Ericsson Review
284 23-3183 | Uen

Achieving carrier-grade Wi-Fi in the 3GPP world

Users switch between cellular and Wi-Fi networks regularly. The process is not always as seamless as it could be, sometimes requiring several painful steps. Hotspot 2.0 is starting to change all that.

STEPHEN RAYMENT AND JOAKIM BERGSTRÖM

Shortly after the close of the 2012 Mobile World Congress, the GSMA announced a plan to collaborate with the Wireless Broadband Alliance (WBA) to simplify Wi-Fi-hotspot access for smartphones and tablets[1]. Intended to provide subscribers with seamless cellular-to-Wi-Fi roaming, this joint GSMA/WBA initiative is based on the WBA Next Generation Hotspot (NGH) program[2] and the Wi-Fi Alliance Passpoint certification[3] – known in the industry as Hotspot 2.0.

The need for such an initiative has risen out of the rapid rise in mobile subscriptions and explosive growth in demand for mobile broadband. Numbering 6 billion at the end of 2011, mobile subscriptions are expected to hit the 9 billion mark by the end of 2017[4]. Mobile-data usage is expected to grow 15 times between 2011 and 2017[4]. To provide this massive number of users with good service, Hotspot 2.0 will build on the roaming principles that have successfully supported global growth in the mobile industry.

Now that the first phase of the initiative – Hotspot 2.0 Release 1 – has been launched, Ericsson and other telecom vendors are setting their sights on the next step – network-directed roaming, which will be developed in Hotspot 2.0 Release 2 and in the ANDSF enhancements in 3GPP Rel 12.

The Hotspot 2.0 standard uses operator-provided information stored in a subscriber's SIM to automate the search for available networks and the associated login procedure – removing the need for cumbersome manual steps, and improving user experience. However, the decision to switch is still determined by the device. To implement Wi-Fi that is truly carrier-grade, control needs to be handed back to the network operator.

The existing 3GPP ANDSF standard provides operators with a mechanism for handling traffic on public data networks. Operators can list their preferred networks and provide policies for how

