Seamless Session Transfer

WBA Whitepaper

Source: Wireless Broadband Alliance
Author: Wireless Broadband Alliance
Issue date: 24 December 2012
Version: 1.00
Document status: Final

About the Wireless Broadband Alliance

Founded in 2003, the aim of the Wireless Broadband Alliance (WBA) is to secure an outstanding user experience through the global deployment of next generation Wi-Fi. The WBA and its industry leading members are dedicated to delivering this quality experience through technology innovation, interoperability and robust security.

Today, membership includes major fixed operators such as BT, NTT Communications, Comcast and Time Warner Cable; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Google and Intel. WBA member operators collectively serve more than 1 billion subscribers and operate more than 1 million hotspots globally. They also work with international operators to drive innovation, deliver seamless connectivity and optimize network investments.

The WBA Board includes AT&T, BT, Boingo, Cisco, China Mobile, Intel, iPass, KT, NTT, DOCOMO and Orange France.

More information about WBA: contactus@wballiance.com

www.wballiance.com
www.twitter.com/wballiance

© Copyright 2020 Wireless Broadband Alliance Ltd ("WBA"). All rights reserved. While every effort is made to ensure the information in this report is accurate, the WBA does not accept liability for any errors or mistakes which may arise in relation to the material. All copyright material and trademarks used in this report are the property of their respective owners.

Undertakings and Limitation of Liability

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement. In addition, the WBA (and all other organisations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organisations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organisations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third-parties.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

Wireless Broadband Alliance

Driving next generation Wi-Fi experience

Contents

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

Executive Summary

Mobile data growth is putting pressure on the operators to look at the options to address the demand and to improve quality of experience for their users while keeping their CAPEX/OPEX low. Wi-Fi has become a standard feature in smart phones, tablets and notebooks. Cellular data offloading to Wi-Fi is helping operators to address the data growth issues. However, users want to have a seamless connectivity experience when they move between Wi-Fi and cellular networks.

This paper looks at the Seamless Session Transfer (SST) solutions between Wi-Fi to Wi-Fi and Wi-Fi to cellular networks. It presents the state of the art of seamless session transfer in the industry, reviews the SST work in various organizations including WBA, WFA, IEEE, 3GPP, IETF and GSMA, presents case studies, highlights some of the session continuity issues, and makes recommendations for the way forward including potential future WBA SST trials and continuation of the effort within the GSMA/WBA joint task force.

The ability to continue a seamless session is not trivial. The SST is a complex subject and there are many studies on it. However, most of the proposed solutions mainly focus on the technical aspects of the SST issues. Many roaming and business issues are not addressed. In SST scenarios, inter-operator roaming becomes an important element, especially in the future heterogeneous multi-access networks. To achieve SST with IP Mobility, flexible and scalable inter-operator roaming arrangements are required. This can be realized by separating the service and access operators, and the roaming infrastructure inter-connecting different operators. To provide clear guidelines on STT issues involving roaming and business aspect further work is needed. This is where WBA and GSMA can help.

Although many standards on enabling SST have been available, there is no large-scale real-life SST trial implementing the standards, where the solutions could be evaluated, the potential issues could be discovered and the SST guidelines and recommendations can be established. Hence, it is important that WBA/GSMA to initiate SST trials.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

1. Introduction

Seamless session transfer between Wi-Fi networks and Wi-Fi to cellular networks has been the great vision for many years. There has been substantial amount of work taking place in the industry. However, the recent significant changes in the Wi-Fi and cellular industry are driving the need for making it possible.

The growth on the demand for wireless data traffic as a result of the mass adoption of mobile devices like smartphones, tablets and notebooks is putting pressure on mobile operators to provide a quality of experience for their customers. The projected data growth demand is huge and the operators are looking at various options including offloading 3/4G data to Wi-Fi.

Nowadays, Wi-Fi has become a standard feature in virtually every notebook, smartphone and tablet sold. Wi-Fi offers a low cost, simple architecture, large bandwidth and uses non-licenced spectrum solution. Hence, it is an attractive option for operators to offload their 3/4G data traffic to Wi-Fi. Many operators have started deploying large numbers of Wi-Fi hotspots globally. However, mobile devices and networks have varying degrees of Wi-Fi support, resulting in interoperability issues and poor user experiences.

Users just want to stay connected to the best network anytime and anywhere. Hence, seamless session transfer will be increasingly important to bring a complete transparent experience to the users independent of the wireless technology that may be in use. The end user experience should be seamless and consistent over Wi-Fi and 3/4G technologies.

Seamless experience over Wi-Fi networks and its integration with the cellular networks has been studied in many organizations such as the WBA Next Generation Hotspot (NGH) Program [12], WFA Passpoint certification program [13], 3GPP Wi-Fi cellular network interworking [6], and IEEE 802.11u WLAN interworking with external networks [9].

One of the key issues in enabling seamless session continuity between Wi-Fi/Wi-Fi or Wi-Fi/cellular networks has been the auto connection to Wi-Fi hotspots involving network discovery and easy of roaming. It has been a gating factor in making seamless session transfer reality. WFA Hotspot 2.0 technology and WBA NGH are the industry initiatives addressing simple connectivity, network discovery and easy roaming to Wi-Fi hotspots, globally - removing the manual intervention process for connecting to Wi-Fi hotspots.

Addressing the auto connectivity issue is an important step in making seamless session continuity a reality. But, there are still significant technical and business issues to be resolved to enable a seamless user experience when users move around and switch their network connection from cellular to Wi-Fi or Wi-Fi to Wi-Fi. This WBA whitepaper looks at these issues, reviews the Seamless Session Transfer (SST) current state of the art in various organizations and deployments, and provide recommendations for the future work in the industry.

Please note that 3/4G and cellular are used interchangeably in this document.

2. Seamless Session Transfer Overview

2.1 What is Seamless Session Transfer

Seamless Session Transfer (SST) is about enabling a user experience by maintaining connectivity when switching between different networks, Examples include maintaining connectivity when roaming between different Wi-Fi networks, or while switching between cellular and Wi-Fi networks, supporting seamless offloading to Wi-Fi network and connecting to the preferred network perhaps with highest bandwidth. In the mobility management for networks, the issue of SST is important for guaranteeing service continuity and quality-of-experience when a mobile device connects to another network.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

2.1.1 SST Types

In a multi-access networking environment, the mobile device needs to reconfigure its IP addresses when it connects to a different network or when the subnetwork changes within the same network. Based on the networks which the session transition takes place, two session transfer types are considered within the scope of this work as described below:

Wi-Fi to Wi-Fi Session Transfer: This is a session transfer within a single network with a localized mobility. It is also called Horizontal Handover or Homogeneous Handover.

Wi-Fi to Cellular Session Transfer: This is a session transfer across different networks with a global mobility. It is also called Vertical Handover or Heterogeneous Handover. When considering the SST between cellular and Wi-Fi, mobile device is assumed to be simultaneously connected to both Wi-Fi and cellular.

Note also that there are two different ways of doing the session transfers:

Break before make: This is where the device is only able to maintain connectivity to a single radio access/network. This sort of hand-over is typical for inter-rat mobility in same-operator mobile networks.

Make before break: The device is able to maintain connectivity across two or more radio access/networks. This sort of hand-over is typical for intra-rat mobility within 3G and 4G networks.

2.1.2 SST Processing

SST processing overall can be treated in several unique steps as described below:

Initiation: Start searching for a new link performing network discovery, network selection and handover negotiation

Preparation: Set up a new link performing layer-2 (L2) connectivity such as authentication, association, and IP connectivity.

Execution: Transfer connection from one access network to another one performing handover signaling, context transfer, packet reception and release of old network resources.

2.1.3 SST Control

SST control involves handling the session handover procedures. Either the mobile device or the network or both may be involved in making session transfer decision and control. Different types of controls are described below:

Mobile Device Controlled - Mobile Device makes session transfer decision and execution. The major advantage with this solution is that it may work over any Wi-Fi access networks including public Wi-Fi hotspots, office Wi-Fi and home Wi-Fi.

Network Initiated and Network Controlled - Network makes use of events, commands, and information to decide if session transfer is needed/desired, to select the target, and to command the terminal to transfer the session. The advantage with the network-based scheme is that it simplifies the mobile device SST support, but instead, requires that there is Mobile IP (MIP) support in the network. The network is responsible for managing IP mobility on behalf of the mobile device. This means that the mobility entities in the network are responsible for tracking the movements of the mobile device and initiating the required mobility signaling on the behalf of the mobile device.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

Mobile Device Initiated and Network Assisted - Mobile device makes use of information available to it and network assists in the processing of session transfer.

2.2 Reasons for SST

Most of the IP-based applications use the IP address of the mobile device. The IP address is at the same time the location identifier of the mobile device from the IP routing point view and the mobile device identity from the IP session point of view. The IP address can also be used to identify a subscription in the operator subscriber management systems. These are the root of the fundamental problems in IP Mobility for networking nodes. When the IP address changes, not only the routing of IP packets changes, but also the identity of the host changes. As a result, IP-based communication breaks in most cases.

An overarching driver for SST is user experience. When using Wi-Fi and/or cellular, users always want to be "Best Connected" and don't care about the underlying technologies. Application-specific experience aside, the average user's patience is generally an important factor. Even if network connection and services were to recover eventually, if the recovery does not complete fast enough, the users would be tempted to fiddle with his device's settings, such as disconnecting and reconnecting to the network explicitly. It stands to reason to posit that any session transfer that leaves the user feel tempted to fiddle with his device's settings is a session transfer that leaves much to be desired.

It is highly desirable, from an end user perspective, to have network services that simply continue to work regardless of how the users move about. Ideally, the users should never have to notice that their network connection has "moved" because of any glitch in connectivity that they can perceive as they use network services, the users should not have to consciously disconnect and reconnect as they move.

Thus, there are two points of reference framing the motivation and consideration for Seamless Session Transfer:

1. **To prevent the users from having to consciously disconnect and reconnect their network services when moving about.** This is gauged by how long the typical user would put up with service disruption until he feels compelled to fiddle with his device's settings, and exemplified by the VPN use case. VPN clients, when unable to reach VPN servers, typically time out in the order of seconds. As such, one can reasonably posit that a session, upon transfer, should fully recover in the order of seconds such that the typical users do not feel compelled to fiddle with their devices' settings, and in such manner that even VPN clients not explicitly supporting mobility would not time out and disconnect (hence compelling the user to deliberately disconnect and reconnect).

