

Operations and Management Area Working Group  
Internet-Draft  
Intended status: Informational  
Expires: January 4, 2018

B. Pularikkal  
Cisco Systems  
T. Pauly  
Apple Inc.  
M. Grayson  
S. Gundavelli  
Cisco Systems  
S. Touati  
Ericsson  
July 3, 2017

Carrier Wi-Fi Calling Deployment Considerations  
draft-pularikkal-opsawg-wifi-calling-03

## Abstract

Carrier Wi-Fi Calling is a solution that allows mobile operators to seamlessly offload mobile voice signaling and bearer traffic onto Wi-Fi access networks, which may or may not be managed by the mobile operators. Mobile data offload onto Wi-Fi access networks has already become very common, as Wi-Fi access has become more ubiquitous. However, the offload of mobile voice traffic onto Wi-Fi networks has become prevalent only in recent years. This was primarily driven by the native Wi-Fi Calling client support introduced by device vendors. The objective of this document is to provide a high level deployment reference to Mobile Operators and Wi-Fi Operators on Carrier Wi-Fi Calling.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 4, 2018.

## Internet-Draft Carrier Wi-Fi Calling Deployment Considerations July 2017

## Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terminology . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Architecture Overview . . . . .	<a href="#">6</a>
<a href="#">4.</a>	Wi-Fi Calling Deployment Considerations . . . . .	<a href="#">8</a>
<a href="#">4.1.</a>	Wi-Fi to Packet Core Integration . . . . .	<a href="#">8</a>
<a href="#">4.1.1.</a>	Untrusted Model . . . . .	<a href="#">8</a>
<a href="#">4.1.1.1.</a>	IPSec Tunnel Negotiation . . . . .	<a href="#">9</a>
<a href="#">4.1.2.</a>	Hybrid Model . . . . .	<a href="#">10</a>
<a href="#">4.1.3.</a>	Trusted Model . . . . .	<a href="#">11</a>
<a href="#">4.1.4.</a>	Model Selection Criteria . . . . .	<a href="#">13</a>
<a href="#">5.</a>	Subscriber Onboarding into Wi-Fi Access Network . . . . .	<a href="#">14</a>
<a href="#">5.1.</a>	Authentication and Identity Management . . . . .	<a href="#">14</a>
<a href="#">5.2.</a>	Hotspot 2.0 for Seamless Onboarding . . . . .	<a href="#">15</a>
5.2.1.	Hotspot 2.0 Inter-Operator Roaming for Wi-Fi Calling	17
<a href="#">6.</a>	Wi-Fi calling deployment in restrictive networks . . . . .	<a href="#">17</a>
<a href="#">7.</a>	RF Network Performance Optimization . . . . .	<a href="#">18</a>
<a href="#">7.1.</a>	Radio Resource Management . . . . .	<a href="#">18</a>
<a href="#">7.2.</a>	Wi-Fi Roaming Optimization . . . . .	<a href="#">19</a>
<a href="#">7.2.1.</a>	Fast BSS Transition . . . . .	<a href="#">19</a>
<a href="#">7.2.2.</a>	802.11k based Neighbor Reports . . . . .	<a href="#">19</a>
<a href="#">7.2.3.</a>	802.11v based Assisted Roaming and Load Balancing . .	<a href="#">20</a>
<a href="#">8.</a>	QoS Deployment Considerations for Wi-Fi Calling . . . . .	<a href="#">20</a>
<a href="#">8.1.</a>	Wi-Fi Access Network QoS . . . . .	<a href="#">20</a>
<a href="#">8.2.</a>	End to End QoS . . . . .	<a href="#">21</a>
<a href="#">9.</a>	Wi-Fi Calling Client Considerations . . . . .	<a href="#">23</a>
<a href="#">9.1.</a>	Access Selection Criteria . . . . .	<a href="#">23</a>

<a href="#">9.2.</a>	Inter-RAT Handover . . . . .	<a href="#">24</a>
<a href="#">9.3.</a>	MTU Considerations . . . . .	<a href="#">24</a>
<a href="#">9.4.</a>	Congestion Management . . . . .	<a href="#">24</a>
<a href="#">9.5.</a>	NAT Traversal . . . . .	<a href="#">25</a>
<a href="#">10.</a>	Acknowledgements . . . . .	<a href="#">25</a>

<a href="#">11.</a>	Informative References . . . . .	<a href="#">25</a>
	Authors' Addresses . . . . .	<a href="#">26</a>

## [1.](#) Introduction

There are several SP Managed and Over the Top Voice Solutions deployed today which can leverage Wi-Fi access networks. Some of these solutions rely on standalone applications installed on the Mobile Handset and other Mobile devices such as tablets. Also there are solutions, which leverage dedicated hardware built exclusively to support Voice over Wi-Fi.e.g,in enterprise type environments. The scope of this document is VoWiFi solutions, which are deployed by Mobile Network Operators also known as Wireless Carriers. VoWiFi from the context of Mobile Voice offload is often referred to as Carrier Wi-Fi Calling. The deployment of Carrier Wi-Fi Calling requires some kind of integration between the Wi-Fi Access network and Mobile Packet Core. Carrier Wi-Fi calling solutions deployed today predominantly uses an 'untrusted Wi-Fi' model that delivers simple IP connectivity to facilitate Mobile Packet Core integration. With this 'untrusted' approach, Mobile Operators are able to make use of the existing Wi-Fi deployment footprint regardless of whether it is owned by the MNOs or by their roaming partners or Wi-Fi Operators without any kind of partnership with the MNOs. This model has definitely allowed MNOs to accelerate the adoption of Wi-Fi calling. However, this comes with some caveats, as depending on the Wi-Fi network, there may be no visibility or control over it by the MNO, impacting its ability to carry voice calls without compromising end user experience.

It is in the interest of both MNOs as well as Wi-Fi Operators to improve the quality of experience for Wi-Fi Calling delivered over a Wi-Fi access network. MNOs have the incentive to make sure that the end user experience does not get compromised while the voice service is offloaded over Wi-Fi access. Wi-Fi operators have the business incentive to enter into roaming partnerships with the MNOs and support Wi-Fi calling with certain Service Level Agreements. In some

deployments, it is possible for the MNOs to own some Wi-Fi hotspot deployments. In such cases, MNO will effectively be the Wi-Fi operator as well.

Objective of this document is to provide a Carrier Wi-Fi Calling deployment reference to Wi-Fi Operators and MNOs with primary focus on the Wi-Fi Access Network and the Wi-Fi to Packet Core integration aspects.

## [2.](#) Terminology

### Service Provider (SP)

Refers to a provider of telecommunications services such as Broadband Operator or Mobile Operator. An SP may provide several telecommunications services.

### APP

Refers to computer program typically designed to run on Mobile devices such as smartphones and tablets.

### Wireless Fidelity (Wi-Fi)

Technology that allows devices to wirelessly connect using 2.4 GHz and 5.0 GHz unlicensed radio bands. Wi-Fi is defined as part of IEEE 802.11 standards

### Voice over Wi-Fi (VoWiFi)

Any solution, which supports voice services over Wi-Fi.

### Mobile Network Operator (MNO)

A wireless communications service provider who owns and operates licensed wireless access network and the backend infrastructure to offer mobile voice, data and multimedia services.