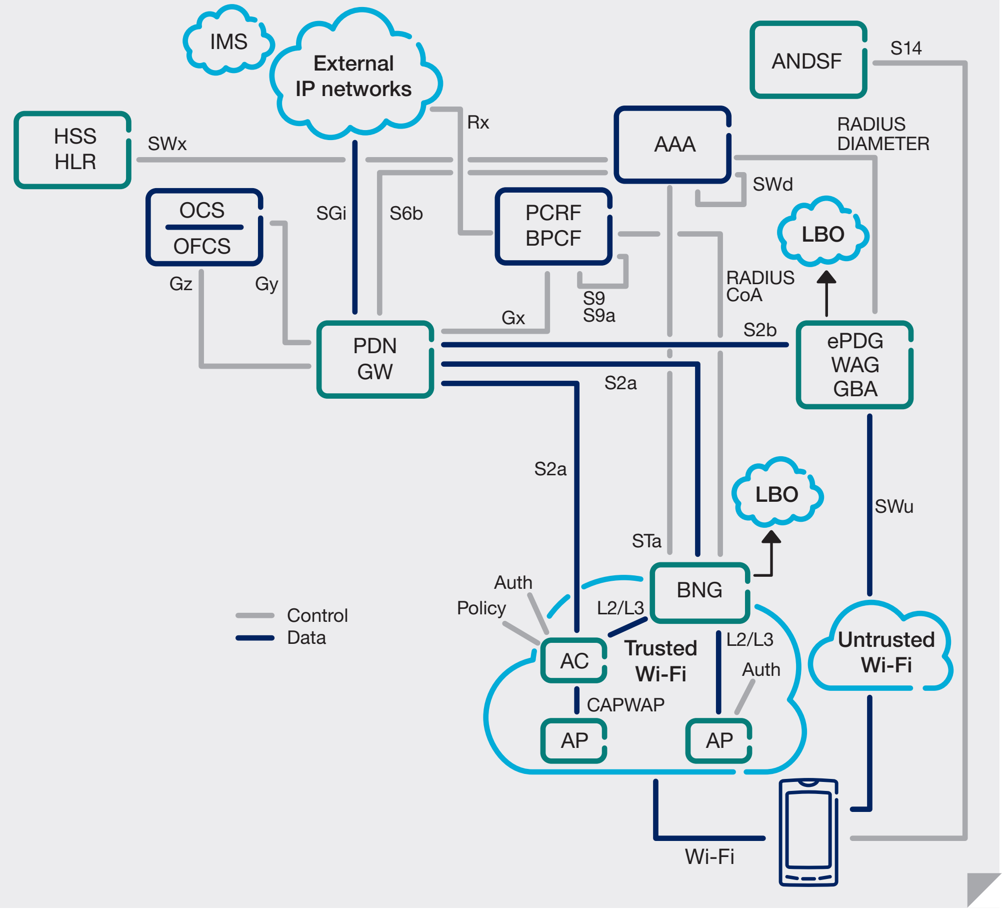
BOX A **Terms and abbreviations**

AAA	authentication, authorization and accounting
AC	access controller
AES	Advanced Encryption Standard
ANDSF	access network discovery and selection function
ANQP	Access Network Query Protocol
AP	access point
BNG	Broadband Network Gateway
BPCF	Broadband Policy Control Function
BSS	Business Support Systems
CAPWAP	Control and Provisioning of Wireless Access Points
CoA	Change of Authorization
DPI	deep packet inspection
DSMIPv6	Dual-stack Mobile IPv6
EAP	Extensible Authentication Protocol
EAP-AKA	EAP-Authentication and Key Agreement
EAP-TLS	EAP-Transport Layer Security
EAP-TTLS	EAP-Tunneled TLS
EPC	Evolved Packet Core
EPS	Evolved Packet System
ePDG	Evolved Packet Data Gateway
GBA	Generic Bootstrapping Architecture
GTP	GPRS Tunneling Protocol
HESSID	Homogenous Extended Service Set ID
HLR	home location register
hPCRF	home PCRF
HSS	Home Subscriber Server
IKEv2	Internet Key Exchange version 2
IP-CAN	IP connectivity access network
IPsec	IP Security
I-WLAN	interworking wireless LAN
ISMP	inter-system mobility policies
LBO	local breakout
LI	Lawful Interception
MCC	Mobile Country Code
MNC	Mobile Network Code
MO	management object
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
NAI	network address identifier
NGH	Next Generation Hotspot
OCS	online charging system
OFCS	offline charging system
OMA-DM	Open Mobile Alliance – Device Management
PCRF	policy and charging rules function
PDN GW	packet data network gateway
PLMN	Public Land Mobile Network
PMIP	Proxy Mobile IP
PMIPv6	Proxy Mobile IPv6
RAT	radio-access technology
RF	radio frequency
SaMOG	S2a mobility-based on GTP
SSID	Service Set Identifier
TWAN	trusted WLAN access network
UAM	Universal Access Method
UE	user equipment
USIM	Universal Subscriber Identity Module
vPCRF	visited PCRF
WAN	wide area network
WAG	wireless access gateway
WBA	Wireless Broadband Alliance
WFA	Wi-Fi Alliance
Wi-Fi	trademark of the Wi-Fi Alliance
WISPr	Wireless Internet Service Provider roaming
WLAN	wireless local area network
WPA2	Wi-Fi Protected Access v2
XML	Extensible Markup Language

to use them. For the moment, this information is relatively static and is prepared without taking real-time network conditions into consideration.

The goal is to enable carrier-grade Wi-Fi that provides a secure and seamless experience for users, where roaming to and from 3G/LTE to Wi-Fi networks is operator-controlled and network-directed. To fulfill this vision, Ericsson is working with the industry to align both the Hotspot 2.0 Release 2 and ANDSF specifications.

FIGURE 1 Wi-Fi and 3GPP



Vision for heterogeneous networks

As an integral part of the complete mobile-broadband solution, Wi-Fi is a key element of heterogeneous networks. Just like any other radio-access technology (RAT), Wi-Fi needs to be connected to the core network. Viewed in this way, it can be used to deliver the full suite of services available on the cellular data network, becoming more than just an offloading alternative for capacity-challenged networks.

