White Paper

Enriched service over converged Wi-Fi and cellular network

March 2025

GSMA

About the GSMA

The GSMA is a global organisation unifying the mobile ecosystem to unlock the full power of connectivity so that people, industry and society thrive.

Led by our members, we represent the interests of over 1,100 operators and businesses in the broader ecosystem. The GSMA also unities the industry at world-leading events, such as MWC (in Barcelona, Kigali, Las Vegas and Shanghai) and the M360 Series.

Unlock the benefits of GSMA membership

As a member of the GSMA, you join a vibrant community of industry leaders and visionaries – helping to shape the future of mobile technology and its transformative impact on societies worldwide.

Our unique position at the heart of the mobile industry means you get exclusive access to our technical experts, data and analysis – as well as unrivalled opportunities for networking, innovation support and skills acceleration.

For more information, please visit:
http://www.gsma.com/membership/

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Antitrust Notice

The information contained herein is in full compliance with the GSM Association's antitrust compliance policy.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Contents

Contents

Contents

1. Executive Summary

This White Paper has been written by the GSMA 5G Voice over Wi-Fi Task Force (5GVoWiFi TF). The TF was formed by the GSMA Board in 2024 and chaired by China Telecom.

This White Paper is a result of collaboration amongst a number of TF member companies as well as contributions from the Wireless Broadband Alliance (WBA) and Wireless Broadband Association (WBBA).

VoWiFi or Wi-Fi Calling has been deployed by numerous operators worldwide over the past decade, which:

- Enables Mobile Network Operators (MNOs) to re-use the same IP Multimedia Subsystem (IMS) core as used for Voice over LTE (VoLTE)
- Enables the re-use of mobile devices, using the same IMS stack and dialler as for VoLTE,
- Provides a transparent service to end users for voice/video/SMS without the need for additional configuration.

With the advent of the 5G era, there are new requirements emerging for Wi-Fi Calling in 5G:

- Convergence of Wi-Fi Calling with both 5G/4G core networks and seamless interworking with Voice over New Radio (VoNR) as well as VoLTE,
- Providing voice/video/SMS using satellite backhaul for maritime and in-flight scenarios,
- Supporting additional IMS services (such as IMS Data Channel) via Wi-Fi.

The White Paper covers the following:

- Why Wi-Fi Calling is needed under diversified scenarios and services,
- Use cases on the ground, at sea and in the air,
- Network architecture for Wi-Fi Calling via 5G Core (5GC),
- Characteristics of Wi-Fi Calling networks and technologies for performance and security,
- Business models,
- Trials performed by China Telecom on the ground and at sea.

A number of issues are also identified where there are gaps which need to be addressed to further facilitate the deployment and usage of Wi-Fi Calling:

- Operators typically deploy legacy Evolved Packet Data Gateways (ePDGs) to access the 5GC via Wireless LAN (WLAN) rather than the 5G native Non-3GPP Inter-Working Function (N3IWF) or Trusted Non-3GPP Gateway Function (TNGF). In future, it is recommended that MNOs deploy N3IWF which is the native 5G gateway for non-3GPP untrusted access and provides all the advantages of 5G security architecture and common 3GPP and non-3GPP authentication framework. At the time of writing, 3GPP are also considering a proposal to enhance the ePDG by adding a 5G Service Based Interface (SBI).
- Capturing the location information of a WLAN network is a significant challenge where the WLAN access network belongs to another operator or is connected via a satellite. This paper introduces a possible solution to obtain the WLAN location information by incorporating a Locator System entity between the WLAN access network and the ePDG.
- On the WLAN, differentiated services code point (DSCP) is recommended to be used as part of the end-to-end QoS solution. However, some UEs and consumer Access Points (APs) do not support DSCP.

Wi-Fi Calling is a key component of 5G for delivering converged services over heterogenous and complimentary wireless networks.

2. Introduction

The term "Voice over Wi-Fi(VoWiFi)" can also be referred to as "Wi-Fi Calling" and includes other telephony services such video and messaging in addition to voice. The aim of the TF was to facilitate the creation of an inter-operable Wi-Fi Calling ecosystem and enhance the system to support new 5G services with 5G Wi-Fi Calling.

The development of Wi-Fi Calling technology was a natural extension of the trend towards the convergence of fixed and mobile networks. It effectively integrates the resource of wireless and wired networks, realizing seamless indoor and outdoor network coverage and providing users with ubiquitous high-quality voice services. In addition, Wi-Fi Calling makes effective use of existing Wi-Fi infrastructure to reduce the network construction costs for operators and compliments operator provided voice/video services via 3GPP RANs.

The integration of Wi-Fi and LTE networks has been supported by numerous operators worldwide over the past decade. Organizations including 3GPP, GSMA, IEEE 802.11, WFA, WBA and WBBA have also undertaken work related to Wi-Fi Calling in various specifications. For example, the 2016 WBA White Paper "Wi-Fi-Calling Opportunities and Challenges towards 5G" [1] describes business drivers, opportunities and challenges of Wi-Fi Calling, GSMA TS.22 [2] "Recommendations for Minimum Wi-Fi Capabilities of Use" defines requirements for Wi-Fi Calling service in 4G network, and 3GPP standards specifies architectural & handover procedures for 3GPP and non-3GPP network. However, with the deployment of 5G, there are many new requirements emerging for Wi-Fi Calling in 5G:

- Convergence of 5G/4G and Wi-Fi network and seamless interworking between VoNR/VoLTE and VoWiFi,
- Providing voice and short message services using satellite backhaul for maritime and in-flight scenarios,
- Supporting IMS Data Channel interaction over Wi-Fi,
- Supporting higher bandwidth in weak cellular coverage area,
- Enabling various traffic offloading and splitting policies among different services.

A series of new challenges have also emerged, including compatibility of terminal devices under different networks, assurance of end-to-end QoS, and security of Wi-Fi Calling services.

This white paper provides an in-depth introduction to solutions to the new requirements and challenges from different perspectives. The following sections discuss (i) why Wi-Fi Calling is needed under diversified scenarios and services, (ii) typical use cases, (iii) various network architectures, (iv) characteristics of Wi-Fi Calling networks and key technologies for performance and security enhancement of Wi-Fi Calling services, (v) business models in different scenarios, (vi) test results from Wi-Fi Calling practices, and (vii) prospects of future research directions, aiming to provide theoretical support and practical guidance for the development of Wi-Fi Calling technology.

3. Background – Why Wi-Fi Calling

3.1 Diversified Scenario Requirements

3.1.1. Scenarios with Poor Terrestrial Cellular Coverage

According to Ericsson[1], up to 80% of all data traffic is consumed at indoor locations and 90% of our time is spent indoors. In this era, staying connected is not just a convenience but a necessity. Consequently, fast and reliable indoor network connectivity and communication service play a pivotal role for enterprises and consumers alike. However, poor cellular indoor coverage has always been one of the key issues faced by operators, with residential areas and commercial buildings being the most typical scenarios.

- **Residential Areas.** The indoor coverage rate in some residential areas is generally below the level of overall network coverage, and insufficient indoor coverage seriously affects user satisfaction, with poor voice call quality being one of the main reasons for complaints. However, simply constructing more base stations to enhance coverage in typical residential areas such as urban villages, high-rise residential buildings, and remote villages is not an effective solution.
  - **Urban villages:** dense residential buildings lead to severe signal attenuation through walls, making it difficult to solve indoor coverage problems even if the outdoor Base Station (BS) is only 200 meters away.
  - **High-rise residential buildings:** dense deployment of base stations can cause serious inter-cell interference. For example, when there are multiple high-rise buildings around, it is very likely that there will be signals from multiple cells at the same location.
  - **Remote villages:** the cost of BS construction, operation and maintenance is high, but each BS only covers very few users, resulting in a low return on investment.
- **Commercial Buildings.** Shopping malls, offices, and other commercial buildings with large indoor depths also pose challenges for indoor cellular coverage. Typically, large shopping malls and offices can choose to deploy distributed antenna systems. However, for chain hotels, small businesses, and shops, there is currently no cost-effective solution. Table 1 provides example costs involved for enhancing cellular coverage using existing macro/micro approaches.

Compared to the existing solutions for enhancing indoor coverage, Wi-Fi Calling technology is a more attractive solution due to its low cost and ease of deployment, provided there is a good fixed broadband connection. With the continuous improvement of home broadband penetration and the construction of WLAN networks in public areas, Wi-Fi Calling can easily enable users to make native voice/video calls and send messages through the existing ubiquitous Wi-Fi network. Furthermore, seamless handover between VoWiFi and VoNR/VoLTE (e.g., when moving between indoor and outdoor) significantly improves user experience and satisfaction. The integration of Wi-Fi and 5G networks can be a key direction for future network evolution.

	OPTIMIZE EXISTING SURROUNDING BSS	BUILD MORE SMALL BSS IN RESIDENTIAL AREAS	INSTALL PICO SITES
Disadvantages	Poor performance	Difficult construction and high cost	High cost and serious interference
Estimated Costs	55,000 – 68,000 USD	14,000 USD/15,000 m^2	275 USD per unit

Table 1, Cost for enhanced cellular coverage using existing macro/micro approaches

1 Ericsson Blog, "5 ways indoor 5G will change your life (and mine)" (July 2023).

3.1.2 Scenarios under Non-Terrestrial Networks

In scenarios where terrestrial cellular network coverage is unavailable, but non-terrestrial networks (NTN) are accessible, such as at sea, in the air, or during emergency rescue, there are also urgent needs for reliable communication solutions.

- **At sea:** crews'/passengers' mobile numbers cannot be reached, and they cannot effectively make calls.
- **In the air:** passengers may miss important work calls or unable to receive SMS verification codes during flights.
- **Emergency rescue:** existing solutions require Unmanned aerial vehicles (UAVs) to carry small base stations, but their large size and high weight affect the flexible operation of UAVs.

According to the Ministry of Transport (MOT) of China, by the end of 2023, China had 620 million air passenger trips, and 258 million sea passenger trips for the year. This demonstrates there is a large market for in-flight and maritime voice and message services. Considering the widespread support for data transmission via NTN in many ships and aircrafts, and the ground satellite equipment can convert satellite signals into Wi-Fi signals, integrating NTN and Wi-Fi networks to support Wi-Fi Calling for voice and message services is a cost-effective and viable alternative. This also offers a lightweight and flexible choice for emergency rescues. Therefore, Wi-Fi Calling can enhance the communication capabilities in scenarios where traditional terrestrial cellular networks are limited or unavailable.

3.2. Enriched Service Requirements

Real-time communication services based on IP Multimedia Subsystem (IMS) Data Channel (DC), integrating AI and AR technology, bring revolutionary changes to user communication experience, and offer new development opportunities for various industries, further promoting digital transformation and intelligent upgrading. However, some DC calling services may require high transmission bandwidth and low latency, and dialing DC calls in indoor scenarios with poor cellular coverage is prone to phenomena such as slow data transmission rate and video stuttering, resulting in poor user experience. In indoor scenarios with weak cellular coverage, Wi-Fi Calling-based DC call can access to the IMS network through Wi-Fi Calling to ensure the smooth operation of DC call service, effectively improving user experience.

4. Use Cases

4.1 Wi-Fi Calling Use Cases on the Ground

On the ground, users inside buildings or on high-speed vehicles can easily use Wi-Fi Calling services by connecting to residential or public Wi-Fi networks. With Wi-Fi Calling, users can enjoy seamless voice and message services just as they would with the cellular network, without any additional operations.

4.1.1 Use Case 1 –Wi-Fi Calling Handover between Wi-Fi Networks

A user, staying in a hotel with poor cellular signal due to its complex building structure, urgently needs to contact a business partner to discuss contract details but the voice call via cellular access cannot be dialled out. Fortunately, there are strong Wi-Fi signals all over the hotel. After connecting to the Wi-Fi network, the user can directly dial his business partner's number without additional applications. The call can be quickly connected with stable and smooth communication. During the call, the user needs to go downstairs to the front desk of the hotel to get a document. As the user moves, the phone automatically connects to the Wi-Fi network with stronger signal, and the call is seamlessly switched between Wi-Fi access points (APs) on different floors with the same service set identifier(SSID).

4.1.2 Use Case 2 – Wi-Fi Calling Handover between Wi-Fi and Cellular Networks

A traveler is on a high-speed train journey to a given destination. Due to the rapid movement and penetration loss caused by the metal structure of the train, the cellular signal is poor. Upon boarding, the traveler notices the sign advertising free Wi-Fi service and connects his/her device to the Wi-Fi network on the train. The Wi-Fi equipment customized by railway companies can achieve good data rates during high-speed movement. Therefore, when the traveler calls a friend to discuss the details of the upcoming trip, the call is initiated first on the Wi-Fi network, and as the train stops at a station where the cellular signal is stronger, the call can smoothly switch to the cellular network. Throughout the call, both the traveler and his/her friend are completely unaware of the use of Wi-Fi Calling and the handover between cellular and Wi-Fi networks.

4.2 Wi-Fi Calling Use Cases at Sea or in the Air

To meet the communication requirements of passengers and staff, shipping companies and airlines can cooperate with operators to support Wi-Fi Calling services via satellite equipment. In this scenario, companies can subscribe to Wi-Fi Calling services for all employees. Alternatively, passengers may need to subscribe to Wi-Fi Calling services by themselves. After subscribing to the Wi-Fi Calling services, users can make or receive calls, send and receive messages by connecting to the Wi-Fi networks on the ship or aircraft.

4.2.1 Use Case 1 – Wi-Fi Calling Message Service

A passenger is enjoying a vacation on a cruise ship but finds that there is something wrong with a credit card. The passenger contacts the bank's online customer service to handle the account issues and is asked to provide a verification code for identity verification. As the mobile signals cannot reach the cruise ship, the passenger decides to use the cruise's Wi-Fi Calling service. After connecting to the Wi-Fi network provided by the cruise's satellite equipment, the passenger subscribes to the Wi-Fi Calling service and then soon receives SMS verification codes to ensure the security of account operations related to the credit card.

4.2.2 Use Case 2 – Wi-Fi Calling Voice Service

A passenger is on a business trip and needs to be ready to answer important business calls from clients at any time. To avoid missing any important calls on the plane, the passenger has subscribed to the Wi-Fi Calling service in advance. Once connected to the in-flight Wi-Fi network, the passenger's smartphone can make and receive calls using the Wi-Fi Calling function, just as it would on land. When the business client calls the passenger, a clear conversation ensues as if the connection were provided via terrestrial networks.

4.3 Wi-Fi Calling for IMS DC

Real-time communication services based on IMS DC has high requirements of bandwidth for data transmission. In environments with poor cellular coverage, users attempting to make a DC call often experience degraded call quality due to insufficient signal strength. This situation leads to a suboptimal calling experience, which can be frustrating for users.

However, leveraging Wi-Fi signal coverage allows users to initiate Wi-Fi Calling. In this context, users can handover from cellular to Wi-Fi if cellular coverage is poor and make or receive calls just as they would on cellular network. This capability not only enhances voice call quality but also enables users to access a diverse array of DC applications for interaction, thereby enriching their communication experience.

There is a scenario where a user is engaged in a DC call in an area with poor cellular coverage. Besides, the operator to which the user subscribes has launched Wi-Fi Calling service and DC calling on its network, and user's smartphone supports these services. The user initiates a DC call over the cellular network. Once the call is connected, the user attempts to transfer files during the conversation. By opening the floating window on the dialer and clicking the file transfer button, the user selects a specific file and confirms the transfer. However, the transmission is interrupted due to the poor cellular signal. Since the user's smartphone supports the Wi-Fi Calling service, this call can seamlessly handover to Wi-Fi Calling without any noticeable disruption. With Wi-Fi Calling, user can continue to transfer files smoothly, ensuring continuity and stability throughout the process. Moreover, with the help of Wi-Fi Calling, user can also conduct DC video call and watch live streaming, etc., as shown in Figure 1.

In this case, the inherent link guarantees provided by Wi-Fi Calling ensure sufficient bandwidth for DC calls, allowing users to conduct DC calls with minimal interruption and smooth interaction.

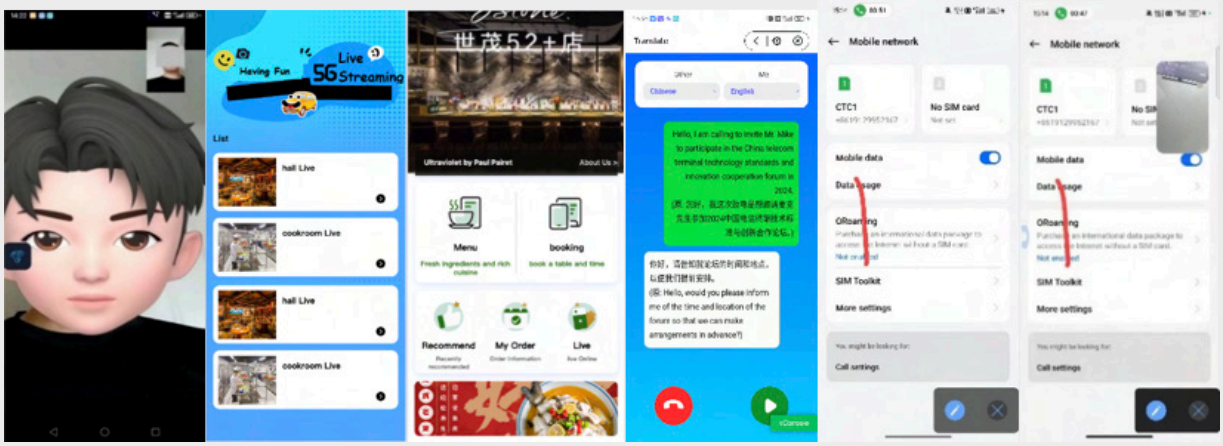


Figure 1, Video call, live streaming, reservation assistant, real-time translation and screen sharing based on DC call on Wi-Fi Calling

5. Network Architecture

5.1 Architecture for Wi-Fi Calling Service on 5GC and WLAN Access

3GPP TS 23.501 [3] depicts two ways for a UE to connect to a 5G Core Network (CN) over WLAN access:

- via the Non-3GPP Inter-Working Function (N3IWF) or Trusted Non-3GPP Gateway Function (TNGF), as is defined in TS 23.501 [3] clause 4.2.8;
- via the Evolved Packet Data Gateway (ePDG), as is defined in TS 23.501 [3] clause 4.3.4.

There are few mature N3IWF and TNGF devices, but connecting to 5G Core Network(5GC) through ePDG is widely supported, enabling operators to provide Wi-Fi Calling service for 5G users.

The reference architecture for Wi-Fi Calling using ePDG is shown in Figure 2. Only those network elements necessary for provision of Wi-Fi Calling Service are shown in this figure, others are not, for example, other Call Session Control Function (CSCFs) in IMS system.

This architecture supports the following enriched features:

- providing Wi-Fi Calling service for 5G users as well as current 4G users;
- maintaining call continuity by handover procedure among LTE access, NR access and WLAN access;
- ensuring the same experience of 5G innovative services, e.g. 5G MESSAGE and Next Generation Real Time Communication, both over 3GPP access or WLAN access.