### 3rd Generation Partnership Project (3GPP)

3GPP unites seven telecommunications standards development organizations known as Organizational Partners and provides their members with a stable environment to produce the reports and specifications that define 3GPP technologies

### Global System for Mobile Association (GSMA)

GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors.

### User Equipment (UE)

Term represents any device used directly by an end user to communicate.

### Internet-Draft Carrier Wi-Fi Calling Deployment Considerations July 2017

#### Wireless Local Area Network (WLAN)

Refers to IEEE 802.11 based Wi-Fi access networks and represents an extended service set consisting of multiple access points.

#### Long Term Evolution (LTE)

Is the fourth generation 3GPP standard set for wireless communication of mobile devices in end-to-end IP environment.

#### Evolved Packet Core (EPC)

Represents the Core Network in the 3GPP LTE system Architecture.

#### Packet Data Network (PDN)

PDN represents a network in the packet core a Mobile UE device wants to communicate with. PDN generally is mapped to a set of related services.

#### Access Point Name (APN)

APN represents a set of services available to a specific PDN. Typically UE devices will be configured to access multiple APNs corresponding various services in the packet core.

#### Trusted WLAN Access Gateway (TWAG)

Performs the gateway function between a trusted WLAN access network and packet core. It acts as the default gateway and DHCP Server for UE devices connected to the WLAN access network for trusted Wi-Fi to packet core integration model.

#### Evolved Packet Data Gateway (ePDG)

ePDG performs the gateway function between WLAN access network and Mobile Packet core in an untrusted model. Main function of ePDG is to secure the data transmission with a UE connected to the EPC.

#### PDN Gateway (P-GW)

P-GW is the subscriber session anchor in EPC. It enforces policy and also has a role in IP persistence in roaming scenarios. Based up on the policy, P-GW steers traffic towards various PDN networks corresponding to various APNs.

#### IP Multi-Media Subsystem (IMS)

#### Internet-Draft Carrier Wi-Fi Calling Deployment Considerations July 2017

An Architectural framework for delivering IP multimedia services. And is defined in 3GPP

#### Policy and Charging Rule Function (PCRF)

A system in EPC, which detects service data flows, applies policies and QoS to subscriber flows to and supports flow based charging

#### Session Initiation Protocol (SIP)

SIP is an application layer control protocol that can establish, modify and terminate multimedia sessions or calls.

#### Real-time Transport Protocol (RTP)

RTP is a transport protocol, which provides end-to-end delivery services for data with real-time characteristics such as interactive audio and video.

#### Proxy Mobile IPv6 (PMIPv6)

PMIPv6 is a network based mobility management protocol standardized by IETF and adopted in 3GPP.

#### GPRS Tunneling Protocol (GTP)

Group of IP based communications protocols used in 3GPP architectures.

#### S2a Interface

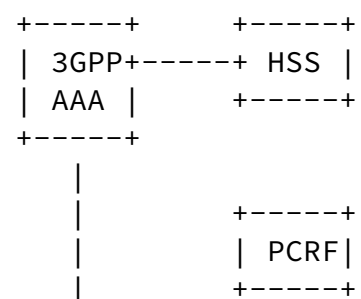
Is the interface between TWAG and P-GW and can be either GTP or PMIPv6 based

#### S2b Interface

Interface between ePDG and P-GW and can be either GTP or PMIPv6

### [3.](#) Architecture Overview

This section provides a very high level overview of the end-to-end Architecture for Carrier Wi-Fi Calling. It is outside the scope of this document to provide a detailed Architecture description, as all the functional entities and the protocol interfaces are well defined in the 3GPP and GSMA specifications [3GPPTS23.402,GSMAIR61,GSMAIR51]. Figure-01 below is used to describe the Architecture components at a high level.



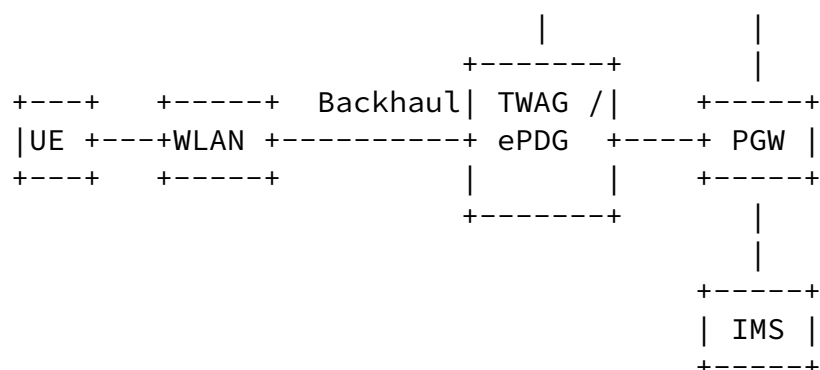


Figure 1: High Level Architecture

The UE is the end user device such as a smartphone running native Wi-Fi Calling client. The UE is connected to a Wi-Fi access network, which is represented by the block WLAN in the diagram. Depending up on the trust model, TWAG or ePDG gateway is used to integrate the WLAN access network to the MNO packet core. More details around this untrusted and trusted approaches are covered in the next section. The P-GW acts as the common anchor for the subscriber sessions regardless of whether the UE is connected to Wi-Fi or LTE (not shown), allowing the preservation of the IP Session during a handover between LTE and Wi-Fi. IMS provides several functions related to SIP based call control signaling, namely SIP authentication, basic telephony services, supplementary services, interworking with other IMS systems, and offload into circuit switched voice networks. In addition to voice, the same IMS infrastructure may be leveraged for other multi-media functions such as video calling. The IMS framework consists of several functional entities and is omitted for the sake of simplicity here. PCRF performs classical Policy and Charging Rule functions in the Mobile Packet Core. For the Wi-Fi calling solution, it will trigger the establishment of the default and dedicated bearers on the S2a or S2b interfaces for SIP and RTP traffic between the PGW and the TWAG/ePDG.



This section covers deployment considerations for an end-to-end Wi-Fi calling Architecture that can influence the quality of experience, availability and monetization aspects of the solution offering.

#### [4.1.](#) Wi-Fi to Packet Core Integration

There are three different Architecture options available for Wi-Fi to Packet Core integration for the deployment of Wi-Fi calling. Each of these models are described in the sub-sections below:

##### [4.1.1.](#) Untrusted Model

This model is built around the assumption that the Wi-Fi access network is 'unmanaged' or untrusted from the MNOs perspective. Since this model does not rely on any security or data privacy implementations on the Wi-Fi access network, it requires the establishment of an IPSec tunnel between the UE device and the Mobile Packet Core. The ePDG gateway acts as the IPSec tunnel termination point on the packet core side. The ePDG handles the user authentication as well as the establishment of an S2b packet data network connection towards the P-GW using the GTP based S2b interface. This Architecture model is illustrated in figure-2 below.

