC network operator.

Up to Release 9, the offload shown in Figure 4-2 was the only way to offload data from the EPC to WLAN. For offload from 3G systems this feature is described in [18], and for offload from EPC it is described in [5]. IFOM was introduced with Release 10 for the client based mobility. It is still not available for the network based mobility, however, a study item for Release 12 is ongoing resulting in a technical report [19].

5 Network Discovery and Selection

Cellular networks and Wi-Fi hotspots have different deployment scenarios. While a UE is aware of neighboring cells, there is currently no similar mechanism for Wi-Fi where the access is opportunistic. These networks also do not have control over the access and protocol state of the other access network.

While the connection manager in the device can take care of discovery, prioritized selection of certain networks, traffic prioritization, and user authentication, there is not much consistency due to the proprietary solutions. This is where the two functions described in this chapter assist and allow the mobile network operators to provision the required policies.

5.1 Access Network Discovery and Selection Function

Many older wireless technologies are still maintained and new RATs are deployed in addition to them. This creates dense wireless environments with RATs which may be used to complement each other. Modern phones with multi-mode chipsets supporting several RATs can benefit from the intelligent control and prioritization thereof. The Access Network Discovery and Selection Function (ANDSF) allows the provisioning of policies to the UE for intersystem mobility and routing, as well as access network discovery. It offers a way for the network operators to dynamically control and define preferences how, where, when, and for what service a device can use a certain RAT. It can be used for both inter-technology as well as intra-technology access network selection.

5.1.1 Architecture

The ANDSF server is an entity in the EPC and communicates with the client (UE) over the S14 interface [5], which is realized above the IP level. Its role is to extend the Public Land Mobile Network (PLMN) selection and reselection procedures as specified in [20] and in [4], without influencing them. Figure 5-1 shows the architecture with the Home-ANDSF in the Home PLMN. For the roaming scenario, there is a Visited-ANDSF in the Visited PLMN, which takes precedence over the H-ANDSF. In any case, the ANDSF should not influence the PLMN selection and reselection procedures as specified in [20] and in [4].

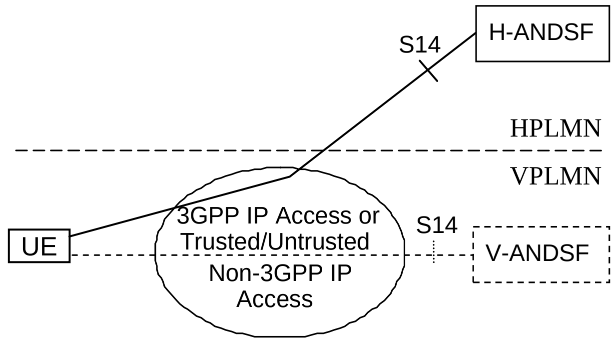

Figure 5-1: ANDSF (Roaming) Architecture

5.1.2 Information Exchange Procedure

There are two options for the ANDSF to exchange information with the UE: The ANDSF can push information, or the UE pulls it by querying the ANDSF server. If the UE submits an ANDSF pull query, it also can include further information in its request such as its location and the discovered radio access networks (RANs). Obviously, the home operator has then to ensure that ANDSF complies with national privacy requirements, because the location information is considered sensitive.

In both cases (push and pull), a secure connection, e.g. a PSK-TLS connection, is required. If such a secure connection does not exist and the ANDSF wants to push information to the UE, the server first sends an SMS with the information how the UE shall establish it. The preferred method here is the Generic Bootstrapping Architecture (GBA) Push Information defined in [21]. An alternative is the Open Mobile Alliance (OMA) Device Management (DM) bootstrap mechanism (OMA-ERELD-DM-V1_2) for the application layer authentication and an https tunnel for transport security.

The UE can request the information using a PSK-TLS secured connection based on the GBA method specified in [22]. To establish such a connection it needs the ANDSF server IP address. This can either be statically stored in the UE by the network operator, or alternatively discovered with a DHCP query or by a DNS lookup with the fully qualified domain name[3] of an ANDSF server as specified in the access control list (ACL). In the roaming scenario, both the H-ANDSF and the V-ANDSF addresses need to be known by the UE, refer to [23] for more detailed information.