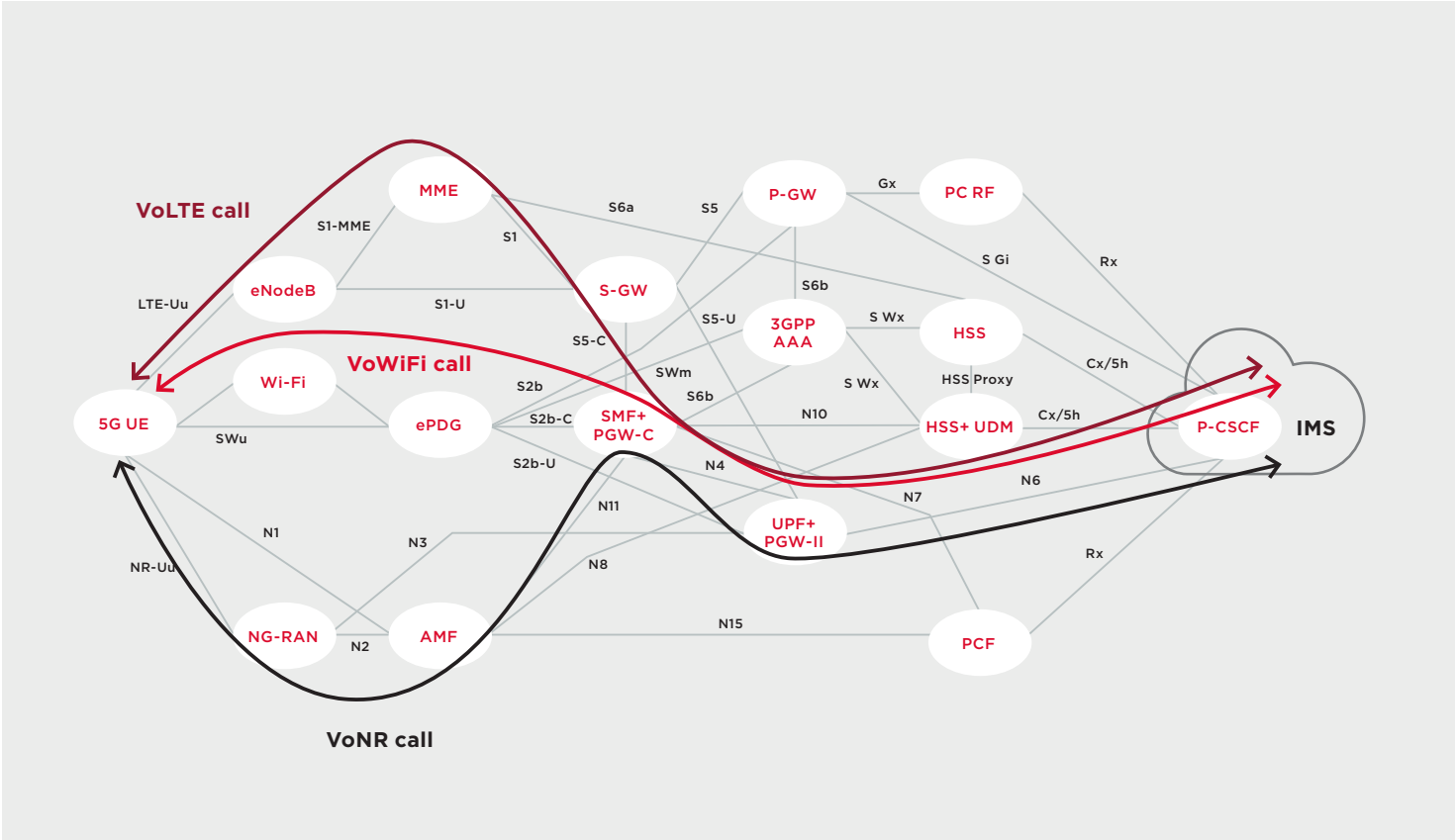


Figure 2, Architecture for Wi-Fi Calling service on 5GC and WLAN access via ePDG

5.2 Architecture for Wi-Fi Calling Service over Specific WLAN Access Scenarios

To ensure that Wi-Fi Calling service is accessible via permitted WLAN network, the operator needs to acquire the location of the Wi-Fi AP user is accessing and confirm whether the Wi-Fi AP belongs to the range of allowed WLAN access networks.

As an optional solution defined in 3GPP TS 23.402 [4] and 3GPP TS 29.273 [5], the WLAN access network can provide WLAN location information to the 3GPP AAA server via the SWa reference point. The 3GPP AAA server stores this information and provides it to the ePDG, via the SWm interface, during the Authentication and Authorization procedure or upon request of the ePDG. Then the ePDG propagates the WLAN location information to the PDN GW. But how to obtain WLAN location information provided by other operator or third party is not explicitly defined within 3GPP standards. As a result, obtaining WLAN location information can be a significant challenge in cases the user connects through a WLAN access network that belongs to another operator or a satellite.

To facilitate WLAN location sharing between different operators and to enable WLAN location acquisition in scenarios such as in the air or at sea, this section proposes an alternative solution to obtain the WLAN location information by incorporating a Locator System entity between the WLAN access network and the ePDG. Other location acquisition methods may also apply as needed.

5.2.1 WLAN Access Specified by Operators

The operator may specify that Wi-Fi Calling service is available to users in certain WLAN access networks, such as Home Broadband Network or Public Wi-Fi Network provided by the operator itself. In this situation, the operator needs to determine from the location of the Wi-Fi AP whether user is allowed Wi-Fi Calling service.

The reference architecture in Figure 3 shows that a UE connects to the 5GC from a Home Broadband Network.

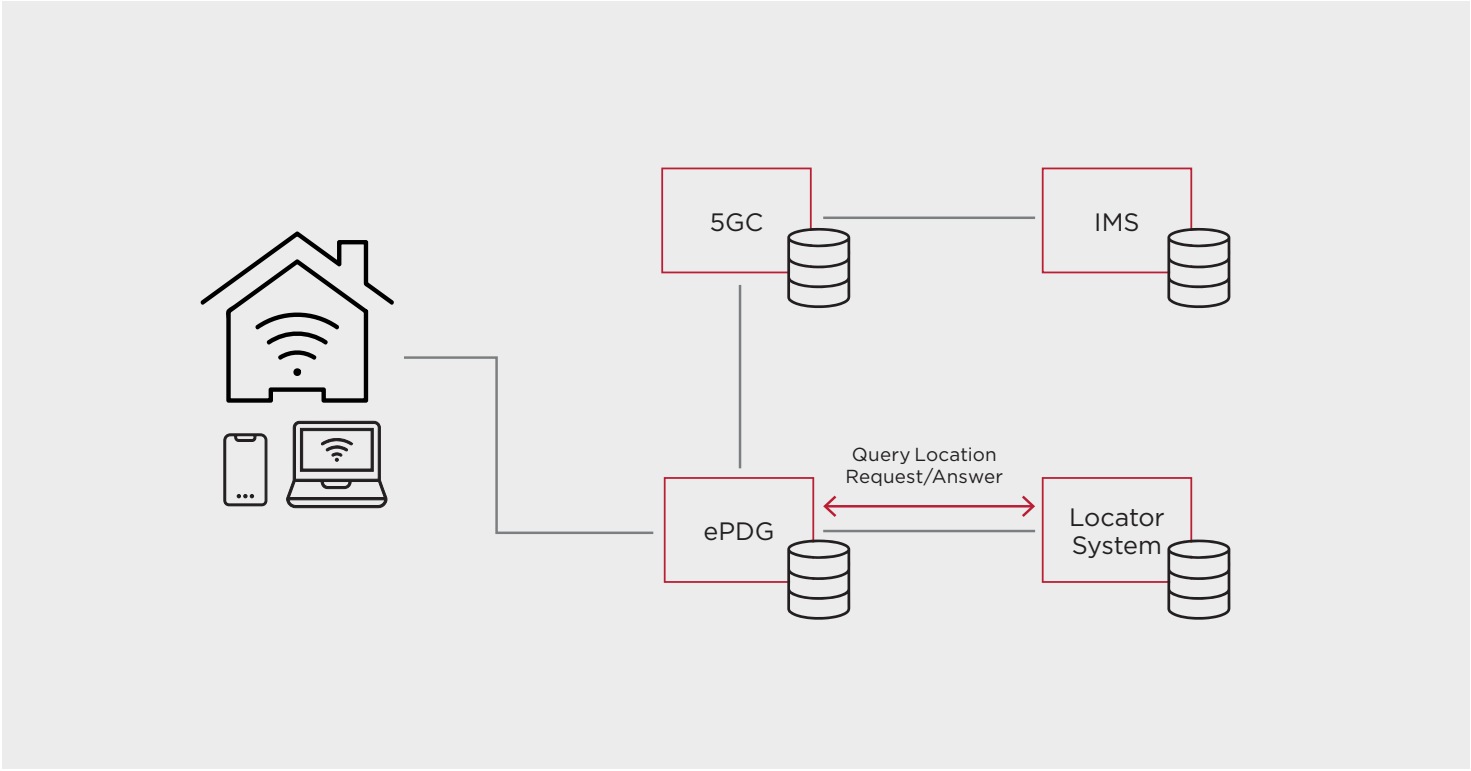


Figure 3, Architecture for Wi-Fi Calling service including Locator System

A Locator System is managed by the operator itself, which stores the location information of allowed WLAN access networks for Wi-Fi Calling service, including:

— Attached UE's local IP address and optionally User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) source port number, if Network Address Translation (NAT) is detected;
— Civic address information of the WLAN AP to which the UE is attached;
— User Account information authorized to use the WLAN access network, etc.

NOTE 1: UE local IP address is either the public IPv4 address and/or IPv6 address assigned to the UE by the Broadband Forum (BBF) domain in the non-NAT case, or the public IPv4 address assigned by the BBF domain to the NATed Residential Gateway (RG) that is used for this, UE (defined in 3GPP TS 29.212 [6]).

NOTE 2: The UE local IP address is used by the UE for sending all IKEv2 messages and as the source address on the outer header of the IPsec tunnel to the ePDG (defined in 3GPP TS 23.402 [4]).

When a user tries to connect to the 5GC over a WLAN access network, the ePDG provides UE's local IP address and port number in a Query-Location-Request message to the Locator System to confirm whether the user is allowed to use Wi-Fi Calling service through this WLAN access network. The Locator System can also return the civic address information and User Account information in a Query-Location-Answer message.

5.2.2 WLAN Access Provided by Other Operators

The reference architecture in Figure 4 shows the exchange of location information between different operators to support provision of Wi-Fi Calling service to users accessing from a WLAN access network that belongs to other operators.

The Locator System of operator A and the Locator System of operator B are inter-connected and share the list of UE local IP addresses of allowed WLAN access networks for Wi-Fi Calling service. When a user of operator A tries to connect to the 5GC over a WLAN access network provided by operator B, the Locator System of operator A first confirms whether the UE local IP address from operator B is in the allowed address list, and then forward the Query-Location-Request message from the ePDG to the Locator System of operator B. Then the Locator System of operator B can return civic address information and User Account information.

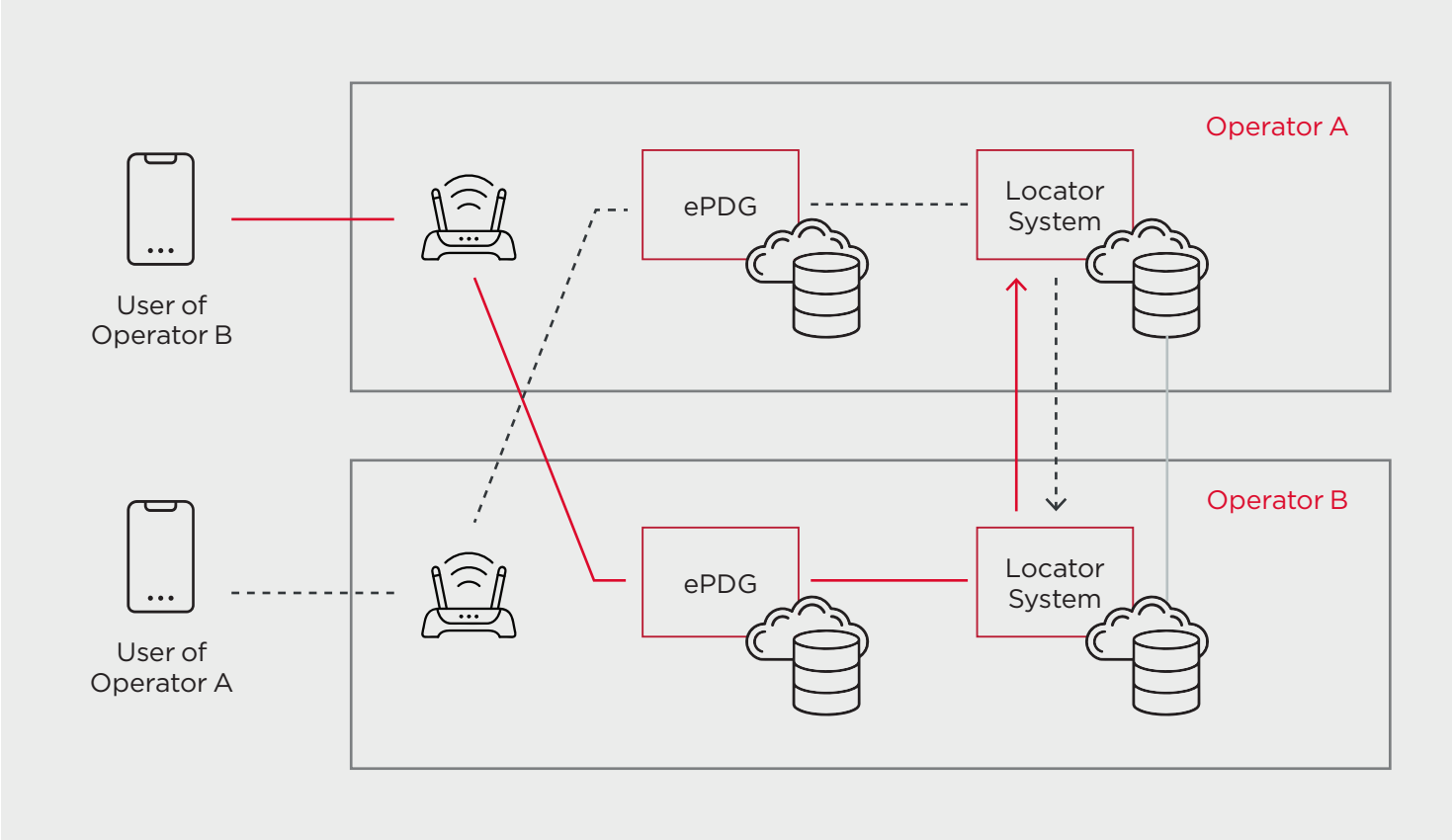


Figure 4, Architecture for Wi-Fi Calling service interworking with Locator Systems

5.2.3 WLAN Access in the Air or at Sea

Figure 5 shows the reference architecture for Wi-Fi Calling service in the air or at sea.

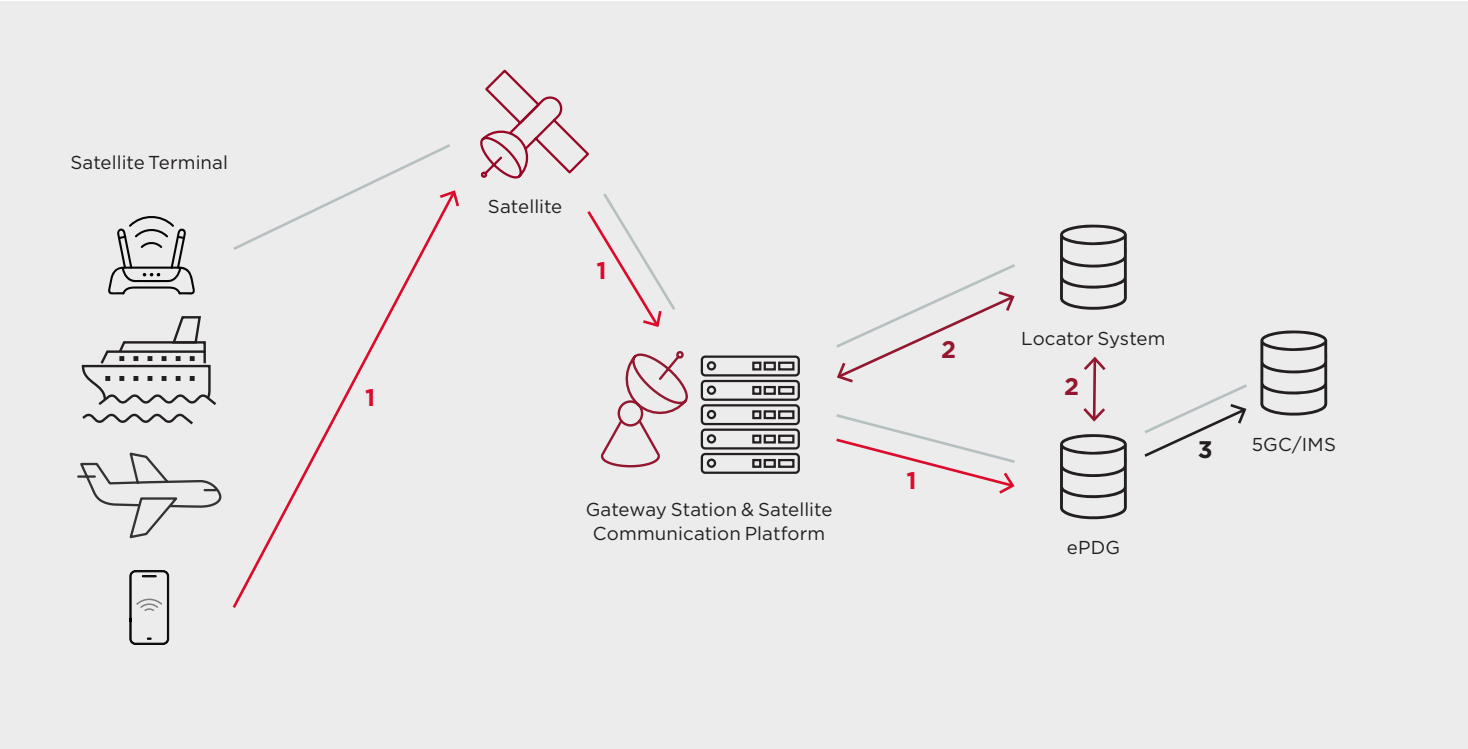


Figure 5, Architecture for Wi-Fi Calling service in the air or at sea

For a user on an airplane or a ship, the user's terminal device can connect to the 5GC using satellite backhaul technology, through the WLAN access network on the plane or on the ship (e.g., Fixed Wireless Access [FWA] supporting NTN connectivity). In this case, if the operator wants to confirm the location of the user, the Locator System needs to connect to the Satellite Communication Platform and forward the Query-Location-Request message from the ePDG. The Satellite Communication Platform may return the Aircraft Identity or the Ship Identity and the associated location information to ePDG to indicate the user location information. The ePDG can then report the location information of the user within the message to 5GC/IMS. Further detailed procedures shown in section 6.6.