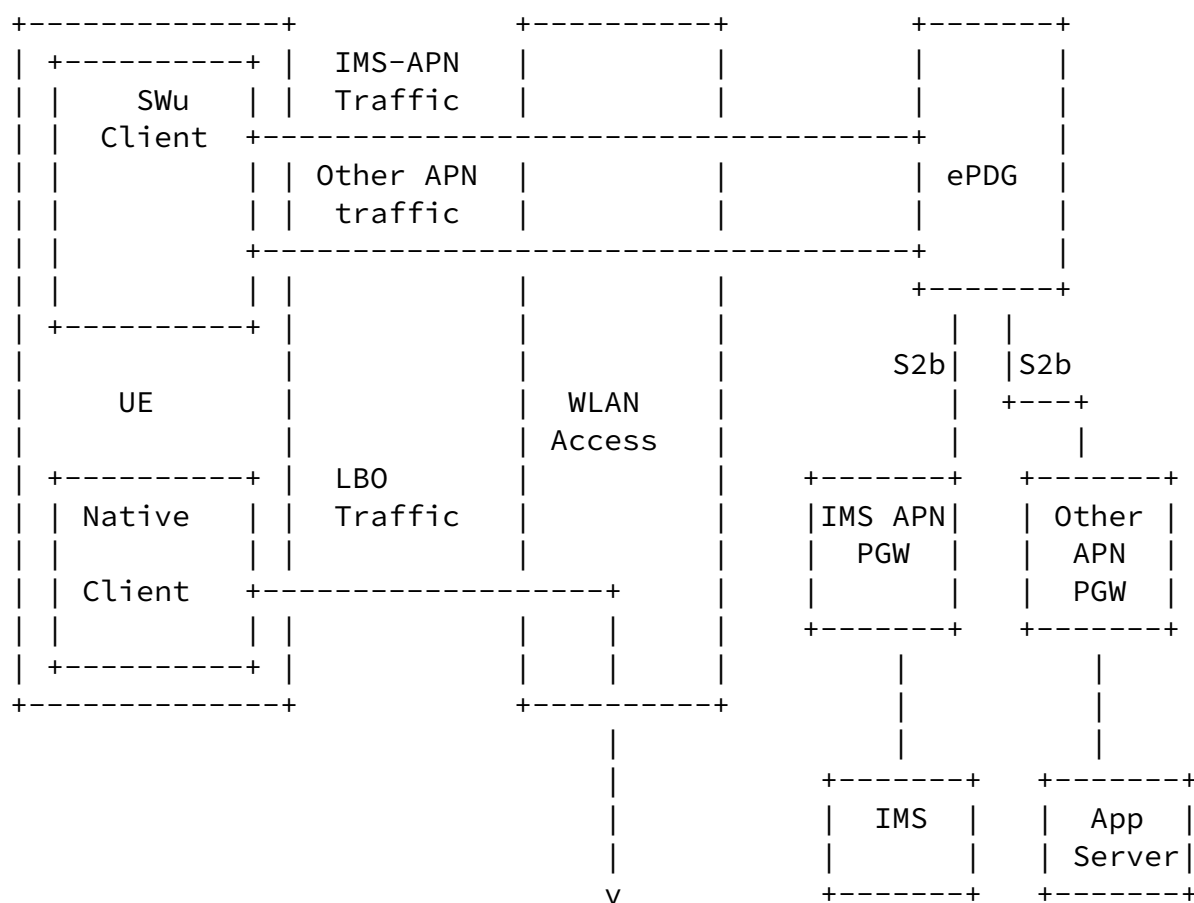


Figure 2: Untrusted Wi-Fi to Packet Core Integration Model for Wi-Fi Calling

The Wi-Fi calling client implementation uses the ePDG client for IMS APN while the default PDN or Internet APN traffic is locally offloaded (Local Breakout LBO) into the Wi-Fi access network. The "untrusted Wi-Fi" architecture supports multiple APN over SWu, allowing the MNO to also route specific applications traffic associated with one or more APN through the Packet Core, in addition to the IMS APN, if required.

#### [4.1.1.1. IPSec Tunnel Negotiation](#)

The IPSec tunnel from the UE to the ePDG is negotiated using IKEv2. The parameters for tunnel negotiation in Wi-Fi Calling are as follows:

- o The Initiator Identifier (IDi) will be in ID\_RFC822\_ADDR (email

address) form, and be based on the UE's IMSI@Realm.

## Internet-Draft Carrier Wi-Fi Calling Deployment Considerations July 2017

- o The Responder Identifier (IDr) will be in ID\_FQDN form, and be the APN name that the tunnel should access through the ePDG.
- o EAP should be used for mutual authentication. When on a device with a SIM card, EAP-AKA should be used. On other devices, EAP-TLS is preferred. EAP-Only authentication (in which the server certificate is not sent in an CERT payload) may be used to reduce packet size, but only with mutually authenticating EAP types such as EAP-AKA or EAP-TLS.
- o Strong encryption and authentication algorithms should be used, such as ENCR\_AES\_CBC, PRF\_HMAC\_SHA2\_256, AUTH\_HMAC\_SHA2\_256\_128, and Diffie-Hellman Group 14.
- o The Configuration Request should specify an IPv4 or IPv6 addresses used for handover. The UE may also request ePDG-specific attributes such as P\_CSCF\_IP4\_ADDRESS and P\_CSCF\_IP6\_ADDRESS.

### [4.1.2.](#) Hybrid Model

3GPP TS 23.402 also defines the concept of "trusted Wi-Fi" architecture, providing another method to integrate with the packet core. The trustworthiness of an access network itself is left to the MNO to decide, but it generally relies on some level of control by the MNO of the Wi-Fi access network either in a direct or indirect manner. One of the key characteristics of the "Trusted Wi-Fi" architecture as defined in 3GPP Release 11, is the client-less approach to support the packet core integration. This solution lacked the support for multiple APNs signaling for the UE when over the Wi-Fi access network, therefore all Wi-Fi offloaded traffic was assumed to be part of the default PDN or Internet APN. With this limitation, Wi-Fi calling cannot be supported as it require its own IMS APN. The hybrid architecture proposed here combines the 3GPP release 11 "trusted Wi-Fi" architecture, with the ePDG based untrusted Wi-Fi architecture. This hybrid model simultaneously supports IMS and other applications specific APNs using the untrusted Wi-Fi model, with the TWAG selectively offloading their traffic, while using the S2a interface for all other default PDN traffic toward the default PGW. This Architecture model is illustrated in