2. **To prevent the users from noticing that there has been a session transfer occurring in the first place.** This is the stricter requirement, and is exemplified by the two-way interactive communications applications such as telephony and video chat. Previous studies on call quality suggests that most users can notice an interruption if the telephonic circuit is interrupted for periods in the order of tens of milliseconds.

Taken together, the first suggests a more relaxed requirement, that in order to prevent most users from having to consciously disconnect and reconnect, a session has to be fully restored in a matter of seconds upon transfer. The second suggests a stricter requirement, that in order to prevent the users from noticing any interruption in two-way interactive communications, a session has to be fully restored in the matter of tens of milliseconds upon a transfer.

A classic service that would require session restoration within milliseconds is toll-grade voice-call continuity between mobile and Wi-Fi service. Some file-transfer services do not survive session-loss or break-before-make. We use these as the "hard cases" by which to gauge SST even though they may not be very "exciting" services to demonstrate from a user-experience standpoint.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

It may be reasonable to take the first, more relaxed requirement as the initial goal, and treat the second, stricter requirement as the ideal end goal for SST, with other intermediate objectives and goals to guide the development of SST specifications.

2.3 SST Architecture

There is a considerable amount of work in various organizations in support of Cellular to Wi-Fi and Wi-Fi to Wi-Fi interworking. As shown in the Figure 1, the conceptual architecture for an SST ecosystem has to rely on a multi-device and a multi-application set up. To enable service continuity, the network infrastructure must support the capability to seamlessly aggregate and exchange the end user information regardless of the access network to be able to perform seamless mobility. Therefore, the SST oriented protocols, mobile devices, gateways, and authentication servers play a major role in the core network enabling the SST for both Wi-Fi to Cellular and Wi-Fi to Wi-Fi scenarios.

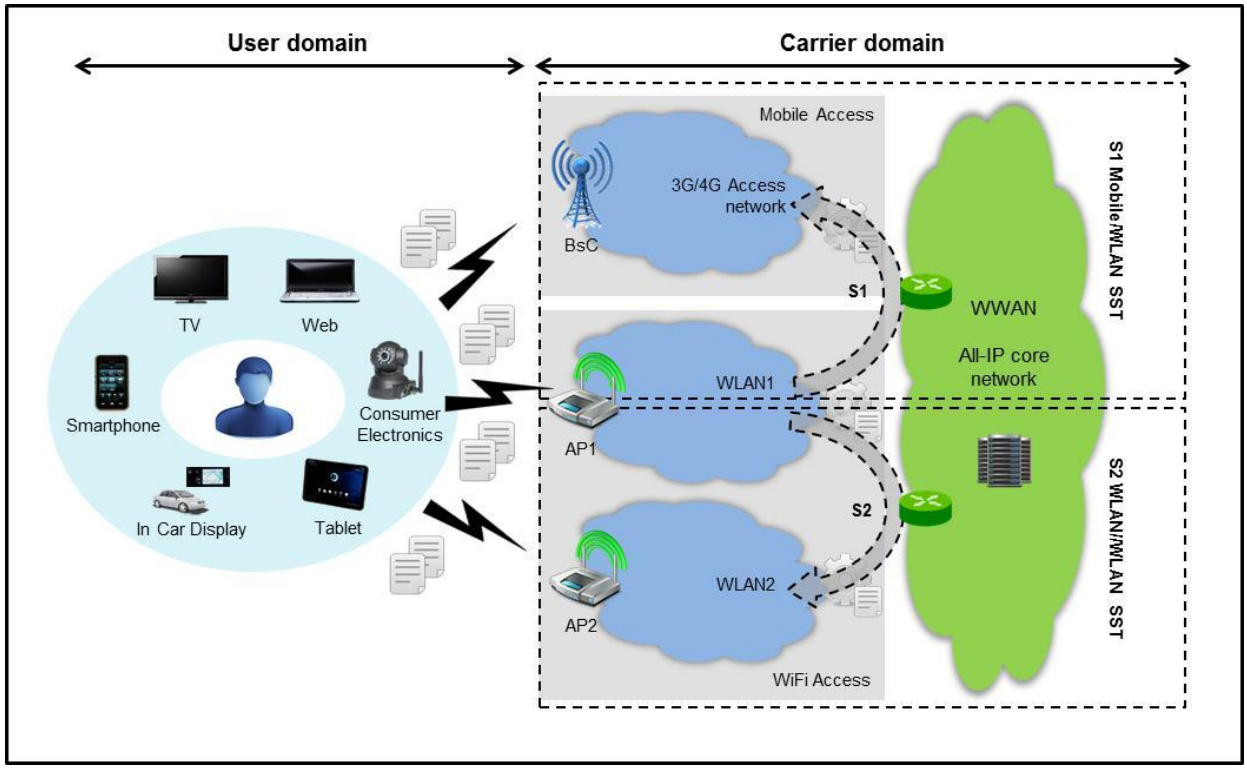

Figure 1 - SST Conceptual Architecture

To achieve the SST, there is a hierarchical architecture in the network regardless whether the SST is layer 2, layer 3, or application implemented. The gateway, which assigns the IP address to the mobile device, acts as the mobility anchor. Within the same network, i.e., from Wi-Fi to Wi-Fi or from cellular to Wi-Fi, the SST can be achieved through either layer 2 or layer 3 mechanisms, as long as access technology between networks is the same. When Wi-Fi and cellular networks are loosely coupled, only can layer-3 mechanism be considered. However, when the two networks are more tightly coupled, layer-2 mechanism could be used for SST.

3. Seamless Session Transfer Scenarios

Maintaining session transfer can be achieved using various mechanisms and creating the uninterrupted user experience. When treating SST, we consider several following broad categories and scenarios:

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

- **Handling IP Address Change** - "IP layer mobility" by maintaining the same IP address or "service layer mobility" by hiding change in IP address
- **Network Types** - Between Wi-Fi to Wi-Fi networks or between cellular to Wi-Fi networks
- **Ownership/Operation of the Networks** – Same or different administrative domains involving roaming. Roaming is a complex issue and it complicates the SST. It is a key factor in achieving SST between Wi-Fi networks and also between Wi-Fi and cellular networks.

These scenarios are discussed in the following sections.

3.1 SST Based on Handling of IP Address Change

The session maintenance could be achieved by various means using either IP address maintenance or mobile device and specific application enablement which could hide and handle IP address change in the system. This section reviews both options.

3.1.1 IP Address Preservation based SST

The requirement for SST between Wi-Fi and cellular networks can be met by IP address preservation mechanisms that use L3 mobility. Mobile IP (MIP) enabled client can seamlessly connect to MIP enabled networks enabling SST by maintaining the IP address provided by the networks. It can give flexibility to users to experience reliable and robust connectivity as they move across multiple spaces between networks.

IP layer handovers within the same access technology (Wi-Fi to Wi-Fi) should be rare, unless the session transfer is between administrative domains.

Since the same IP address is maintained for the application, the change in the network is transparent to the applications and users. Hence, it does not require application specific enablement. However, this scenario is only applicable to where carrier Wi-Fi is deployed. Other Wi-Fi network types such as enterprise Wi-Fi, private Wi-Fi and small shop and free Wi-Fi networks are outside scope of IP Layer mobility.

3GPP has provided multiple solutions for this purpose as described in section 5.2. SST based on IP mobility.

3.1.2 Session Layer Mobility based SST

Today, many popular applications can survive IP address change. Hence, mobile devices and applications already provide support for SST using application layer protocols by reconnecting the same service seamlessly with a different IP address and hiding the changes in IP address from the users. Many well-known browsers, emails, streaming and SIP based applications can adjust to the network layer changes and provide seamless user experience.

Session layer mobility based SST does not require mobility support from the network side. However, it will typically be enabled for each application and puts the burden on device/OS/application vendors so that perceived seamless user experience is provided. Hence, session mobility solution on a platform may not be available for all applications.

Since the session mobility based solution is supported in the mobile devices and applications, it is independent of the Wi-Fi network types such as carrier Wi-Fi, office Wi-Fi and home Wi-Fi. The solution is applicable to all Wi-Fi networks and does not have the limitations of IP layer mobility solution described in 3.1.1, which would be applicable to carrier Wi-Fi networks.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

3.2 SST Based on Network Types and Deployment Scenarios

There are various deployment options that need to be considered within SST scenarios such as where mobility with IP address preservation between cellular and Wi-Fi is required but these two access networks could be from the same operator or from different operators where it involves roaming. Based on the types of the networks, SST scenarios can be categorized in two broad groups:

- Between Wi-Fi networks (Wi-Fi to Wi-Fi)
- Between Wi-Fi and cellular networks (Wi-Fi to cellular)

In general, an administrative domain refers to management of network. In SST scenarios, inter-operator roaming becomes an important element especially in the future heterogeneous multi-access networks. To achieve SST with IP Mobility, flexible and scalable inter-operator roaming arrangements are required. This can be realized by separating the service and access operators, and the roaming infrastructure inter-connecting different operators.

Following sections will treat Wi-Fi to Wi-Fi or Wi-Fi to cellular SST scenarios with various network deployment options.

3.2.1 Wi-Fi to Wi-Fi Seamless Session Transfer

In multi-communication devices, the make-before-break approach is an inherent choice, provided that the mobility solution supports using multiple link interfaces simultaneously and the link-level connectivity can be maintained during the handover. However, make-before-break is not trivial to implement for horizontal handover using a single radio interface - target network discovery, access authentication and latency are essential issues in the case of horizontal handovers.

The Wi-Fi to Wi-Fi SST scenarios belong to a typical horizontal handover model. In this scenario, Figure 2, mobile device roams between Wi-Fi networks. There are two main conditions to enable this:

1. The deployment of access points needs to be accurately planned; and
2. The access network will need to support the updated routing information for the mobile device.