6. Characteristics of Wi-Fi Calling Networks

6.1 Wi-Fi Calling QoS Monitoring

Figure 6 provides an overview of Wi-Fi Calling QoS Monitoring.

The following sub-sections discuss network characteristics that impact on QoS.

6.1.1 Bandwidth

Bandwidth refers to the data rate that can be used by a particular flow at a given time. Bandwidth is usually dependent on the line rate of the link, which means that there is a limited amount of bandwidth available for all flows and that they must share this bandwidth. When flows require more bandwidth than is available, QoS mechanisms are used to prioritize and provide availability to higher-priority flows while lower-priority flows are either queued or discarded. The ideal bandwidth for a good quality of experience depends on the type of system being used for the call as well as how many concurrent users. In most circumstances, a minimum bandwidth of 80 Kbps for voice is enough for a single Wi-Fi Calling session. If that session becomes interactive or multiple users are needing to use the same link, then one must consider 1-5 Mbps for good quality of experience.

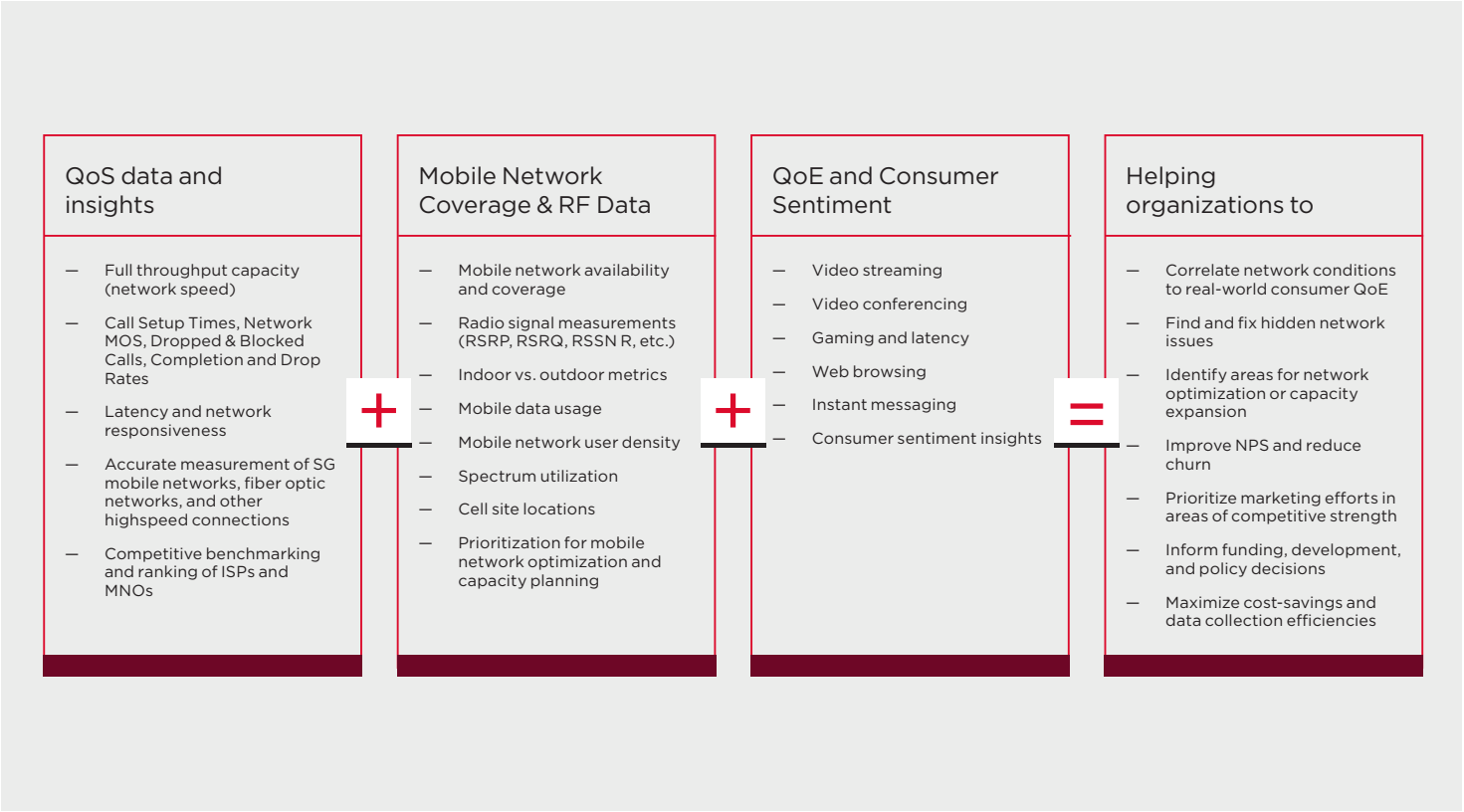


Figure 6, Wi-Fi Calling QoS monitoring

6.1.2 Latency

Latency is a measurement of the time delay between the transmission and the reception of a packet. Typically, this is a round-trip measurement, meaning that the calculation measures both the near-end to far-end and the far-end to near-end directions simultaneously. This measurement is critical for voice applications, in which too much latency can affect call quality, leading to the perception of echoes, incoherent conversation or even dropped calls.

6.1.3 Jitter

Jitter is a measurement of the variations in the time delay of packet deliveries between source and destination. There are several reasons why packets experience different delay between source and destination, such as:

— packets taking different routes,
— packets queued and sent in bursts to the next hop,
— prioritization at random moments

Packets are therefore received at irregular intervals. The direct consequence of this jitter is on the user experience.

Jitter is measured in milliseconds (ms), and ideally, an acceptable jitter level should stay below 30 ms. Anything higher than 30 ms, and you may start to see issues with audio or video quality.

6.1.4 Packet Loss

Packet loss is where the transmitted packet is not received by the destination. Packet loss can happen for a number of reasons, such as packet corruption during the transmission can cause receiver to discard the packet, receive buffer limitation cause receiver to discard the packet, to prevent network congestion packets could be discard by the transmitter, or network congestion causing excessive delay can lead the receiver to discard the packet.

Network congestion can also cause packets to be discarded, as networking devices must drop packets (thrown away) in order not to saturate a link in congestion conditions. Packet loss can also severely negatively impact the quality of Voice over Internet Protocol (VoIP). Packet Loss of 1–2% is acceptable for VoIP while not effecting Quality of Experience (QoE). However, anything over 5-7% is considered high when significantly affect consumers QoE. Packet loss can cause issues like choppy sounds, silences, delays, garbled sounds, and scrambled or reordered conversations.

6.1.5 Ideal QoE Metrics

Table 2 provides a guideline to the ideal set of metrics for a good quality of experience with Wi-Fi Calling for consumers. Each metric also depends on other factors like type of device, radio conditions, environment as well as features used in Wi-Fi Calling session (e.g. adding video). See subsection 6.5.2 for other metrics that can be taken into account to determine QoE.

METRIC	IDEAL RANGE	ACCEPTABLE	UNACCEPTABLE
Bandwidth for voice (bits per second)	1-5 Mbps	80 Kbps	< 70 Kbps
Latency (millisecond)	90-120 ms	150 ms	> 250 ms
Jitter (millisecond)	20-30 ms	50 ms	> 150 ms
Packet Loss (percent)	1-3%	3%	> 6%
Download Speed (bits per second)	5-25 Mbps	1 Mbps	< 500 Kbps
Upload Speed (bits per second)	5-25 Mbps	1 Mbps	< 500 Kbps

Table 2, Wi-Fi Calling QoE metrics

6.2 Wi-Fi AP Configuration Recommendation

By leveraging existing Wi-Fi infrastructure for voice and video communication, Wi-Fi Calling on smartphones has emerged as a key element of communication for consumers and enterprises, offering flexibility and efficiency for all users. Additionally, the mobility provided by smartphones enables everyone to stay connected from anywhere with internet access, enhancing convenience, productivity and collaboration.

However, ensuring a seamless and high-quality Wi-Fi Calling experience remains a challenge. Poor voice quality not only frustrates users but also hampers productivity, making it a key Wi-Fi requirement for many networks. This section considers various techniques to configure Wi-Fi network for optimal voice performance, as indicated in Figure 7.

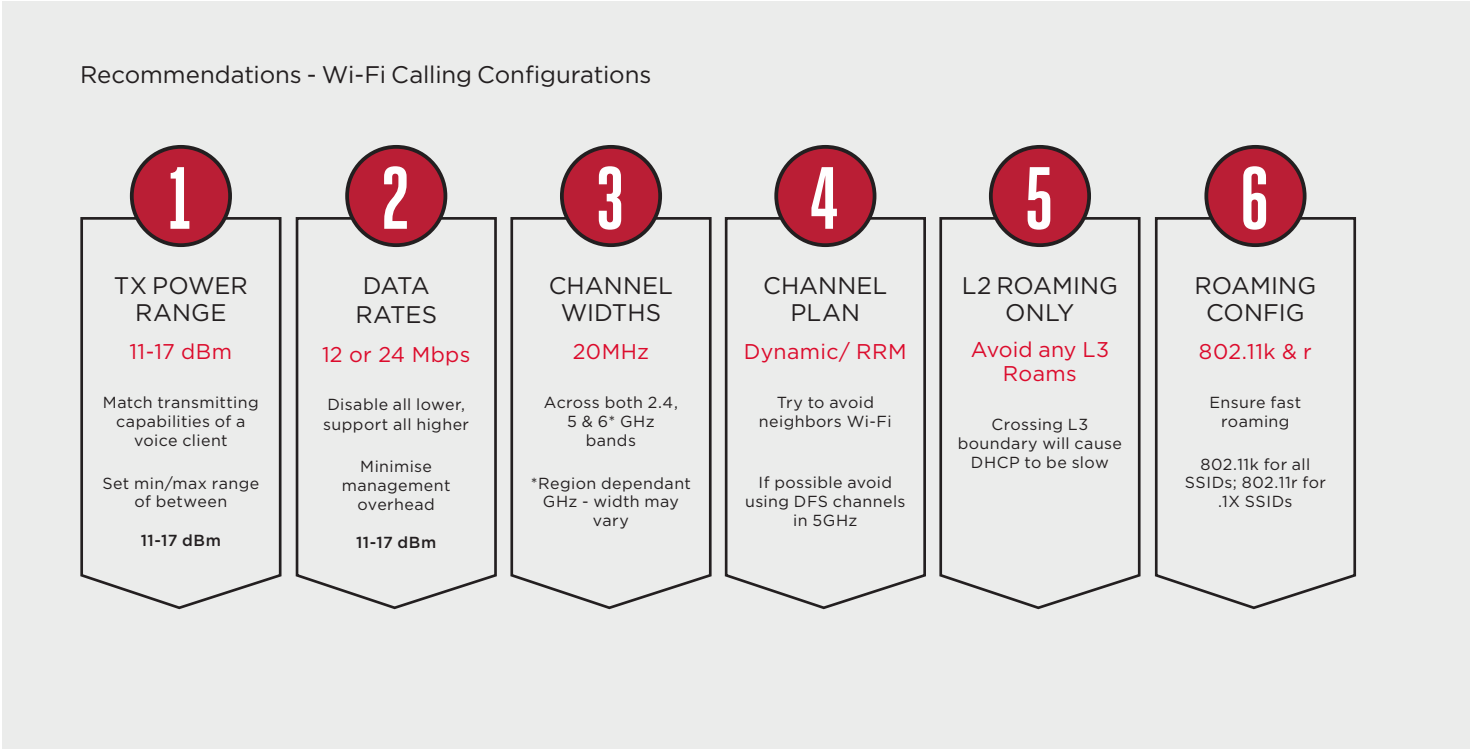


Figure 7, Recommendations of Wi-Fi Calling Configurationsa

6.2.1 Transmit (Tx) Power Range

Setting Tx power levels within an appropriate range is fundamental to maintaining consistent Wi-Fi signal coverage while minimizing interference. Configure access point transmit power levels between 11-17 dBm to ensure proper coverage while matching most clients Tx capabilities. While dynamic transmit power adjustment is acceptable, defining a controlled min/max range is advisable.

NOTE: Transmit power range recommendation of 11-17 dBm is because typical client devices operate somewhere around 14dBm so this means the APs will be operating at a similar level to the client devices but also with some flexibility to turn their radios up and down to compensate for some environmental changes. This is just a rule of thumb and general best practice recommendation, and there can be a lot of things that would affect this specific to the environment.

6.2.2 Data Rates

Balancing performance with overhead management is achievable by controlling minimum and supported data rates. Set the minimum data rate to 12 Mbps for lower density networks and 24 Mbps for higher density networks, and disable lower data rates while supporting higher ones. Low density and higher density networks are referring to the amount of client devices, not the amount of data being transferred. This reduces overhead from legacy, inefficient modulations and lower data rates, thus enhancing overall performance. To guarantee good quality of service for consumers for Wi-Fi Calling, one must also consider the data rates from the access point to the network. In that case, a date rate of 32 Mbps is desired to maintain the equivalent data rate from the access point to the device.

NOTE: Based on many years of testing experience, Ekahau recommends either 12 or 24 Mbps as the minimum basic rate to configure your networks to transfer the data over the air for the management and control traffic. See **https://www.ekahau.com/blog/voice-over-wi-fi-6-key-configuration-tips/ for more information.**

6.2.3 Channel Widths

Channel width plays a significant role in throughput capacity and co-channel interference (CCI) potential. It is recommended to use 20 MHz wide channels across the 2.4 GHz, 5 GHz, and 6 GHz bands to strike a balance. While wider channels offer increased throughput capacity but 20 MHz channels minimize CCI, ensuring a stable voice communication environment.

NOTE: The best practice recommendation for channel widths is to use the widest channel you can in your environment without introducing excessive channel interference on your network, it's a fine balance and a trade-off: wider channels mean faster data rates, but could also mean a poorer quality network.

6.2.4 Channel Planning

Effective channel planning is crucial for mitigating interference and optimizing performance. Utilize dynamic/automatic channel selection and radio resource management (RRM) features to avoid interference from neighboring networks automatically. Whenever feasible, avoid using Dynamic Frequency Selection (DFS) channels in the 5 GHz band to maintain stability as clients can not actively probe on DFS channels and they might take longer to discover Basic Service Set Identifiers (BSSIDs) on this frequency band.

NOTE: 20MHz is the minimum / smallest channel width you can configure and the safest option to minimize co-channel interference. You can still use your controllers RRM to dynamically assign the channels for your radios but not to dynamically change their channel widths to wider than the parameter you have set.

6.2.5 Layer 2 Roaming

Minimizing disruptions during device roaming is imperative for seamless voice sessions. Ensure voice clients stay within the same Layer[2] network as they move between access points. "Layer 2 roaming" refers to a network design where a wireless device, like a voice client, seamlessly moves between different access points while staying within the same Layer 2 network, meaning it maintains its VLAN and subnet, ensuring a smooth transition without experiencing any disruption in connectivity, particularly important for voice calls that require low latency. Crossing Layer 3 boundaries triggers DHCP/IP renewal, leading to disruptive delays in voice sessions.

6.2.6 Roaming Configuration

Leverage standards such as IEEE 802.11k-2008 [7] and IEEE 802.11r-2008 [8] to facilitate seamless voice client roaming between APs. This can streamline voice client roaming processes— IEEE 802.11k-2008 [7] provides neighbor reports, while IEEE 802.11r-2008 [8] ensures secure and fast handoffs—and enhances overall user experience.

2 Cisco Certified Expert, The Layer 2 Roaming Process, Jan 2024

6.2.7 Summary

Wi-Fi Calling is a critical service for all network environments, from the smallest offices to the largest stadiums. However, it's crucial to remember that proper RF design, strategic AP placement, Wi-Fi network configuration, and ongoing Wi-Fi network management are equally vital aspects of maintaining an efficient Wi-Fi Calling infrastructure. By implementing these recommendations, enterprises can optimize their Wi-Fi networks to deliver exceptional voice quality, seamless mobility, and uninterrupted voice sessions for users.

6.3. Improving Indoor Coverage

Achieving consistently reliable and high-speed indoor coverage isn't as straightforward as it might sound. Obstacles like walls, windows, and various building materials can attenuate radio signals and hamper propagation, while suboptimal AP placement, improper power level configurations, and interference from nearby networks or devices can further degrade indoor connectivity performance. Figure 8 explains why indoor performance is not optimal.

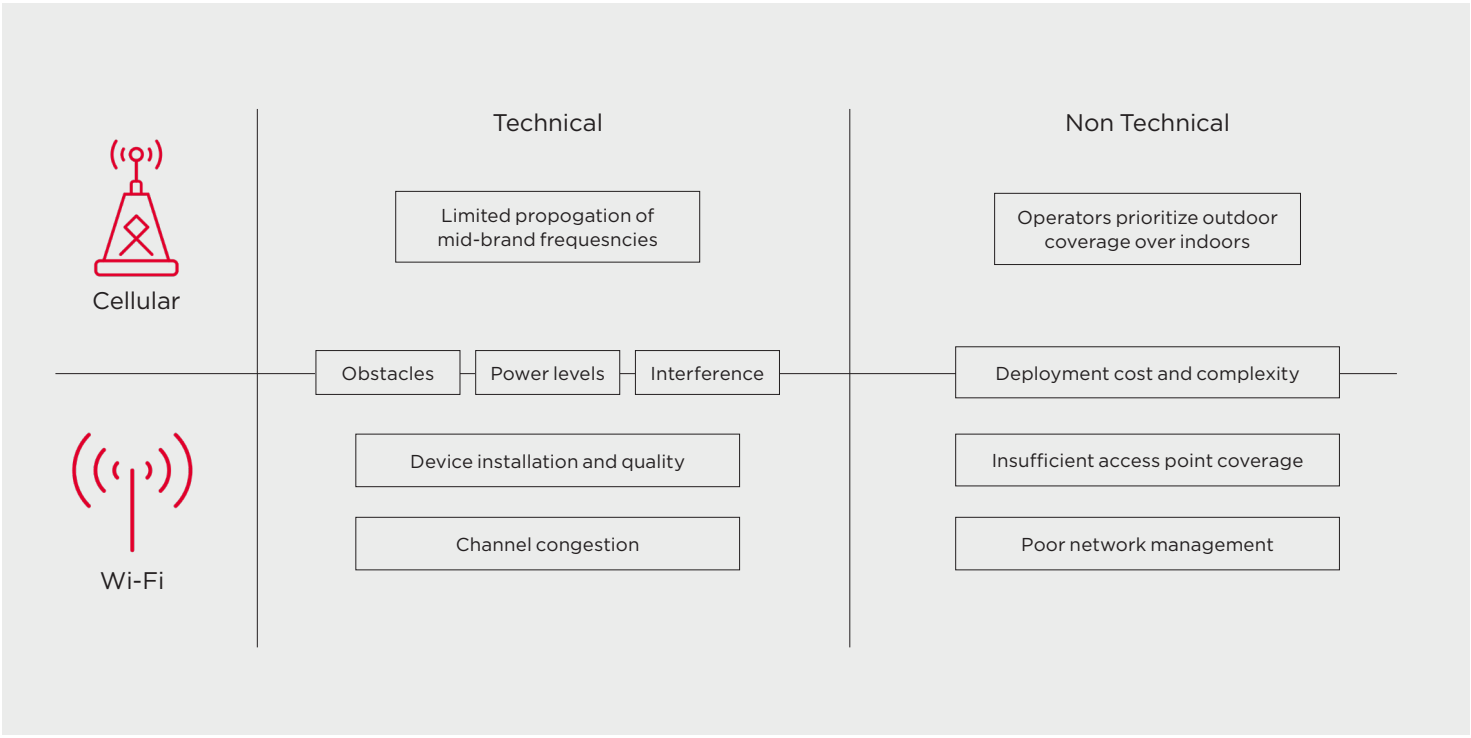


Figure 8, Technical and non-technical issues impacting cellular and Wi-Fi user experience

Figure 9 provides consideration for the improvement of indoor coverage.