figure 3 below

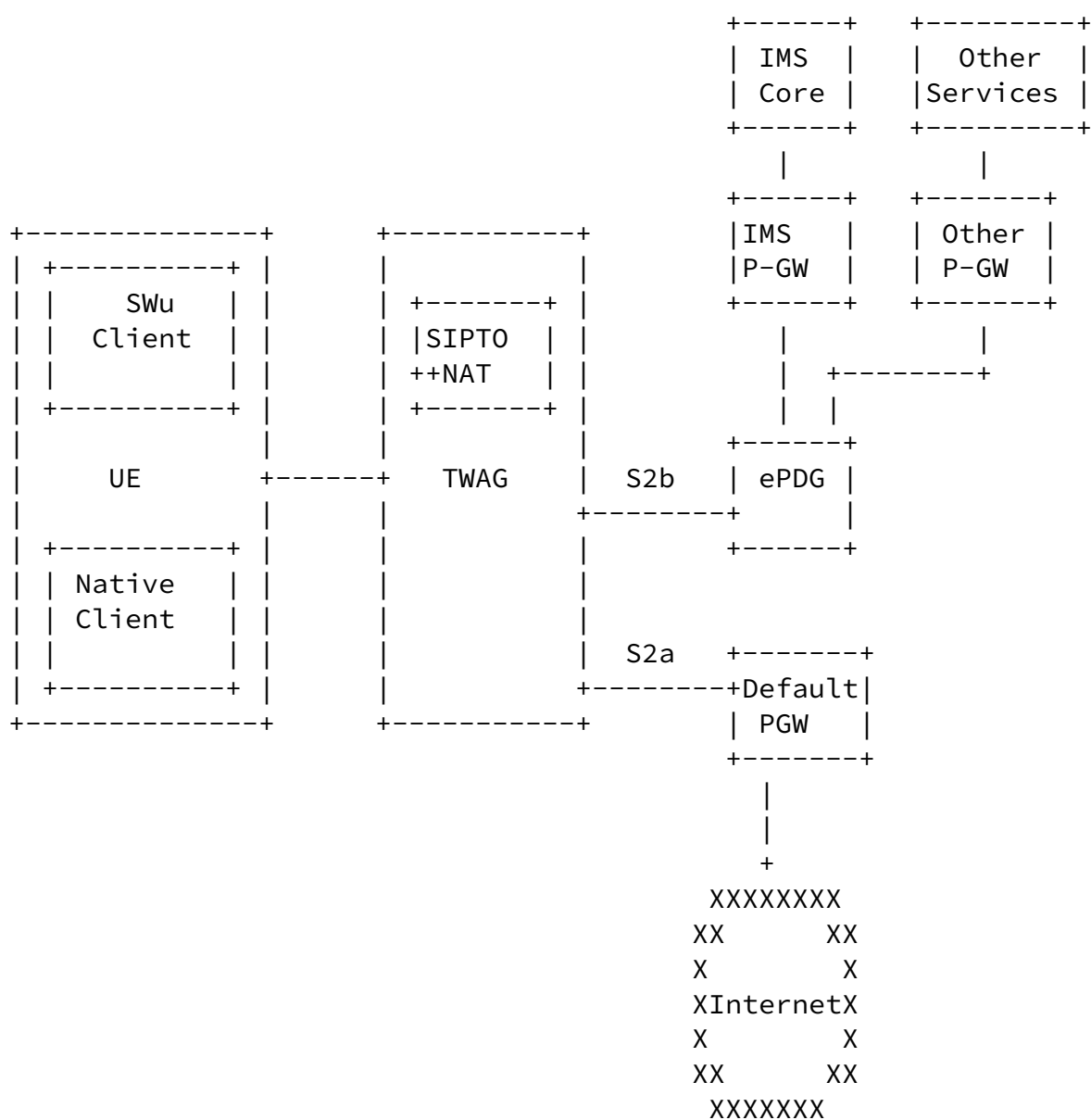
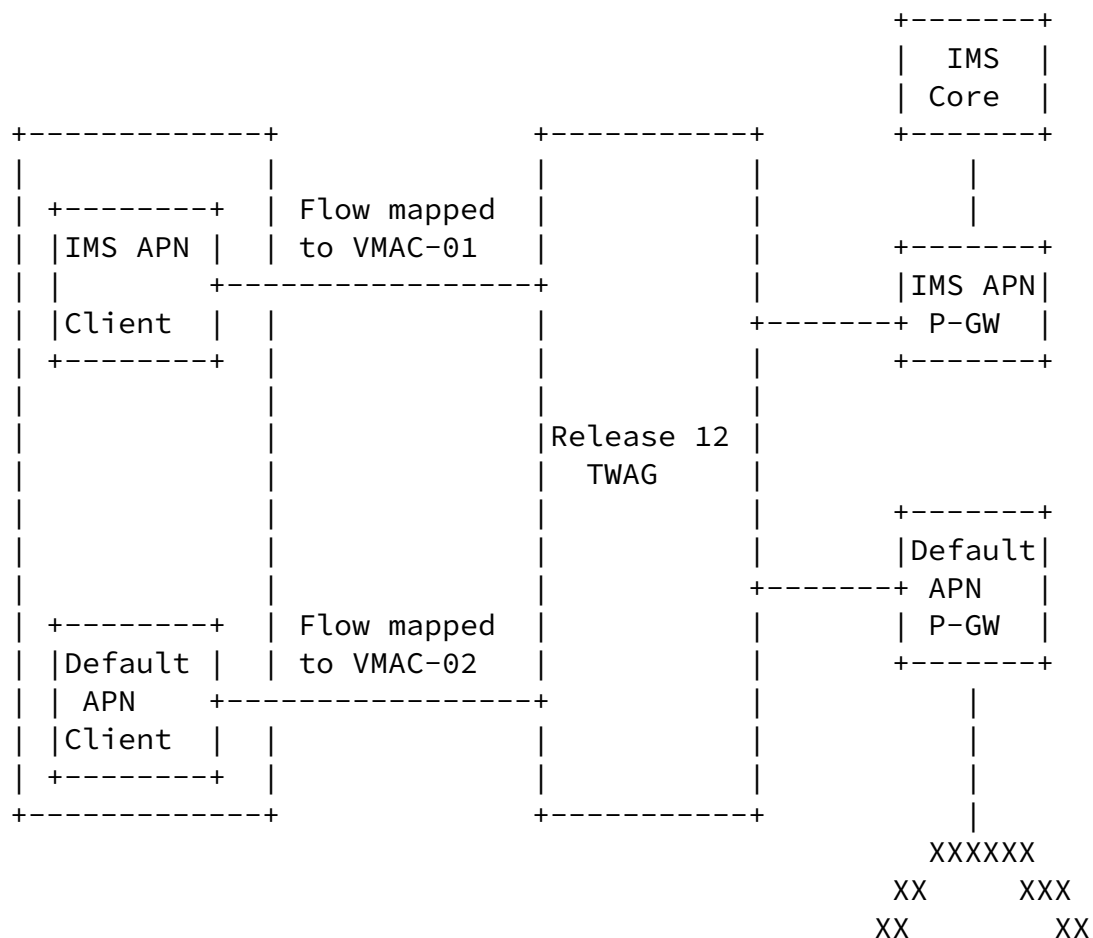


Figure 3: Hybrid Wi-Fi to Packet Core integration model for Wi-Fi calling

#### 4.1.3. Trusted Model

Enhancements introduced in 3GPP release 12 SaM0G specifications provides the ability to support multiple APN over Wi-Fi access making the support of Wi-Fi calling, and other applications specific APNs possible without the need for IPSec connectivity between the UE and the Packet core. This Architecture model is illustrated in figure 4 below



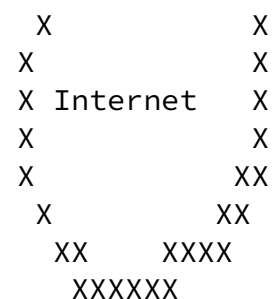


Figure 4: Trusted Wi-Fi to Packet Core integration model for Wi-Fi calling

#### [4.1.4.](#) Model Selection Criteria

Each of the Wi-Fi to Packet Core Architecture models described in the previous sections comes with its own pros and cons. And selection of a specific architecture model depends on several factors. Some of these factors, which can help determine the appropriate model, are listed below:

**\*Wi-Fi Access Network Ownership:** There are several ownership models available when it comes to Wi-Fi to packet core integration. Wi-Fi Access network may be deployed by the MNO to leverage as another RAT to complement 3G and LTE. Alternatively the Mobile Network Operator may deploy a Managed Wi-Fi network for the Enterprise and SMB customers. The MNO managed Wi-Fi footprint is only portion of the overall Wi-Fi deployment. Third parties such as broadband service providers today own a significant portion of the Wi-Fi access network. For third party owned Wi-Fi access, the Mobile Network Operator may or may not have a direct roaming partnership with the

Wi-Fi operator. The ownership model influences the choice of packet core integration architecture.