The signal strength and signal to noise ratio are the most often used metrics when moving from one Wi-Fi AP to another one. Signal strength decreases when the station is getting out of the range of the current AP. When the signal quality reaches a minimal threshold, the mobile device may take the decision to initiate a session transfer in order to connect to other APs offering better signal quality. When a mobile device decides to perform a handoff, it needs to find candidate access points. The mobile device collects information about candidate APs and choses one of them. The selection of which access point to use depends on several parameters such as quality of signal, access network capabilities, user preferences and policy whether it has credentials for the network or not. All of these are typically achieved by the mobile device. The initiation of session transfer is not specified in IEEE 802.11 standards and it is done in vendor specific way.

Transition time for roaming between different APs is one of the most important issues to be aware of in SST. The mobile device's scanning process to find an AP may take several hundred milliseconds and it is an important issue with Wi-Fi to Wi-Fi SST, where a mobile device disassociates AP and associates to another AP seamlessly without loss of connectivity. For this process to be achieved, the deployment of such APs needs to be overlapped in coverage at the borders which gives a mobile device the ability to receive acceptable signal strength from another AP, while it is still connected with its current one.

Many studies attribute delays in Wi-Fi to Wi-Fi handoffs to the scanning phase. However, the authentication phase may also introduce substantial delays in the process. This is particularity true when the authentication of a wireless client requires communication with back-end AAA servers that are not located near the fringe of the wireless access network. In this scenario within the same administrative domain, IEEE 802.11r may be

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

used to enable fast authentication which can reduce the overall time of the session transfer processing, as described in section 5.2.

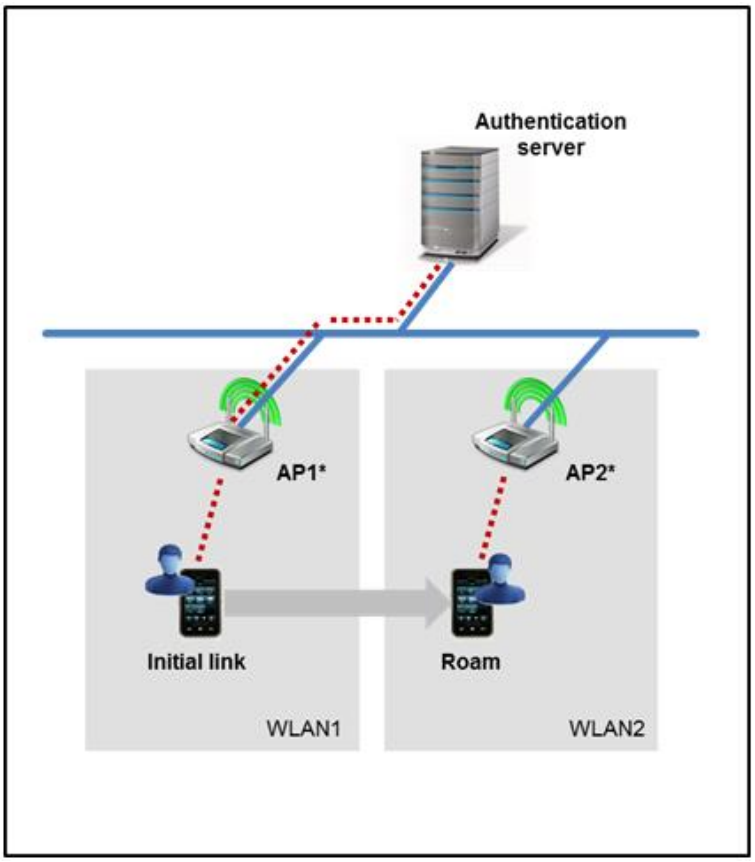

Figure 2 - Wi-Fi to Wi-Fi SST

As long as APs are zoned within the same mobility domain, a layer-2 handover can be supported. If the APs, which are involved in the session transfer, are not within the same mobility domain, a layer 3 session transfer support is needed.

As the mobile device moves around, it may connect to different APs, which may result in subnet change and IP address change. It causes issues between the link layer (L2) and network layer (L3) and thus creating breakage in SST experience. The change in L2 connectivity to the new AP may cause change in IP routing reachability. Therefore, the Wi-Fi access network (Access Router) will need to support the updated routing information for the mobile device and hence, designing L2 handover is important when deploying and configuring the Wi-Fi networks.

Wi-Fi to Wi-Fi session transfer is important for enabling better user experience, additional network capacity and improving coverage in hotspots. However, horizontal handovers between different administrative domains (e.g., operators) resemble vertical handovers - since IP addresses typically change, the new access link characteristics may be totally different and there is no direct connectivity between the old and the new access routers on the access links. The two sub-cases based on the deployments of networks involving administrative domains described in the following sub-sections.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

3.2.1.1 Same Administrative Domain Wi-Fi to Wi-Fi SST

This is similar to enterprise Wi-Fi roaming scenario where mobile devices move from one AP to another AP within the same mobility domain, where the ESS is operated by the same service provider.

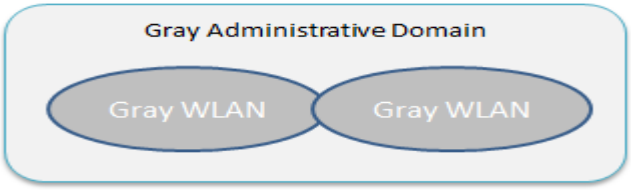

Figure 3 - Same Administrative Domain Wi-Fi to Wi-Fi

The same IP address may be maintained by the network and device, hence seamless session transfer should be supported relatively easy. If the APs belong to same mobility domain, SST can be supported using layer-2 mechanisms. If the APs within the same WLAN belong to different mobility domains, it will involve layer-3 mechanisms to support SST.

Mobility in this scenario can be handled locally, within an administrative domain. Movement within the localized mobility management domain does not require active participation of the mobile device on mobility management signaling.

Wi-Fi to Wi-Fi SST in the same administrative domains relies on L2 triggers. The mobile device and AP need to receive an indication that the handoff is imminent for the L3 mobility protocols to work. The triggers should be received by the mobile device for mobile-controlled handover, and received by the access router for network controlled handovers. Timely reception of the trigger is needed as protocol signaling needs to take place in parallel with the handoff. Protocol signaling over the current link should be completed prior to loss of connectivity.

Even if no change in subnet takes place, the AP may still need to communicate the change in the link reachability to the local access router. In order SST to occur, the mobile device must identify the target AP. When the target AP selection process is completed by the mobile device, the SST process begins through the update of the routing information.

3.2.1.2 Different Administrative Domains Wi-Fi to Wi-Fi SST

This is a case where a mobile device moves from one Wi-Fi network to another Wi-Fi belonging to a different service providers i.e., administrative domains. For example, a user connects to a Wi-Fi serviced by his home service provider at a section of airport. The user starts a VoIP call and moves to another section of the airport where the Wi-Fi hotspot service is provided by a roaming partner of the home service provider. Here, since the two access networks are operated by different providers, the IP address will change and there will be more entities involved to enable seamless session transfer.

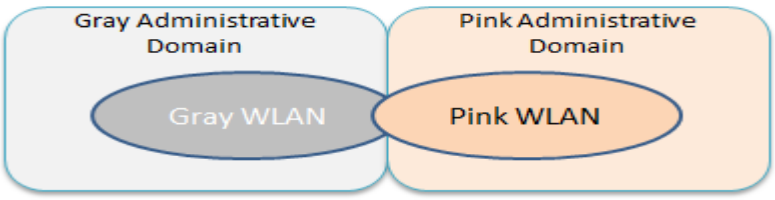

Figure 4 - Different Administrative Domain Wi-Fi to Wi-Fi SST

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

The recent interest has mainly been on improving the vertical handover case. However, the evident need for building additional network capacity and bettering the indoors coverage in hotspots with short range radio technologies has made horizontal handovers an important topic, as well. Yet horizontal handovers between different administrative domains (e.g., operators) tend to resemble vertical handovers in a sense that IP addresses typically change, the new access link characteristics may be totally different and there is no direct connectivity between the old and the new access routers on the access links.

Inter-operator Wi-Fi roaming measurements and understanding the impact of the access authentication in a roaming environment are essential knowledge for operators when they start to deploy seamless mobility infrastructure in Wi-Fi environment.

The requirement for these additional entities in the inter service case may conspire to prevent the possibility of effecting seamless session transfer depending on whether the two Wi-Fi service providers have roaming agreements and it could be easily discovered by the mobile device.

If the two service providers do not have a roaming agreement in place, due to authentication and association delays and IP address changes, the seamless session transfer becomes more unlikely under this scenario. Even though the mobile device/user might have two separate credentials for both networks that can be used for access, in this scenario, we assume there will not be any session transfer available for the user and it is outside scope of this work.

3.2.2 Wi-Fi to Cellular SST

In this scenario mobile device roams between Wi-Fi and cellular networks. The SST infrastructure is the combination of network infrastructure from one or multiple operators. Thus, this scenario relies on SST infrastructure (e.g. Packet Data GW) that supports cellular network IP access to external IP networks and SST protocols (e.g. PMIP, GTP) that enable communication between both networks.

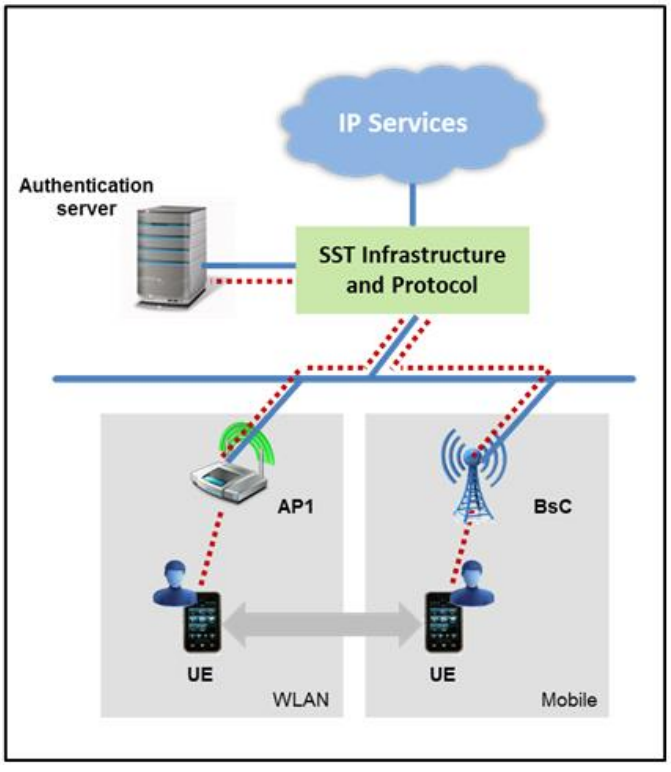

Figure 5 - Wi-Fi to Cellular SST

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

The SST solutions may be network, client or mixed mode based. For the PMIP case, the GW acts as the local mobility anchor (LMA) and the access gateway (e.g., ePDG) acts as the mobile access gateway (MAG) in the PMIP architecture.