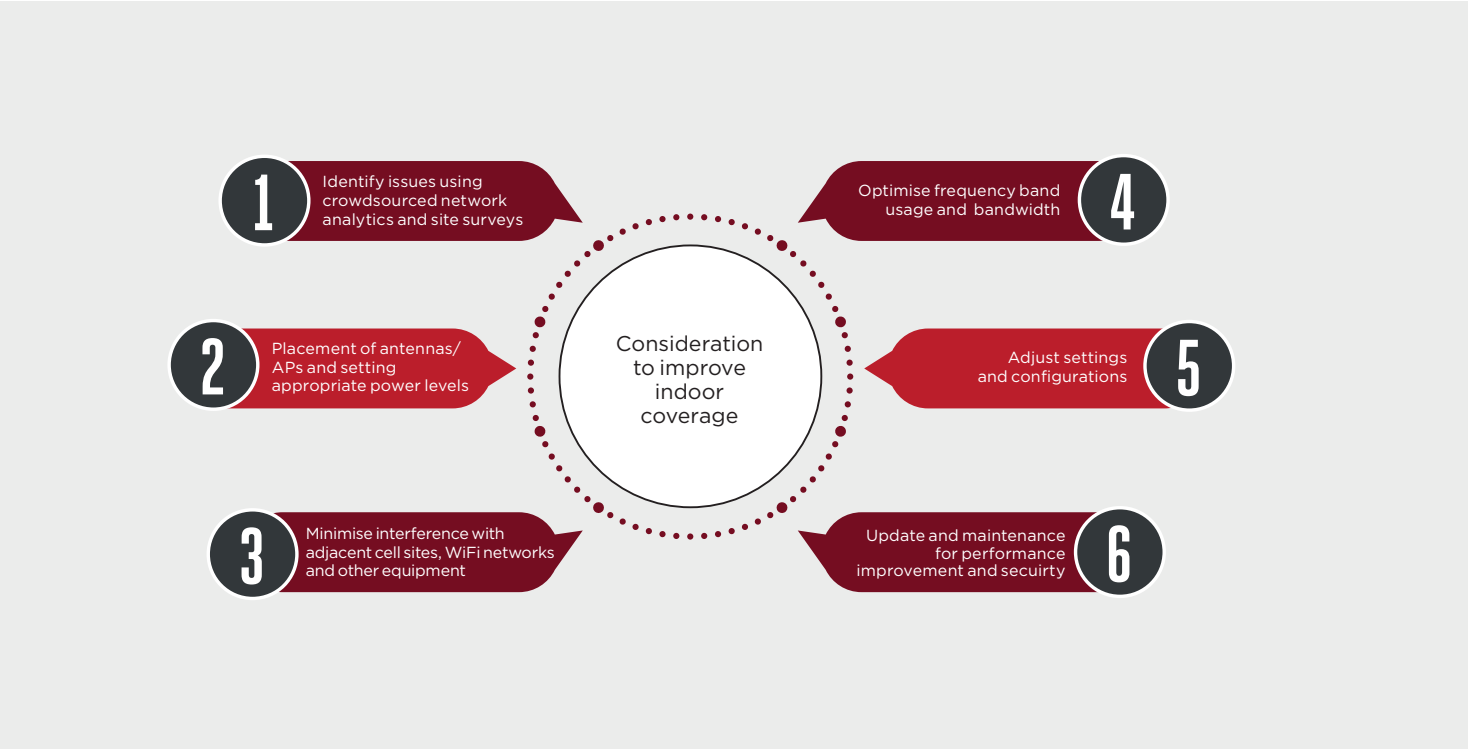


Figure 9, Consideration to improve indoor coverage

For improving Wi-Fi performance, consumers and enterprises could upgrade their APs to take advantage of newer technologies or deploy additional APs to extend coverage. However, to achieve the best performance improvements, operators and deployers should also consider different aspects such as the network's current gaps, weak signal areas, and sources of interference or poor performance before, during, and after the deployment of additional equipment:

1. They should proactively identify so-called "dead zones" in Wi-Fi and other network performance issues by leveraging crowdsourced data, site surveys, and capturing user feedback.
2. They should properly position antennas and APs for optimal coverage with appropriate power levels to areas with weak signal.
3. They should design a network that fits within the site-specific requirements for antenna placement and power distribution and minimizes interference with adjacent Wi-Fi networks and other equipment.
4. They should deploy frequency bands effectively, allocate adequate bandwidth for capacity, and minimize interference through techniques like channel bonding and DFS. "Channel bonding" in Wi-Fi refers to the practice of combining two or more adjacent Wi-Fi channels together to create a wider channel, essentially increasing the available bandwidth for data transmission, resulting in faster speeds.
5. They should optimize network parameters for specific use cases and environments, for example, by adjusting QoS policies and security protocols.
6. And finally, it is essential to regularly maintain the firmware on APs and connected devices to ensure optimal performance and minimize potential vulnerabilities. This involves allowing the AP is automatically run updates to make sure it has the latest improvements.

6.4 Wi-Fi Calling End-to-End QoS Strategy

As Wi-Fi Calling traffic flows over the home network and bearer network, which are IP-based and apply the best-effort model, the service experience of Wi-Fi Calling can deteriorate when there is network congestion. Hence, a mechanism to ensure end-to-end QoS of Wi-Fi Calling should be supported by the nodes involved in Wi-Fi Calling traffic processing including UE, AP, bearer network and ePDG. Wi-Fi Calling traffic can be identified by each node and differentiated from other data flows both on uplink (UL) and downlink (DL) directions, and higher service classes/tags should be allocated and resources prioritized for Wi-Fi Calling service. Figure 10 depicts a reference architecture for end-to-end QoS strategy of Wi-Fi Calling service.

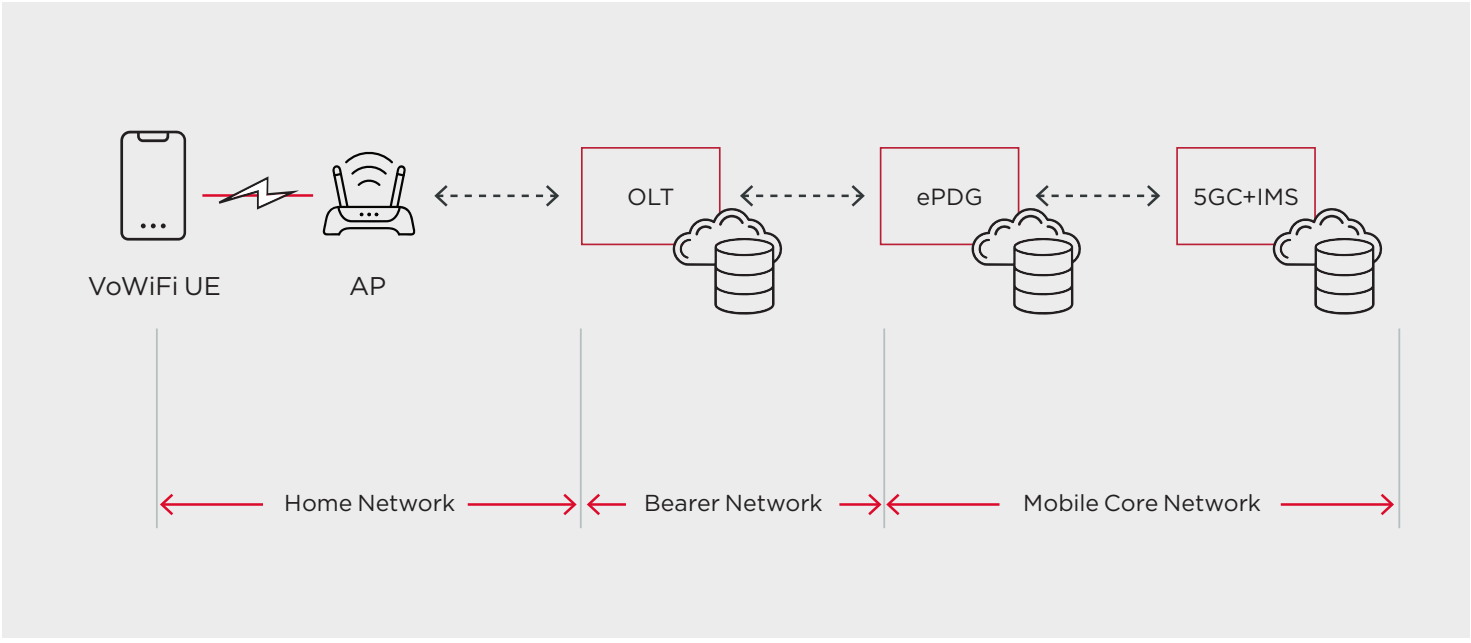


Figure 10, Reference network architecture for end-to-end QoS assurance of Wi-Fi Calling

Table 3 summarizes the identification and mapping of Wi-Fi Calling traffic. Both the AP and UE need to support differentiated services code point (DSCP[3]), otherwise this mechanism will not be applicable.

NOTE: End-to-end QoS mapping scheme for Wi-Fi Calling service at sea or in the air is for further study.

	UE	AP	BEARER NETWORK	ePDG
UL	Map differentiated services code point (DSCP) to Wi-Fi multiMedia (WMM)	Map DSCP to VLAN tag	Map VLAN tag into tags recognized by bearer network devices	Based on QoS class identifier (QCI) from 5GC
DL		Map DSCP to WMM	Map tags from bearer network into VLAN tag	Map QCI into DSCP

Table 3, Suggested mapping scheme of Wi-Fi Calling services

6.4.1 UE-side QoS Strategy

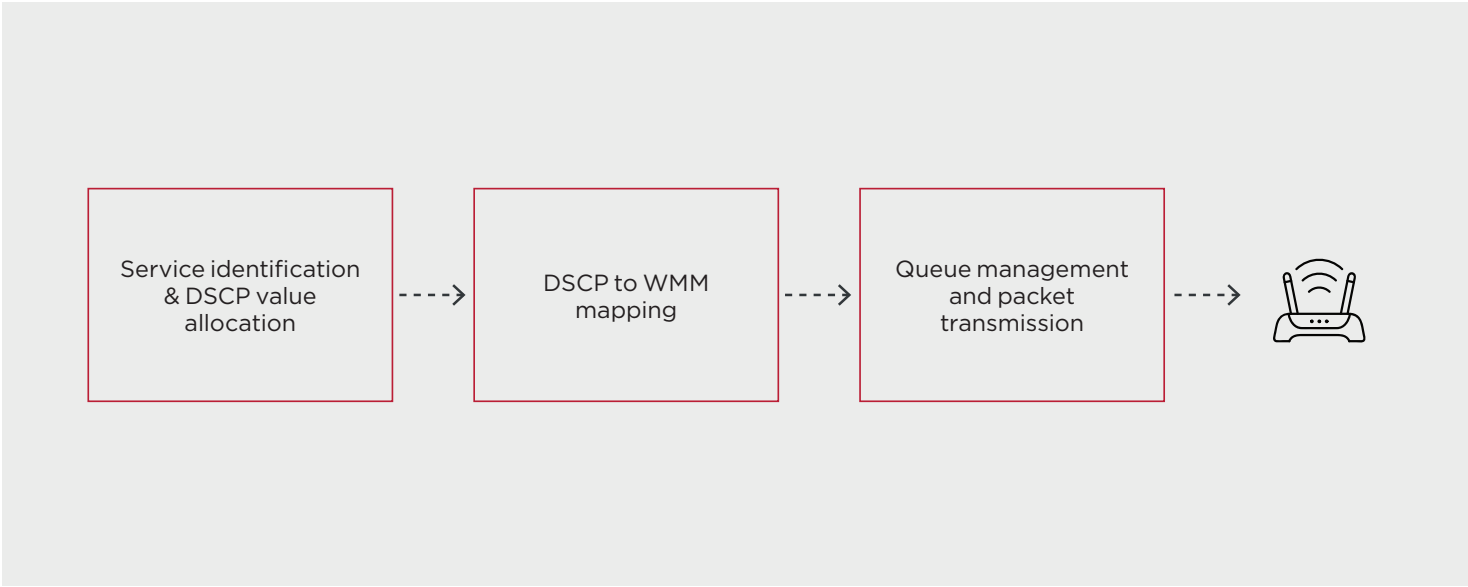


Figure 11, UE-side UL QoS solution

3 Some UEs and consumer grade APs do not support DSCP.

A UE-side UL QoS management mechanism is shown in Figure 11. It includes the following processes:

— Service identification and DSCP value allocation: The UE distinguishes different types of data for Wi-Fi Calling services, including voice, video and signaling, and allocates specific DSCP values to each type of data based on the DSCP classification of common services recommended in IETF RFC 4594 [9]. For example, Figure 3 in IETF RFC 4594 [9] recommends to assign a DSCP value of 46 for IP voice data, a value of 34, 36 or 38 for multimedia conferencing data and a value of 40 for signaling data. And Table 3 in GSMA PRD IR.34 [10] (Guidelines for IPX Provider networks) recommends to assign a DSCP value of 46 for conversational traffic class. Thus, for Wi-Fi Calling video calling, it is recommended to assign a DSCP value no less than 34 to ensure the smoothness of video calls.
— DSCP to WMM mapping: After the DSCP values are allocated, UE maps them to different access categories (AC) and user priorities (UP), which are specified in WMM to achieve Wi-Fi QoS Management. The mapping scheme between DSCP, UP and AC is specified in IETF RFC 8325 [11]. Based on IETF RFC 4594 [9], IETF RFC 8325 [11] and GSMA PRD IR.34 [10], a recommended mapping scheme of Wi-Fi Calling services is shown in Table 4. Note that for signaling, IETF RFC 8325 [11] recommends to configure UP value of 5 and AC value of AC_VI.
— Queue management and packet transmission: Wi-Fi Calling data packets are pushed into different queues according to different ACs. Packets are transmitted based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism with different channel access parameters set for different ACs in IEEE 802.11-2016 [12], which ensures a higher MAC layer transmission probability for high-priority queue.

WI-FI CALLING DATA CLASS	DSCP VALUE	UP	AC
Voice	46	6	AC_VO(voice)
Video calling	34/36/38/46	4/6	AC_VI(video)/ AC_VO(voice)
Signaling	40	5	AC_VI(video)

Table 4, Recommended mapping scheme of Wi-Fi Calling services

For DL Wi-Fi Calling data transmission, no additional optimization is required at the UE side.

6.4.2 AP-side QoS Strategy

For UL data transmission, AP receives packets from UE and recognizes the DSCP value in the packets. Then, AP adds the VLAN tag according to the mapping rules between DSCP and VLAN priority which is up to operators' configuration. In order to provide better QoS for Wi-Fi Calling service, higher-priority VLAN tags can be tagged for Wi-Fi Calling packets. For example, if AP detects a packet with a DSCP value of 46, it knows that this packet belongs to voice and then AP tags it with the highest priority (e.g., VLAN PRI in VLAN tag is set to 7). The AP then pushes packets into different VLANs in accordance with the VLAN tags and transmits them to the bearer network.

For DL data transmission, AP removes the VLAN header of DL packets and performs 'DSCP to WMM mapping' as well as 'queue management & packet transmission' procedures as describe in clause 6.4.1.

6.4.3 Bearer Network QoS Strategy

For UL data transmission, the edge device of the bearer network (e.g., optical line terminal (OLT)) receives the packets with VLAN tag from AP and re-encapsulates the packets with tags that can be recognized by bearer network devices. In order to identify Wi-Fi Calling traffic from others and provide differentiated QoS, the higher class of service (CoS) should be allocated. For example, 802.1Q-in-802.1Q (QinQ) CoS as described in IEEE 802.1ad-2005 [13] can be applied for layer 2 devices, and then QinQ CoS can be mapped to DSCP for layer 3 devices based on MNO's policy. Finally, the packets marked with DSCP are transferred to ePDG.

For DL data transmission, the packets marked with DSCP from ePDG should be identified and mapped in reverse sequence as in UL data transmission.

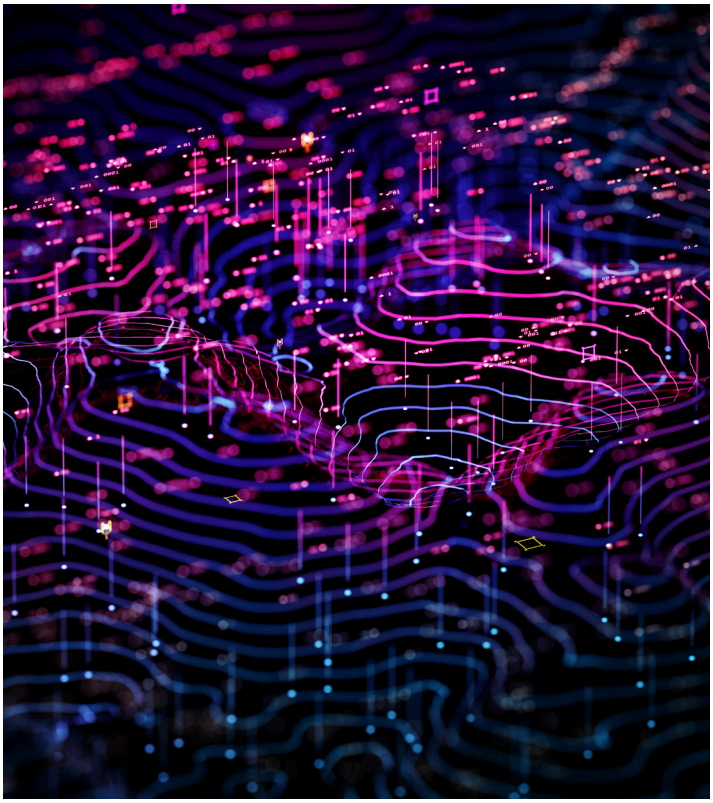
As Wi-Fi Calling traffic is marked with higher CoS, Bearer Network devices can identify and prioritize these traffic during forwarding, therefore, proper traffic models can be applied to provide sufficient bandwidth for Wi-Fi Calling services.

6.4.4 ePDG-side QoS Strategy

The PDN connection for Wi-Fi Calling service is provided by IPsec connectivity between the UE and the ePDG concatenated with S2b bearer(s) between the ePDG and the UPF/PGW-U. In IMS Call procedure, dedicated S2b bearers for audio (and video) is established on S2b with specified traffic flow templates (TFT, i.e. packet filters) and bearer QoS parameters (i.e. QCI, ARP, MBR, GBR).