\*Backhaul Network Ownership: From the context of this discussion here, the backhaul refers to the connectivity between WLAN Access network and the Packet core. It consists of a combination of wired access network of the hotspot, Broadband access last mile, Wi-Fi operator core network, Internet etc. These connectivity aspects will be deciding factor for the choice of Wi-Fi packet integration model. For example, Wi-Fi access network may be owned and or operated by the MNO, but if the backhaul involved a third party connection or Internet where MNO does not have control over security and QoS, an untrusted packet core integration may be the viable solution.

\*Mobile Offload Requirements: Choice of the Wi-Fi to packet core integration model is not only influenced by voice offload but data offload as well. The untrusted Wi-Fi and the hybrid architectures do support a flexible offload model, allowing the Mobile Network Operator to choose which traffic to backhaul to the Mobile Packet Core to provide charging and added value services, while also leveraging local breakout capabilities on the device. Using the untrusted, and when applicable, the hybrid models allow the Mobile Network Operator to leverage their deployed network architecture for Wi-Fi calling. This makes both the hybrid and the untrusted Wi-Fi architectures valid options to consider depending on the Wi-Fi network ownership requirements.

\*Device Capabilities: This greatly influences the choice of Wi-Fi to packet core integration. For example, a trusted approach with multiple PDN support requires the capability on the device to comply

with 3GPP release 12 SaMOC enhancements, while the untrusted or hybrid model can leverage existing implementations and do provide a similar level of functionality.

\*Support of Non-SIM devices: The MNO can provide value-added services, including voice services on Non-SIM devices. The Untrusted Wi-Fi architecture is compatible with Non-SIM devices and provide the same capabilities to these devices as for the SIM devices.

\*Network Readiness: This is another influencing factor for the choice of the trust model, as there are dependencies on the Packet Core

network elements as well as Wi-Fi access network for the implementation of these models.

## 5. Subscriber Onboarding into Wi-Fi Access Network

Subscriber onboarding into a Wi-Fi access network is the process of getting connected to a WLAN access network and be able to offload mobile traffic successfully. In order to provide a seamless end user experience for Wi-Fi calling, the handset should be able to get connected to the WLAN with minimum or no user interaction. A seamless WLAN onboarding is critical for the smooth hand off of the voice call from LTE to Wi-Fi. There are several factors, which can influence the Wi-Fi onboarding experience. Proper choice of the available deployment options can ensure the subscriber onboarding experience is quite seamless.

### 5.1. Authentication and Identity Management

Before the UE device can successfully get associated with a WLAN access network it needs to get authenticated with the WLAN network. There are several types of user authentication options in use such as Web Portal based authentication, EAP-TTLS, EAP-TLS, EAP-SIM, EAP-AKA etc. Choice of the authentication mechanism depends up on the deployment preferences of the Wi-Fi operator. Web portal based authentication relies on an Open SSID configuration. Once the portal has successfully authenticated the UE device, the traffic is carried over the WLAN air interface without any encryption. EAP authentication mechanisms relies on secured SSIDs mandate the 802.11i based air encryption of the subscriber data in the WLAN access network.

In order to support Wi-Fi calling, one of the EAP based mechanisms will be preferred over the web portal based authentication. In the case of Web based authentication, the user needs to manually enter the username and password credentials or in some cases sign up for a service via Operator portal. But with any of the EAP methods, once the credentials have been established on the UE device, then

authentication happens automatically without user intervention and greatly improves the onboarding experience.

If the Wi-Fi operator decides to use a secured SSID for subscriber



authentication, choice of the EAP method depends up on the business model. A Standalone Wi-Fi operator may need to rely on non-SIM based EAP authentication mechanisms such as EAP-TTLS or EAP-TLS for their home subscribers. A Wi-Fi operator who has a roaming partnership with an MNO could allow the uSIM credentials of the MNO subscriber to be used for the access. In this case, the Wi-Fi operator will act as a proxy and authenticate the customer credentials with the MNO HSS.

Identity management deals with establishing subscriber identity and associated credentials on the UE device for WLAN onboarding. Identity management and authentication goes hand in hand. Option leverages the same set of identity and credentials (unified identity) for WLAN onboarding and packet core connectivity will simplify the identity management for Wi-Fi calling. However this requires that the WLAN access network is either owned by the MNO or by their roaming partner. With unified identity, typically uSIM credentials will be leveraged for both WLAN onboarding as well as packet core connectivity for SIM devices, and an EAP method used for Non-SIM devices.

## [5.2.](#) Hotspot 2.0 for Seamless Onboarding

Ability for a handset to Seamlessly get connected to WLAN access network is one of the key factors which will influence the overall subscriber experience with Wi-Fi calling. Passpoint specifications defined by the Wi-Fi alliance under the Hotspot 2.0 program supports automatic discovery, selection and onboarding of Wi-Fi clients on to a compatible Wi-Fi access network. Figure-5 below is used to illustrate the hotspot 2.0 solution at a high level:



discovery of WLAN network resources by the UE device. ANQP server is

Internet-Draft Carrier Wi-Fi Calling Deployment Considerations July 2017

typically collocated on the Access Point (AP) or the Access Controller (AC). A Hotspot 2.0 compatible UE device will have a built in ANQP client. When a UE roams into the coverage area of a Hotspot 2.0 enabled network, it automatically learns about the network capability via Beacon or Probe Response. Then UE requests a set of network and service level information from the WLAN network. Based up on the info UE can decide which WLAN access is the most preferred and the type credentials it can use for getting connected.

#### [5.2.1.](#) Hotspot 2.0 Inter-Operator Roaming for Wi-Fi Calling

MNOs can enter into roaming partnership, which will allow Wi-Fi calling clients to automatically get connected to the WLAN access. This also allows the devices to leverage uSIM credentials or EAP credentials for Non-SIM devices for getting authenticated with the WLAN network. The Wi-Fi operator AAA will function as a proxy in this case and completes the authentication by interfacing with the MNO AAA Server and HSS, for EAP\_SIM/EAP\_AKA in the MNO packet core.

### [6.](#) Wi-Fi calling deployment in restrictive networks

The use of IPSec to establish a connection to the ePDG, require that the access network allow IPSec tunnel establishment. But some networks won't allow IPSec traffic either as a security policy or as a side-effect of only allowing "web traffic". In addition, many mainly corporate environments do deploy an HTTP proxy which will also prevent the establishment of an IPSec tunnel. Performing changes to these deployments may not always be possible or cost effective for the corporation or the public venues, especially in an "Untrusted Wi-Fi" model without the MNO involvement. In such situations, the mobile device can leverage the IPSec TCP encapsulation as described in [draft-paulu-ipsecme-tcp-encaps-04](#) and in 3GPP TS 24302, which define the encapsulation of IPsec traffic in TCP. The Mobile device shall enable the TCP encapsulation only after failing to establish an IPSec connection to the ePDG. Figure 6 below shows the TCP encapsulation with the use for TLS to traverse a Proxy and reach the ePDG.