Wi-Fi networks are consistently high performing owing to their inherent small-cell architecture and their use of widely available unlicensed spectrum. Thus, adding Wi-Fi to the set of accessible radios can help to optimize user experience. But integration of Wi-Fi into the cellular network, requires that a number of elements be considered:

- pico base stations house Wi-Fi and multimode small-cell licensed-band radios;
- common network nodes perform aggregation of cellular and Wi-Fi networks;
- unified network management; and
- many integrated back-end network elements, including HSS/HLR, OCS/OFCS and PCRF/BCRF, enable unified services and features.

The enablement of industry standardization and solutions that push performance beyond standards to enable leading-edge services are important aspects of the vision for fully integrated Wi-Fi and cellular networks. Figure 1 shows an architecture for interworking Hotspot 2.0 access networks with a 3GPP-based core network using well-established protocols for access and core network interworking. The architecture is based on Wi-Fi Alliance and 3GPP R11 specifications. For completeness, the illustration shows how untrusted Wi-Fi (residential) can interwork with the EPC, to, for example, support voice when only Wi-Fi coverage is available, however this is not elaborated further in this article.

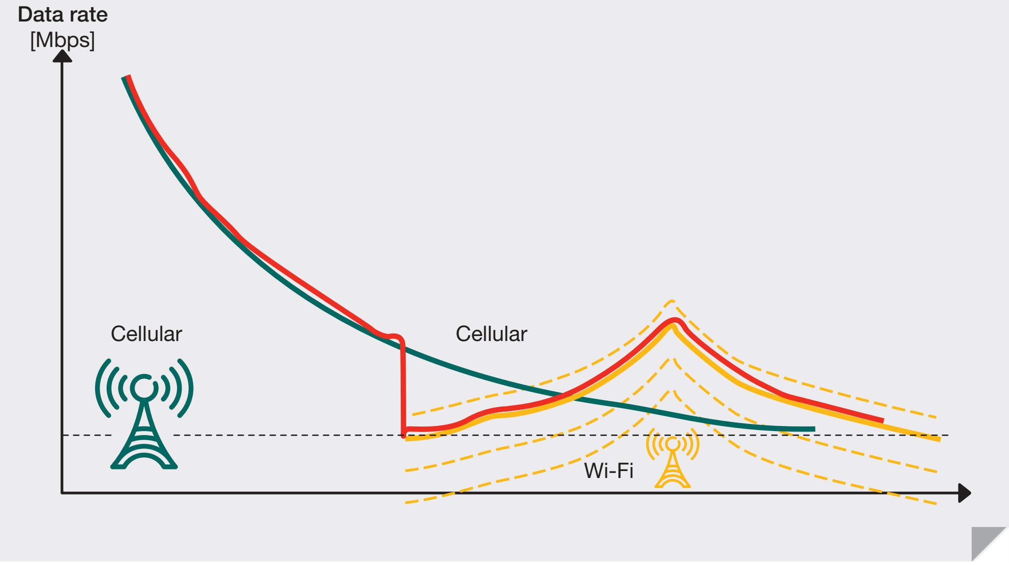
Use case

The following use case is based on a typical dual-mode smartphone scenario where a subscriber is using the cellular data network of their service provider to browse the web while walking around a busy downtown area. The user enters a shopping mall where carrier Wi-Fi coverage is available. As data usage in the area is high, the cellular network signals the smartphone to switch to Wi-Fi. The Wi-Fi radio in the smartphone detects a Hotspot 2.0 access point (AP) which it queries, using the Access Network Query Protocol (ANQP) to find out whether or not the user's home network can be reached through this Wi-Fi network. If it can, the cellular network takes the decision to switch the user's internet connection from cellular to Wi-Fi, based on ANDSF-provisioned policy for this location. Using the EAP-AKA mechanism, the smartphone switches and starts authentication with the AAA server of the cellular network using the user's SIM card credentials. On successful authentication, the access controller (AC) sets up a GTP tunnel to the PDN GW to access a carrier-managed connection to the internet, and the user continues to browse, enjoying good service performance.