There are many options for Wi-Fi and cellular interworking ranging from a quite simple cellular and Wi-Fi interworking to fully seamless inter-system operation. The Wi-Fi could be an integral part of the 3GPP system or the two systems could be separate or loosely coupled.

For IP preservation based solution to be viable, there is a need for significant integration between the Wi-Fi and 3/4G networks. Also, there would be a need for many deployed Wi-Fi networks which would be able to support for it. IP preservation based L3 handover requires significant preparation and context transfer between two networks and hence the network controlled handovers could put significant burden on the operators and core network components.

Wi-Fi to cellular use cases have been discussed extensively in [3]. 3GPP TR 22.934 introduces several scenarios, representing various levels of integration between Wi-Fi and 3GPP networks [3].

Scenario 1 – Common Billing and Customer Care

This is the simplest scheme of 3GPP and Wi-Fi interworking. It integrates a single billing and customer services. The customer receives one bill from the mobile operator for the usage of both cellular and Wi-Fi services. Customer care is also integrated

Scenario 2 – 3/4G system based Access Control and Charging

Wi-Fi authentication, authorization, and accounting (AAA) is handled by 3GPP standards back-end. This requires AAA for subscribers in the Wi-Fi to be based on the same AAA procedures used in the cellular data networks. It means a mobile subscriber can use his or her subscriber identity module/ UMTS-SIM (SIM/USIM) to access Wi-Fi services.

Scenario 3 – Access to cellular system packet service (PS) based services

Subscribers can access 3G packet service, which is extended to the Wi-Fi. IMS based services such as instant messaging, location based services and presence based services can be implemented

The main goal for mobile operator is to provide access to its 3GPP data services to subscribers in a Wi-Fi environment. Mobile subscriber should be able to have access/select 3GPP data services through the Wi-Fi access network. Although the user is allowed access to the same 3GPP data services over both the 3GPP and Wi-Fi access networks, service continuity is not a requirement for this specific scenario.

Scenario 4 – Service Continuity

In this case, PS services will remain connected after handing over between Wi-Fi and cellular. This scenario allows supporting PS services in scenario 3 during and after change of access between Wi-Fi and UTRAN/GERAN. The change of access maybe noticeable to the end-user but there will be no need for services reestablishment due to the different access network capabilities. There may be a change in service quality after the transition from different access network. Hence, it is possible that some services may not survive, as the continuing network may not support an equivalent service.

Scenario 5 – Seamless Service

Seamless service continuity is supported in this scenario. Therefore, a user session during mobility (cellular to Wi-Fi) should continue and no noticeable disruption shall be experienced by subscribers.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

However, this scenario requires a tight integration support between Wi-Fi and cellular networks. The seamless service continuity between cellular and Wi-Fi can be achieved by supporting three main aspects as below:

1. Proper interworking architecture
2. Fast Inter-systems handovers
3. QoS on both cellular and Wi-Fi

Optimized and non-optimized handover between 3GPP and non-3GPP networks are defined in TS 23.402 [4].

Different access networks often represent disparity in link characteristics. For example, link bandwidth, latency, bit-error rate and the degree of bandwidth asymmetry may differ considerably. Therefore, sudden changes in the access link characteristics due to vertical or horizontal handovers may interfere with the transport layer protocols and with the applications that base their protocol behavior on the measured end-to-end path conditions [14].

Also note that direction of the transition either from Wi-Fi to cellular or from cellular to Wi-Fi could involve different characteristics such as sudden loss of network connectivity when moving from Wi-Fi to cellular, although network connectivity could be available when transitioning from cellular to Wi-Fi.

In some cases, it may not be possible to support SST where services using resources specific to the source domain that cannot be maintained using resources in the target domain.

3.2.2.1 Same Administrative Domain Wi-Fi to Cellular SST

The Wi-Fi is integrated in operator's network. The operator operates both Wi-Fi and cellular access networks**.** The mobile device moves between two authenticators in the same domain. It could be any of the scenarios 1, 2, 3, 4 and 5 in section 3.2.2.

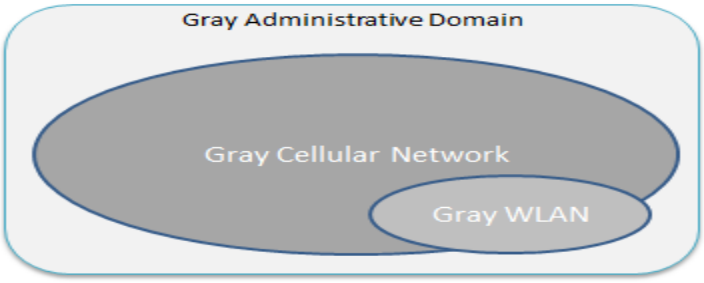

Figure 6 - Intra Administrative Domain Wi-Fi⇔Cellular SST

To date, most network policy control infrastructures are applied within a homogeneous network scenario where a single network operator owns and controls the end-to-end networks. As we move to a heterogeneous operator environment then the various networks may be owned by different operators and the various technologies may not always offer the same underlying policy enforcement mechanisms.

3.2.2.2 Different Administrative Domains Wi-Fi⇔Cellular SST

The scenarios described in [6] all relate to the case where the networks are owned and operated by separate parties. The mobile device moves between two different domains.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

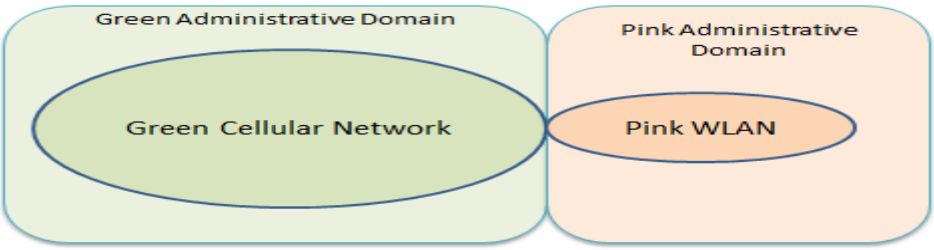

Figure 7- Different Administrative Domains Wi-Fi⇔Cellular SST

The cost of building coverage for both Wi-Fi and cellular networks might be too high to justify the investments. As a result, operators may reduce the cost of building the infrastructure by sharing access networks. Sharing can be handled in two ways. Either the access network is shared in a way that each operator sees it as their own network or the sharing is based on roaming where customers are allowed to attach to visited operators' networks. SST across administrative domains is rather a challenging topic from IP Mobility point of view. This is mostly due the nature of inter-operator roaming settlements and the heavy involvement of inter operator AAA infrastructure during handovers.

Mobile operators are used to have control over the mobile devices that attach to their networks. In cellular technologies, the network can even instruct a mobile device to initiate a handover. When coupled with the network access authentication, it is even possible to steer mobile device's inter-operator roaming and target access network selection. These kinds of features are generally missing from current IP Mobility solutions. Current solutions are more or less mobile node centric when it comes to the session transfer decision making. However, mobile operators deploying large wireless network infrastructure are looking into similar properties also on the newer IP optimized radio access technologies. Reasons for doing such mobility management and steering of roaming can be based on commercial arrangements, optimizing the service accessibility or then just load balancing [14].

SST with a 3rd-party provider requires a prior interworking agreement, and the corresponding technical arrangements. If the mobile operator has no service agreement with Wi-Fi service provider, mobility and SST may not be possible for the third party scenario. If this is the case, then SST is out-of-scope.

The backend support systems, roaming and inter-operator interconnection architectures are essential from SST support point of view. SST environment could be a complex composition of heterogeneous access networks inter-connected via a flexible roaming infrastructure.

When users have multiple billing relationships with different access networks and so effectively multiple home operators, it is therefore no longer clear who owns the customer experience. In a heterogeneous networking environment, where networks belong to multiple administrative domains, even guaranteeing a baseline QoS might turn out to be hard, if not impossible.

Each radio has own IP address and hence the seamless session transfer and mobility is more challenging. Because Mobile Operator has no WLAN service agreement with subscriber, mobility and seamless session transfer may not possible for the third party scenario.

4. Seamless Session Transfer Requirements

To achieve seamless session transfer between Wi-Fi to Wi-Fi and Wi-Fi to cellular networks, the following requirements should be considered for networks, devices and applications. Some of the IP flow mobility requirements are provided in [1]. Please see section 5 for further information on various SDOs work.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

- For the handover among Wi-Fi APs, the IP address shall be preserved for the same connection if there is a need from service or application perspective.
- Service continuity shall be maintained so that the application will not be interrupted and impact to the user experience shall be minimized.
- The service continuity shall be achieved when a mobile device moves from cellular to Wi-Fi and vice versa.
- If the mobile device is under the coverage of more than one access, including cellular and Wi-Fi accesses and communicates using multiple accesses simultaneously, it shall be possible to select one access when a flow is started and re-distribute the flows to/from a UE between accesses while connected.
- It shall be possible for the operator to enable and control via policies the simultaneous usage of multiple accesses. The operator may also provide policy on the distribution of IP flows between available accesses.
- The use of different accesses for applications/flows will be based on the operator's policy as well as the user's preferences.
- The impact to the mobile device and the network shall be minimized to achieve the seamless session transfer.

Although the network based mobility solutions in general will offer the opportunity for IP preservation without requiring mobile device's networking stack change, but in reality the mobile device needs to carefully present a single virtual service point to applications on the host when the IP address actually switched from one radio interface to another.

3GPP TR 22.934 [3] provides some service requirements for 3GPP and Wi-Fi interworking including network selection, access control, authentication, security, roaming, terminal aspects, charging and billing.