Internet-Draft Carrier Wi-Fi Calling Deployment Considerations July 2017

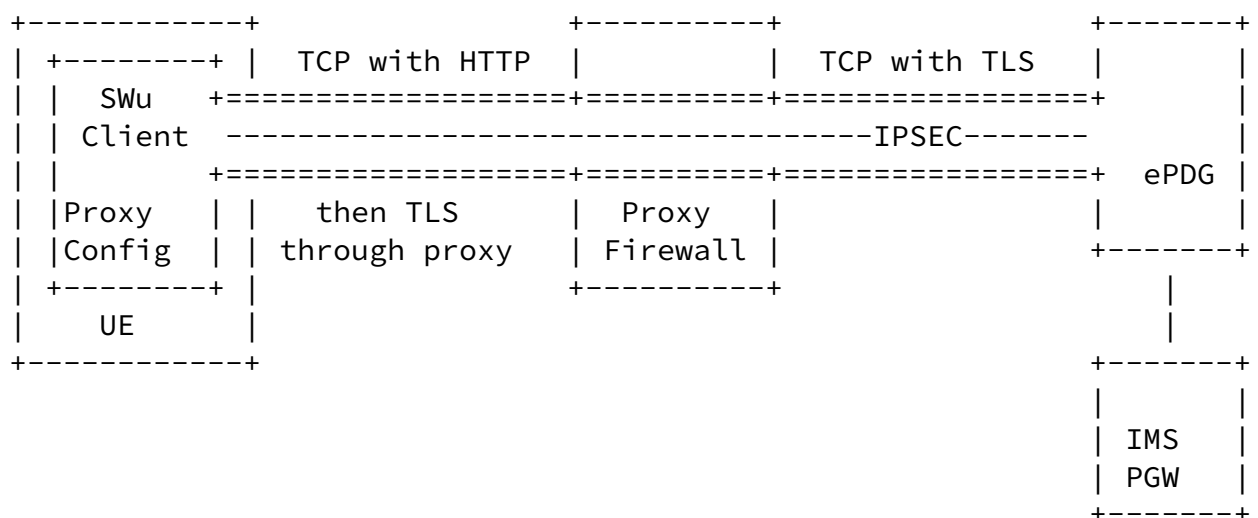


Figure 6: Use of TCP encapsulation for IPsec

When an HTTP proxy is deployed, the UE should connect to the eDPG through the proxy and then establish a TLS connection toward the eDPG. TLS is not used for securing the link, but to traverse the HTTP Proxy, and is configured with NULL-Cipher. This model allows Wi-Fi calling to operate even in restrictive networks.

## 7. RF Network Performance Optimization

Quality of the Wi-Fi calling experience would be as good or as bad as Radio network itself. Three network performance KPIs which impact the quality of voice are latency, jitter and packet drops. A healthy network is critical to ensure that these KPIs will meet the thresholds allowed to meet the acceptable voice quality. This section primarily talks about various performance optimization mechanisms available on the Wi-Fi Radio network.

## [7.1.](#) Radio Resource Management

Radio Resource Management (RRM) aka Wi-Fi SON refers to the co-ordinated fine-tuning of the various RF network parameters among access points connected in a Wi-Fi network. It is very typical for Wi-Fi deployments from multiple operators to co-exist in the same hotspot. Scope RF fine tuning will be limited to the access points which are managed by the same operator in a specific hotspot. RRM fine-tuning will be typically performed by a centralized entity such as Access Controller. Some deployments which may not leverage AC such as Residential Gateways could leverage a cloud based RRM or SON Server. RRM controller continuously analyze the existing RF environment automatically adjust the power and channel configurations of access points to help mitigate issues such as co-channel interference and signal coverage. A proper implementation of RRM can greatly

Pularikkal, et al.

Expires January 4, 2018

[Page 18]

---

Internet-Draft Carrier Wi-Fi Calling Deployment Considerations July 2017

influence the RF performance and will have a positive impact on network KPIs that influence the Wi-Fi calling experience.

## [7.2.](#) Wi-Fi Roaming Optimization

Roaming from the context of the discussion here refers to the hand off of a UE device from one Access Point to another Access Point in the same Extended Services Set (ESS) or mobility domain. Unlike cellular roaming between base stations, which is initiated by the network, in Wi-Fi the roaming is initiated by the UE device. A UE typically decides to disconnect from the current access point when some of the RF measurements such as RSSI, SNR etc. drops below certain threshold. There are other APs in the range with acceptable measurements the UE will start re-association process with one of the target APs. End user experience for a Wi-Fi call, which is active at the time of the hand off, will depend up on multiple factors. One critical factor is the time taken for the UE traffic to resume during the hand off. Also it is important that UE is able to make the optimum selection of the target AP from the list of available APs in the range. Discussed below are few IEEE 802.11 based mechanisms available to optimize the roaming.

### [7.2.1.](#) Fast BSS Transition

IEEE 802.11r based fast BSS transition (FT) helps reduce the handoff time for a UE when it roams from one AP to another within an ESS,

which is enabled, with an EAP based authentication. Without FT, the UE will have to go through the full authentication process with the RADIUS server and device fresh set of encryption for 802.11i air encryption. When FT is enabled, the client will have an initial handshake with the target AP while still connected to the original AP. This handshake allows client and target APs to derive the encryption keys in advance to reduce the hand off time. Fast Transition can significantly improve the end user experience for the voice calls, which are active during a hand off.

#### 7.2.2. 802.11k based Neighbor Reports

IEEE 802.11k enhancements allow a UE device to request from the current AP to which it is connected for a recommended list of neighboring APs for roaming. Up on receiving the client request, the AP responds with a list of neighbors on the same WLAN with the Wi-Fi channel numbers. Neighbor list is created by the AP based up on the Radio Resource Measurements and includes the best potential roaming targets for the UE. Neighbor list allows UE to reduce the scanning time when it is time to roam into a new AP in the same WLAN and there by improves the roaming performance. It is recommended to enable

802.11k along with Fast BSS transmission for optimum roaming performance.

#### 7.2.3. 802.11v based Assisted Roaming and Load Balancing

Typical WLAN deployments will have APs with overlapping coverage areas. This is done on purpose to seamless handoff and also to address capacity requirements. Load distribution of UEs in the same coverage area may be helpful to proactively manage the bandwidth requirements and there by improve the subscriber experience. In the most rudimentary form, some of the load balancing solutions relies on the brute force method of ignoring the association requests from a UE by the APs with high load. Another more sophisticated mechanism is to leverage 802.11v based network assisted roaming. 802.11v allows unsolicited BSS transmission management messages from AP towards the client with a list of preferred APs to make roaming decisions. If the AP is experiencing high load, or bad connectivity from the client it may send an unsolicited BSS transmission management frame with the recommended list of APs to roam into. Depending up on the client

implementation, it may or may not honor this info while making oaming decisions.