Hotspot 2.0

The WFA, which is responsible for the certification of Wi-Fi products, has created Hotspot 2.0 – a technical specification that brings together a number of industry standards. Targeting service providers in the hotspot Wi-Fi market, the specification tries to apply the simplicity of cellular roaming to Wi-Fi. The program run by WFA is called Wi-Fi

FIGURE 2 **Wi-Fi selected over cellular**



CERTIFIED Passpoint, and Ericsson has been a key contributor to it, providing equipment as part of the certification test bed.

Today, connecting to a hotspot can be an awkward and inconsistent experience for subscribers who may need to go through several manual steps to switch network. These steps can include searching for a network, enabling a connection to that network and entering account credentials by launching a web browser. Some mobile-device operating systems, such as iOS, have already automated parts of the switching process using a captive portal method – WISPr or UAM – and some third-party applications called connection managers embed this capability. However, these solutions are only available for certain devices, and are offered by a limited range of carriers; they are far from widespread.

The aim of Hotspot 2.0 is to change this – supporting widespread automatic switching to Wi-Fi. As an industry-wide solution, Hotspot 2.0 will drive network interoperability and standardized network association, authentication, security, sign-up and policy control for mobile devices in a way that is completely transparent to the user. Release 1 – completed in June 2012 – specified the capabilities for network discovery and selection, and secure authentication. Certified handsets and access points supporting theses capabilities are now starting to appear on the market. Release 2, planned for 2013, will include additional capabilities to deliver operator policy to devices and enable immediate account provisioning.

Release 1

Network discovery and selection – which enables mobile devices to discover and select networks automatically without subscriber intervention – is a key element of the initial release. Using ANQP (specified in the IEEE 802.11u-2011 amendment[5]) mobile devices can query hotspots for a range of parameters that are useful in the process of selecting a network. The complete list of information elements supported by the protocol is provided in Table 1, and includes parameters such as the hotspot operator's domain name, the roaming partners accessible via the hotspot and IP address-type (IPv4 or IPv6) availability. All of these parameters are useful for determining which available network best fits the subscriber. There are several credential types that can be used to grant a device access to the network, including:

- SIM/USIM-based authentication, which is widely used in cellular networks today;
- a username-password key; and
- certificate-based credentials for fixed operators and Wi-Fi-only devices.

In all these cases, users will no longer need to enter credential information manually to establish a connection.

Table 1: ANQP information elements

ANQP elements
Service-provider identification
3GPP cellular network information
NAI realm list
Roaming consortium list
Hotspot identification
Domain name list
Venue name
Venue information
Operator-friendly name
Network characteristics
IP address-type availability
WAN metrics
Connection capability
Operating class
Network authentication type
Beacon frame elements
HESSID
Access network type
Internet available
BSS load

Ericsson's Virtual AP capability already enables multi-operator roaming – where a single hotspot broadcasts multiple beacons (SSIDs) so that several service providers can offer connections to the same AP. The Virtual AP ensures full traffic-segregation and individual operator-defined AAA rules and policy application. However, the multiple-SSID approach limits the maximum number of roaming operators – typically to eight – and the transmitted beacons occupy excessive amounts of radio airtime.

To establish a connection to their preferred provider automatically in Hotspot 2.0, mobile devices can use ANQP to determine which service providers are available via a given hotspot. This protocol identifies providers through their MCC and MNC numbers, realm information or roaming consortium element, enabling a wide range of roaming capabilities without having to broadcast provider information.

Naturally, security is of great importance. All Passpoint devices use WPA2-Enterprise security to authenticate and secure the air link between the device and the hotspot. WPA2 uses four-way handshaking and AES encryption, offering a level of security that is comparable to cellular networks.

The Hotspot 2.0 specification supports four standard protocols commonly deployed in the industry:

- **EAP-SIM – for devices with SIM credentials;**
- **EAP-AKA – for devices with USIM credentials;**
- **EAP-TLS – for use on both the client and server side, with a trusted root certificate; and**
- **EAP-TTLS with MSCHAPv2 – for user-name-password credentials.**

The specification adds to WPA2-Enterprise security by incorporating features to mitigate common attack threats in public Wi-Fi deployments, including layer-2 traffic inspection, filtering and broadcast/multicast control.