5. SST Related Work in Various Organizations

This section provides the state of the SST efforts in various organizations including IEEE, WFA, 3GPP, GSMA, IETF, and WBA. However, we limit the scope to review to solutions that are mature enough to be adopted by the industry. We should note that even with mature protocols, there could be issues that do not show up until in large scale deployment such as mobile operator networks.

5.1 IEEE Work

IEEE has several SST related work items as described in the following sections.

5.1.1 IEEE 802.21

IEEE 802.21 is a standard published in 2009 [10]. The purpose is to improve the user experience of mobile device by facilitating handover between heterogeneous access networks

802.21 Media Independent Handover (MIH) provides information independent of the media type. It is a framework that enables transparent service continuity. MIH provides link layer intelligence to upper layers to optimize handovers with network discovery and handover command capabilities. It defines an MIH Function and provides a protocol interface to communicate between peer MIH peers. However, it does not define policies or an inference engine required to optimize user experience during a handover. 802.21 Event Service provides triggers and events that minimize connectivity disruption during handover.

IEEE 802.21 helps make handover decisions involved in handover Initiation, network selection and interface activation but the handover execution is outside its scope. It can provide measurements, triggers, neighbor list

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

etc. IEEE 802.21 supports cooperative handover decision making between network and mobile device. However, there is no known large scale deployment of IEEE 802.21.

5.1.2 IEEE 802.11r – Fast BSS Transition

For successful implementation of seamless session transfer from Wi-Fi to Wi-Fi it will be important for mobile devices to quickly perform a handoff from one AP to another AP in order to be able to maintain session continuity, particularly to maintain acceptable voice quality.

IEEE 802.11r (Fast BSS Transition), is a ratified amendment fully incorporated into the IEEE Standard 802.11-2012 [9]. Fast BSS Transition reduces the authentication time required when a mobile device is handed off from one AP to another. With Fast BSS Transition when a mobile device associates with an AP, it pre-authenticates with all other access APs at the same time within the same ESS. Pre-authentication reduces the handover time within the same ESS.

5.1.3 IEEE 802.11ai – Fast Initial Link Setup (FILS)

For successful implementation of seamless session transfer from 3G/4G to Wi-Fi it will be important for mobile device to quickly establish an initial link to the AP, to be able to maintain session continuity, particularly to maintain acceptable voice quality.

The IEEE 802.11ai Task Group is working on enhancements to the 802.11-2012 standard to decrease the time it takes a mobile device to set up a link with an AP (including scanning for an AP, authenticating, negotiating QoS parameters, and associating with the AP).

However, this work is still at the early stage and the ratification of 802.11ai amendment could take a couple more years.

5.2 3GPP work

The 3GPP EPC provides interworking functionality between 3GPP and non-3GPP (both trusted and non-trusted) access technologies according to the 3GPP specifications which gives new options for mobility through the use of inter-technology handover over several access network technologies.

As it is specified in TS 23.402 [4], the Evolved Packet System (EPS) introduced a heterogeneous 3GPP system, where multi-access technologies are connected to a common core network, called EPC.

One fundamental difference between the 3G network and the EPC is the capability of integrating non-3GPP access technologies such as Wi-Fi and WiMAX into the EPC core network defined by 3GPP and thus provide access to Packet Data Networks (PDNs).

In the past number of years, 3GPP has been working specifications for the integration of Wi-Fi and 3GPP networks, most commonly based on the TS 23.234 “I-WLAN” standard [5], and mobility management [6].

In I-WLAN mode, MIP is supported to provide seamless roaming. However, I-WLAN specs only address the Wi-Fi interworking and mobility with 3GPP networks leaving out non-3GPP access networks. To fill the gap, 3GPP has recently developed the EPC architecture to support the interworking and the mobility for these other access technologies.

As defined in the EPC architecture [4], MIP, GTP and PMIP all support IP-session continuity. However, due to the heavy overhead added to the mobile device and the lack of majority vendor support, MIP has not gained that much traction.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

Interworking of Wi-Fi networks with cellular networks has been part of 3GPP specifications since Release 6 in 2006. WLAN interworking allows operators to integrate WLAN access into the cellular packet core network, providing harmonized and secure traffic handling for both cellular and WLAN access. With packet core network integration, an operator can gain improved visibility and control over WLAN traffic and the customer experience. Furthermore, users are able to reach familiar 3G/LTE services via both cellular and Wi-Fi accesses. This makes Wi-Fi a truly integral part of mobile broadband access. WLAN interworking enables selected Wi-Fi users to be linked to operator functions like Charging, Policy Control, Deep Packet Inspection, QoS and Lawful Interception

Since Release 8 in 2008, 3GPP specifications have supported seamless session transfer between Wi-Fi and 3GPP access networks including UMTS and LTE [7]. Subsequent releases have added continuous enhancements to the capabilities. There are three classes of solutions described in the 3GPP specifications and the corresponding interfaces are S2a, S2b and S2c. The architecture showing the three interfaces is depicted in the Figure-8. In all cases, session transfer is provided between the 3GPP network and the Wi-Fi network with the P-GW acting as the user plane anchor between the two access networks. The S2a and S2b approaches employ network–based protocols such as the GTP and PMIP. The S2c uses host-based mobility protocol, i.e., DSMIPv6. The PMIPv6 and DSMIPv6 will be described in the IETF section. All three approaches are described in 3GPP specification TS23.402.

Operators can provide interworking for both trusted and untrusted WLAN networks. Whether a WLAN is trusted or not in 3GPP terms is determined by the home operator and depends on the hotspot deployment scenario (e.g. the security of the WLAN network) and the business relation between the Wi-Fi provider and the mobile operator. For example, when a subscriber of Mobile Operator A using a Wi-Fi enabled handset connects to Wi-Fi Operator B's Wi-Fi hotspot, Operator B's hotspot might be considered as untrusted WLAN access. Therefore, the handset has to establish a secure tunnel to an ePDG before the traffic is routed to Operator A's core network. In contrast, if the subscriber connects to Operator A's own Wi-Fi hotspot, the mobile core network can consider it as trusted Wi-Fi access and no secure tunnel is needed when the traffic is routed to the core network.

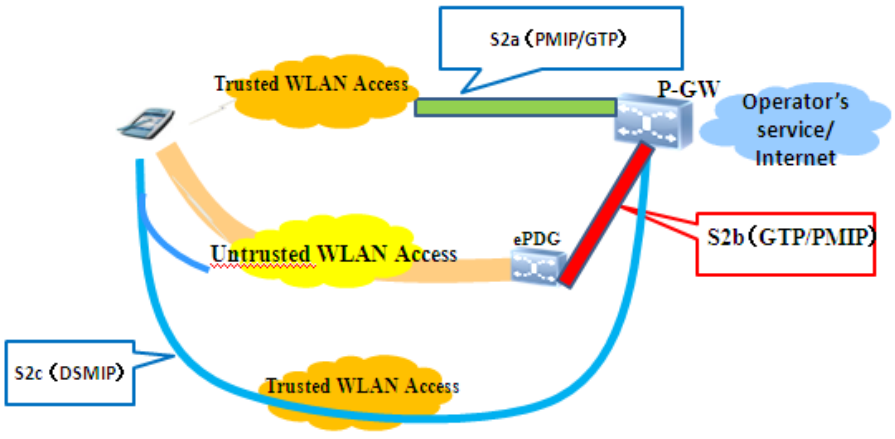

Figure 8 - WLAN and cellular interworking

S2a: The WLAN is considered to be a trusted non-3GPP access network. This solution can allow unmodified UEs to access the P-GW through S2a. In this option, the UE connects to the WLAN using standard secure Wi-Fi procedures without the need for mobility or tunneling support in the UE. Either PMIPv6 or (as of Release 11) GTP protocols can be used for the interface between the WLAN and the P-GW. Either IPv4 or IPv6 may

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

be used in the transport layer. Seamless session transfer is not supported in 3GPP Release 11. SST is being discussed in Release12 when this whitepaper is drafted.

S2b: The WLAN is considered to be an untrusted non-3GPP access network. The UE must establish a secure IPsec/IKEv2 tunnel to a network element, the ePDG, through which the P-GW is then accessed. Either PMIPv6 or (as of Release 10) GTP protocols can be used for the interface between the ePDG and the P-GW. And either IPv4 or IPv6 transport may be used.

S2c: This approach can be used over either trusted or untrusted non-3GPP access networks. The UE must connect to the P-GW using DSMIPv6 which is described in the following IETF section. This MIPv6 protocol is "dual stack" in that it uses either MIPv4 or MIPv6 mobility constructs and operates over either IPv4 or IPv6 networks. In Release 10, the S2c option added support for IP mobility per flow in addition to IP session mobility.

In 3GPP, work/study items related to session mobility are still ongoing in Release 12, including NB-IFOM and SaMOG. The NB-IFOM study aims to add the IP flow mobility feature of S2c to S2a and S2b. The ongoing SaMOG study will investigate IP address preservation and simultaneous access 3GPP services thorough different APNs over S2a etc. The P4C work item in Release 12 handles the converged policy control for S2a and S2c based on the PCC architecture. The interworking architecture (two policy control systems in mobile and the fixed network respectively) for S2b and S2c has already been defined in Release 11.

In the 3GPP evolved core network, network-based mobility mechanism support is provided via the S2a interface for trusted non-3GPP access technologies and via the S2b interface for untrusted non-3GPP access technologies. In both cases, the PDN GW acts as the Local Mobility Anchor (LMA). In case of trusted non-3GPP access technology, the access gateway (AGW) within the non-3GPP access network acts as the Mobility Access Gateway (MAG), whereas in case of untrusted non-3GPP access the Evolved Packet Data Gateway (ePDG) acts as the MAG.

3GPP also introduced GTP to support IP mobility in all-IP core networks. GTP is a network-based IP-level mobility protocols that support uninterrupted handoff by maintaining the same IP address when moving from one network to another. It is a tunneling protocol over UDP/IP used to build GTP tunnels and map traffic into different tunnel flows from the SGSN to the GGSN in 3G architectures and from the SGW to the PWG in EPC architectures. GTP is tailored for 3GPP networks and it is often criticized for not being a suitable mobility protocol for other non-3GPP access technologies.

LTE has been designed to be an all-IP and support only packet-switched services thereby providing seamless IP connectivity between heterogeneous access networks without any interruption to the mobile device's application during mobility and service.