## [8.](#) QoS Deployment Considerations for Wi-Fi Calling

This section covers the traffic prioritization mechanisms available in various segments of the overall traffic path of the Wi-Fi calling signaling and bearer sessions. Flexibility control of the QoS implementations will depend up on various factors such as ownership and management of the WLAN access network, Wi-Fi to packet core integration model etc.

### [8.1.](#) Wi-Fi Access Network QoS

Traffic prioritization in the WLAN for Carrier Wi-Fi calls can be achieved by implementing Wi-Fi Multimedia (WMM). WMM consists of a subset of IEEE 802.11e enhancements for Wi-Fi. WMM defines four Access Categories, AC1, AC2, AC3 and AC4. AC1 is mapped against voice, AC2 is mapped against video, AC3 is mapped against best effort traffic and AC3 is mapped against Background traffic. Each of these Access Categories is mapped against one or more 802.11e User Priority (UP) values. UP has range from 0 to 7. Higher UP values typically gets more expedited over the air treatment EDCA mechanism for channel access defined in 802.11e is modified to make sure that traffic in higher UP queues get higher priority treatment. WMM can only leveraged if the client can do the right classification and Access points also support it.

### [8.2.](#) End to End QoS

While QoS on the WLAN access network is critical, that by it may not be sufficient to maintain the subscriber quality of experience. It is important to enable QoS prioritization across all the network segments, which form part of the end-to-end voice path. Flexibility of the QoS implementation along the network segments will depend up on the trust models, which are discussed earlier. For example, if the transit path between WLAN network and Packet Core is include Internet, no QoS prioritization can be implemented over the Internet backhaul. How ever for deployment scenarios in which all network segments along the voice traffic path are managed either by the

Mobile operator or their partners, then it makes much easier to implement end to end QoS. End to end QoS Classification for Wi-Fi calling is illustrated in figure 7 below.

Voice UP 6  
Voice Sig. UP 4

Voice DSCP 46  
Voice Sig. DSCP 24

+-----+  
| WMM or WMM+AC |

+-----+  
| DiffSrv QoS |



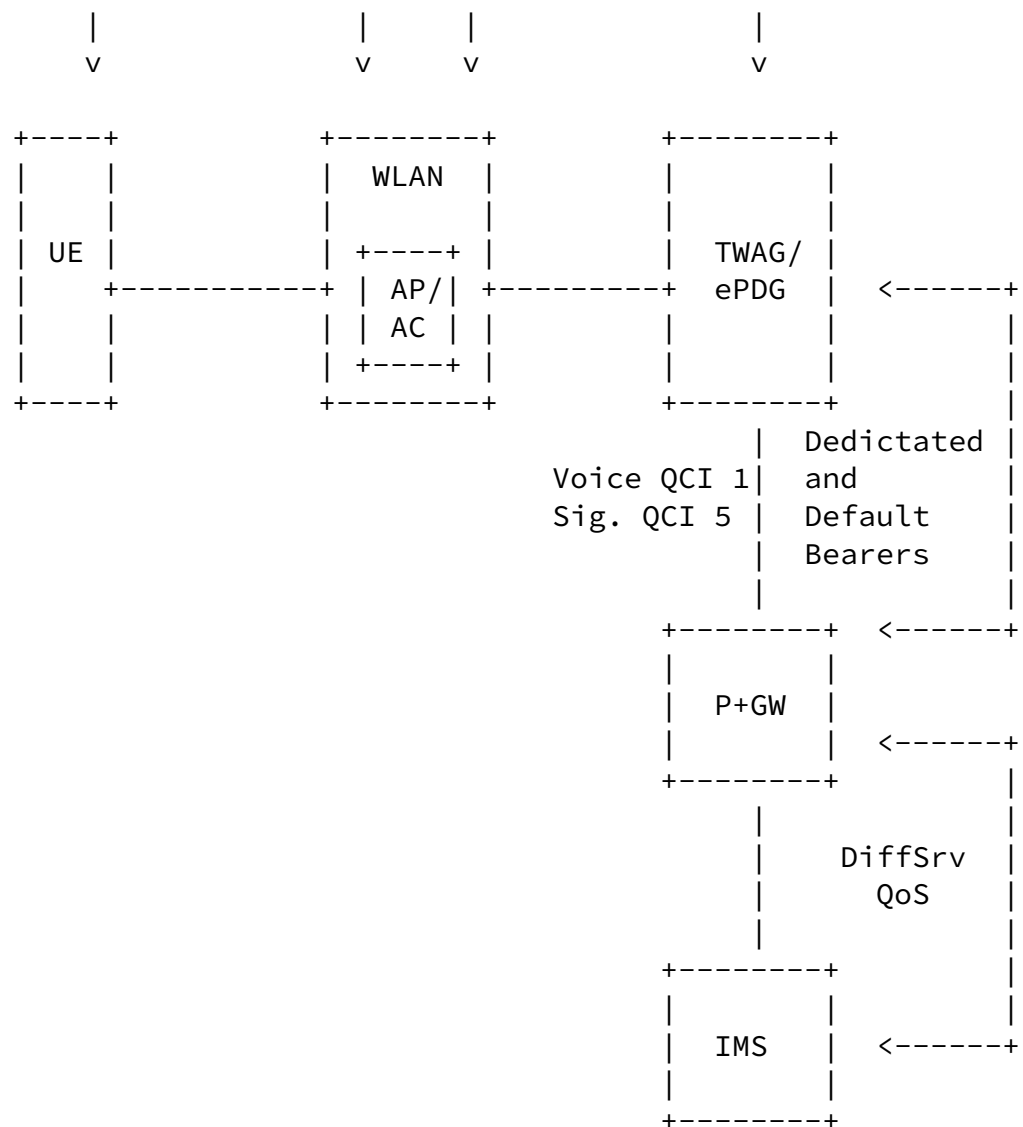


Figure 7: End-to-end QoS Reference Model

This QoS reference model assumes that, MNO or their roaming partners manage all the segments in the end-to-end path for voice signaling and voice bearer traffic. Model also assumes that transit path between WLAN and Packet core is private and secured and does not traverse Internet.

QoS reference model leverages WLAN access network leverages WMM that is described in the previous section, UP value of 6 is typically used for voice bearer traffic and UP value of 4 is used for voice signaling traffic. In order for voice to get the proper prioritization, WMM needs to be supported and enabled on both UE and the WLAN network.

In the transit IP network between WLAN and packet core, DSCP based QoS prioritization can be deployed if the connectivity is part of a managed transport. DSCP value of 46 is typically used for marking voice bearer and DSCP value of 24 is typically used for marking voice signaling. Proper traffic prioritization will depend up on whether DiffSrv QoS is enabled in the transit network.

Between P-GW and ePDG or TWAG, dedicated bearer with QCI value 1 will be established dynamically for voice calls. For signaling traffic a default bearer with QCI value of 5 will be used. These QCI values are mapped against specific QoS SLAs and allocation retention policies (ARP).

## [9. Wi-Fi Calling Client Considerations](#)

Wi-Fi Calling client device functionality requirements depend on the on the models used for WLAN to packet core integration. At a minimum the clients should support IMS User Agent as defined in the 3GPP spec and be able to send and receive both IMS signaling and bearer traffic over a Wi-Fi access point. In addition, an SWu client that supports IPsec will can use ePDG-based packet core integration. This section talks about some of the client side implementation considerations for Wi-Fi calling.