A GTP tunnel on S2b transports the packets of an S2b bearer between the ePDG and the UPF/PGW-U. The ePDG stores the mapping between UL packet filters it receives from the SMF/PGW-C and the corresponding S2b bearer, then routes UL packets to the different bearers based on the UL packet filters. The UPF/PGW-U stores the mapping between DL packet filters and an S2b bearer, then routes DL packets to the different bearers based on the DL packet filters. The packets are transmitted according to the assigned QCI (and other Qos parameters) on S2b.

A SWu instance (i.e., a IPSec tunnel) transports the packets of all S2b bearers for the same PDN Connection between the UE and the ePDG. For DL packets from S2b interface to SWu interface, the ePDG may support the mapping from 3GPP QoS to DSCP marking. The mapping rules depend on operator policy. For UL packets from SWu interface to S2b interface, the ePDG forwards packets based on the UL packet filters to the corresponding bearer.



6.5 UE Optimized Handover Strategies

Wi-Fi Calling allows users to make voice calls via Wi-Fi networks, providing an alternative for traditional cellular networks. However, the environment in which Wi-Fi Calling operates is often complex and dynamic, involving multiple types of networks such as Wi-Fi, LTE, and NR. Hence the handover between different network types and coverage areas pose a significant challenge in maintaining call continuity and call quality, which emphasizes the critical importance of handover mechanisms.

Generally, the Wi-Fi Calling handover could be categorized into two types: Handover within the Wi-Fi Network, and Handover between Wi-Fi and Cellular Networks. UE should avoid call performance issues during handover, also could utilize the handover mechanism to solve the call performance issues.

6.5.1 Handover within the Wi-Fi Network: Out-Of-Service Timer

During moving between different Wi-Fi APs, a customized Out-Of-Service (OOS) timer can effectively help maintain the call continuity and reduce dropped calls.

Figure 12 shows a success case of the optimized strategy during handover, which is possible to happen in the environment without cellular coverage, e.g., on ships.

Normally UE should start an OOS timer when it has lost the connection with the original Wi-Fi AP. The OOS timer (if enabled) shall be configured with an appropriate value (which is based on the experiences of user's patience and usage scenarios, e.g., 20 - 30s for UE moving on the ships), meanwhile network side shall have a timer slightly longer than UE's OOS timer (e.g., 35s) to maintain the call session. In this way, UE will be able to have enough time to connect to the new Wi-Fi AP so that call drop issue can be avoided.

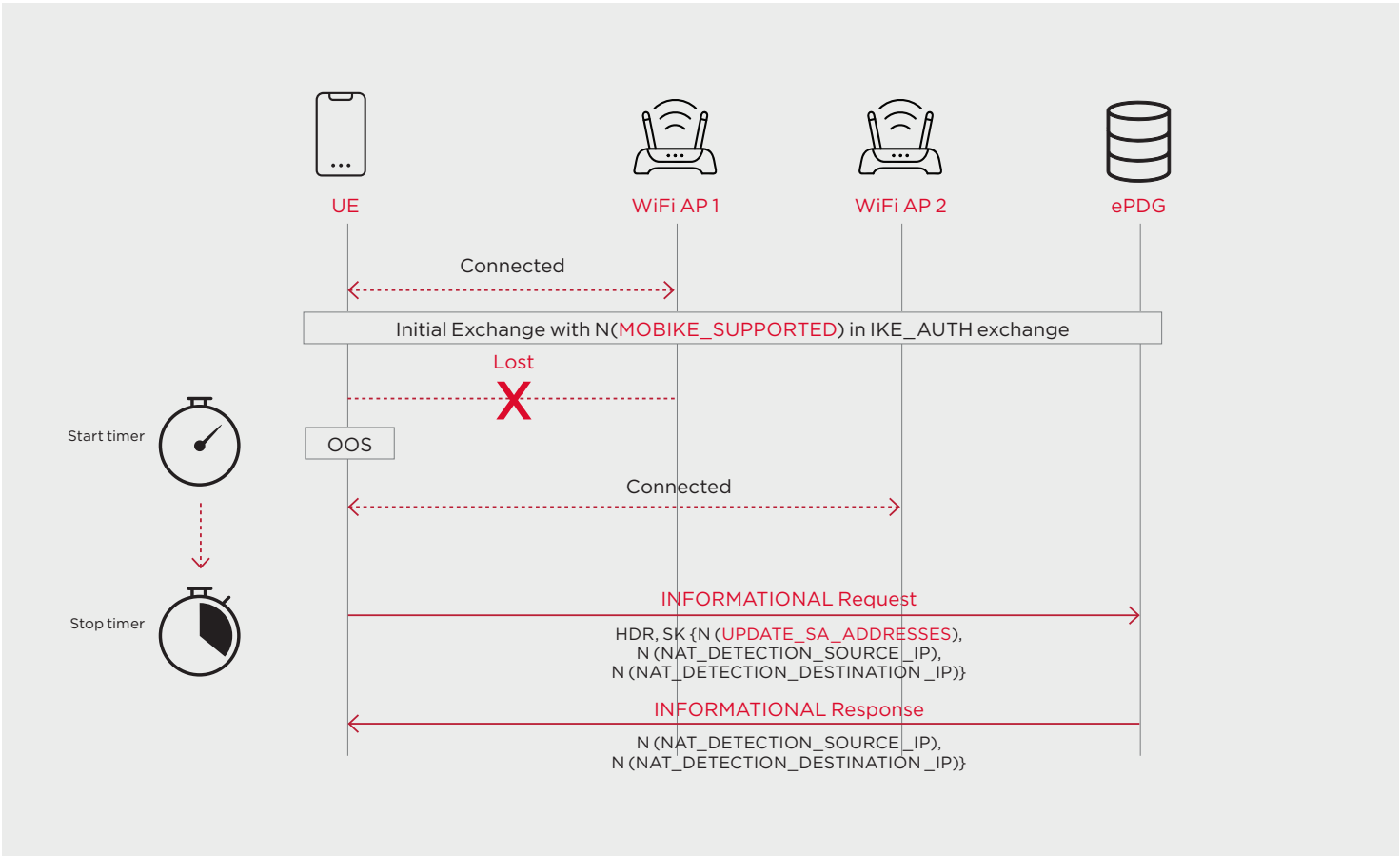


Figure 12, Handover within the Wi-Fi Network

6.5.2 Handover between Wi-Fi and Cellular Networks: QoE Mechanism

Reference Signal Strength Indicator (RSSI) and Reference Signal Received Quality (RSRQ) of Wi-Fi and cellular network are generally utilized to determine whether to handover to or from a Wi-Fi network, but other factors, such as network congestion in the Wi-Fi network may lead to poor voice call quality over Wi-Fi Calling. For this reason, only considering the RSSI/RSRQ thresholds for handover is not enough, combining with other factors, such as packet loss rate, uplink delay, round-trip time (RTT), channel load, to make a comprehensive judgment of the Wi-Fi network is needed. An evaluation of the quality of the Wi-Fi network should be used to dynamically adjust the thresholds for handover to/from Wi-Fi.

It is suggested to introduce the QoE parameter for Wi-Fi Calling handover. The QoE parameter is based on RSSI, packet loss rate, uplink delay, RTT, channel load and other parameters. When the QoE threshold meets the handover condition, then handover the voice call from Wi-Fi to cellular. The QoE mechanism for Wi-Fi is up to UE implementation. If any of parameters listed in Table 2 in section 6.1.5 for Wi-Fi network are considered unacceptable, then handover to cellular network should be considered.

Figure 13 shows a success case of the optimized handover strategy from Wi-Fi to cellular.

In this case, the Wi-Fi signal strength is not poor but network congestion occurs, e.g., one Wi-Fi AP is serving too many devices. The UE takes 'packet loss rate' into consideration for the handover decision. As the Real-time Transport Protocol (RTP) packet loss rate has exceeded a threshold and there is no other Wi-Fi AP could be connected, the UE triggers handover from Wi-Fi to Cellular and the voice quality becomes good again.

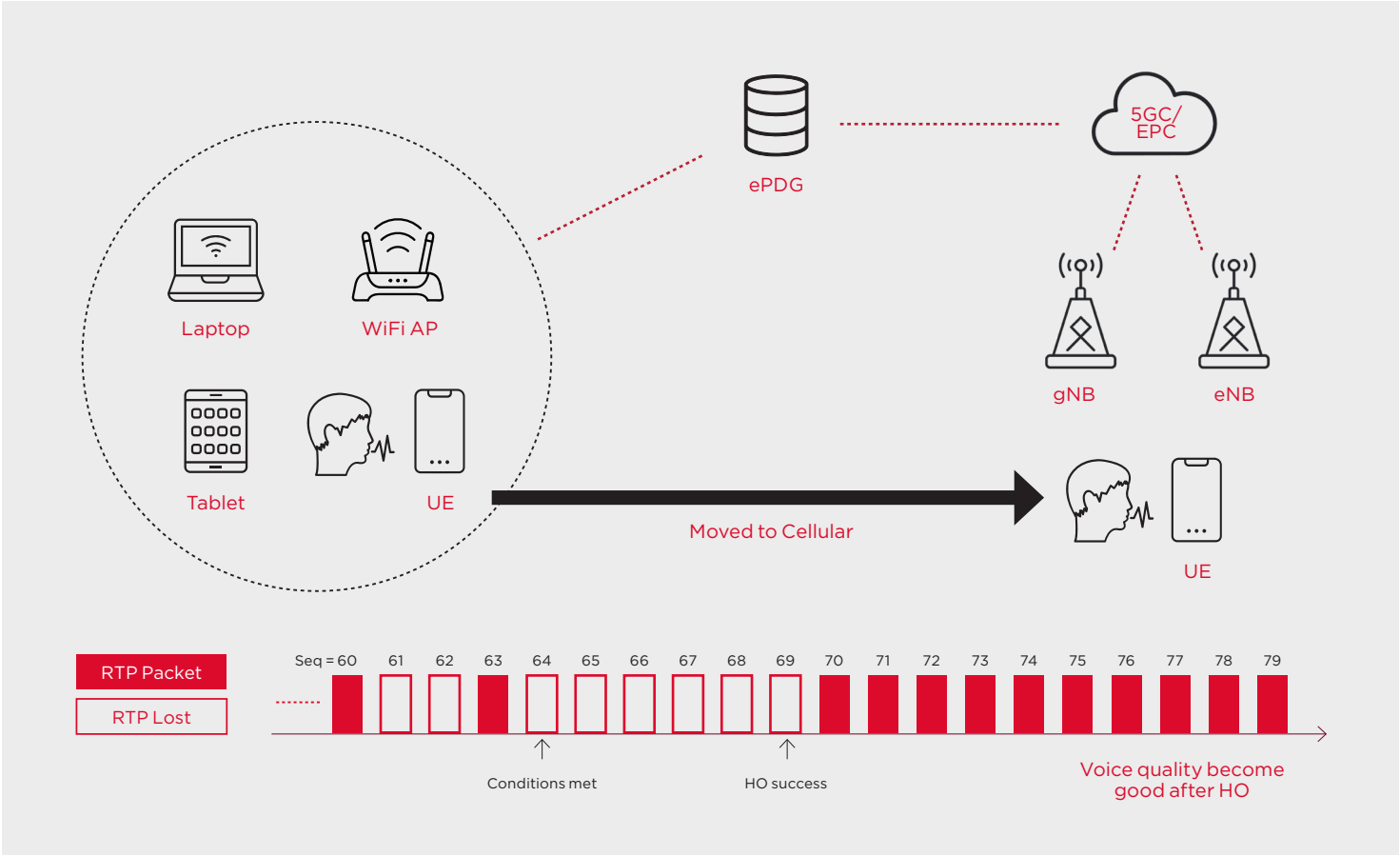
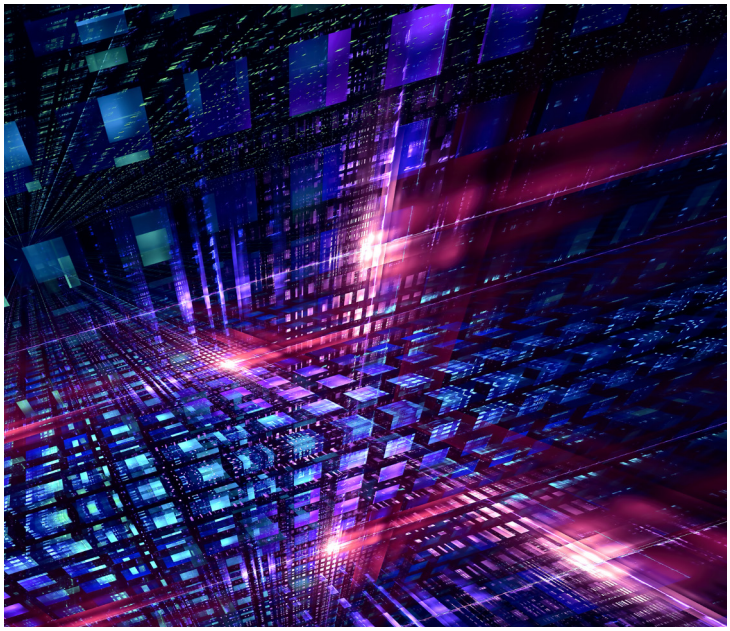


Figure 13, Handover from Wi-Fi to Cellular

6.5.3 Handover from Wi-Fi to Cellular: Avoid VoWiFi to VoNR Failure



In the scenario where the UE initially registers IMS voice over Wi-Fi and camps on NR Standalone (SA) simultaneously, if the UE moves away from the Wi-Fi hotspot, the handover condition will be met as the signal changes. However, handover action from VoWiFi to VoNR will fail if the network supports VoNR but does not support the handover between VoWiFi and VoNR.

For the above scenario, it is suggested to lower the priority of camping on NR SA during Wi-Fi Calling (e.g., prioritize camping on LTE to allow the UE switch to VoLTE). A success case is shown in Figure 14. With the priority of camping on NR reduced, the UE can successfully handover to LTE to ensure call continuity.

NOTE: The above handover strategy also applies to video call scenarios.

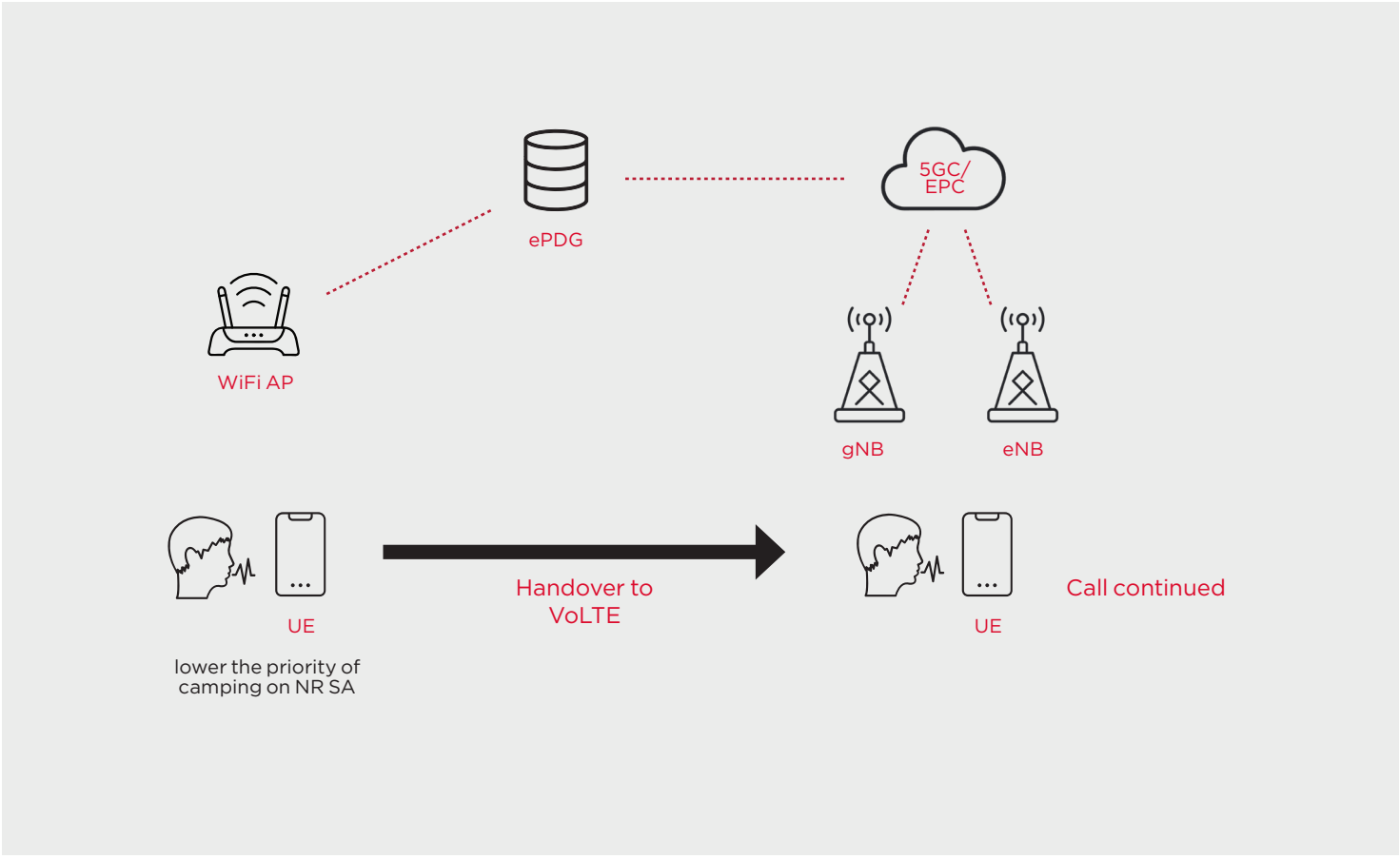


Figure 14, Handover from Wi-Fi to LTE with the priority of camping on NR reduced

6.6 User Location Acquisition at Sea / in the Air

The operator's Locator System stores the location information of users who access from the operator's own WLAN access network, including UE local IP address and port number (if NAT is detected), civic address information, and User Account information.

For scenarios in the air or at sea, the WLAN access network on an airplane or a ship is not provided by the operator itself. Thus, the Locator System will forward the Query-Location-Request message received from the ePDG to the Satellite Communication Platform to request the user location information, such as the Aircraft Identity or the Ship Identity to which the UE is attached. Acquisition of user location information during Initial Attach procedure is depicted in Figure 15.