5.1.3 Communication

The ANDSF information is communicated over the S14 interface using the OMA DM. With this device management specification, configure a UE with the parameters required by a particular network operator. These parameters are set with a Managed Object (MO) which contains the nodes *Policy*, *DiscoveryInformation*, *UE_Location*, *ISRP*, and *Ext*. Further interior nodes and leaves exist. The OMA DM is defined in XML.

[3] Andsf.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org

The logical structure of the ANDSF MO as specified in Rel. 10 to date is shown in Figure 5-2. The interior nodes are explained below.

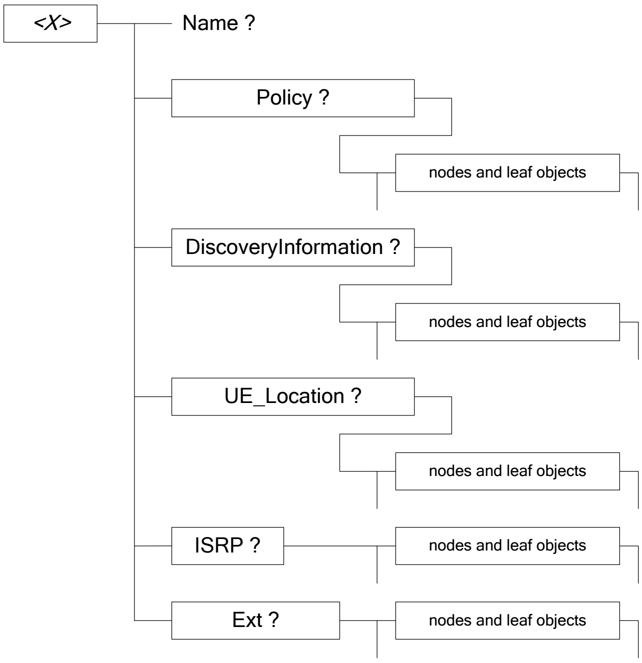

Figure 5-2: ANDSF MO Top Nodes

5.1.4 Nodes

Inter-System Mobility Policies (ISMPs) are provisioned with the policy node. It can contain a set of policies that shall be prioritized and at any time only one policy shall be active. Each policy contains rules for what access network it shall be valid, in which area, and at what time. The Update Policy node defines if the UE should request an update of the policies if there are no valid rules. An example of the policy node according to the Rel. 10 specification is shown in Figure 5-3.

