Understanding WLAN offload in cellular networks


Clock
Downloads
Stocks
Documents
Mail
Chat
Shopping
Financial
Settings
Security
Game Center
Camera
Video
Gaming
Favorites
Shopping
Phone
Wifi Tracker
Sketch
Travel

Introducing Wi-Fi™ Offload

The rapid adoption of new devices bringing new mobility usages, such as smartphones and tablets, confirms a predicted explosion of data consumption, following an exponential trend. The need for more data is synonym of a rise in network capacity demands. However, the capacity of a given network access technology network is limited by the laws of physics. The current cellular network deployed, such as 3G, LTE, LTE-A, suffers from limited licensed spectrum availability restraining the potential capacity increase. One of the foreseen solutions for meeting the capacity crunch is to increase the carrier-to-interference ratio while decreasing cell size and deploying small cell technologies.

Wi-Fi™, as part of the small cell technologies ecosystem is ideally positioned to extend the existing cellular network capacity. Given its unlicensed spectrum (ISM bands) available worldwide and widely adopted technology standard, Wi-Fi™ appeals to many operators as a cost-effective mean of offloading large amounts of mobile data traffic especially indoor where most of the traffic is generated. Operators are already taking advantage of devices supporting Wi-Fi™ as a tool to meet capacity demands by letting the user offload manually its traffic on standalone networks. This first stage of Wi-Fi™ off-loading is often associated with a manual hotspot selection followed by cumbersome logging procedures.

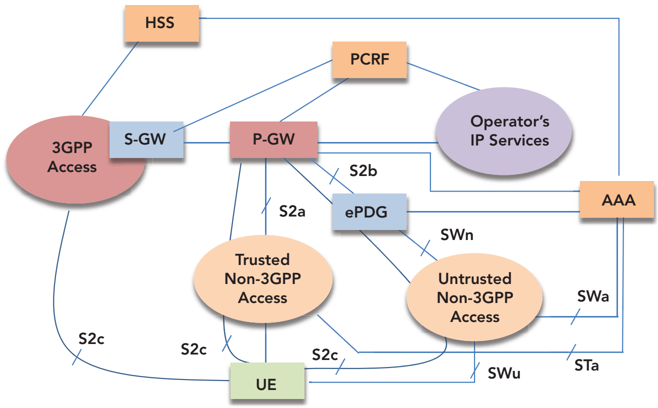
In fact, the coming challenge for Wi-Fi™ offload is to provide a converged network solution for a seamless, transparent and better user experience. The user will not have to interact with its smartphone or mobile device in any way to switch from 3G/LTE to Wi-Fi™. The data stream will even be able to use both connections at the same time depending on QoS requirements. The solutions chosen in the standards to reach the radio access convergence rely mainly on the usage of the user USIM and the addition of new network elements into mobile core networks to handle selection, authentication, security, flow control, and handovers.

This short guide explores the technical aspects of Wi-Fi™ offload architecture and its related capabilities. It is presenting the different types of possible integration into existing mobile networks to provide a viable and efficient way to offload subscriber traffic. It concludes with an overview on testing methods.

Architecture

Before explaining each technical element, this section explains the positioning of the Wi-Fi™ Offload technology in the EPC (Evolved Packet Core).

The following diagram shows the Non-Roaming EPC Architecture defined by 3GPP TS23.402.



S-GW: Serving GW

P-GW: PDN GW

AAA: 3GPP AAA Server

ePDG: enhanced Packet DataGateway

S2a: Provides user plane with related control and mobility support between trusted non-3GPP IP access and Gateway

S2b: Provides user plane with related control and mobility support between ePDG and Gateway

S2c: Provides user plane with related control and mobility support between UE and Gateway

This reference point is implemented over trusted and/or untrusted non-3GPP access and/or 3GPP access.

SWn: Reference point between untrusted non-3GPP IP access and ePDG

Traffic on this interface for a UE-initiated tunnel must be forced towards ePDG. This reference point has the same functionality as Wn defined in TS 23.234 [5].