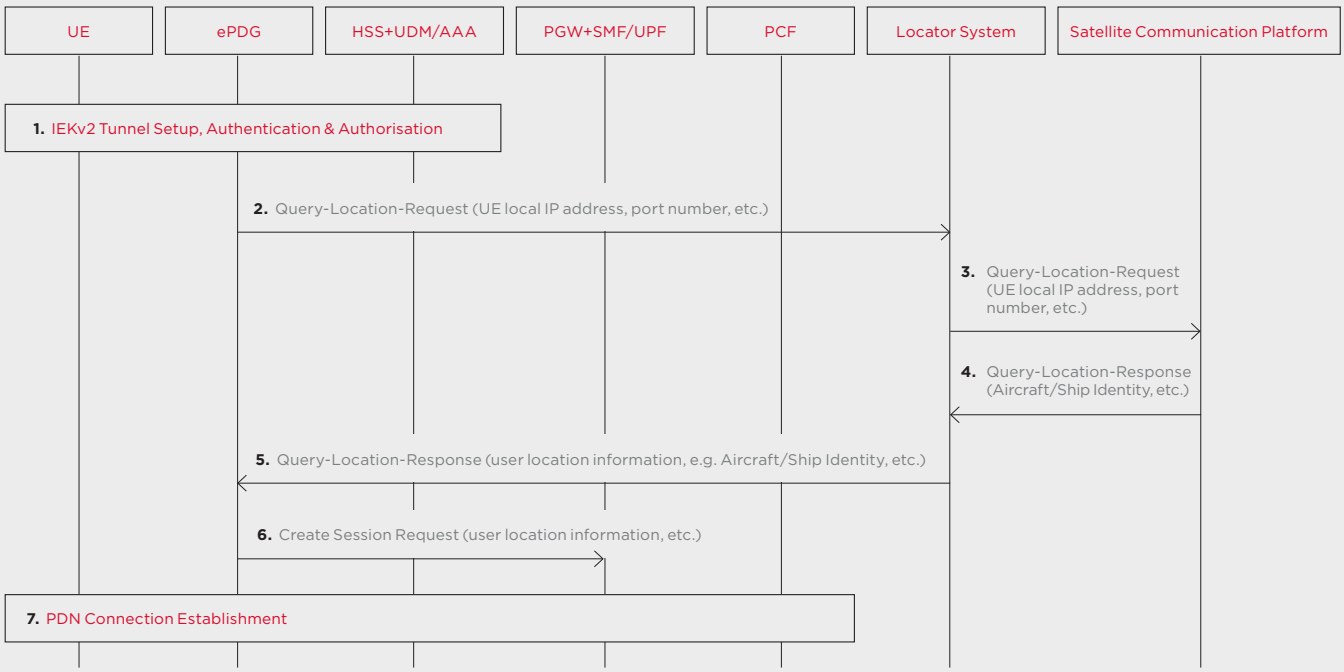


Figure 15, Acquisition of user location information during initial attach procedure

1. The UE starts the IKEv2 tunnel establishment procedure. The Authentication and Authorization procedure is executed between the UE and the 3GPP AAA Server via ePDG, as described in 3GPP TS 23.402 [4] section 7.2.4.
2. The ePDG sends Query-Location-Request message to the Locator System with UE Local IP and port number.
3. The Locator System forwards Query-Location-Request message to the Satellite Communication Platform.
4. The Satellite Communication Platform returns the Aircraft Identity or the Ship Identity to which the UE is attached.
5. The Locator System returns the user location information to the ePDG.
6. The ePDG sends a Create Session Request message to the PGW+SMF, including the user location information obtained from the Locator System.
7. The PDN connection is established by IPsec connectivity between the UE and the ePDG concatenated with S2b bearer(s) between the ePDG and the PGW+SMF/UPF, as described in 3GPP TS 23.402 [4] section 7.2.4.

Provision of user location information during IMS Call procedure is depicted in Figure 16. The SIP signaling in IMS Call procedure is as defined in 3GPP TS 23.228 [14] section 5.6 and 5.7. The Rx messages between P-CSCF and PCF are defined in 3GPP TS 29.214 [15] while the N7 messages between PCF and PGW+SMF are defined in 3GPP TS 29.512 [16].

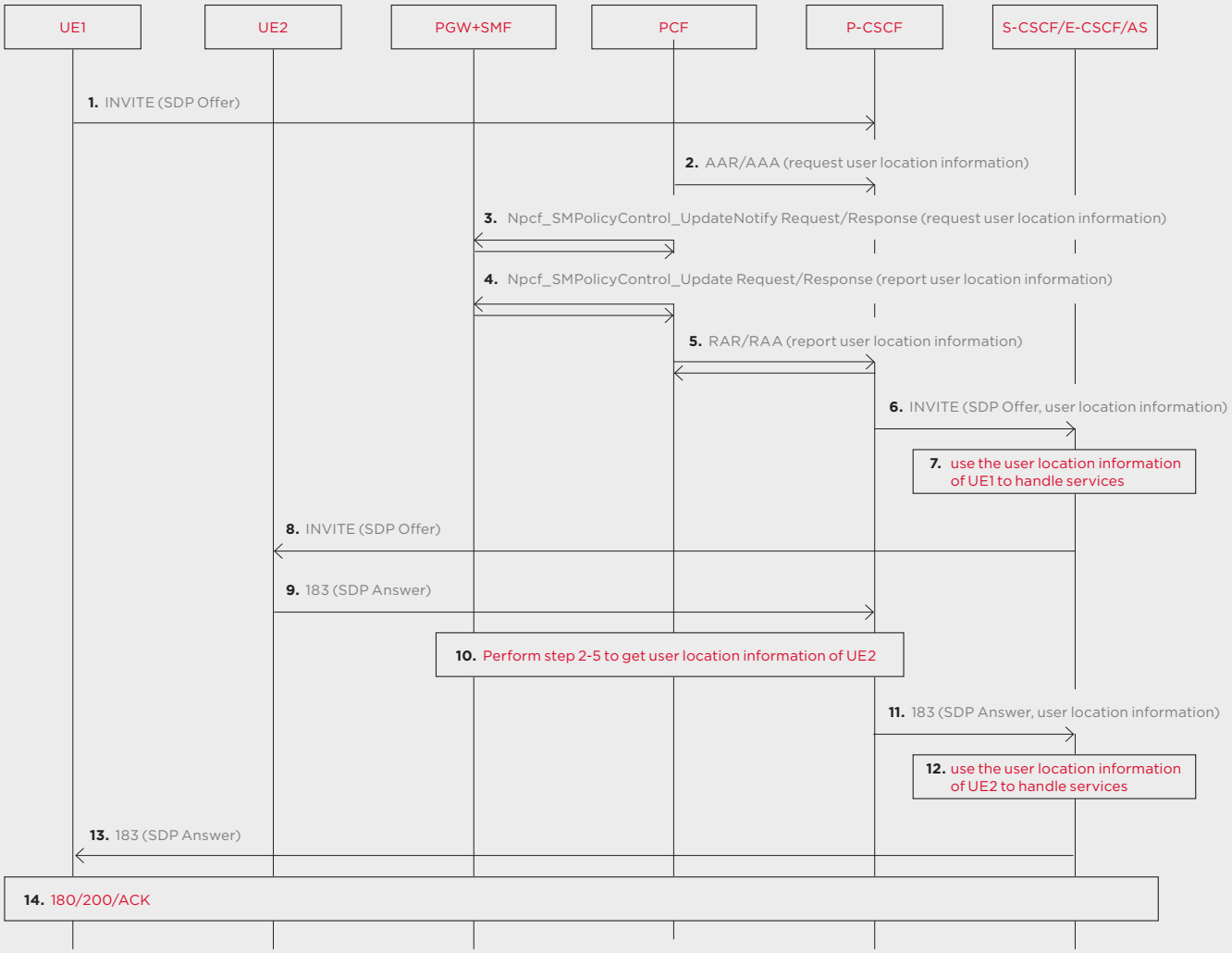


Figure 16, Provision of user location during IMS Call procedure

1. UE1 initiates an IMS call to UE2 via SIP INVITE message with SDP offer.
2. Upon receiving the INVITE message from the UE1, the P-CSCF sends AA-Request message to the PCF over Rx to request the user location information of UE1.
3. The PCF sends Npcf_SMPolicyControl_ UpdateNotify Request message to the PGW+SMF over N7 to request the user location information.
4. The PGW+SMF sends Npcf_SMPolicyControl_ Update Request message to report the user location information of UE1 which it has received from the ePDG during Initial Attach Procedure.
5. The PCF reports the user location information to the P-CSCF via RAR message.
6. The P-CSCF delivers the INVITE message to the S-CSCF/E-CSCF/AS by including the user location information within the P-Access-Network-Info header.
7. The S-CSCF/E-CSCF/AS may use the user location information to handle services. (e.g. The E-CSCF needs to route the emergency call request to a correct emergency centre based on accurate user location information.)
8. The INVITE message is sent to UE2.
9. UE2 returns SIP 183 message with SDP answer.
10. The step 2-5 is performed again for getting the user location information of UE2.
11. The P-CSCF delivers the 183 message to the S-CSCF/E-CSCF/AS by including the user location information of UE2.
12. The S-CSCF/E-CSCF/AS may use the user location information of UE2 to handle services.
13. The 183 message is sent to UE1.
14. The following SIP messages are performed to establish the call between UE1 and UE2.

6.7 Flexible Traffic Splitting Solution for Enriched Services

As shown in the use case of Wi-Fi Calling for IMS DC, the types of IMS services nowadays are becoming increasingly diverse, with bunches of data services via IMS DC in addition to audio and video, which may have differentiated requirements on QoS and data transmission. When network conditions change, some user traffic related to dedicated IMS services can be offloaded from 3GPP access to non-3GPP access path (e.g. Wi-Fi path), while other types of IMS services remain on the 3GPP access path. For instance, traffic of video and IMS DC services can be offloaded to the Wi-Fi path, leaving audio traffic on 3GPP access network. Another similar case is also applicable to IMS DC services (e.g. offloading the IMS DC file transfer service to the Wi-Fi path while keeping the IMS DC real-time translation service on the 3GPP access path). Moreover, even traffic from the same IMS DC service may be split into multiple access paths.

As per 3GPP TS 23.502 [17] clause 4.22.1, a Multi-Access (MA) PDU Session may be a PDU Session associated with one 3GPP access and one non-3GPP access both connected to 5GC, or a PDU Session associated with one 3GPP access connected to Evolved Packet Core (EPC) and one non-3GPP access connected to 5GC, or a PDU Session associated with one non-3GPP access connected to EPC and one 3GPP access connected to 5GC. Figure 17 below shows one typical traffic splitting scenario for IMS DC Service. PGW-C + SMF and UPF + PGW-U are dedicated for interworking between 5G System (5GS) and EPC. The entire IMS network can be treated as a Data Network without awareness of how traffic is split between 3GPP access and non-3GPP access.

As defined in 3GPP TS 23.501 [3], for uplink traffics, Access Traffic Steering, Switching and Splitting (ATSSS) rules are provided to or preconfigured in the UE, which indicate how the uplink traffic should be routed across 3GPP access and non-3GPP access. Then UE can apply the ATSSS rules, using the Application descriptors and/or IP descriptors to identify the application traffic. For downlink traffics, N4 rules are provided to the UPF, which indicate how the downlink traffic should be routed across 3GPP access and non-3GPP access. The UPF can apply the Packet Detection Rule (PDR) to detect packets and identify the application traffic, then handle the traffic with corresponding Multi-Access Rule (MAR).

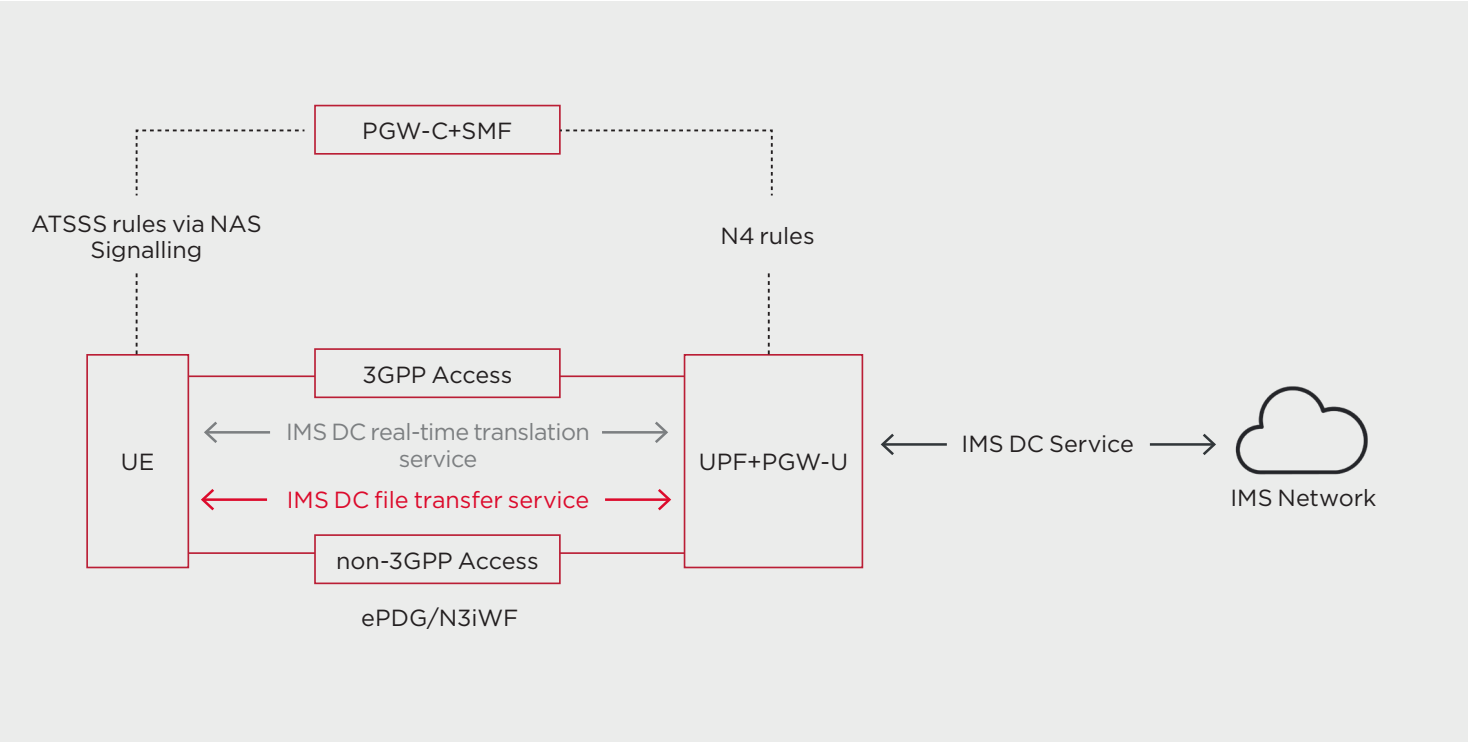
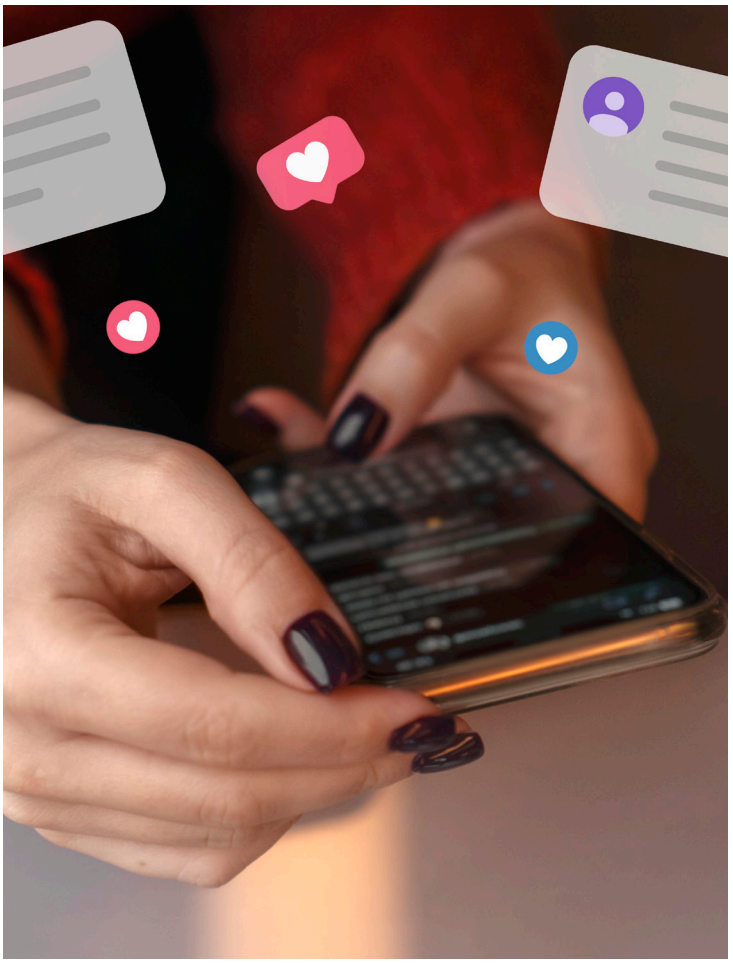


Figure 17, IMS DC Service traffic splitting

However, when it comes to different IMS services, they are all treated as the same service (i.e. IMS Communication Service) to 3GPP core network, and the application descriptor used in the SIP-level is not visible to the core network either, which means the current mechanism may not be able to identify different IMS services (e.g. audio, video, data) and further different IMS DC services at 3GPP core network side. At the UE side, although there are application descriptors and IP descriptors in the ATSSS rules, the application descriptors always reflect as OS specific Application Identifier (OSAppId) without any association with specific IMS services, and different IMS DC services always present the same IP address but dynamic ports which cannot be reflected in the preconfigured ATSSS rules.

Based on the above gap analysis, the following enhancements might be required:

— The optimization for the traffic descriptor in ATSSS rule and Application identifier in PDR to identify the IMS services with finer granularities;
— Interworking between IMS and 3GPP core network on dynamical service/application related data (e.g. application identifier, port number, etc.) transmission of specific IMS services and IMS DC services.



6.8. Security Considerations

There are a number of different security aspects associated with the Wi-Fi Calling service which need to be considered:

— **UE security** including protection against device hacking and malicious applications;
— **Wi-Fi Calling access security** including protection against VoWiFi user account takeover, eavesdropping or tampering of traffic;
— **Wi-Fi Calling and SIP signalling security** including protection against message injection and message eavesdropping attacks;
— **Network infrastructure security and Interconnect security** including protection against attacks from a compromised UE and compromised ePDG;
— **Fraud considerations** including protection against International Revenue Share Fraud (IRSF).

For further details, see Annex B.

6.9. Interworking between 3GPP and Non-3GPP Networks

The seamless integration of cellular and WLAN technologies is critical for maintaining service continuity and enhancing user experience, especially for services like Wi-Fi Calling. When signal changes and triggers the handover between 3GPP and non-3GPP, PDU session or PDN connection should not release. Handover of a PDU Session or PDN connection procedure between untrusted/trusted non-3GPP and 3GPP access have been defined in 3GPP TS 23.502 [17] and 3GPP TS 23.402 [4]. Meanwhile, GSMA PRD IR.51 [18] and GSMA PRD NG.115 [19] have also specified handover scenarios that UE or network must support to guarantee the voice continuity between cellular and WLAN access and introduced the management objects parameters as specified in 3GPP TS 24.167 [20]. The management objects are used to indicate to the UE which type of handover of IMS PDN connections between non-3GPP and 3GPP access network are allowed, such as Allow_Handover_PDN_connection_non-3GPP_and_NG-RAN, and Allow_Handover_PDN_connection_WLAN_and_EPS. These handover capability parameters can either be pre-configured or updated in the UE via an over the air (OTA) upgrade.

