TELECOM INFRA PROJECT

Plug-n-Play Core Integration for Mobile Data Offload (MDO)

TIP White Paper

Date: June 2021

Document Version: 1.0

Confidentiality Level: Green [Public Access]

Authors

Rajesh Rasalkar

Systems Architect, Facebook

rrasalkar@fb.com

Christophe Chevallier

Connectivity Technologies & Ecosystems Manager, Facebook

christophec@fb.com

Evgeniy Makeev

Software Engineer, Facebook

evgeniym@fb.com

Sourabh Nanoti

Software Engineer, Facebook

sourabhn@fb.com

Shah Rahman

Engineering Lead, Facebook

shahrahman@fb.com

TIP Document License

By using and/or copying this document, or the TIP document from which this statement is linked, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to copy, display and distribute the contents of this document, or the TIP document from which this statement is linked, in any medium for any purpose and without fee or royalty is hereby granted under the copyrights of TIP and its Contributors, provided that you include the following on ALL copies of the document, or portions thereof, that you use:

1. A link or URL to the original TIP document.

2. The pre-existing copyright notice of the original author, or if it doesn't exist, a notice (hypertext is preferred, but a textual representation is permitted) of the form: "Copyright © <<year>>, TIP and its Contributors. All rights Reserved"

3. When space permits, inclusion of the full text of this License should be provided. We request that authorship attribution be provided in any software, documents, or other items or products that you create pursuant to the implementation of the contents of this document, or any portion thereof.

No right to create modifications or derivatives of TIP documents is granted pursuant to this License. except as follows: To facilitate implementation of software or specifications that may be the subject of this document, anyone may prepare and distribute derivative works and portions of this document in such implementations, in supporting materials accompanying the implementations, PROVIDED that all such materials include the copyright notice above and this License. HOWEVER, the publication of derivative works of this document for any other purpose is expressly prohibited.

For the avoidance of doubt, Software and Specifications, as those terms are defined in TIP's Organizational Documents (which may be accessed at https://telecominfraproject.com/organizational-documents/), and components thereof incorporated into the Document are licensed in accordance with the applicable Organizational Document(s).

Disclaimers

THIS DOCUMENT IS PROVIDED "AS IS," AND TIP MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THE DOCUMENT ARE SUITABLE FOR ANY PURPOSE; NOR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

TIP WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE DOCUMENT OR THE PERFORMANCE OR IMPLEMENTATION OF THE CONTENTS THEREOF.

The name or trademarks of TIP may NOT be used in advertising or publicity pertaining to this document or its contents without specific, written prior permission. Title to copyright in this document will at all times remain with TIP and its Contributors.
This TIP Document License is based, with permission from the W3C, on the W3C Document License which may be found at https://www.w3.org/Consortium/Legal/2015/doc-license.html.

Change Tracking

Date	Revision	Author(s)	Comment
Apr 22, 2021	V1.0	Rajesh Rasalkar Sourabh Nanoti Shah Rahman Evgeniy Makeev Christophe Chevallier	

Table of Contents

Abstract

As mobile data capacity demands continue to grow, MNOs and especially MVNOs are faced with greater competition and stagnant or falling revenue per subscriber. Mobile Data Offload (MDO) is an effective technique for addressing capacity needs in the face of congestion in cellular networks. This white paper demonstrates a way to do the core integration for seamless mobile Wi-Fi offload using a Plug-n-Play tested architecture.

1

Introduction

Overview

As mobile data capacity demands continue to grow, Mobile Network Operators (MNOs) and especially Mobile Virtual Network Operators (MVNOs) are faced with greater competition and stagnant or falling revenue per subscriber. 5G, CBRS, and Wi-Fi6 will soon be interwoven into our future wireless networks, making it even more important for Connectivity to bridge the divide between consumer demand and network availability. The post-COVID-19 world will simply see further convergence of various access networks, where our teams are working hard to make the convergence simpler and easier.

Mobile Data Offload (MDO) is an effective technique for addressing capacity needs in the face of congestion in cellular networks, especially when there is a lack of spectrum, sudden load on the network, or other challenges due to which mobile operators are unable to effectively use cellular networks. Offloading to a Wi-Fi network from an LTE or 3G network can be achieved several different ways. Many of these offload methods face a common challenge on how to offer similar QoE between cellular and Wi-Fi networks.

In this white paper we:

- Discuss the challenges with existing methods of Mobile Data Offload (MDO)
- Outline benefits and concept of simplified and Plug-n-Play core integration
- Show how Network Operators who want to provide a seamless mobile Wi-Fi offload can utilize this Plug-n-Play architecture

Current Challenges with MDO Core Integration

The Third-Generation Partnership Project (3GPP) standard differentiates two types of Wi-Fi access (also referred to as non-3GPP IP access):

- **Untrusted:** Introduced in the early stages of the Wi-Fi specification in 3GPP Release 6 (2005), untrusted access includes any type of Wi-Fi access that either is not under control of the operator (public open hotspot, subscriber's home WLAN, etc.) or that does not provide sufficient security (authentication, encryption, etc.).
- **Trusted:** Trusted access generally refers to operator-built Wi-Fi access with over-the-air encryption and a secure authentication method. Trusted non-3GPP IP access was introduced only with the LTE standard in 3GPP Release 8 (2008). Although most of today's offload designs are built on the trusted model, this type of access is natively integrated into LTE's evolved packet core (EPC).