In 3GPP access technologies, we can only choose between two network-based mobility protocols (PMIPv6 or GTP) and the selection of one mobility protocol over the other has no impact on the terminal since the network choice of protocol is transparent to the mobile device. But, we should note that even if multiple mobility protocols are supported in a network deployment, only a single protocol is used at a time for a given mobile device and access type.

5.3 WFA work

WFA has several programs relevant to the SST. Following sections provides a short description of them.

5.3.1 Passpoint (Hotspot 2.0)

WFA Passpoint Release-1 enables improved Wi-Fi hotspot connectivity experience, making hotspot network access as easy as cellular network access by simplified Wi-Fi hotspot network discovery, automatic Wi-Fi hotspot authentication and easy roaming [13]. It has not yet focused on session continuity issues. Hotspot 2.0

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

Release 2 program includes provisioning of operator policies and user credentials. Elements of HS2.0 subscription management object (MO) will control some aspects of Wi-Fi roaming and handover.

5.3.2 Voice over Wi-Fi

WFA certification for Voice Enterprise and WMM admission control is launched in May 2012. Voice enterprise was formed in 2005. This group determined market-driven interoperability requirements for certification of voice-enabled client devices and Wi-Fi infrastructure products. The certification program focuses on an enterprise test plan comprising; voice metrics performance in a loaded network, fast BSS transition based upon IEEE 802.11r, voice handoff performance in an enterprise environment, and radio resource and spectrum management features related to voice and efficient handoff.

5.3.3 Converged Wireless

The Converged Wireless Group (CWG) develops and maintains test methodologies and performance criteria for the RF performance evaluation of Wi-Fi mobile “converged devices”. “Converged devices are defined as handset devices that incorporate both cellular and Wi-Fi functionality. Due to the many potential applications and deployment scenarios that converged equipment may function in, a uniform method of profiling the RF performance of converged devices is required. The test document maintained by the CWG contains the proposed test methodologies and performance criteria for the RF performance evaluation of Wi-Fi mobile converged devices. This test plan is part of the CTIA and Wi-Fi Alliance certification programs.

5.4 IETF work

The IETF (Internet Engineering Task Force) defines IP layer mobility protocol that could be used in Wi-Fi and cellular network seamless handover scenarios. There are mainly two types of IP mobility protocol that are defined in the IETF and are currently being used in 3GPP specification: DSMIPv6 and PMIPv6.

DSMIPv6 (Dual Stack Mobile IPv6) is specified by RFC 5555 [15]. It is the extension of mobile IPv6 and NEMO specifications. DSMIPv6 can support both IPv4 and IPv6 transport even if there is Network Address Translation (NAT) in the path. It also supports both IPv4 and IPv6 home address. Besides the basic mobility support, there are some extensions of RFC5555 to allow DSMIPv6 support flow based mobility. An IP flow could be identified by the IP layer five-tuple. DSMIPv6 allows one IP flow move from one access network to another and still maintain the session continuity.

PMIPv6 (Proxy Mobile IPv6) is network based mobility protocol specified by RFC 5213 [16]. It is used to facilitate IP-level session continuity. PMIP-based handover relies on the network’s mobility agent rather than the mobile device to detect the mobile device’s movement and performs IP mobility signalling. Network based means the basic PMIPv6 does not require any special support of the mobile device. It has the same basic principle as the client based mobility protocol such as DSMIPv6. The difference is that there is a MAG function in the network which is used for sending mobility binding update on behalf of the mobile device. There is ongoing work that extends PMIPv6 to support flow based mobility.

For the future evolution of mobile IP, the IETF founded DMM (Distributed Mobility Management) working group. DMM aims to eliminate the centralized anchoring point of current IP mobility protocol by introducing distributed and dynamic anchoring concepts. Currently the DMM working group is focusing on defining 'Solution Requirements'. The target time of the DMM working group to finish its work is March 2013.

5.5 GSMA Work

GSMA Terminal Steering Group Wi-Fi (TSG-WIF) is working on terminal’s Wi-Fi requirements. It consolidates terminal Wi-Fi requirements based on network/connectivity use cases, Wi-Fi experiences from operators and inputs from relevant standardization bodies. It defines a minimum set of Wi-Fi capabilities covering authentication, security, connection management and usability requirements; it includes references to relevant

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

work driven by the 3GPP, the Wi-Fi Alliance on Hotspot 2.0 and by OMA on the Connection Manager. It serves as a baseline for operators' terminal requirements, terminal implementations and related standardization activities.

GSMA TSG-WIF work also considers terminal's requirements for network handover support including IPv6, ICMPv6, IETF neighborhood discovery, DHCP support, and others [8].

The second phase of TSG-WIF work is under progress and expected to be completed in 2013.

Additionally, the joint taskforce between GSMA-WBA is addressing the SST with IP preservation topic on the Phase-2 of the work (2012-13). Section 8 provides this initiative's findings from the first phase of its work.

GSMA TR-61 specifies a common technical solution for roaming service between Wi-Fi service providers from an inter-operator perspective [7]. It describes access interfaces including connection and authentication procedures in interoperable way to implement Wi-Fi roaming.

6. Available SST Solutions and State of the Industry

Seamless session continuity is a well-known research topic that has been studied for a number of years. Many solutions have been available and proposed for seamless session transfer.

In the past few years, operators have taken steady steps to evolve towards a single all-IP packet core network. For operators this accomplishment has been both an operational as well as a business imperative. The economics of IP networking have been clear from the beginning; but, the implementation of all-IP mobile packet core networks has been a long winding road. However, with the beginning of LTE deployments, some operators have largely transitioned to basic all-IP networks. This is a significant step forward in enabling seamless session transfer between Wi-Fi and cellular networks. With these transitions, operators and vendors are at a unique interception for enabling seamless session transfer leveraging the deployed all IP-based networks and services.

WBA has trialed the Next Generation Hotspots demonstrating end-to-end seamless authentication over Wi-Fi and mobile networks [12]. This is a very important step in enablement of end-to-end SST functionality.

As described in section 5.2, there are various work items going on in 3GPP. Some of them have been available and some of them are currently under progress such as L3 optimized handover, LTE/Wi-Fi carrier grade aggregation. However, it will be a while before these solutions to be defined and deployed in the industry.

As can be seen from Section 5, the availability of Seamless Session Transfer to the Mobile / Wi-Fi marketplace depends greatly on an alignment of standards-based specification, infrastructure implementation and certification, device-introduction to mobile end-users and the creation of interworking arrangements with disparate operators.

7. Case Studies

7.1 Swisscom Case Study

In 2004, Swisscom launched the first solution for seamless handover between Wi-Fi and cellular technologies that maintained the IP, with automated Wi-Fi authentication using EAP-SIM. This decision was as a result of Swisscom's vision of having a fully seamless customer experience, irrespective of the access technology.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

7.1.1 Implementation

The lack of devices, software implementations and standards were circumvented by the development of an implementation of Mobile IP according to RFC 3220 within the connection manager (UDM) of Swisscom for mobile broadband data services.

Swisscom used standardized features and technologies of cellular, Wi-Fi and IP technology. Nevertheless, this vision of seamless connections over heterogeneous technologies demanded major development efforts on network and client sides. The main obstacles to implement a seamless handover solution were the lack of a standardized hardware that supported Wi-Fi and cellular at the same time on client side. The absence of session continuity between Wi-Fi and mobile broadband and only a few devices that supported EAP-SIM authentication out of the box required strong partnerships with hardware suppliers. No devices were available at that time which was designed for this functionality. The mobile network was challenged by adding a so called home agent (HA). This required a close collaboration with a strong network solution provider.

7.1.2 Solution

Swisscom developed a data card in a close partnership with a hardware supplier containing cellular and Wi-Fi and a connection manager, which is called Unlimited Data Manager and which was able to maintain the Mobile IP (MIP) tunnel. All of these products were combined under the brand of "Mobile Unlimited", data services for notebooks exclusively.

In the core network, MIP was designed to support seamless and continuous Internet connectivity. On the network side a HA was integrated within the mobile core. Additionally, a decision about the placement of the foreign agent had to be taken. Swisscom decided to put it in the client and create a VPN like connection to the mobile network to simplify the network design and such an implementation created additional complexity into the network and the client to network dependency has to be maintained over years. There are some restrictions when it comes to traffic inspection of the MIP tunnel and the data payload is reduced due to nature of the tunnel header.

Furthermore, the market penetration of MIP based solution is rather low, hence the innovation of the available products are modest.

7.1.3 Benefits

Swisscom sees the benefit for “Mobile Unlimited” customers as follows:

- Session continuity (e.g. VPN and HTTPS connections). Many applications using secure connection (e.g. SSL/TLS or IPsec) cannot handle IP address changes while the session is ongoing.
- Mobile network inter- and intra-frequency handovers: A mobile network can be configured and tuned for a variety of different intra- and inter system handovers (e.g. 2G <=> 3G <=> 4G). Depending on the mobile network provider and the terminal features, there are limitations and/or restrictions and technology changes might lead to IP changes and session interruptions and the mobile device has to re-establish the connection again.
- Mobile network stabilization: During movement an intersystem or cellular handover can take some time or fail. MIP protects from connection drops and ensures session continuity that connectivity can be re-established without impacting the customer/ applications.
- Broken connectivity detection and re-establishment: Today‘s MIP implementation monitors the link and performs a technology switch if the link underlying is not working anymore due to:.
  - Failed PWLAN authentications

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

- Successful PWLAN authentications but backend issues preventing the client to get real connectivity
- Mobile network connection successfully established but no traffic is possible

• Application stabilization: MIP parameterizes the TCP/IP stack to the very best compatibility and performance from the perspective of connectivity assurance. This allows users to use their applications as usual even when using mobile network technologies.

7.1.4 The Mobile Device Support for SST

Often, mobile operators and WISPs lack visibility on the customer's computing device. The Unlimited Data Manager (UDM) addresses several issues customers usually face. :

It provides automatic "one-click" connection setup and maintenance with the ability to (auto) select the "best" connection method available. Moreover, it supports various ways to customize the notion of "best" from the user's as well as from the corporate customer's perspective.