However, the interoperability policies between 5GS, Evolved Packet System (EPS) and WLAN can differ significantly across various operators and roaming areas, leading to potential service disruptions and compatibility challenges. In addition, the existing solution for UE to obtain the updated interoperability policies based on terminal manufacturer customization and OTA updates is difficult to ensure timely information updates, and can lead to compatibility issues and heavy testing work.

To mitigate these issues and ensure a more robust and adaptive network interworking, introducing explicit indication of interworking policy will be helpful. Specifically, the 3GPP and non-3GPP interworking policy should be provided by cellular network and/or Wi-Fi network as defined in GSMA PRD TS.63 [21]:

1. When UE access to 5GS, the interworking policy may involve:
    - Whether handover to EPC/ePDG is supported
    - Whether handover to N3IWF is supported
2. When UE access to EPS, the interworking policy may involve:
    - Whether handover to EPC/ePDG is supported
    - Whether handover to N3IWF is supported
3. When UE access to N3IWF, the interworking policy may involve:

Whether handover to EPS is supported

    - Whether handover to 5GS is supported
4. When UE access to EPC/ePDG, the interworking policy may involve:
    - Whether handover to EPS is supported
    - Whether handover to 5GS is supported

By implementing these interworking capability indications, the UE's handover decision can be more feasible, thereby improving the reliability and performance of Wi-Fi Calling services.

6.10 Regulatory Aspects of Wi-Fi Calling

This section covers the following regulatory aspects of Wi-Fi Calling:-

- ePDG Selection,
- Emergency Calling,
- Lawful Interception (LI)

6.10.1 ePDG Selection

3GPP has defined the regulatory and operator requirements for the ePDG selection procedure for non-emergency services in 3GPP TS 23.402 [4] clause 4.5.4. In essence, the UE shall:

- select an ePDG in its HPLMN for the non-roaming scenario,
- select an ePDG in the VPLMN for the roaming scenario,
- select an ePDG in the HPLMN for the roaming scenario when not registered to a 3GPP RAN in the VPLMN and there is no ePDG available in the VPLMN.

The means of determining each of the ePDG FQDNs are defined in 3GPP TS 23.402 [4] clause 4.5.4.

6.10.2 Emergency Calling

Smartphones give priority to 3GPP networks on initiating an emergency call when both 3GPP and Wi-Fi networks are available. If there is no 3GPP network available, then emergency calling can be initiated via Wi-Fi and 3GPP has defined procedures for the provision of emergency call via Wi-Fi in 3GPP TS 23.402 [4] clause 4.5.7.2.

In this scenario, the UE shall select an emergency ePDG as described in 3GPP TS 23.402 [4] clause 4.5.4a. Emergency calls must be completed in the country where the UE is located. In the HPLMN, the UE can be provided with a FQDN for the emergency ePDG. In the more general case, if this FQDN is not provided or if the UE is roaming, then the UE shall construct an emergency Visited Country FQDN as specified in 3GPP TS 23.402 [4] clause 4.5.4a.

Emergency calling is also possible for UE's in limited service state (e.g. no SIM, unauthenticated SIM etc.) and will be completed via so-called anonymous IMS emergency call as specified in 3GPP TS 24.229 [22] clause 5.1.6.8.2 and profiled in GSMA PRD IR.92 [23] section 5.2.1.

6.10.3 Lawful Interception

Lawful Interception (LI) is applicable to Wi-Fi Calling.

Based on regulations of the country where the UE is located, SIP signalling data and voice media shall be accessible to the authorities in that country.

For the roaming scenario, null IMS encryption shall be used by the HPLMN as specified in 3GPP TS 33.203 [24] and profiled in GSMA PRD IR.92 [23] section 5.2.

7. Business Models

There are a variety of use cases for Wi-Fi Calling as described in Section 4, which can be categorized into Wi-Fi Calling on the ground, Wi-Fi Calling at sea and Wi-Fi Calling in the air. As to the deployment and monetization of these use cases, there are a variety of business models to choose from, which will require more cooperation between MNOs and their business partners, and bring new requirements for MNO's network and billing system.

For the use cases of Wi-Fi Calling on the ground, Wi-Fi Calling is deployed as an effective tool to improve poor cellular coverage with lower cost, especially in some compact settlement areas in the city and some remote areas in the countryside.

By expanding Wi-Fi Calling use cases to no cellular coverage scenarios at sea or in the air, various value propositions are emerging, along with some new requirements:

- Billing based on differentiated QoS: Wi-Fi service at sea or in the air are provided by satellite links, which are quite limited in bandwidth and therefore costly to maintain a good quality of Wi-Fi Calling. More bandwidth and higher priority of IMS voice/video flows should be allocated to ensure a better quality of experience for specific customer with higher Service Level Agreement(SLA). For billing system, charging should be differentiated on the basis of the SLA with customer. For the network, mechanism to provide differentiated QoS for IMS voice/video flows via satellite links should be supported.
- Billing based on scenarios: MNOs may implement a tiered pricing model for various usage scenarios considering factors like the costs of Wi-Fi Calling provision, customer segments. The billing system should fetch the corresponding Ship/Flight Identity and/or associated geolocation, and be able to distinguish different scenarios and apply differentiated charging accordingly.
- Flexible subscription process: Wi-Fi Calling service subscription varies for use cases at sea or in the air. Pre-subscription of Wi-Fi Calling is applicable for crews on law enforcement vessels and offshore support vessels, while personal customers may like to subscribe Wi-Fi Calling on demand, for example, by scanning a QR code with their smart phone after boarding a cruise ship or a plane. It is required that flexible subscription process and access-control mechanism be supported by MNO's system.

Annex A provides some examples for understanding these business models and the monetization of Wi-Fi Calling services.

8. Trials

This section provides details of assorted trials of Wi-Fi Calling for different use cases.

8.1 Trials on the Ground

From 2023 to 2024, China Telecom collaborated with multiple terminal manufacturers to initiate a series of Wi-Fi Calling pilot projects, and proposed a converged network solution of 5G SA and Wi-Fi Calling that supports smooth handover between Wi-Fi Calling and VoNR/VoLTE. The pilot results are as follows:

— The deployment of Wi-Fi Calling has significantly improved the service coverage and calling performance of users in scenarios with poor cellular coverage. Test results for the trials users in typical scenarios such as chain hotels, basements, and rural areas are shown in Figure 18. It can be seen that after Wi-Fi Calling was supported, the average service coverage rate increased by 35.7%, and the average call success rate increased by 21%. Finally, the average MOS in these areas increased by 50%.

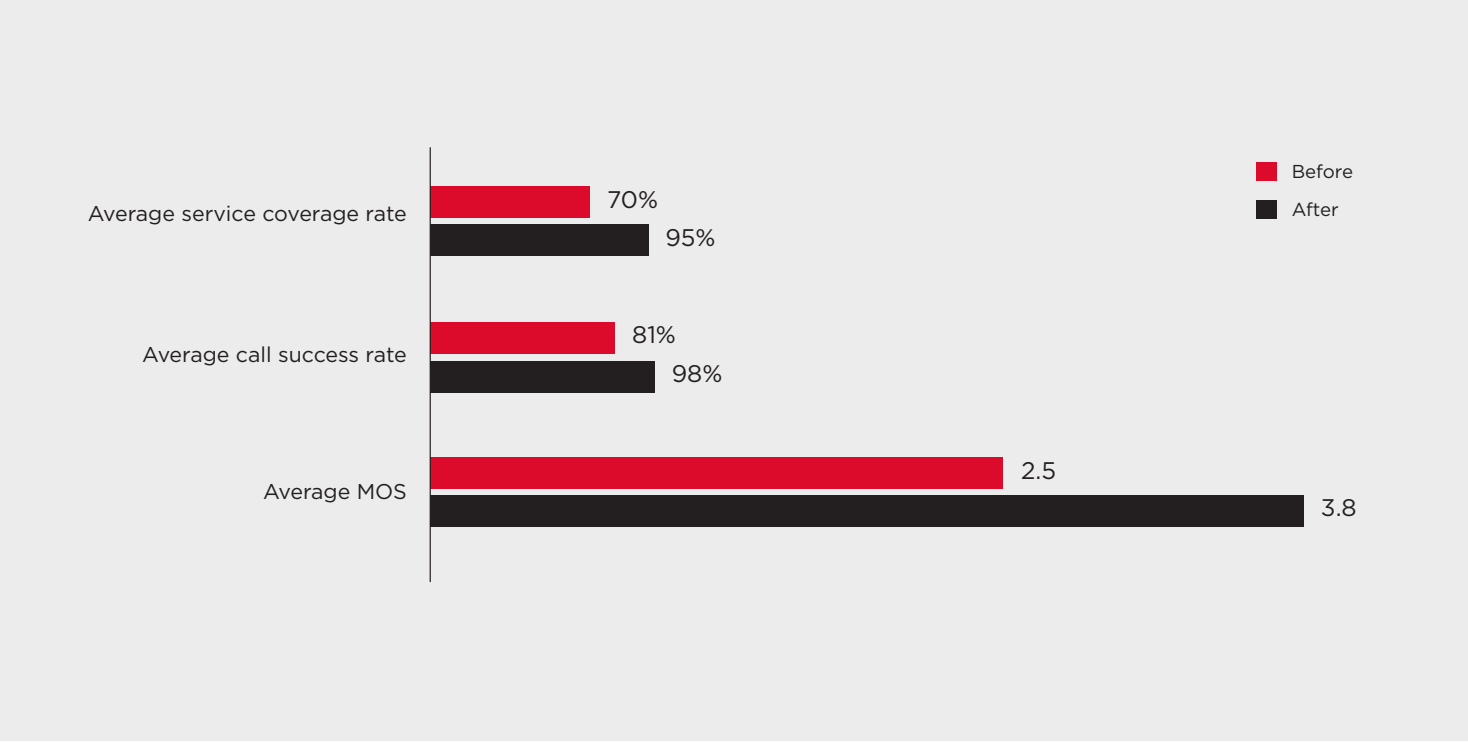


Figure 18, Calling performance for the trial users: Before vs. After deployment of Wi-Fi Calling

— The performance of Wi-Fi Calling calls is compared to traditional cellular calls with the voice quality, handover delay results and call setup time (Mobile Originate, MO) based on the field test data and network operational metrics shown in Table 5.
— Wi-Fi Calling effectively increased user retention and satisfaction. According to statistical data, the average daily Wi-Fi Calling registration duration of a single user was about 1.85 hours, and the average daily Wi-Fi Calling call time of a single user reached 16.8 minutes, accounting for 15% of the total daily call time. The total call time of the trials users in the pilot increased by 5.62% after Wi-Fi Calling was supported. Furthermore, the follow-up surveys of 1099 Wi-Fi Calling users showed that 80% of the users experienced improvements in signal and call quality.

TESTING ITEMS	WI-FI CALLING	VoLTE
MOS	>3.5	>3.5
Intra-system handover delay	~100ms	~70ms
Inter-system handover delay	~100-300ms	100ms-200ms
Call Setup time (MO)	~1900ms	~2200ms

Table 5, Wi-Fi Calling performance vs. VoLTE performance

8.2 Trials at Sea

Commencing in May 2024, China Telecom has conducted maritime pilots and trials in collaboration with maritime law enforcement clients. In this pilot, satellite equipment was deployed on the law enforcement vessel to provide Wi-Fi coverage, and mobile phones were able to access the network provided via the APSTAR-6D satellite system with connectivity to the network ePDG. The test results are as follows.

— Wi-Fi Calling service can be used normally at sea. Functional tests show that the registration of Wi-Fi Calling services, the use of voice, video, message services, as well as handover between Wi-Fi and cellular networks on the shore can all be supported.
— Wi-Fi Calling can effectively meet the communication needs at sea. Performance testing results in Table 6 indicate the MOS and user performance, confirming the reliability and efficiency of Wi-Fi Calling services at sea.

TESTING ITEMS		RESULTS
Ping delay		610 ms
Data rate (UL/DL)~100ms		1/2 Mbps
Voice/ Video call	MOS (average/maximum)	3.4/4.3
	Connection delay	4-5 s
	Connection rate	100%
	User experience	Similar to that on land via satellite

Table 6, Wi-Fi Calling performance testing results at sea

9. Conclusions

As an alternative network access technology, Wi-Fi Calling complements cellular coverage, providing a cost-effective solution for operators to offer high-quality voice services to users, even in areas with no cellular network coverage.

In terms of future development and research trends, the expansion of Wi-Fi Calling into scenarios in the air and at sea is an exciting frontier. The implementation of Wi-Fi Calling on ships and airplanes can facilitate the breaking down of communication barriers, not only enhancing the convenience and safety in these environments for users but also creating new business opportunities for operators.

The integration of Wi-Fi and cellular network can evolve to support high bandwidth, interactive, intelligent IMS services. For example, for IMS DC services, users can transfer files and use AI services smoothly during voice calls, even in no cellular coverage, via Wi-Fi Calling. Furthermore, flexible and differentiated traffic offloading policies for different services between 3GPP and non-3GPP accesses, such as IMS DC, voice, data, can lead to improved user experience.

End-to-end QoS assurance mechanism can effectively address low-clarity and stuttering in some Wi-Fi Calling video calls on land, and provide priority guarantee for Wi-Fi Calling calls in the air or at sea. Post publication of this White Paper, the GSMA 5G Wi-Fi Calling Task Force plans to conduct a joint Wi-Fi Calling end-to-end QoS proof of concept (POC) with WBBA. The results from this POC may be shared in a future White Paper.

As Wi-Fi Calling evolves, ensuring its security remains a top priority. Robust encryption protocols and authentication mechanisms must be developed to protect user privacy. And solutions to safeguard against potential threats caused by ePDG exposure to the public network should be studied.

Wi-Fi Calling plays a vital role in the future of converged 3GPP and non-3GPP access to operator services. The continuous exploration and innovation in areas such as Wi-Fi Calling in the air and at sea, innovative Wi-Fi Calling services, flexible traffic splitting solutions, end-to-end QoS assurance, QoE considerations for handover, and security considerations, will facilitate the redefinition of communication boundaries and the advent of a new era of seamless, immersive, and secure voice and data services.

Acknowledgments

Thanks are extended to the following companies and organisations that contributed to the successful completion of this White Paper.

— China Telecom
— Honor
— Mediatek
— Ookla
— Telstra
— Wireless Broadband Alliance
— WBBA

The above are listed in alphabetical order and does not represent any other ranking.

Glossary

Term	Description
3GPP	Third Generation Partnership Project
4G	4th Generation (of Mobile Technology)
5G	5th Generation (of Mobile Technology)
5GC	5G Core (Network)
AAA	Authentication, Authorisation & Accounting
AC	Access Category
AC_VI	AC_Video
AC_VO	AC_Voice
AI	Artificial Intelligence
AKA	Authentication & Key Agreement
AMF	Access & Mobility Management Function (part of 5GC)
AP	Access Point
AR	Augmented Reality
ARP	Allocation, Retention & Priority
AS	Application Server (part of IMS)
ATG	Air to Ground
ATSSS	Access Traffic Steering, Switching and Splitting
BBF	Broadband Forum
BS	Base Station
BSSID	Basic Service Set Identifier
CCI	Co-Channel Interference
CDR	Call Detail Record
CN	Core Network

Term	Description
CoS	Class of Service
CSCF	Call Session Control Function (part of IMS)
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
dBm	Decibels (relative to 1 millewatt)
DC	Data Channel
DDoS	Distributed Denial of Service (attack)
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DMZ	De-Militarized Zone
DNS	Domain Name System
DSCP	Differentiated Services Code Point
E-CSCF	Emergency CSCF
eNodeB	Evolved Node B (4G RAN)
EPC	Evolved Packet Core (4G Core)
EPS	Evolved Packet System (4G)
ePDG	Evolved Packet Data Gateway
FWA	Fixed Wireless Access
GB	Giga Bytes
GBR	Guaranteed Bit Rate
GHz	Giga Hertz
GPRS	General Packet Radio Service
GSMA	GSM Association
GSM	Global System for Mobile (Communication)

Term	Description
GTP	GPRS Tunneling Protocol
H.248	ITU-T Signalling Recommendation for media gateway control
HSS	Home Subscriber Server (part of EPC)
HSS+UDM	Hybrid HSS & UDM (part of hybrid EPC/5GC)
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	IP Security
ISP	Internet Service Provider
ITU-T	International Telecommunications Union (Telecommunications)
LAN	Local Area Network
LI	Lawful Interception
LTE	Long Term Evolution
MA	Multi Access
MAC	Media Access Control
MAR	Multi-Access Rule
Mbps	Mega bits per second
MBR	Maximum Bit Rate
MHz	Mega Hertz
MME	Mobility Management Entity (part of EPC)
MNO	Mobile Network Operator
MO	Mobile Originate

Term	Description
MOS	Mean Opinion Score
MS	Milleseconds
N3IWF	Non-3GPP Access Interworking Function (part of 5GC)
NAT	Network Address Translation
NG	Next Generation
NR	New Radio
NTN	Non-Terrestrial Networks
OAM	Operations, Administration and Management
OLT	Optical Line Terminal
OOS	Out of Service
OSAppId	OS specific Application Identifier
OTA	Over the Air
PCF	Policy Control Function (part of 5GC)
PCRF	Policy, Charging and Rules Function (part of EPC)
P-CSCF	Proxy CSCF
PDN	Packet Data Network
PDU	Packet Data Unit
PDR	Packet Detection Rule
P-GW	PDN Gateway (part of EPC)
PGW-C+SMF	Hybrid PGW-C & SMF (part of hybrid EPC/5GC)
PGW-U+UPF	Hybrid PGW-U & UPF (part of hybrid EPC/5GC)
PGW-C	P-GW Control Plane
PGW-U	P-GW User Plane
QCI	QoS Class Identifier
QinQ	Queue in Queue

Term	Description
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RFC	Request for Comments (an IETF document)
RG	Residential Gateway
RRM	Radio Resource Management
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Reference Signal Strength Indicator
RSSNR	RS Signal to Noise Ratio
RTC	Real Time Communication
RTP	Real Time Protocol
RTT	Round Trip Time
SA	Standalone
SBI	Services Based Interface (5GC)
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMF	Session Management Function (part of 5GC)
SMS	Short Messaging Service
SSID	Service Set Identifier
TCP	Transmission Control Protocol

Term	Description
TF	Task Force
TFT	Traffic Flow Template
Tx	Transmit
TNGF	Trusted Non-3GPP Access Gateway Function (part of 5GC)
UAV	Unmanned Aerial Vehicles
UDM	Unified Data Management (part of 5GC)
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UL	Uplink
UP	User Priority
UPF	User Plane Function (part of 5GC)
VLAN	Virtual LAN
VoIMS	Voice over IMS
VoIP	Voice over IP
VoLTE	Voice over LTE
VoNR	Voice over NR
VoWiFi	Voice over Wi-Fi
VPN	Virtual Private Network
WBA	Wireless Broadband Alliance
WBBA	World Broadband Association
WFA	Wi-Fi Alliance
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WMM	Wi-Fi Multimedia (AC)