### [9.1. Access Selection Criteria](#)

The client device must select which RAT (cellular or Wi-Fi) it will use for communication to the cellular network. Commonly deployed access selection criteria is described below:

Device Local Policy Profile: In this case, the logic is defined by locally configured policy. Local policy may allow the end user to set preferences. It is also possible for carriers to push these profiles to the device. Some MNOs may prefer cellular instead of Wi-Fi for voice service when both RAT technologies are available. Some other carriers may have Wi-Fi preferred approach for IMS APN when both RAT technologies are available. If Passpoint is enabled on the Wi-Fi access network, the client may take into account network loading conditions learned from the ANQP server to decide whether to offload IMS traffic into the Wi-Fi network.

## [9.2.](#) Inter-RAT Handover

Inter-RAT handover refers to the handover of an active voice call without service disruption when the UE switches out from one RAT technology to another. Implementations must support handovers between Wi-Fi and LTE.

Handover between LTE and Wi-Fi is achieved by maintaining IP or IPv6 addresses between the LTE interface and the IPsec tunnel over Wi-Fi. If the IPsec tunnel is negotiated while a call is already in progress, the IKEv2 Configuration Request should specify the local address of the LTE interface in order to get assigned the same address on the IPsec tunnel. Similarly, handover from an IPsec tunnel over Wi-Fi to LTE requires the LTE interface to be brought up with the same address as the tunnel. Maintaining the address allows the client to not interrupt TCP or UDP connections that are using the local address for communication. In a system that uses POSIX sockets, for example, the handover must be done in such a way that the sockets do not need to be closed and re-opened.

## [9.3.](#) MTU Considerations

When handing over between LTE and IPsec tunnels over Wi-Fi, the client device should be aware of the Maximum Transmission Unit (MTU) of each interface. It is possible that the effective MTU for the IPsec tunnel (which can be calculated as the MTU of the Wi-Fi interface minus the overhead for ESP encryption) is notably smaller than the effective MTU of the LTE interface. For UDP flows, they should avoid sending large datagrams that could get fragmented when handing over between RATs. For TCP flows, the Maximum Segment Size based on the MTU SHOULD be re-calculated upon handover.

## [9.4.](#) Congestion Management

Radio Network Performance management and QoS considerations described earlier can significantly contribute to the overall QoE for Wi-Fi calling. A client driven congestion management mechanism can positively augment the overall experience. The idea is to dynamically change the bandwidth requirements for the call based up on the network congestion conditions. Network resource requirements (bandwidth, packets per second etc.) per call are directly proportional to the type of codec and the packetization rate.

Sometimes it may be desirable to switch out to a lower audio codec to keep the drop, delay and jitter characteristics under acceptable levels during periods of network congestion. Explicit Congestion Notification for RTP over UDP defined in [RFC 6679](#) can be used to inform network congestion to the end clients. But this requires the

## Internet-Draft Carrier Wi-Fi Calling Deployment Considerations July 2017

network elements to mark the ECN bits on the IP header of the packet when congestion conditions are encountered.

### [9.5.](#) NAT Traversal

Since NATs are very commonly deployed primarily due to the shortage of IPv4 address space, a client side implementation should support NAT traversal for Wi-Fi calling. IPsec implementation on the client side should support the detection of NAT gateways as defined in [RFC 7296](#) specification. If a NAT gateway is detected, client should send all subsequent IPsec traffic from port 4500. If NAT is detected ESP packets must be UDP encapsulation using port 4500. If NAT devices are not detected, SWu may use pure ESP encapsulation without UDP. It is important to understand the implications on firewall rules with and without NAT so that the Wi-Fi calling does not get blocked by the firewall. Many deployments may allow ESP with UDP encapsulation by default but may block ESP only tunnels.

### [10.](#) Acknowledgements

Authors would like to acknowledge the inputs and advice provided by Eduardo Abrantes and Ajoy Singh.

### [11.](#) Informative References

- [IR51] "IMS Profile for Voice, Video and SMS over untrusted Wi-Fi access Version 5.0", 2017.
- [IR92] "IMS Profile for Voice and SMS Version 10.0", 2016.
- [RFC4066] Liebsch, M., Ed., Singh, A., Ed., Chaskar, H., Funato, D., and E. Shim, "Candidate Access Router Discovery (CARD)", [RFC 4066](#), DOI 10.17487/RFC4066, July 2005, <<http://www.rfc-editor.org/info/rfc4066>>.

- [RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", [RFC 4187](#), DOI 10.17487/RFC4187, January 2006, <<http://www.rfc-editor.org/info/rfc4187>>.
- [RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", [RFC 4555](#), DOI 10.17487/RFC4555, June 2006, <<http://www.rfc-editor.org/info/rfc4555>>.
- [RFC4881] El Malki, K., Ed., "Low-Latency Handoffs in Mobile IPv4", [RFC 4881](#), DOI 10.17487/RFC4881, June 2007, <<http://www.rfc-editor.org/info/rfc4881>>.

- [RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", [RFC 5213](#), DOI 10.17487/RFC5213, August 2008, <<http://www.rfc-editor.org/info/rfc5213>>.
- [RFC5568] Koodli, R., Ed., "Mobile IPv6 Fast Handovers", [RFC 5568](#), DOI 10.17487/RFC5568, July 2009, <<http://www.rfc-editor.org/info/rfc5568>>.
- [RFC5944] Perkins, C., Ed., "IP Mobility Support for IPv4, Revised", [RFC 5944](#), DOI 10.17487/RFC5944, November 2010, <<http://www.rfc-editor.org/info/rfc5944>>.
- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", [RFC 6275](#), DOI 10.17487/RFC6275, July 2011, <<http://www.rfc-editor.org/info/rfc6275>>.
- [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, [RFC 7296](#), DOI 10.17487/RFC7296, October 2014, <<http://www.rfc-editor.org/info/rfc7296>>.
- [TS22228] "Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1", 2010.
- [TS23402] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture Enhancements for non-3GPP Accesses.", 2009.

[TS23852] "Study on S2a Mobility based on GPRS Tunneling Protocol (GTP) and Wireless Local Area Network (WLAN) access to the Enhanced Packet Core (EPC) network (SaMOG); Stage 2", 2011.

[TS29273] "Evolved Packet System (EPS); 3GPP EPS AAA interfaces", 2011.

#### Authors' Addresses

Byju Pularikkal  
Cisco Systems  
170 West Tasman Drive  
San Jose  
United States

Email: byjupg@cisco.com

Pularikkal, et al.

Expires January 4, 2018

[Page 26]

---

Internet-Draft Carrier Wi-Fi Calling Deployment Considerations July 2017

Tommy Pauly  
Apple Inc.  
1 Infinite Loop  
Cupertino, California 95014  
US

Email: tpaully@apple.com

Mark Grayson  
Cisco Systems  
10 New Square Park  
Feltham  
United Kingdom

Email: mgrayson@cisco.com

Sri Gundavelli  
Cisco Systems  
170 West Tasman Drive

San Jose  
United States

Email: sgundave@cisco.com

Samy Touati  
Ericsson  
300 Holger Way  
San Jose, California 95134  
US

Email: samy.touati@ericsson.com