Release 2

The second release of the specification is currently being drafted – adding operator policy control and immediate account provisioning. The certification program for this release is planned for late 2013.

While Release 1 supports automatic network selection based on user preferences, pre-provisioned operator policy, and network availability, it does not support the capability to deliver operator-specific policies – this will be included in Release 2.

Immediate account provisioning, also referred to as online sign-up, is a standardized and secure process that enables new user accounts to be created at the time of connection. By supporting this process, a cross-vendor subscription-provisioning methodology can be adopted for non-subscribers – providing, easy access to people using Wi-Fi-only (non-SIM) devices who have no other means of signing up, hence creating value for the operator.

Shifting control

To ensure the best user experience, subscribers should be connected to the most appropriate network given the time of day, their current location and account preferences. To prioritize the list of networks correctly for a given user, the ability to apply operator policies is essential. Operators need to be able to control whether a device uses cellular or Wi-Fi, and in the case of Wi-Fi, which network would ensure the best user experience. Users still have control over when they connect to a residential or enterprise network by manually selecting the local Wi-Fi network.

BOX B

Wi-Fi handover behavior

Today

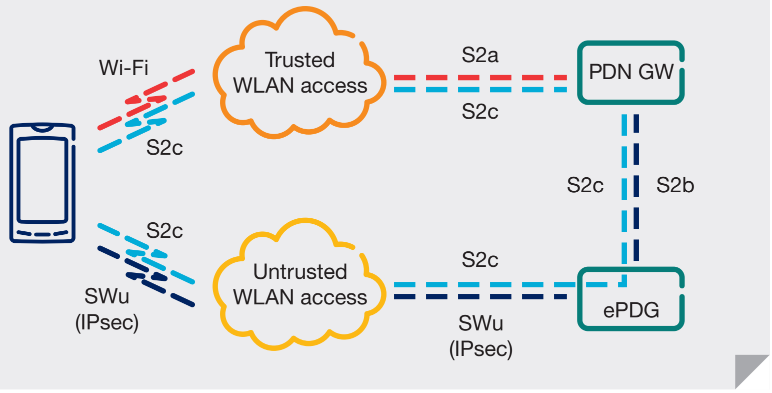
All handsets switch to Wi-Fi when it is available.

Wanted

Possibility for access selection in operator public hotspots, depending on:

- **radio characteristics and load situation;**
- **subscription parameters; services;**
- **other policies.**

FIGURE 3 **Interface architecture**



Operator policy has been included for some time in the 3GPP interworking wireless local area network (I-WLAN) specification[6]. The ANDSF[7] mechanism provides devices with additional information to expedite discovery and selection. Mobile WLAN devices use PLMN selection – based on operator-defined priorities that are preprogrammed into the SIM – to choose the appropriate operator network[6]. Such priorities can be further modified according to management objects (MOs), as specified in 3GPP TS24.235[8].

The ANDSF mechanism augments PLMN selection, providing improved control over the network-access decisions made by devices. Through a set of operator-defined rules, ANDSF guides devices through the decision-making process of where, when and how to choose a non-3GPP network. Interaction between a device and the ANDSF server uses the S14 IP interface, and data – MOs in OMA-DM compatible XML – can be transported over any available network. Typically, operator policies are pre-stored in devices before they are shipped. However, the controlling ANDSF server can push policies to devices and devices can use the pull mechanism to access policies at any time. When roaming, the ANDSF server of the visited network takes precedence.

When a device sends location information – which may include geographical, cellular area and WLAN SSID descriptors – to the ANDSF server, discovery information is sent back to the device providing it with a list of alternative access networks, such as a list of Wi-Fi network SSIDs within the current cell ID. At the same time, intersystem mobility policies (ISMPs) are sent to the mobile device, providing prioritized rules that control which network should be chosen. Each rule specifies a location and/or time – for example, a certain Wi-Fi network can be valid when a device is in a particular cell at a certain time of day. The device will choose the network with the highest priority.