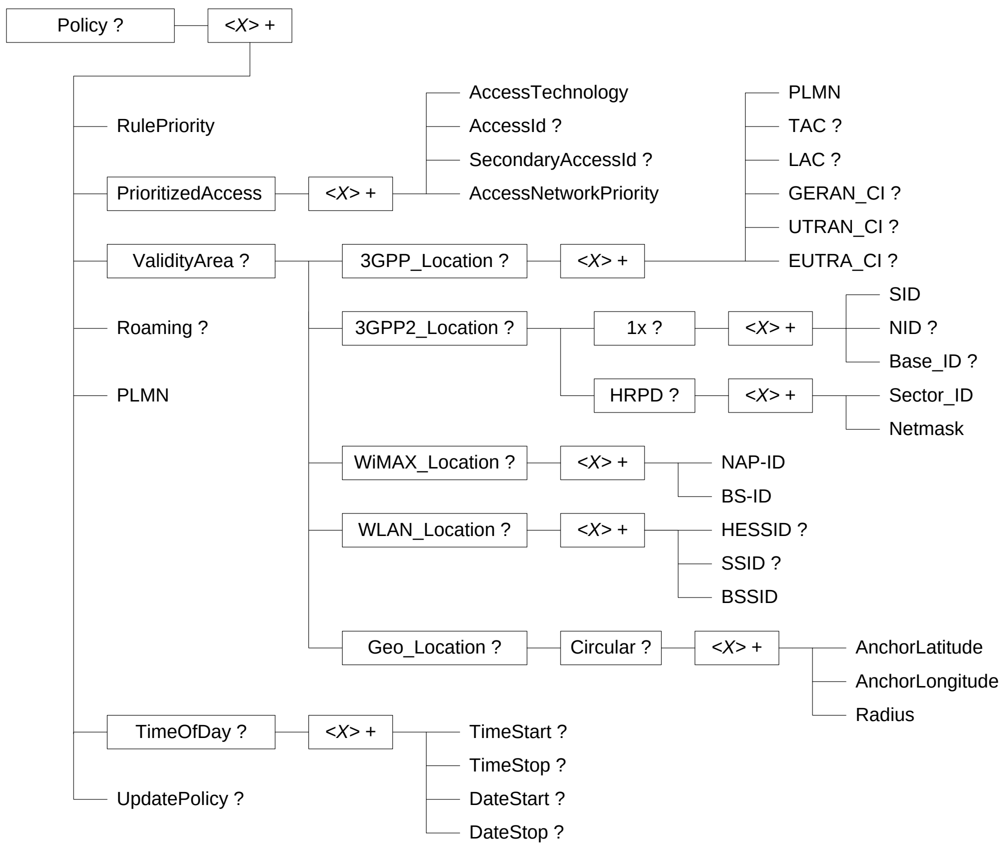

Figure 5-3: ANDSF MO Policy Node

If both policies (ISMP and ISRP) are available, in certain UEs the ISRP may take precedence for the routing of IP traffic. Refer to the specification [23] for details.

With the *Discovery Information Node* a network operator can define what radio access technologies are available at a certain location or in a certain area. The UE may use this information as a guidance for network discovery and detection.

The *Location Node* acts as a placeholder for the current location of the UE. If the position described in this node does not correspond to the real UE location, a trigger event in the UE may be used to update and fill in all information regarding the discovered access technologies.

If a UE is capable or configured for IFOM, Multiple-Access PDN Connectivity (MAPCON), or non-seamless WLAN offload, it can use the *Inter-System Routing Policy (ISRP)* rule. For each of these services, there is a container: „ForFlowBased“ for IFOM, „ForServiceBased“ for MAPCON, and „ForNonSeamlessOffload“ for non-seamless WLAN offload. Each of these containers can describe several flow distribution rules, routing criteria with conditions on where and when a rule applies, and the rule priority.

In order to allow vendor-specific policies and rules, an *Ext Node* has been defined. There are no further interior nodes or leafes defined in the specification.

5.2 Access Network Query Protocol (ANQP)

Before associating with a hotspot AP it is often helpful to obtain more information first. This allows an informed decision about which AP to associate with, and to query multiple networks in parallel. A device can even discover information about other APs that are not from the same provider but from one which has a roaming agreement.

5.2.1 Generic Advertisement Service (GAS)

In order to query information in an unassociated state, the IEEE 802.11u amendment adds the generic advertisement service (GAS) to the 802.11 standard. It uses individually addressed Public Action management frames that are already used for AP to unassociated-station communications, and Intra-BSS communication. GAS provides transparent layer 2 transport of information in generic containers. Available advertisement protocols are ANQP, Media Independent Handover (MIH) Information Service, MIH Command and Event Services Capability Discovery, and Emergency Alert System (EAS).