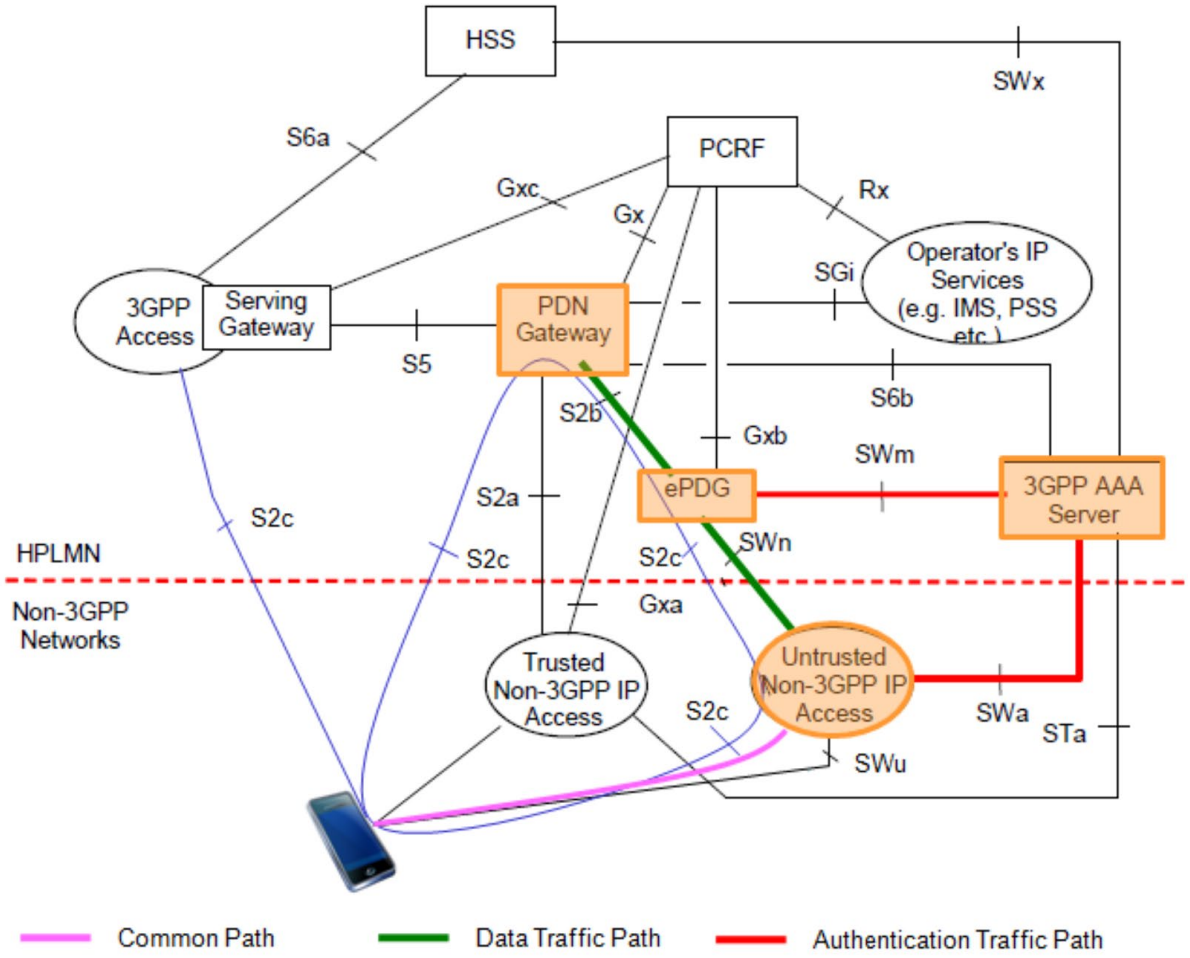

Figure 1 - Standard Carrier Wi-Fi architecture allows MDO through Wi-Fi offload

A variety of point solutions can be applied to improve aspects of network performance. While network performance can be achieved in a variety of ways, integrating with core network's backend elements, e.g., HSS, PCRF and OCS of an operator can allow an offload network offer: seamless authentication, policy and billing experience that is similar to that of an operator's LTE network.

However, a key challenge in such integration lies in the way most integration gateways work today that are too complex, too cumbersome, and too time consuming to make any integration work in operator's production networks practical. Either control-plane-only integration that operates only at the AAA level or data-plane integration that

requires an ePDG or TWAG to connect to a PGW that is intrusive to the operator's core network.

In recent years, the mobile operators are aware of the facts and there are two of the three key factors that drive Plug-n-Play integration of mobile core elements: HSS, PCRF and OCS as laid out in the Carrier Wi-Fi architecture, over which MDO is a key service provided.

1. **Devices.** *Subscribers need a good quality of experience and the movement from cellular to Wi-Fi and back needs to be seamless.*

   Initially, subscribers need to have operator's Wi-Fi network profile pushed to the device. And ultimately, an intelligent Connection Manager is paramount for tackling the device or client challenge of carrier Wi-Fi (i.e., having seamless roaming to Wi-Fi). Distribution channels for reaching all end devices, mobile or stationed is the biggest barrier. Device manufacturers, OS vendors as well as application developers (standalone apps or embedded SDK) have each attempted to address the distribution challenge, only to have limited reach.