Wireless services are inherently less reliable than traditional wired services, therefore need for automatic connection re-establishment, session continuity assurance and seamless handover capabilities including (802.1 x authentications like EAP-SIM, EAP-AKA, EAP-TLS) are important factors that add value to users. The main capabilities supported by UDM could be summarized as follows:

- Unify management of devices and services in one application
- Support the user selecting the right device & service and plan based on needs
- Employ seamless handover component to provide for uninterrupted service
- Allow the integration of additional application and services
- UDM's skinnable GUI delivers the brand to users' desktops.

- The UDM supports and unifies Ethernet, WLAN, GPRS/EDGE, UMTS/HSxPA, LTE, WiMax and, Dialup technologies

7.1.5 Today's Challenges

Swisscom applied a simple rule in UDM that defines Wi-Fi as the preferred access technology as long as the response time of the data packages remain in a certain range. With the evolution of the cellular access technologies like HSPA(+) and LTE, we may need a differentiated view on what the best network is. Wi-Fi is in most cases still the first choice, but a premium customer may get even a better user experience on cellular, depending on the congestion situation of the currently used Wi-Fi hotspot.

Since Swisscom decided to launch its data subscription more and more based on different bandwidth graduation instead of volume, a policy controlled service differentiation selection is required and access technology selection enforcement is desired.

A specific and customized client should not be needed anymore. Instead it shall be integrated in the user equipment's operating system. The provider shall still be capable to control user equipment specific settings and therefore some sort of mobile device management is needed (i.e. ANDSF).

Today's challenge is to evaluate and design the next generation solution that covers the present and future demand of mobile data access. Swisscom supports and tries to influence all industry initiatives that promote the adoption of single standards related to seamless authentication and handover between wireless technologies.

The target is to simplify the core network. Since the anchoring point for cellular, Wi-Fi and Mobile IP is not centralized, Swisscom is looking into solution that controls all data traffic in a single box like GGSN/PGW.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

Swisscom is constantly developing new service functions spread over all access technologies. Harmonizing the service experience over different access platforms with different intentions is getting more and more complex.

7.2 Green Packet Case Study - Client Based SST Solution

Green Packet has mobile client based SST solution that is composed of two parts:

a. Client Mobile IP Module
b. Connection Manager

The Mobile IP Module includes MIP signal control and MIP tunnel management. It is used to communicate with Home Agent (HA) for MIP registration and MIP tunnel data traffic encapsulation.

The Connection Manager is to enhance the function of OS native connection manager, which supports the following capabilities:

- Helps end user easily configure the WiFi and cellular network parameters
- Smart connection to best network according to current time, location and signal strength
- Improve SST performance when network handover happens (make before break)
- Fast detect the network disconnection and resume network as soon as possible
- Simultaneously keep both Wi-Fi and cellular connection to support MAPCON/IFOM

7.2.1 Client MIP Solution

The Client MIP solution includes MIPv4 and DSMIPv6, which can be deployed on laptop and mobile device.

7.2.1.1 Session Transfer Scenarios

1. 3G handover to Wi-Fi: When mobile device detects available Wi-Fi connection, it connects to Wi-Fi before detaching from cellular
2. Wi-Fi hard handover to 3G: Non seamless session transfer takes place when:

   a. Mobile device fast moves out the Wi-Fi signal coverage
   b. AP lost power
   c. AP reaches the max capacity; mobile device is disconnected by AP
   d. CM detects the Internet access lost and tries to resume it in 3G/4G

3. Wi-Fi soft handover to 3G takes place when:

   CM detects Wi-Fi QoS is bad, before it disassociates Wi-Fi, it connects to 3G. Mobile device then actively disconnects from Wi-Fi

4. Wi-Fi handover to Wi-Fi

   a. Same SSID, different BSSID and mobile device IP address can be maintained
   b. Same SSID, different BSSID and mobile device IP address changed
   c. Different SSID and mobile device IP address changed

7.2.1.2 SST Performance Requirement

The key factor which affects the performance of SST is the network handover latency. Such SST process includes:

a. New link discovery and establishment
b. MIP signal HA via new link

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

The MIP signaling is one round MIP registration request and reply between mobile device and HA which costs very little compared to new link discovery and establishment.

7.2.1.3 3GPP Solution to improve SST

Using the optimized CM could reduce the network handover latency in Wi-Fi to 3G session transfer case. Make before break is a very key feature in optimized CM to improve SST performance.

For Wi-Fi to cellular case, signal strength assistance is used in handover optimization. When Wi-Fi signal strength is lower than certain value but not disconnected yet, CM will try to establish 3G connection for standby. After certain criteria matched, Client MIP module will signal HA with link changed. And then, the running session can be smoothly and seamlessly transferred to new link.

7.2.1.4 Limitation

For Wi-Fi to Wi-Fi case, the disassociation and association to AP in layer 2 and IP connectivity process may take seconds to complete on mobile device. During the handover process, some latency sensitive session may be broken, such as video chat, VoIP and etc.

For Wi-Fi hard handover to 3G case, mobile device always need to detect the network unavailability which costs a lot of efforts and discover/establish new link which bring a lot of latency in handover process. In this case, latency sensitive session may be lost as well.

7.2.1.5 Mixed MIP Solution

For Wi-Fi trusted by cellular operator, PMIP (S2a) may be used to support SST. But when user moves to airport, coffee bar, library or home, the user may prefer to connect to some untrusted Wi-Fi for free to use or better QoS. In this case, to support SST, PMIP in I-WLAN (S2b) and DSMIPv6 (S2c) may be the choices to support SST.

Therefore, mobile device should support the handover between different IP mobility mechanisms.

7.2.2 IP Mobility Mechanisms

The IP mobility mechanisms supported by 3GPP and non-3GPP accessed within an operator and its roaming partner's network may be based on static configuration or dynamic configuration. Choosing which one to use depends on operators' preferences or roaming agreement or both.

1. For static configuration case, mobile device just loads the profile provisioned in the terminal. Then the preferred IP mobility mechanism in this network is chosen and launched by mobile device.
2. For dynamic configuration case, it consists of IP mobility management protocol selection between Network Based Mobility (NBM), DSMIPv6 or MIPv4; and the decision on IP address preservation if NBM is selected

Upon initial attachment to a non-3GPP access and upon handoff to non-3GPP accesses, the mobile device performs IPMS by providing an indication during network access authentication for EPC. For trusted access, the indication is provided before an IP address is allocated to the mobile device, while in untrusted access network, the indication is provided during IKEv2 signaling for IPSec tunnel establishment with the ePDG.

After IP mobility selection is done, mobile device will launch selected mobility mechanism in current network.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

8. Identified Issues and Recommendations

There is a tremendous amount of work on seamless session transfer. Some of the solutions use proprietary technologies that are not standard based, on which devices and networks could not benefit in a scalable fashion. When evaluating any SST solution, it is necessary to assess what it buys to the end user and why operators, mobile device/OS vendors would consider such a solution.

WBA/GSMA joint task force phase-1 work on Wi-Fi roaming touches on the session continuity issue and states “It is highly desirable for both the end user and the service provider to have the ability to seamlessly move an IP session between cellular access and Wi-Fi access. This functionality also enables more sophisticated mobility scenarios such as MAPCON and IFOM as defined in 3GPP. Several protocols (PMIP, DSMIPv6, GTP) and interfaces (S2a, S2b, S2c) can be used to achieve this objective. The techniques can also include GAN mechanism defined by 3GPP in the past. These issues are not roaming specific and are a general problem to be addressed in heterogeneous networks. It first needs to be determined when operators would have this capability deployed in their home networks. Although this appears to be the direction in which the industry is headed, it was considered too complex of a problem, given several solution options, to handle in phase 1. The group has decided to defer this topic to Phase 2.” As a continuation of our WBA SST work, GSMA/WBA joint task force will have a survey of operators and device vendors to find out their positions and plans for deploying network based SST solution and device vendors to support it. It will also look into the requirements for seamless service continuity between cellular and Wi-Fi networks and how they can be met. However, local mobility within hotspots and across hotspots is not within scope of the task force.

Most of the Wi-Fi and cellular deployments today is with little integration providing non-seamless offload. Most of the current Wi-Fi traffic does not go through the 3GPP core networks. Non-seamless Wi-Fi offload is how most operators want to deal with excessive user data. However, non-seamless offload may not always be satisfactory for user experience. Full integration with the mobile core is important to some carriers. Because operators introduce many new nodes into the mobile network, seamless integration with the packet core must work efficiently without placing an undue burden on the 3G/4G infrastructure.

Introducing IP Mobility paradigm into a mobile operator network infrastructure that has not originally been designed IP Mobility related requirements in mind is an important issue. For example, the introduction of IP mobility as an inter-technology and inter-operator handover solution into the 3GPP requires major architectural redesign in order to meet all goals set by all-IP requirements. One of the notable challenges is the huge installed base of old infrastructure that the operators wish to continue using, even if new features are being developed and incrementally deployed.

Today, there is little consistency between the mechanisms used by Wi-Fi operators and those used by cellular operators to control, for example, network discovery, network selection, traffic prioritization, user authentication, roaming capabilities and quality of service (QoS).

3GPP has provided multiple solutions for this purpose including host based (S2c) or network based mobility (S2b / S2a), use of trusted (S2a) versus un-trusted (S2b) WLAN access or both, mobility protocol for network based mobility (PMIP or GTP). However, none of these solutions are currently known to be deployed and it is unclear if vendor community equally supports all of the specified solutions. It is recommended that IEEE/ 3GPP/IETF/WFA could continuously complete the unspecified solutions, improve the performance through optimized the protocols. For example, 3GPP is suggested to finish the S2a solution in R12.

The mobile device is one of the key aspects to support SST. It is recommended that OS and mobile device vendors incorporate SST related features in a proper way into the devices. Mobile device are taking more control of the user experience and are imposing their own network selection and traffic routing policies. It can be difficult to override the mobile device behavior and the diversity between vendors on device policies, which can make it difficult to guarantee the user experience.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

Wi-Fi is emerging as a standard option in mobile devices. However, mobile devices have varying degrees of Wi-Fi support, resulting in interoperability issues and poor user experiences. The role of device manufacturers in connecting the Wi-Fi ecosystem is a crucial one. Mobile devices can combine multiple technologies on one device. The mobile device has the most up-to-date knowledge of the surrounding networks in its vicinity. It is highly unlikely that different network access operators would share the information of neighboring networks with each other. The user experience of heterogeneous networks is therefore very dependent on the device connection manager, and hence on the device vendor, which attempts to balance between the user preferences, various types of network policies and what it can discover about the available access networks to make the correct connectivity decision automatically on behalf of the user. However, Connection Manager (CM) behavior varies significantly between OEMs/Operating systems providers. Some operators have attempted to overcome the behavior of device connection managers with third-party applications. If the mobile device communicates its network knowledge with the home network mobility or policy management entities there is a better chance for more intelligent network driven mobility.