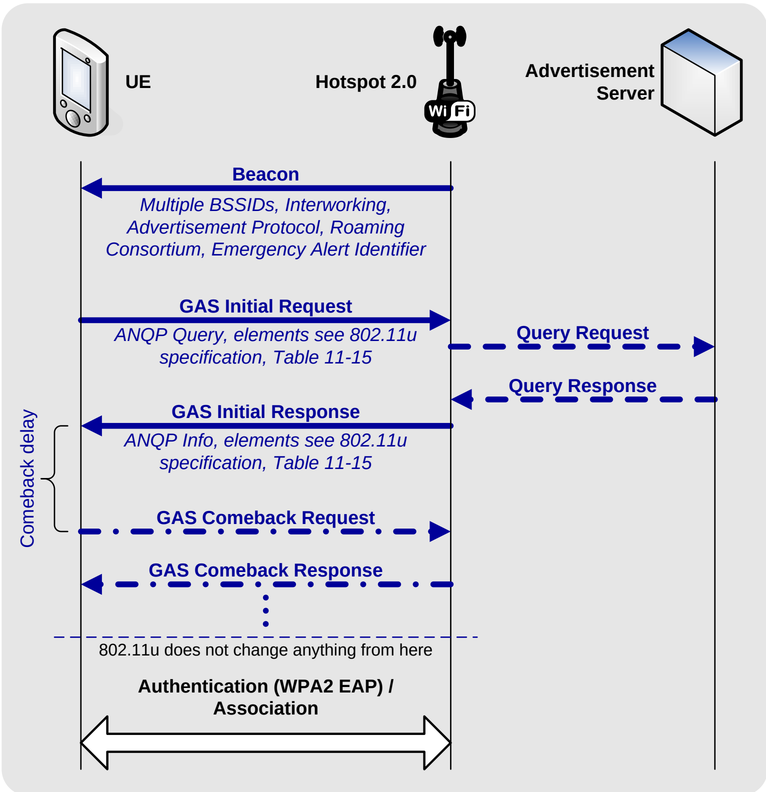

Figure 5-4: GAS Message Sequence

An example of a GAS information exchange is depicted in Figure 5-4. When a device detects the presence of the Interworking element in the beacon or probe response, it knows the AP supports GAS. The device then sends a GAS Initial Request frame to the AP, which may retrieve further information from an advertisement server. Within a certain time, the AP has to reply to the device with the GAS Initial Response. If the information exceeds the maximum data burst length (MMPDU length) and therefore does not fit entirely in the GAS Initial Response, or if the query response from the advertisement server arrives too late, the device shall send one or multiple GAS Comeback Requests after a certain comeback delay to retrieve the (remaining) information.

5.2.2 ANQP Information Elements

In order to exchange information in a standardized and secure way, the 802.11u specification defines a list with ANQP elements for communicating information before associating. The following table lists the available elements [7] with a short description. The first two are used to query information and all but the first element are used to indicate information in a response. While usually a device queries an AP and the AP responds back to the device, the first four elements can also be used to exchange information in any direction, even e.g. among APs.

ANQP Information Elements

Info Name	Type	Description
ANQP Capability list	Q *	List of information and capabilities that have been configured or are available on a device or AP.
ANQP vendor-specific list	Q, R *	Can be used to query information not defined in the standard.
TDLS Capability	Q, R *	May be used to discover TDLS capabilities of another STA.
ANQP Query list	R *	List with Info IDs of ANQP Response elements.
IP Address Type Availability information	R *	Information about the availability and the type of IP address that could be associated to the device after successful authentication, e.g. IPv4, IPv6, public, port-restricted, NATed.
Venue Name information	R	One or several venue name fields with an UTF-8 formatted string and a language code field.
Emergency Call Number information	R	List of emergency phone numbers that are used in the geographical area.
Network Authentication Type information	R	Supported authentication methods e.g. set of EAP methods, or http/https or DNS redirection, or if on-line enrollment is supported.
Roaming Consortium list	R	List with service providers where the AP could successfully authenticate a device with valid credentials.
NAI Realm list	R	List of NAIs of service providers accessible through this AP, optionally with EAP methods to be used for authentication.
3GPP Cellular Network information	R	Cellular information such as country code and network code to help a device selecting an AP to access 3GPP networks.
AP Geospatial Location	R	The AP's geospatial location as a Location Configuration Report.
AP Civic Location	R	A Location Civic Report.
The AP Location Public Identifier URI	R	URI where the device can retrieve more location information.
Domain Name list	R	One or more domain names of the AP and network operator.
Emergency Alert Identifier URI	R	URI for Emergency Alert System message retrieval.
Emergency NAI	R	NAI for devices that do not have valid credentials to authenticate to the network but have the intention to do so.
Neighbor Report	R	List with reports about neighboring APs for the benefit of STAs in a preassociated state.

Type:
Q ANQP Query
R ANQP Response
* May be transmitted/requested from both, an AP as well as a device

5.2.3 Example ANQP Procedure

A mobile device might detect one or several hotspot beacons. Using GAS it can query each hotspot AP with the discovered SSID. From the responses the device can learn the AP operator's domain names and Network Access Identifier (NAI) realm lists. By checking its stored credential list and their associated NAI realms, it can determine if it can successfully authenticate with one of these networks. In case there is more than one match, the operator policy for network selection is used. The device then authenticates to that network using the credentials that are indicated in the ANQP NAI Realm list.

For further examples and use cases, please refer to the Informative Annex V.2 of [7].

6 Summary

WLAN-Offload offers a new way to extend the capacity and coverage of an LTE network. WLAN networks are integrated to complement LTE networks and allow the use of each technology's advantages according to the actual demand. For example the WLAN is optimized for indoor and for crowded areas, whereas the LTE network is designed for complete coverage in all areas. Depending on the trust relationship the WLAN may be integrated as a trusted or a non-trusted access technology.