2. **Network SLAs.** *The Wi-Fi network needs to have SLAs and needs to work (almost) as well as the mobile network.*

   Data and KPIs needed to monitor and run a reasonably good Wi-Fi network is a key challenge with network SLAs. Some predictive analytics/ML in the future to predict network failures or low performance can be useful here. However, with strong analytics capability in Wi-Fi policy and performance monitoring solutions, there is an opportunity to normalize Wi-Fi network SLAs with that of mobile data networks. One of the most important things here is not so much the KPIs, but creating a truly **multi-tenant**, and completely **on-premise**, system that can work in harmony with the operator's existing EPC zero disruption or intrusion to it. Multi-tenant because we may have scenarios where the Wi-Fi network belongs to an ISP, but the subscriber belongs to the MNO. On-premise because most

cloud-based solutions are unacceptable by operators who are highly regulated in several emerging and developing countries in terms of in-country data requirements similar to GDPR.

This is a key motivation for developing a Plug-n-Play mobile EPS core integration architecture that allows Wi-Fi vendors and ecosystem partners to bring their solutions with a single-point of integration rather than several different functions and interfaces, as generally specified in 3GPP standard.

3. **Network Functions.** *The unique way to monetize Wi-Fi is to give perks and services over it (e.g., use it for streaming high-quality video, making voice and video calls, etc.; and/or charge for it at a discounted rate).*

   Some operators combine these two (services and discount) by letting a subscriber use Wi-Fi at a discounted rate and give a smaller quota in exchange over cellular data (as another way of alleviating congestion in LTE networks using this exchange as an incentive). To provide any kind of service, a mobile operator needs to address two items:

   1) the ability to enforce that service at the subscriber level, and
   2) the ability to tie it to the existing data plans over a single wallet.

   Both items are possible, almost seamlessly, by integration through 3GPP SWx (non-3GPP users), Gx (policy rules) and Gy (online charging) interfaces for these services in the operator's core network and then enforcing them all in the Wi-Fi network or in an access gateway (the PCEF functionality). While SWx/S6a integration can suffice in offering free Wi-Fi service for offloaded customers, it is not sufficient since the operator is unable to offer any service that is tied to their existing business models and practices.

   Unfortunately, most operators cannot monetize Wi-Fi as a standalone service. This necessitates the need for Plug-in-Play integration in order to leverage the

mobile operator's existing monetization techniques over cellular networks as well as the ability to update the monetization offerings on an ongoing basis, based on changing user behaviors, application demands, and market dynamics.

2

Key Considerations

An integrated Wi-Fi solution allows operators to intelligently offload traffic while providing complete control and visibility of the user context. The cellular and Wi-Fi integration architectures can be classified into two different approaches:

1. **Managed Offload:** Integration with core network authentication and policy management systems
2. **Integrated Offload:** Integration of Wi-Fi data traffic into the core network for seamless mobility and feature parity

At the high-level, the mobile core elements: HSS, PCRF and OCS require that there is a clear relationship between WLAN connection/association (it implies one access request/auth cycle), accounting session and Gx/Gy session:

1. For every new WLAN connection/association, there will be authentication necessary and this authentication will be optimized via multiple SWx/S6a auth vectors and/or fast-reauth), followed by AAA server registration, Gx and Gy session establishment and accounting session start (depending on the offload mode: free, metered or unified).

2. A session can be started, stopped, started multiple times within the lifetime of one WLAN connection, where WLAN connection implies one access request/auth cycle. In some cases, session termination results in a new connection request (Access Request). Session and association/connection lifetime relationship depends on multiple factors:

    - Parameters used in Access-Accept
    - Capability and configuration of WLC
    - Vendor-specific implementation

3. In a non-roaming case, session termination normally results in WLAN dis-connection or de-association. Hence, it results in session termination towards Gx and Gy:

- Session termination (mainly during AP roaming) may not always result in Gx and Gy termination (please refer to the subsequent section on roaming for more details).
- WLAN connection termination will result in Gx and Gy session termination.

4. During roaming, it is possible that:
    - RADIUS Accounting-Stop and Access-Request may come out of order;
    - RADIUS Accounting-Stop is never received, and new Access-Request is received;
    - Instead of sending RADIUS Accounting-Stop and RADIUS Accounting-Start, WLC sends interim accounting updates with same account-session-id; and
    - UE may or may not trigger a new DHCP request and this implies that in the post-roaming RADIUS Accounting messages, the IP address of the UE may change.
5. Different AP and WLC from different vendors have different behavior and it varies further if 802.11r and/or OKC is enabled in WLC and/or AP (for the initial revision, it is assumed that 802.11r and OKC in WLC and/or AP is disabled. This implies that every AP roam would trigger a new "RADIUS Access-Request"/Association/Connection/Authentication sequence towards PCEF.

Additionally, some of the following aspects complicate the MDO support through Carrier Wi-Fi architecture, especially in the EPS core integration aspect:

1. DRA in front of HSS, PCRF and OCS that is part of operator's EPS or mobile core elements
2. IMSI and data path flow association: UE MAC or IP address

3

High-Level Architecture

A unified Carrier Wi-Fi architecture is shown in Fig 2, such architecture that addresses the problem statement in Section 2 by offering MDO through Wi-Fi offload.