Ericsson's role in the standardization work currently being carried out by the WFA is to ensure that ANQP network parameters, specified in Release 1, are included in Release-2 policies in such a way that operators maintain control over devices when they choose a network. Ericsson is also responsible for ensuring that operator policies defined in Hotspot 2.0 are fully integrated into 3GPP Rel 12 policy.

Choosing the right RAT

The policy tools described so far are valuable to the operator as they support control over user experience and take static or slowly changing network parameters into account. However, they do not cater for the rapidly fluctuating RF environment experienced by a mobile device. To illustrate the point, when a mobile device moves into an area covered by both Wi-Fi and 3G, it may decide to switch to Wi-Fi, even

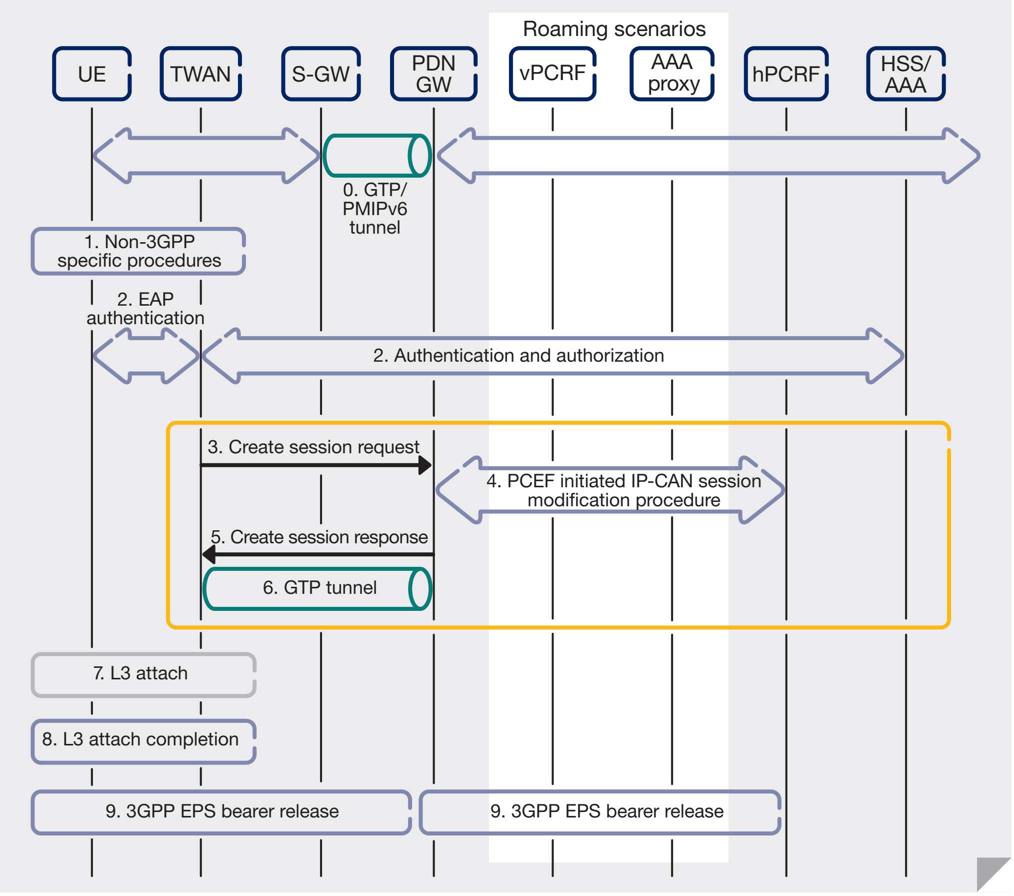

Roaming scenarios
UE
TWAN
S-GW
PDN GW
vPCRF
AAA proxy
hPCRF
HSS/ AAA
0. GTP/ PMIPv6 tunnel
1. Non-3GPP specific procedures
2. EAP authentication
2. Authentication and authorization
3. Create session request
4. PCEF initiated IP-CAN session modification procedure
5. Create session response
6. GTP tunnel
7. L3 attach
8. L3 attach completion
9. 3GPP EPS bearer release
9. 3GPP EPS bearer release

FIGURE 4 **S2a session mobility**

though the coverage offered by the 3G network is better.