In the newest releases a paradigm change has occurred. Instead of a handover for the complete connection, single traffic flows are routed over one access technology while the remaining ones are routed over the other. This way the elaborated QoS feature in LTE may be used for delay or jitter sensitive data flows like voice or video conferences, whereas less time critical services may be routed over the cost-effective WLAN when available. Corresponding handover procedures for the partial offload of certain flows are controlled by the network operator to ensure best user experience.

In order to be accepted and provide the same ease of use as cellular technologies, also the security features are automated almost completely. The authentication is done using credentials of the USIM card and the same authentication validation as in LTE. From this follows that in the ideal case the user does not perceive the offload and only recognizes an enhanced data rate using the mobile services.

References

[1] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2011-2016." Cisco Systems Inc., Feb. 14, 2012. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf

[2] "Heterogeneous Networks: Meeting Mobile Broadband Expectations With Maximum Efficiency," Ericsson AB, February 2012. http://www.ericsson.com/res/docs/whitepapers/WP-Heterogeneous-Networks.pdf

[3] 3GPP TS 23.234 "3GPP system to Wireless Local Area Network (WLAN) interworking; System description"

[4] 3GPP TS 24.234 "3GPP System to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 3"

[5] 3GPP TS 23.402 "Architecture enhancements for non-3GPP accesses"

[6] 3GPP TS 23.261 "IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2"

[7] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11™-2012, 29 March 2012

[8] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 9: Interworking with External Networks, IEEE Std 802.11u™-2011, 25 February 2011

[9] IETF RFC 3748 "Extensible Authentication Protocol (EAP)"

[10] Wi-Fi Alliance®, "Launch of Wi-Fi CERTIFIED Passpoint™ Enables a New Era in Service Provider Wi-Fi®," AUSTIN, TX, June 26, 2012

[11] IETF RFC 5555 "Mobile IPv6 Support for Dual Stack Hosts and Routers"

[12] A. de la Oliva, C.H. Bernardos, M. Calderon: "IP Flow Mobility: Smart Traffic Offload for Future Wireless Networks", IEEE Communications Magazine, Oct. 2011

[13] IETF RFC 6089 "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support"

[14] IETF RFC 5213 "Proxy Mobile IPv6"

[15] C. J. Bernardos: "Proxy Mobile IPv6 Extensions to Support Flow Mobility", IETF draft, http://datatracker.ietf.org/wg/netext

[16] 3GPP TS 23.401 "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access"

[17] G. Punz: "Evolution of 3G Networks", Springer Wien New York, 2010.

[18] 3GPP TS 23.327 "Mobility between 3GPP-Wireless Local Area Network (WLAN) interworking and 3GPP systems"

[19] 3GPP TS 23.861 "Network based IP flow mobility"

[20] 3GPP TS 23.122 "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode"

[21] 3GPP TS 33.223 "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function"

[22] 3GPP TS 33.222 "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)"

[23] 3GPP TS 24.302 "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3"

Index

About Rohde & Schwarz

Rohde & Schwarz is an independent group of companies specializing in electronics. It is a leading supplier of solutions in the fields of test and measurement, broadcasting, radiomonitoring and radiolocation, as well as secure communications. Established more than 75 years ago, Rohde & Schwarz has a global presence and a dedicated service network in over 70 countries. Company headquarters are in Munich, Germany.

Regional contact

Europe, Africa, Middle East
+49 89 4129 12345
customersupport@rohde-schwarz.com

North America
1-888-TEST-RSA (1-888-837-8772)
customer.support@rsa.rohde-schwarz.com

Latin America
+1-410-910-7988
customersupport.la@rohde-schwarz.com

Asia/Pacific
+65 65 13 04 88
customersupport.asia@rohde-schwarz.com

China
+86-800-810-8228 /+86-400-650-5896
customersupport.china@rohde-schwarz.com

Environmental commitment

- Energy-efficient products
- Continuous improvement in environmental sustainability
- ISO 14001-certified environmental management system

Certified Quality System
ISO 9001

Rohde & Schwarz GmbH & Co. KG
Mühldorfstraße 15 | D - 81671 München
Phone + 49 89 4129 - 0 | Fax + 49 89 4129 – 13777

www.rohde-schwarz.com