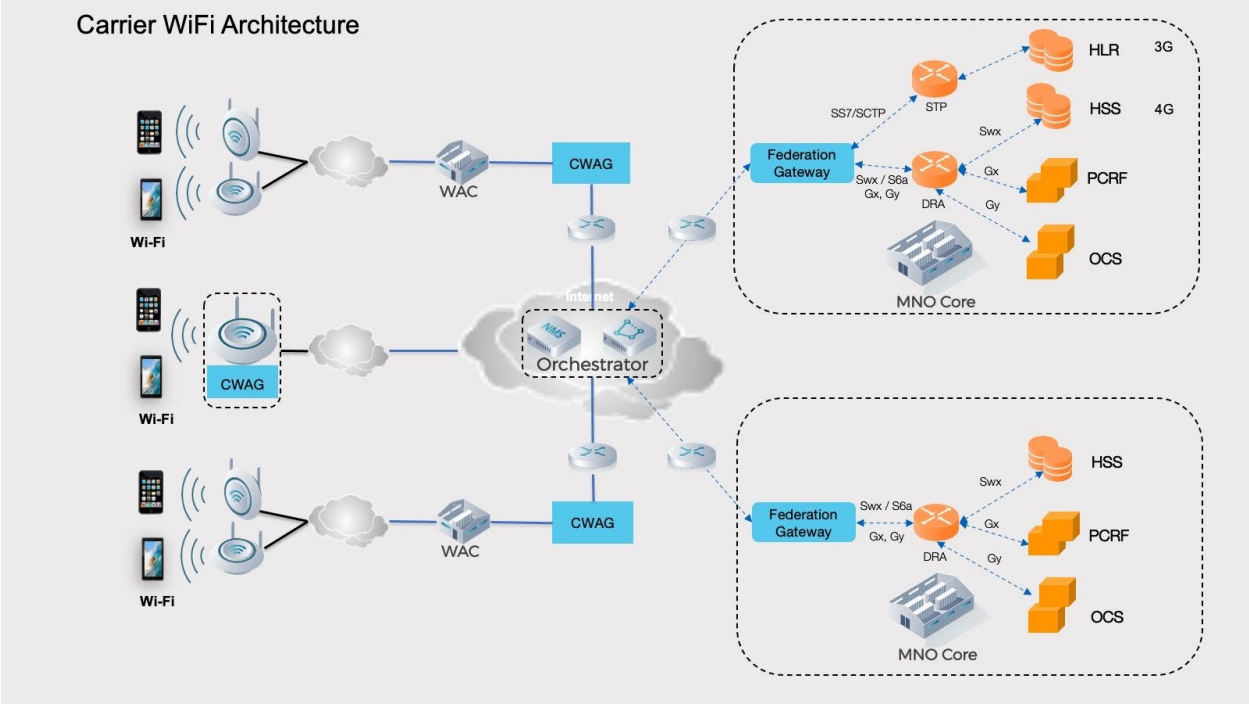

Figure 2: A flexible Carrier Wi-Fi architecture allows MDO through Wi-Fi offload for 3G or 4G LTE networks

In this approach, the offload solution allows the reuse of credentials (using the SIM module for instance) to automatically authenticate to the Wi-Fi networks. This may be done using EAP-SIM/AKA methods and requires a common AAA authentication server (a services gateway) that provides 3GPP interfaces to the operator's HLR/HSS (subscriber databases) and Policy and Charging Rules Function (PCRF) to authenticate the user and enforce usage policies. The WLAN network enforces the access policies as determined by the core network.

In the Carrier Wi-Fi architecture, there are three possible use cases that are supported for MDO:

1. **Free:** Offers free Wi-Fi offload that relies on authenticating mobile data users against MNO's HSS/HLR (no direct monetization of Wi-Fi networks).
2. **Metered:** Offers limited Wi-Fi that relies on authenticating mobile data users against MNO's HSS/HLR and accounting of data consumed on the Wi-Fi network against OCS or PCRF.
3. **Unified:** Offers full Wi-Fi solution that relies on metered integration as well as enforcement of mobile data policies and charging from PCRF rules as best as possible on the Wi-Fi network.

Introduction to Federation Gateway

The Federation Gateway (FGW) integrates the MNO core network with any wireless network, such as LTE or Wi-Fi by using standard 3GPP interfaces to existing elements, such as HSS/HLR, MSC/VLR, PCRF and OCS/OFCS. It acts as a proxy between any non-3GPP network and MNO's 3GPP network and facilitates core functions, such as authentication, data plans, policy enforcement, and charging to stay uniform between an existing MNO network and non-3GPP network by translating between 3GPP standard protocols (e.g., Diameter, SCTP, TCP and interfaces, e.g., SGs, S6a, SWx, Gx and Gy).

In essence, FGW forms the essential security binding and trust boundary between an operator's existing mobile core elements and Wi-Fi offload elements. This requires it to ensure that all incoming signaling from Wi-Fi networks is strongly secured using an end-to-end secure transport protocol, e.g., gRPC / HTTP2 and TLS. Additionally, the clean separation between the mobile core and Wi-Fi domains of the network is ensured using gRPC based on versioning and backward compatibility. By design, FGW is stateless and assumes that all 3GPP interfaces leverage 3GPP releases to remain forward and backward compatible towards the mobile core elements. For the purpose of MDO, only a subset of 3GPP release-12 and -13 is identified for SWx, S6a, Gx and Gy so that FGW can offer a Plug-n-Play EPS core integration for Wi-Fi offloading.

Fig 3 shows a typical FGW structure with only a subset of 3GPP interfaces / protocols towards MNO mobile core.