Currently, there are many options to support SST which makes it a challenge for device vendors to implement all of them and mobile operators to deploy in large scale. Industry needs a convergence of solutions to a standards based one that will promote easy support of the SST by mobile devices and networks.

Due to the issues with Wi-Fi availability, coverage and power consumption, users quite often turn off Wi-Fi radio on their mobile devices. This certainly breaks the SST experience. Later on, the users will have to remember turning Wi-Fi on their devices, connect to Wi-Fi network available around them, and then initiate a session such as watching video over the Internet. These issues are gating blocks for creating good SST experience for the users. The spotty availability of Wi-Fi is still a deterring factor for causing undesirable user experience. In support of this, there is a great need for large scale availability of roaming agreements between Wi-Fi and cellular network operators to be put in place and made available for the users to roam.

Mobile devices may use significant power for Wi-Fi - even when they are in idle mode. Hence, users turn off Wi-Fi to save power. This also breaks the SST experience. Unnecessary power consumption issue needs to be fixed by smarter implementation of mobile devices and also availability of a standards based solution will help the issue significantly.

Depending on operators' near-term and long-term goals and the availability of standards supported by clients, mobility approaches will be chosen accordingly by operators to maximize their subscriber experience while minimizing network costs and complexity at different stages of migration.

Also, most of the proposed solutions mainly focus on the technical aspects of the SST issues. Many roaming and business issues are not addressed. In SST scenarios, inter-operator roaming becomes an important element especially in the future heterogeneous multi-access networks. To achieve SST with IP Mobility, flexible and scalable inter-operator roaming arrangements are required. To provide clear guidelines on STT issues involving roaming and business aspect further work is needed. This is where WBA and GSMA can help.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

9. Conclusions

Seamless connectivity experience between Wi-Fi and other networks has been the great vision for many years. However, SST is a very complex topic. Many standards based solutions such as PMIPv6, DSMIPv6 etc., have been available for enabling network based SST. But, there has been a lack of interest from the operators for making that happen since it involves additional CAPEX and OPEX and as a result they are not that motivated.

There is also a difference of opinions on how these IP address maintenance (network based) versus service level continuity (mobile device based) solutions will be deployed by different operators. For example, some operators are content by loosely coupled solutions that enable their customers access to both their cellular and Wi-Fi networks and hence they have currently no marketing requirement for IP address preservation. The common approach is to keep their voice traffic on their cellular networks and offload the heavy data traffic to Wi-Fi such as internet access and video streaming, where the applications are less sensitive to IP address change. For the other more important IP address change sensitive applications such VoIP, they are not too concerned about providing seamless experience because they do not offer VoIP as a separate service and it is typically a third party application, which operator typically get no additional revenue for. Hence, there is less motivation for them to invest in network solutions that will support SST. Also, the service continuity is possible without IP address preservation which most mobile devices currently support. Hence, IP address preservation is considered to be a low priority for some operators.

On the other hand, many mobile device, OS and application vendors are currently providing capabilities that hide IP address change and create seamless user experience without requiring any changes in the network side. Hence, many well-known applications can currently survive IP address change. This trend is expected to continue and many more applications are expected to be available in the future.

In view, the SST is still in its progress, the real deployment and trial results are still rare for reference. However, after many years of discussions and work in many industry organizations and the need for cellular data offloading to Wi-Fi, we recently started seeing some market need for making it possible. One of the gating blocks for achieving SST is the lack of seamless network discovery and automatic network connection to Wi-Fi networks. However, WFA Passpoint Certification addresses these issues and this is a very important step towards making SST a reality. The industry wide initiatives overseen by the key organizations such as WFA, WBA, 3GPP and the GSMA will be critical to the uptake of carrier Wi-Fi and seamless operation of these networks.

Currently, there are many options to support SST which makes it a challenge for device vendors to implement all of them and mobile operators to deploy in large scale. Industry needs a convergence of solutions to a standards based one that will promote easy support of the SST by mobile devices and networks.

We have reviewed a number of SST solutions coming from various organizations that could be considered relatively mature enough to be adopted by the industry. However, we should note that even with currently available some solutions/protocols, there could be issues that do not show up until in large scale deployment by mobile operator networks.

In the future, cellular offload to multiple Wi-Fi networks, roaming agreements with multiple Wi-Fi service providers become more important. WBA has trialed the Next Generation Hotspots demonstrating end-to-end seamless authentication over Wi-Fi and mobile networks [12]. This is a very important step in enablement of end-to-end SST functionality. As a next step, WBA members will be considering to perform end-to-end trials of the SST solutions including Wi-Fi to Wi-Fi and Wi-Fi to cellular scenarios. Although, there is no single solution recommendation in the scope of this whitepaper, WBA end-to-end trial results will help the industry assess solutions, identify the issues and make recommendations based on their findings.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

Acronyms and Abbreviations

3GPP	Third Generation Partnership Project
3G	3rd-generation mobile wireless standards
4G	4th-generation mobile wireless standards
AAA	Authentication, Authorization and Accounting
AP	Access Point
APN	Access Point Name
CAPEX	Capital Expenditure
DSMIP	Dual Stack Mobile IP
EAP	Extensible Authentication Protocol
EAP-SIM	EAP Subscriber Identity Module
EPC	Evolved Packet Core
ePDG	evolved Packet Data Gateway
GERAN	GSM/EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTP	GPRS Tunneling Protocol
HA	Home Agent
HoA	Home Address
IETF	Internet Engineering Task Force
IFOM	IP Flow Mobility
IKEv2	Internet Key Exchange version 2
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv4	IP version 4
IPv6	IP version 6
I-WLAN	interworking wireless local area network
LMA	Local Mobile Anchor
LTE	Long Term Evolution
MAG	Mobile Access Gateway
MIP	Mobile Internet Protocol
NEMO	Network Mobility
OPEX	Operational Expenditure
PDG	Packet Data Gateway
PDN	Packet Data Network
PDP	Packet Data Protocol
PGW	PDN Gateway
PMIP	Proxy Mobile IP
S2a	PMIP based interface between PGW and trusted non-3GPP access
S2b	PMIP based interface between PGW and non-trusted non-3GPP access
S12	GTP based interface between 3GPP access and SGW
SaMOG	S2a Mobility based on GPRS tunneling protocol
SGW	Serving Gateway
SGSN	Serving GPRS Support Node
SST	Seamless Session Transfer
TTG	Tunnel Termination Gateway
UMTS	Universal Mobile Telecommunications System
WAG	Wireless Access Gateway
WLAN	Wireless Local Area Network

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

References

[1] 3GPP TR 22.937, “Requirements for service continuity between mobile and Wireless Local Area Network (WLAN) networks”, Release 11, September 2012..

[2] 3GPP TS 23.234, “3GPP system to wireless local area network (WLAN) interworking; system description”, Release 11, September 2012.

[3] 3GPP TS 22.934, “Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking”, Release 11, December 2012.

[4] 3GPP TS 23.402, “Architecture enhancements for non-3GPP accesses”, Release 11, December 2012.

[5] 3GPP TS 24.234, “3GPP system to wireless local area network (WLAN) interworking; WLAN user equipment (WLAN UE) to network protocols”, Release 11, December 2012.

[6] 3GPP TS 23.327, “Mobility between 3GPP-WLAN interworking and 3GPP systems”, Release 11, March 2012.

[7] GSMA IR 61, “WLAN Roaming Guidelines (also known as Inter-Operator handbook)”, version 5.0, February 2012.

[8] GSMA TS.22, “Recommendations for Minimal Wi-Fi Capabilities of Terminals”, v1.0, GSMA TSG-WIF, June 201

[9] IEEE Std. 802.11, “IEEE standard for wireless LAN medium access control (MAC) and physical layer specifications”, 2012.

[10] IEEE Std. 802.21, “Standard for local and metropolitan area networks: Media independent handover services”, April 2009.

[11] WBA/GSMA Joint Task Force, “Wi-Fi Roaming Whitepaper”, v1.0, February 2012.

[12] WBA, “Next Generation Hotspot Trials Report”, June 2012,

[13] WFA, “Wi-Fi CERTIFIED Passpoint™: A new program from the Wi-Fi Alliance® to enable seamless Wi-Fi® access in hotspots”, White Paper, 2012.

[14] J. Korhonen, “IP Mobility in Wireless Operator Networks”, Dissertation, University of Helsinki, November 2008.

[15] IETF RFC-555, "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, December 2009.

[16] IETF RFC-5213, “Proxy Mobile Ipv6”, RFC-5213, August 2008.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance

Participant List

Representatives	Company
Necati Canpolat	Intel Corporation
Tiago Rodrigues	WBA
Bruno Tomas	WBA
Finbarr Coghlan	Accuris Networks
Nigel Bird	Orange
Erin Hall	AT&T
Bow Ch'ng	Comcast
Leo Nikkari	Comcast
Hanspeter Stofer	Swisscom
Ellen Encinares	SMART Communications
Arnel Cervantes	SMART Communications
Marie Romano	SMART Communications
Sun Tao	China Mobile
Liu Dapeng	China Mobile
Hui Deng	China Mobile
Irene Hu	China Unicom
Carolyn Heide	Ruckus Wireless
James Murphy	Juniper Networks
Rodolphe Savoure	Trustive
Stephen Rayment	Ericsson
Vinod Sundarraj	Juniper Networks
Zi Xiang Lee	Green Packet
Amanda Xiang	Huawei Xiang
Hisao Goda	NTT
Yataka Kuno	NTT
John Smith	Cisco

WBA would like to acknowledge the leadership team, Necati Canpolat (Intel) as the project leader and contributing companies highlighted on participant list.

Wireless Broadband Alliance Confidential & Proprietary.
Copyright © 2020 Wireless Broadband Alliance