References

1. WBA White Paper “Wi-Fi Calling-Opportunities and Challenges towards-5G”
2. GSMA PRD TS.22 “Recommendations for Minimum Wi-Fi Capabilities of Use”
3. 3GPP TS 23.501 “System Architecture for the 5G System; Stage 2”
4. 3GPP TS 23.402 “Architecture Enhancements for non-3GPP Accesses”
5. 3GPP TS 29.273 “Evolved Packet System (EPS); 3GPP EPS AAA interfaces”
6. 3GPP TS 29.212 “Policy and Charging Control (PCC), Reference Points”
7. IEEE 802.11k-2008 “IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement of Wireless LANs”
8. IEEE 802.11r-2008 “IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Fast Basic Service Set (BSS) Transition”
9. IETF RFC 4594 “Configuration Guidelines for Diffserv Service Classes”
10. GSMA PRD IR.34 “Guidelines for IPX Provider Networks”
11. IETF RFC 8325 “Mapping Diffserv to IEEE 802.11”
12. IEEE 802.11-2016 “IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”
13. IEEE 802.1ad-2005 “IEEE Standard for Local and Metropolitan Area Networks-Virtual Bridged Local Area Networks - Amendment 4: Provider Bridges”
14. 3GPP TS 23.228 “IP Multimedia Subsystem (IMS); Stage 2”
15. 3GPP TS 29.214 “Policy and Charging Control over Rx Reference Point”
16. 3GPP TS 29.512 “Session Management Policy Control Service; Stage 3”
17. 3GPP TS 23.502 “Procedures for the 5G System”
18. GSMA PRD IR.51 “IMS Profile for Voice, Video and SMS over untrusted Wi-Fi access”
19. GSMA PRD NG.115 “IMS Profile for Voice, Video and Messaging over untrusted WLAN connected to 5GC”
20. 3GPP TS 24.167 “3GPP IMS Management Object (MO); Stage 3”
21. GSMA PRD TS.63 “UE Wi-Fi Calling Requirements Specification”
22. 3GPP TS 24.229 “IMS Profile for Voice and SMS” IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3”
23. GSMA PRD IR.92 “IMS Profile for Voice and SMS”
24. 3GPP TS 33.203 “3G security; Access security for IP-based services”
25. GSMA PRD FS.22 “VoLTE Security Analysis and Recommendations “
26. GSMA PRD FS.21 “Internet Signalling Security Recommendations”
27. GSMA PRD FS.19 “DIAMETER Internet Security”
28. GSMA PRD FS.20 “GPRS Tunnelling Protocol (GTP) Security”
29. GSMA PRD FF.21 “Fraud Manual”

Annex A
Example Business Models

This annex provides several example business models and charging models as a helpful guideline. Individual MNOs can decide for themselves and independently which model is best for them considering their market demands, commercial ambitions and even government regulation.

A.1 Business Models on Land

This business model is applicable to most individual customers when using Wi-Fi Calling on land.

Wi-Fi Calling is a value-added service to the customer's original plan to optimize the service experience, especially when the cellular coverage is poor. Deployment of Wi-Fi Calling is an equivalent alternative to the construction of base stations, which allows MNO effectively improve poor cellular coverage with lower cost. Consumer can make inbound or outbound calls, send or receive text messages via cellular or Wi-Fi network with the same experience, and all the calls and text messages are included in his/her plan.

Usually, MNO will not charge extra fees from customer for his usage of Wi-Fi Calling services. Although not direct income from the customers, MNO may still benefit from diversified service, better customer satisfaction and retention rate, reduced expense on base stations construction.

Table 7 provides some example charging models as a helpful guideline.

TYPE OF FEES	CHARGED PARTY	CHARGING PARTY	CHARGING MODE	NOTE
Wi-Fi Calling service fees	Customer	MNO	— Per minute Based on call duration.	Fees can be included in customer's plan.
	Customer	MNO	— Per delivered message	Fees can be included in customer's plan.

Table 7, Examples of charging models on land

A.2 Business Models in the Air

This business model is applicable to airline companies and their passengers. MNO partners with airline companies and satellite companies to provide Wi-Fi Calling services to passengers via Wi-Fi provided by satellite or ATG (Air to Ground) equipment on the flight. Flight passengers may subscribe Wi-Fi Calling services before or after boarding on the plane, and make inbound or outbound calls, send or receive text messages on demand and pay the fees to the Airline company or MNO.

Table 8 provides some example charging models as a helpful guideline.

TYPE OF FEES	MODEL	CHARGED PARTY	CHARGING PARTY	CHARGING MODE	NOTE
Satellite equipment	-	Airline company	Satellite company	— One-time expense	Expense for satellite equipment provision and installation.
Satellite data package	-	Airline company	Satellite company	— Per plane per month — Per plane per year Based on the data allowance.	For example, 30GB data per month for a plane.
Wi-Fi Calling service package	A	Airline company	MNO	— Per plane per month — Per plane per year Based on the total allowed call duration and message number for a plane.	MNO wholesales Wi-Fi Calling service package to Airline company. For example, a total of 1000 minutes of calls and 2000 messages per month for a plane.
		Passengers	Airline company	— Per flight Based on total call duration or message number that the passenger allowed to use on the flight.	Airline company charges individual passengers for their use of Wi-Fi Calling Services. For example, 30-minute call duration and 100 messages at most for the passenger on the flight. Passenger's subscription of Wi-Fi Calling service is based on and can be combined with the subscription of satellite data traffic service from airline company.
Satellite data traffic fees	B	Passengers	Airline company	— Per flight Based on the data allowance that the passenger can consume on the flight.	Airline company charges the passengers for their use of satellite data traffic. For example, 1GB data at most for the flight.
Wi-Fi Calling service package		Passengers	MNO	— Per minute for voice call — Per message Based on the call duration and the number of messages of passenger during the entire flight.	MNO charges individual passenger for his use of Wi-Fi Calling Services. Passenger's subscription of satellite data traffic service from airline company is a precondition for the subscription of Wi-Fi Calling service. MNO may return portion of the revenue to airline company.

TYPE OF FEES	MODEL	CHARGED PARTY	CHARGING PARTY	CHARGING MODE	NOTE
Satellite data traffic fees	C	Passengers	Airline company	— Per flight Based on the data allowance that the passenger can consume on the flight.	Airline company charges the passengers for their use of satellite data traffic. For example, 1GB data at most for the flight.
Wi-Fi Calling service package		Passengers	MNO	— Per flight Flat charging for allowing to use Wi-Fi Calling for whole trip on the flight Passenger's calls and text messages on the plane are included in their original plan on land.	MNO charges individual passenger for his use of Wi-Fi Calling Services. Passenger's subscription of satellite data traffic service from airline company is a precondition for the subscription of Wi-Fi Calling service. MNO may return portion of the revenue to airline company.

Table 8, Examples of charging models in the air

A.3 Business Models at Sea

A.3.1 Business Models for Law Enforcement Vessels and Freight/Fishing vessels

This business model is applicable to some government/ enterprise customers that need communications services at sea. For example, government department for offshore law enforcement, freight companies and ocean fishing companies.

MNO partners with satellite companies to provide Wi-Fi Calling services to law enforcement vessels and freight/ fishing vessels. Those registered crews are allowed to make inbound or outbound calls, send or receive text messages during their stays on the vessel.

Table 9 provides some example charging models as a helpful guideline.

TYPE OF FEES	MODEL	CHARGED PARTY	CHARGING PARTY	CHARGING MODE	NOTE
Satellite equipment	-	Government department/ freight company	Satellite company	— One-time expense	Expense for satellite equipment provision and installation.
Satellite data package	-	Government department/ freight company	Satellite company	— Per vessel per month — Per vessel per year Based on the data allowance	For example, 30GB data per month for the vessel.
Wi-Fi Calling service package	A	Government department/ freight company	MNO	— Per vessel per month — Per vessel per year Based on a defined number of mobile users (crews) allowed to user Wi-Fi Calling service on the vessel.	For those registered crews, their calls and text messages on the vessel are included in their original plan on land.

TYPE OF FEES	MODEL	CHARGED PARTY	CHARGING PARTY	CHARGING MODE	NOTE
Wi-Fi Calling service package	B	Government department/ freight company	MNO	— Per vessel per month — Per vessel per year Based on the total allowed call duration and allowed message number for the vessel.	For example, totally 1000 minute calls and 2000 messages per month for all the registered crews on the vessel. Those crews are totally free for making calls and sending message.
Wi-Fi Calling service package	C	Crews	MNO	— Per minute for voice call — Per message Based on the call duration and the amount of messages of individual crew during his stay on the vessel.	The fees may be paid by the crew himself or by his company.

Table 9, Examples of charging models for law enforcement vessels and freight/fishing vessels

A.3.2 Business Models for Cruise Ships/Passenger Ships

This business model is applicable to cruise ship companies or passenger ship companies and their passengers.

MNO partners with cruise ship companies and satellite companies to provide Wi-Fi Calling services to passengers via satellite equipment on the ships. Cruise ship passengers may subscribe to Wi-Fi Calling services before or after boarding the ship, and make inbound or outbound calls, send or receive text messages on demand and pay the fees to the ship company or MNO.

Table 10 provides some example charging models for a cruise ship.

TYPE OF FEES	MODEL	CHARGED PARTY	CHARGING PARTY	CHARGING MODE	NOTE
Satellite equipment	-	Cruise company	Satellite company	— One-time expense	Expense for satellite equipment provision and installation
Satellite data package	-	Cruise company	Satellite company	— Per ship per month — Per ship per year Based on the data allowance.	For example, 30GB data per month for a cruise ship.

TYPE OF FEES	MODEL	CHARGED PARTY	CHARGING PARTY	CHARGING MODE	NOTE
Wi-Fi Calling service package	A	Cruise company	MNO	— Per ship per month — Per ship per year Based on the total allowed call duration and message number for a ship.	MNO wholesales Wi-Fi Calling service package to cruise company. For example, totally 1000 minute calls and 2000 messages per month for a cruise ship.
Satellite data package		Passengers	Cruise company	— Per trip — Per day Based on total call duration and message number that the passenger allowed to use on the ship.	Cruise company charges individual passengers for their use of Wi-Fi Calling Services. For example, 30-minute call duration and 100 messages at most for the passenger for the whole trip. Passenger's subscription of Wi-Fi Calling service is based on and can be combined with the subscription of satellite data traffic service from cruise company.
Satellite data traffic fees	B	Passengers	Cruise company	— Per trip — Per day Based on the data allowance that the passenger can consume.	Cruise company charges the passengers for their use of satellite data traffic. For example, 5GB data at most for the whole trip.
Wi-Fi Calling service package		Passengers	MNO	— Per minute for voice call — Per message Based on the call duration and the amount of messages per day or in the whole trip.	MNO charges individual passengers for their use of Wi-Fi Calling services. Passenger's subscription of satellite data traffic service from a cruise company is a precondition for the subscription of Wi-Fi Calling service. MNO may return portion of the revenue to cruise company.

TYPE OF FEES	MODEL	CHARGED PARTY	CHARGING PARTY	CHARGING MODE	NOTE
Satellite data traffic fees	C	Passengers	Cruise company	— Per trip — Per day Based on the data allowance that the passenger can consume.	Cruise company charges the passengers for their use of satellite data traffic. For example, 5GB data at most for the whole trip.
Wi-Fi Calling service package		Passengers	MNO	— Per trip — Per day Flat charging for allowing passenger to use Wi-Fi Calling per day or for the whole trip.	Passengers' calls and text messages on the ship are included in their original plan on land. Passenger's subscription of satellite data traffic service from cruise company is a precondition for the subscription of Wi-Fi Calling service. MNO may return portion of the revenue to cruise company.

Table 10, Examples of charging models for cruise ships

Annex B
Security Considerations

This annex provides details of the various security aspects that need to be taken into consideration for Wi-Fi Calling.

B.1 UE Security

The Wi-Fi Calling stack in the UE is exposed to several attacks from malicious devices or malicious software, which include tampering of Wi-Fi Calling configuration files, logs or live traffic. An attacker can use device rooting or malicious apps to use the UE to attack the network as described in GSMA PRD FS.22 [25] section 4.

A device that is rooted or jailbroken has full access to the kernel and all software stacks, and only limited mitigations are possible. Network traffic from a UE should be assumed to be malicious and a defence in depth approach taken, focusing on signalling security, network infrastructure security and interconnect security to protect the MNO and Wi-Fi Calling against application layer and infrastructure layer attacks. See annex B.4.

A device that has a malicious app installed can be used to attack W-Fi Calling and the MNO although there are some mitigations to these threats that can be applied. These protections rely on the UE operating system and hardware protections, as well as correct configuration by the device distributor.

To minimize threats from malicious apps, the VoWiFi solution should implement the following countermeasures as recommended in GSMA PRD FS.22 [25] section 5:

- **Embedded software stack:** an embedded native stack is used in the UE to make any hacking of that stack more difficult than would be the case for a downloadable stack.
- **User and kernel space separation:** the separation between user space and kernel space ensures that the VoWiFi stack is not directly accessible to unauthorized applications. No application within the user space should have access to the VoWiFi stack.
- **Digital signature verification:** the verification of the digital signatures of apps interacting with the VoWiFi stack ensures the integrity and authenticity of these applications.

It should be noted that, as mentioned in GSMA PRD FS.22 [25], the first countermeasure as depicted as above is security through obscurity and not a foolproof security control, although it raises the bar on who can take advantage of any potential weaknesses in the VoWiFi stack.

B.2 Wi-Fi Calling Access Security

Security between the UE and Network is based on the use of AKA (Authentication and Key Agreement) using a shared secret (located on the UICC and within the Network). AKA enables the mutual authentication of the User and Network and the derivation of a number of other session keys to protect/encrypt traffic for a number of different interfaces.

The UE and the network must conform to the requirements for supporting network attachment to the 5GC via the ePDG from an untrusted WLAN access followed by registration to IMS as specified in GSMA PRD IR.51 [18] section 4.4 and section 2.2 respectively.

NOTE 1: GSMA PRD IR.51 defines access to the EPC via the ePDG. However, the ePDG can also gain access the 5GC as described in 3GPP TS 23.501 [3] clause 4.3.4 and reuses the same security procedures as defined for the legacy EPC. It is also highly unlikely for ePDG-related standards to be enhanced as EPC standards are frozen in 3GPP.

NOTE 2: As specified in 3GPP TS 23.501 [3] section 6.3.6, the UE must be configured with the Non-3GPP access node selection information and identities to enable the selection of the N3IWF (if N3IWFs are deployed) or ePDG (if ePDGs are deployed).

B.3 W-Fi Calling Signalling Security

Wi-Fi Calling uses several signaling protocols that can be exploited and require protocol-aware controls for a number of protocols such as SIP, RTP, SDP, H.248, GTP, IPSec and Diameter. Networks typically deploy application aware firewalls for any interfaces external to its trust domain, i.e. interfaces applicable to interconnect and roaming scenarios. Various GSMA PRDs provide an overview of the threats and recommended counter measures related to interfaces external to the trust domain. See GSMA PRDs FS.21 [26], FS.19 [27] and FS.20 [28].

GSMA PRD FS.22 [25] describes a number of potential attacks and counter-measures related to VoLTE. More generally, the attacks and countermeasures area are applicable to VoIMS and are thus equally applicable to Wi-Fi Calling. MNOs deploying Wi-Fi Calling are strongly recommended to protect their networks from attacks generated by compromised UEs via the implementation of the counter-measures described in FS.22 [25] section 5.

B.4 Network Infrastructure Security and Interconnect Security

Like with any other telco service, the Wi-Fi Calling systems need to be protected against external threats and attacks. Wi-Fi Calling solutions are often open to many networks, even the public Internet, and this expands the attack surface. Furthermore, if the Wi-Fi Calling systems get compromised, they can provide lateral movements to compromise other MNO elements. To prevent these threats, the Wi-Fi Calling solution should implement the following:

1. **Intrinsic security:** like in any critical network system, all Wi-Fi Calling elements need to be hardened at installation time and patched as soon as possible during operations. When security patches are not available for a vulnerability, the firewall can apply a virtual patch that prevents exploiting the vulnerability as a temporal measure.
2. **Perimeter firewall protection:** As any network function that is exposed to external networks and different trust domains, the ePDG can have a perimeter firewall that restricts the acceptable dynamic/static IP ranges, protocols and traffic patterns.
3. **VPN segregation:** The firewall should restrict and segregate the traffic that reaches the ePDG from external sources to IPsec client tunnels started by Wi-Fi Calling UEs. ePDG discards connections that are un-authenticated/un-authorized and logs them.
4. **De-Militarized Zone (DMZ) segregation:** The ePDG could be used as a jump host to reach other targets in the MNO network. To prevent this, the ePDG can be placed in a DMZ that restricts connectivity to the minimum that is needed (AAA, PGW, DNS, OAM). The DMZ also facilitates its re-creation to eliminate hidden agents.
5. **Security Gateway:** When the ePDG is hosted in an external public cloud, a security gateway can secure the connection to the AAA or PGW by creating site-to-site IPsec tunnels that provide confidentiality, integrity and authentication.
6. **Overload protection:** An external botnet could launch a Distributed Denial of Service (DDoS) attack that prevents legitimate users from using the Wi-Fi Calling service. The MNO should have an inbound flow control in the firewall with an anti-DDoS protection that prevents the ePDG capacity from being overloaded. The outbound flow control strategy needs to prevent the overload of the AAA and PGW.
7. **Lateral Movement Detection:** It can be achieved by having some decoys, deceptors or honeypots. These emulate real network functions (e.g., AAA, PGW, DNS, EMS, ...). When a decoy gets contacted, it is a clear indication that a system is compromised.
8. **Strict management plane security:** MNOs need to implement industry-standard control mechanisms for the management network, such as the segregation of the networks and interfaces, encrypted communications and the use of strong authentication (including centralized identity management, multi-factor authentication for users or certificates for machines). It is also highly recommended to use a Privilege Access Management tool, and the use of zero-trust network access.
9. **Real-time monitoring:** having a firewall is not enough, because if an attacker manages to get past it, the attacker remains inside the network for a very long time. A SIEM (Security Information and Event Management) can gather and analyze the logs and CDRs created by the VoWiFi system. This analysis can correlate information coming from different sources, from different subscribers or from different sessions.
10. **A Behavioral Analysis** can be implemented to identify abnormal behavior, and it is useful for both fraud and security use cases.

B.5 Fraud Considerations

Wi-Fi Calling can be used by fraudsters to commit voice or SMS fraud, see GSMA PRD FF.21 [29]. MNOs should pay particular attention to monitor and/or block VoWiFi calls from low-trust IP addresses.

Annex C
Document Management

VERSION	DATE	BRIEF DESCRIPTION OF CHANGE	APPROVAL AUTHORITY	EDITOR /COMPANY
1.0	Feb. 2025	Published	5GVoWiFi TF	Wayne Cutler (GSMA)

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
UK

Email: info@gsma.com