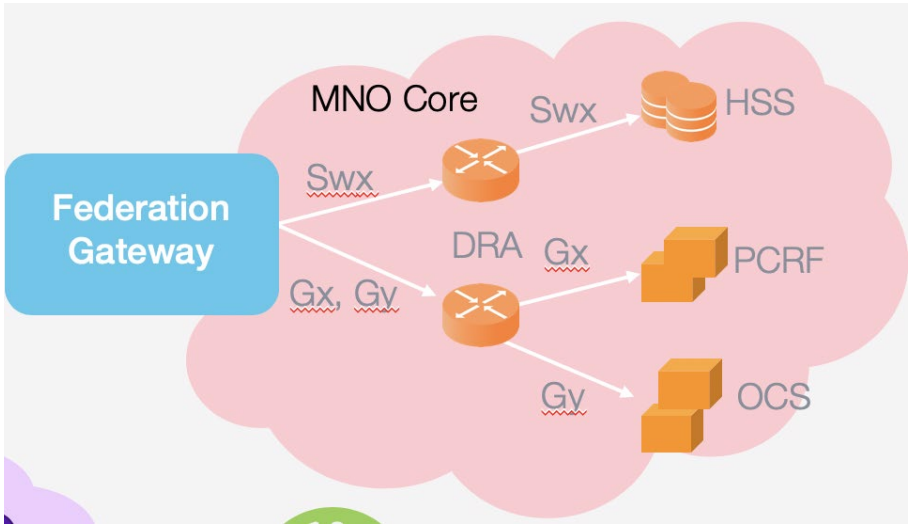

Figure 3: A conceptual FGW acting as a single node towards MNO mobile core

4

Key Assumptions

The Plug-n-Play EPS core integration makes a few key assumptions around the scope to ensure all FGW implementations as well as mobile core element vendors are well prepared for interoperability tests.

- No overlapping of APs and WLCs across Wi-Fi offload networks, whether it is owned by the MNO or ISPs or otherwise (cannot be unmanaged)
- There is usually 1:1 mapping between a WLC and PCEF (outside of the scope of this spec)
- There may be more than a single WLC present per Wi-Fi offload network operator
- Necessarily, FGW will serve more than multiple Wi-Fi offload networks
- IP addresses will be allocated and managed by DHCP service that is owned by operator (or alternatively, a standalone DHCP service that is outside of the scope of this spec)
- LEA/LI is not considered in this solution and will be considered for Version 3.0
- Management aspects of TWANs or APs or WLCs are not in scope of this spec and assumed to be handled by Wi-Fi network owner or mobile network operator
- Multiple sessions per UE is not considered as it is largely irrelevant in the context of MDO. As differentiated packet treatments belonging to different flows/rating groups will be enforced in the PCEF. However, this may become relevant in cases where-in some of the WLCs use multiple account session ids with unique multi-account-session-id during AP roaming. This scenario is not initially considered for this plug-n-play EPS core integration specification (left for future consideration).

With these assumptions, the rest of the document describes the details on how FGW integrates MNO core elements for supporting MDO in a Plug-n-Play way.

5

TIP PlugFest Test Setup & Results

Test Setup

The first interoperability testing of Magma Carrier Wi-Fi/Mobile Data Offload (CWF/MDO) with commercial Evolved Packet System (EPS) was successfully completed in Q2'20. The event was carried out at TIP premises at Menlo Park in the USA. The primary goal of the MDO PlugFest was to validate the interoperability of the Magma Plug-N-Play Carrier Wi-Fi solution with Core elements (core), over standardized interfaces.

The DuT is Magma - Federated Gateway (FGW) and Carrier Wi-Fi gateway (CWAG).

For the core, the main nodes considered are the Policy and Charging Rules Function (PCRF), the Home Subscriber Server (HSS), the Online Charging System (OCS), connected respectively to the FGW through the Gx, SWx, and Gy interfaces through Diameter Routing Agent (DRA). All testing is performed with real equipment, so that the results reflect a real-world service environment.

The test architecture consists of:

- Magma FeG and CWAG
- Amdocs HSS
- Amdocs PCRF
- Amdocs OCS
- Amdocs DRA
- Commercial Off-The-Shelf (COST) Access Point (AP)
- COST, User Equipment (UE)