Policies defined by ANDSF and Hotspot 2.0 will help to overcome some of the problems associated with automatic handover to Wi-Fi networks. However, tracking of rapid changes in the RF environment requires much tighter integration of the Wi-Fi and cellular networks, and is not part of the scope defined for Hotspot 2.0. To help overcome this issue and include real-time RF-environment information to improve the cellular/Wi-Fi decision-making process, Ericsson's concept for heterogeneous-network solutions makes use of information from both the cellular and Wi-Fi networks.

The concept supports integration for legacy devices as well as performance-enhancing features identified for future device types. By using network load data from the cellular and Wi-Fi network in the decision-making process, for example, integrated Wi-Fi solutions can make informed real-time RAT-selection decisions. The concept, for example, enables the network to control Wi-Fi acceptance thresholds for legacy devices. In the example illustrated in **Figure 2** both Wi-Fi and 3G coverage are available. In such situations, devices will not be allowed to connect to the Wi-Fi network if signal strength is below a given level – a parameter that can be updated by the network in real time.

To improve performance and consequently user experience even further, the long-term goal is to improve devices so they can receive instructions from any access network to switch to a different network, and to spread information across networks about signal condition and location.

Session mobility

Referring back to the use case, imagine that our user is watching a streaming video over the cellular network while walking into the mall. When the device switches from one network to another, the video should continue to play without any user intervention. To implement this successfully, full IP-session continuity and IP-address preservation between the cellular and the Wi-Fi network are required.

I-WLAN, which determines how IP-interworking between cellular and non-cellular networks takes place, has been part of 3GPP specifications since Release 6[7]. This type of interworking allows operators to integrate non-cellular access into the cellular packet core network, providing harmonized traffic handling for cellular and Wi-Fi access. With packet core network integration, operators gain improved visibility and control over non-cellular traffic and consequently over the user experience. Subscribers will be able to use their favorite services independent of the access network and without interruption. As such, WLAN is an integral part of mobile-broadband access and the interworking enables subscribers to use WLAN access and still be linked to operator functions including charging, policy control, deep packet inspection (DPI), QoS and Lawful Interception (LI).

Session mobility between 3GPP (such as UMTS and LTE) and non-3GPP (such as WLAN) access networks was first introduced to 3GPP specifications in Release 8, with continuous enhancements to this capability included in subsequent releases.

There are two ways to distinguish mobility in non-3GPP networks – depending on whether the target network is trusted or not and whether the mobility mechanisms used are network based or client based.

Trusted or untrusted

Determining whether or not a Wi-Fi network is trusted in terms of 3GPP standards depends largely on whether the subscriber's home operator trusts the security of the WLAN deployment. The business relationship between the WLAN provider and the home operator is often a factor in this equation. For example, when a subscriber connects to a WLAN provided by an operator other than their home operator, this WLAN might be considered untrusted – particularly if the provider uses the public internet to connect to the home operator. In such a case, the specifications allow the device to establish a secure tunnel to an ePDG before the traffic is routed to the core network of the operator. In contrast, when subscribers connect to their operator's own Wi-Fi, it is considered to be trusted and a secure tunnel is not required.

Network- or client-based

Both network-based and client-based mobility between 3GPP and WLAN (non-3GPP) networks are supported by 3GPP specifications. The 3GPP to WLAN interfaces are S2a, S2b and S2c. The architecture showing the three interfaces is illustrated in **Figure 3**. In all cases, session mobility is provided between the 3GPP network and the WLAN network with the PDN GW acting as the user-plane anchor between the two.

S2a: The mobile device connects to the Wi-Fi network using standard WLAN authentication procedures without any need for mobility or tunneling support in the mobile device. PMIPv6 or (as of Release 11) GTP protocols can be used for the S2a interface between the WLAN and the PDN GW, but GTP is already widely deployed in mobile networks and offers a range of performance advantages over PMIP. Either IPv4 or IPv6 may be used in the transport layer.