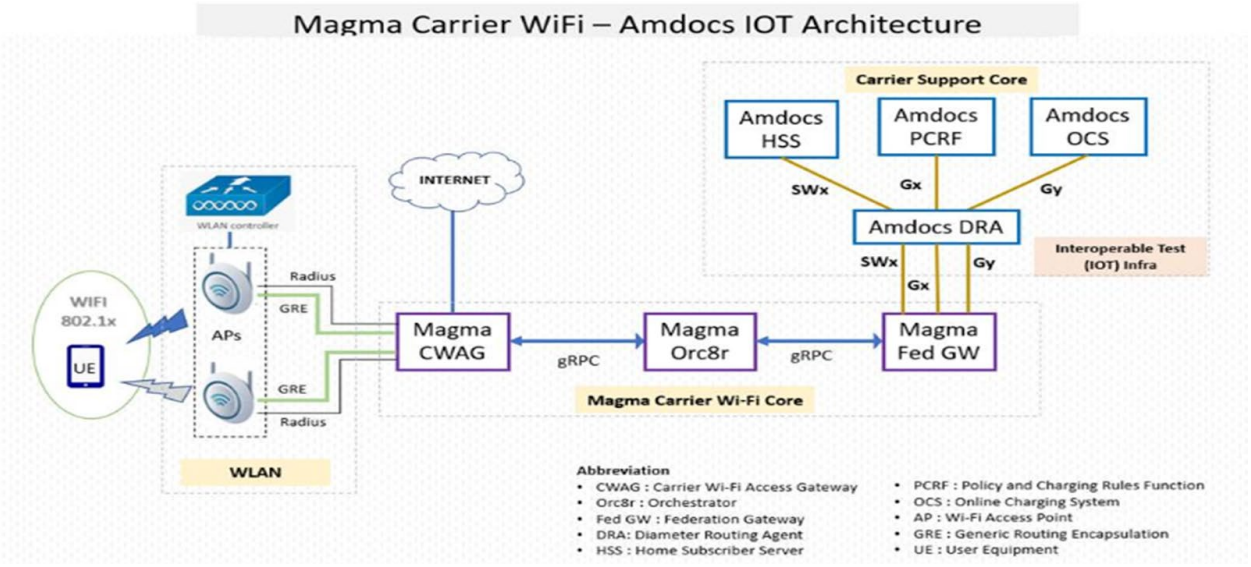

Figure 4: TIP PlugFest Lab

The Federation gateway hosts a centralized control plane interface towards HSS, PCRF, OCS on behalf of distributed Carrier Wi-Fi Access Gateways (CWAG). Following configurations are required on Federation gateway to establish diameter connections with operator core elements. This configuration is typically pushed through Magma NMS UI via Orc8r.

- IP address, Port, Protocol (TCP/SCTP)
- Diameter connection parameters
- Destination host/realm/IP/Port will be of the operators HSS/PCRF/OCS

Following features were considered for the validation which are typical feature set required for a smooth Plug-N-Play core integration of CWF deployment:

1. **SWx (Magma Fed-GW/CWAG <-> HSS)**
    a. EAP-AKA Authentication
    b. Non-3gpp Service Access

2. **Gx (Magma Fed-GW/CWAG <-> PCRF)**
    a. Static Rule and Rule-Based enforcement
    b. Dynamic Rule enforcement
    c. Gx Usage Reporting
    d. Multi rule precedence
    e. UE Mid-session policy updates with RAR
    f. Time of the delay
    g. Gx Revalidation Timeout

3. **Gy (Magma Fed-GW/CWAG <-> OCS)**
    a. Volume based Gy usage reporting
    b. Time based Gy usage reporting
    c. Authorization only flow
    d. "RAR" on charging status change
    e. FUA – Terminate and Redirect

Test Summary

Here is a summary of Interoperability between Carrier Wi-Fi Access Gateway and Federated Gateway and carrier grade EPS nodes (OCS, HSS, and PCRF).

- All P1 test cases passed, demonstrating good interworking between Carrier Wi-Fi and core elements (OCS, HSS, PCRF)
- All 57 test cases (P1, P2 and P3) executed
- 6 issues were identified, 2 issues were resolved, and 4 issues are open at the conclusion of testing

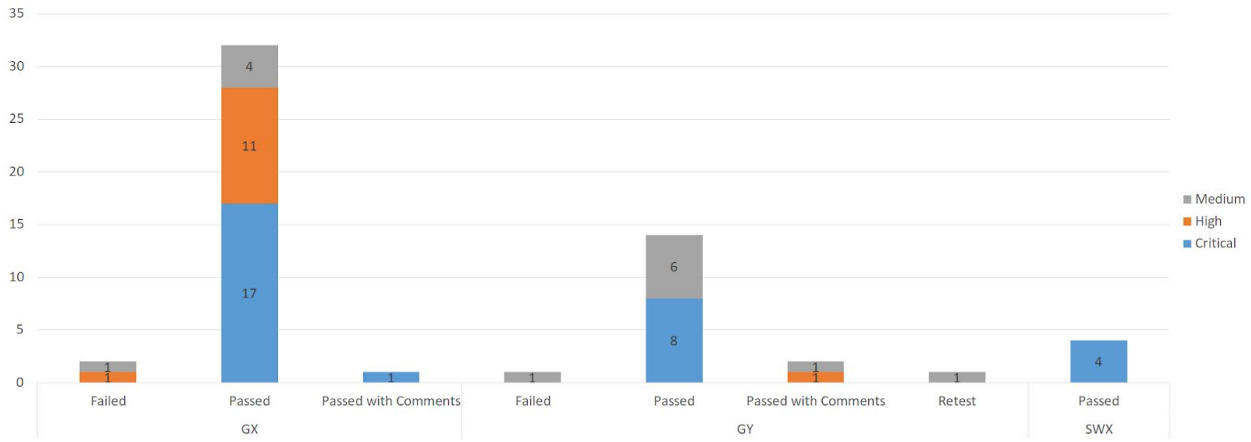

Figure 5: Test Execution Summary

- Pass: feature is working as per 3GPP specifications TS29.273 (SWx), TS 29.212 (Gx) and TS 32.299 (Gy), following test procedure
- Failed: Feature is failing as per test steps during execution.
- Pass with comments: functionality worked but some inconsistency observed

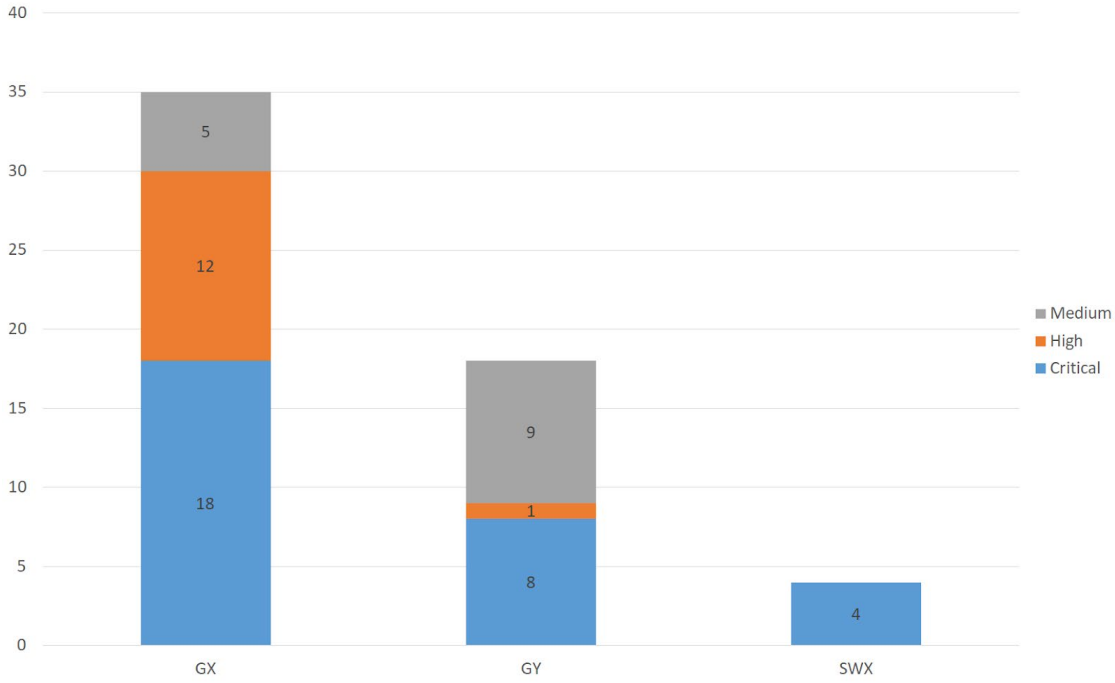

Figure 6: Test cases by priority and interfaces

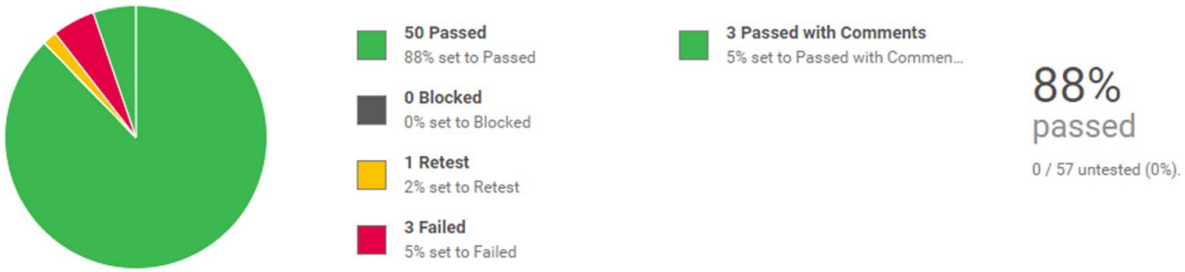

Figure 7: Summary Test Results

With 100% of critical test cases, and 88% overall, the CWAG and FeG listed on TIP Exchange with a PlugFest badge.

6

Real-World Deployments

The Magma-based PnP core integration was implemented at one of the tier-1 operators in APAC. The following architecture depicts the setup at a high level.