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

S2c: This option can be used over both trusted and untrusted non-3GPP access networks. The mobile device must connect to the PDN GW using DSMIPv6. In Release 10, the S2c option added support for IP mobility per flow in addition to IP session mobility. The drawback of this solution is that new clients would be needed, whereas S2a can operate in clientless mode compatible with today's devices.

For operator-deployed and fully integrated Wi-Fi networks, the trusted WLAN model is most appropriate. In this case, the S2a interface is the most cost-effective solution, allowing unmodified mobile devices to access the PDN GW via S2a.

Ericsson has held a leading role in the Release 12 SaMOG project, which aims to add full mobility across the S2a interface, including support from appropriately enabled dual-mode devices. A typical message sequence for session mobility is shown in **Figure 4**.

Conclusion

For most operators, Wi-Fi has become an integral part of their mobile-broadband strategy. Ericsson's concept for heterogeneous networks incorporates Wi-Fi, fully integrating it into mobile-access and core networks.

The evolution of Wi-Fi technology – through Hotspot 2.0, application of operator policy, intelligent RAT selection and GTP session mobility – will bring about a world where people no longer know or care whether they are connected using a cellular or Wi-Fi data network, and operators will be able to control the choice of connectivity to optimize the user experience. Ericsson has a leading role in standardization efforts to ensure that the key elements of Wi-Fi are implemented in 3GPP.

Stephen Rayment

is chief technology officer for Wi-Fi products at Ericsson. Previously, as CTO of BelAir Networks, he led the definition and delivery of the industry's first carrier Wi-Fi solutions. He has over 30 years of product experience in the telecommunications industry and has been active in industry standardization as an officer in IEEE 802.11 and in the Wi-Fi Alliance. Stephen is author of over 25 patents. He holds a B.Sc. and an M.Sc. in electrical engineering, from Queen's University in Kingston, Canada and a diploma in administration, from the University of Ottawa, Canada.

Joakim Bergström

is an expert in new radio-access networks at Design Unit Radio. He has more than 10 years of experience in standardization within the 3GPP RAN area working with HSPA, LTE and their evolution. He holds an M.Sc. in electrical engineering from the Royal Institute of Technology (KTH), Stockholm. Within the radio area, he has coordinated all of Ericsson's standardization activities and projects since 2011.

References

1. WBA and GSMA, March 2012, Press Release, GSMA and WBA collaborate to simplify Wi-Fi hotspot access for smartphones and tablets, available at: http://www.wballiance.com/2012/03/20/gsma-and-wba-collaborate-to-simplify-wi-fi-hotspot-access-for-smartphones-and-tablets/
2. Wireless Broadband Alliance, Next Generation Hotspot Program, available at: http://www.wballiance.com/wba-initiatives/next-generation-hotspot/
3. Wi-Fi organization, 2012, White Paper, Wi-Fi CERTIFIED Passpoint: A new program from the Wi-Fi Alliance to enable seamless Wi-Fi access in hotspots, available at: http://www.wi-fi.org/register.php?file=wp_20120619_Wi-Fi_CERTIFIED_Passpoint.pdf
4. Ericsson, June 2012, Traffic and Market Report, available at: http://www.ericsson.com/res/docs/2012/traffic_and_market_report_june_2012.pdf
5. IEEE, 802.11u-2011 - IEEE Standard for Information Technology-Telecommunications and information exchange between systems-Local and Metropolitan networks-specific requirements-Part II, available at: http://standards.ieee.org/findstds/standard/802.11u-2011.html
6. 3GPP, Technical Specification 24.234, 3GPP system to Wireless Local Area Network (WLAN) interworking, available at: http://www.3gpp.org/ftp/Specs/html-info/24234.htm
7. 3GPP, Technical Specification 24.312, 3GPP Access Network Discovery and Selection Function (ANDSF) Management Object (MO) available at: http://www.3gpp.org/ftp/Specs/html-info/24312.htm
8. 3GPP, Technical Specification 24.235, 3GPP System to Wireless Local Area Network (WLAN) interworking Management Object (MO), available at: http://www.3gpp.org/ftp/Specs/html-info/24235.htm