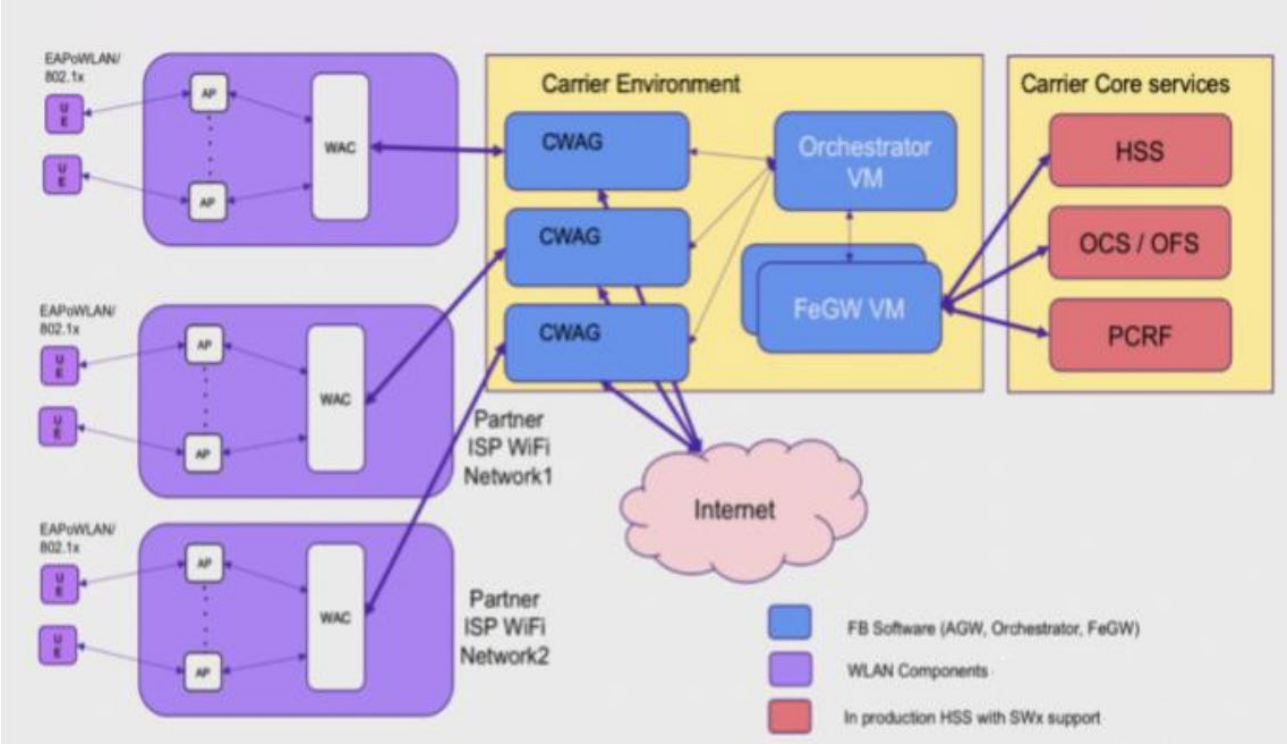

Figure 8: Magma PnP deployment in Tier-1 APAC operator

Requirement from Mobile Operator	Magma Offerings
Carrier grade horizontally scalable MDO solution	Magma provided a cloud-based, microservice-based architecture built on COTS hardware.
No additional costs to the existing MNO vendors	Existing core vendors of the operator were transparent to the MDO solution due to the Federation Gateway.
Minimum interop with the MNO core	Federation gateway acted as a PCEF terminating Swx, Gx and Gy interface towards MNO Core elements. Since all the interfaces are 3GPP compliant, there is minimum integration effort required to enable the MDO solution.
Minimum impact to the networking infrastructure	Magma services are based on HTTPs based GRPC interface. Hence the networking changes were nil. Since the HTTPs port 443 was reachable throughout the network no additional changes were required on the Firewalls/ routers.
Extensible Wi-Fi Access Network	Magma Federation gateway architecture enabled the Wi-Fi access network from the ISP to be a separate network. Geographically the access network could be anywhere in the MNO LTE footprint and MDO will happen if the Wi-Fi traffic is able to reach Federation Gateways over underlying technologies like L2 tunnels over GRE.
Centrally managed subscriber policies	Federation gateway enabled the operator to control the policy and charging for both LTE and Wi-Fi data through a central PCRF/OCS.

7

Next Steps

Following the successful implementation of PnP core integration, it was proven that MDO can be easily added through a Wi-Fi core and Magma-based Federation Gateway. Additionally, the team undertook a few important enhancements, and these are currently under development:

- Supporting 3G subscriber offload through HLR integration
- Supporting 3G subscriber offload through EAP-SIM over Swx/HSS
- Supporting EAP-AKA and EAP-SIM support through S6a interface, potentially eliminating the need for a Swx/AAA license for the HSS
- Augmented networks, where MDO can be offered through different owner networks, e.g., ISP owned Wi-Fi and MNO owned cellular networks in one-to-many or many-to-many scenarios
- Monetization of Wi-Fi networks through MDO
- Gamification of Wi-Fi network usage

8

Conclusion

Core integration is one of the most complex parts of a successful cellular and Wi-Fi network integration as well as offering MDO through Wi-Fi offload networks. PnP core integration proven through Magma technology that is developed by Facebook Connectivity and demonstrated through partnership with Telecom Infra Project (TIP) and Amdocs help drastically reduce complexity of such integration and an end-to-end MDO pilot or trial can be completed as fast as four weeks. Both the technology as well as such speed are unprecedented in the industry and can be extended into future evolution of both types of wireless networks: 5G and Wi-Fi6.

Contact us at magma@fb.com to learn more about the technology as well as potential partnerships to deploy PnP core integration based MDO offering through Magma.

Acronyms

3G	*Third-generation Mobile Networks*
3GPP	*Third-generation Partnership Project*
ARP	*Address Resolution Protocol*
ARPU	*Average Revenue Per User*
AVP	*Attribute Value Pair*
CBRS	*Citizen Broadband Radio Service*
CoA	*Change of Authorization*
CWAG	*Carrier Wi-Fi Access Gateway*
ePDG	*Evolved Packet Data Gateway*
DHCP	*Dynamic Host Control Protocol*
DNS	*Domain Name Service*
DRA	*Diameter Routing Agent*
EPC	*Evolved Packet Core*
EPS	*Evolved Packet System*
FGW	*Federation Gateway*
GDP	*Gross Domestic Product*
GDPR	*General Data Protection Regulation*
gRPC	*Google Remote Procedure Calls*
HETNET	*Heterogeneous Networks*
HLR	*Home Location Register*
HSS	*Home Subscriber Server*
HTTP2	*Hypertext Transfer Protocol (Version 2)*
IMSI	*International Mobile Subscriber Identifier*
IE	*Information Element*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
KPI	*Key Performance Indicator*

LTE	*Long-Term Evolution*
MAC	*Media Access Control*
MDO	*Mobile Data Offload*
MNO	*Mobile Network Operator*
MSC	*Mobile Switching Center*
MVNO	*Mobile Virtual Network Operator*
OCS	*Online Charging System*
OKC	*Opportunistic Key Caching*
OS	*Operating System*
PCRF	*Policy and Charging Rules Function*
PGW	*Packet Gateway*
QoE	*Quality of Experience*
QoS	*Quality of Service*
RAN	*Radio Access Network*
RG	*Rating Group*
SCTP	*Stream Control Transmission Protocol*
SDK	*Software Development Kit*
SGW	*Serving Gateway*
SLA	*Service Level Agreement*
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security*
TWAG	*Trusted Wireless Access Gateway*
UE	*User Endpoint*
USIM	*Universal Subscriber Identity Module*
VLR	*Visitor Location Register*
WLC	*Wireless LAN Controller*
WLAN	*Wireless Local Area Network*