SWa: Connects untrusted non-3GPP IP access with 3GPP AAA Server/Proxy and transports access authentication, authorization and charging-related information securely

STa: Connects trusted non-3GPP IP access with 3GPP AAA Server/Proxy and transports access authentication, authorization, mobility parameters, and charging-related information securely

SWu: Reference point between UE and ePDG and supports handling of IPSec tunnels

The SWu functionality includes UE-initiated tunnel establishment, user data packet transmission within the IPSec tunnel, and tear-down of the tunnel and support for fast update of IPSec tunnels at handover between two untrusted non-3GPP IP accesses.

**Parts in italics are extracts from 3GPP 23.402.*

Refer to section 4.3 of TS23.402 for details of each network element. Additionally, the figure above omits description of interfaces with network elements that are not connected directly to the UE.

The EPC Architecture defines an architecture whereby the UE can communicate via non-3GPP networks.

The following materials outline the features of the EPC Architecture defined by 3GPP TS23.402 from the viewpoint of Wi-Fi™ Offload technology.

Network Selection

With the EPC Architecture, mobile data can be carried over either 3GPP networks or non-3GPP networks, depending on the control policy of the communications carrier. This arrangement is called the ANDSF (Access Network Discovery & Selection Function). The policy definition controls the fine access details according to the time band, location, and network congestion conditions; these details can all be reported to the UE in real time.

Non-3GPP Network Trusted Access and Untrusted Access

The EPC Architecture defines two access paths via non-3GPP networks. The user authentication and mobile data traffic concealment methods are different, depending on the reliability of each path.

The first path is the trusted non-3GPP access path. This path is used when the security level is sufficiently safe. In most cases, access is made via the carriers' own installed Wi-Fi™ access points. In these paths, user authentication is performed in the same way as 3GPP network authentication using the SIM card data.

The second path is the untrusted non-3GPP access path. This path is used when there is no secure safety level. In most case, access is via the Internet using public wireless LAN and security is assured by establishing an IPsec tunnel between the UE and ePDG.

Mobility between 3GPP and Non-3GPP Networks

The EPC Architecture defines a mobility management mechanism assuming handover between 3GPP and non-3GPP networks. Several different approaches have been examined as a mobility management mechanism but every case requires operation centered on PDN-GW (as a mobility anchor) with preservation and management of information about each session (IP address and flow data at access) supporting uninterrupted IP sessions between different networks.

The key Wi-Fi™ Offload technologies are outlined on the next page.

Key Technologies

ANDSF

ANDSF is a policy provided to the UE for connecting with 3GPP and non-3GPP networks; it is defined in 3GPP TS23.402, TS24.302, and TS24.312. ANDSF is one key technology for Wi-Fi™ Offload and it supports two broad policies. The first is the Inter-System Mobility Policy (ISMP) allowing the UE to connect to either only a 3GPP network or only a non-3GPP network and it is used when offloading mobility data. The second is the Inter-System Routing Policy (ISRP) allowing the UE to connect simultaneously to both 3GPP and non-3GPP networks to offload mobile data.

—ISMP —

The ISMP defines rules for the UE to select and enable which network connection to use. Like the IFON (IP Flow Mobility), and MAPCON (Multi Access PDN Connectivity) functions described later, it is used either when the UE does not have a function supporting simultaneous connection to both 3GPP or non-3GPP networks, or when such a function has been disabled.

The ISMP-defined rules are listed below.

- Rules/Priority: Priority of multiple rules
- Access Technology: 3GPP/Wi-Fi
- Enabled Area: 3GPP/3GPP2/WiMAX/Wi-Fi/Position Data
- Flag indicating enabled/disabled rule at UE roaming
- PLMN Code
- Time when rules enabled
- Flag indicating UE required update to policy rules

—ISRP —

The ISRP defines rules for allowing the UE to access multiple networks simultaneously and select the network for offloading the mobility data. The ISRP rules are divided into two broad Routing policies. The first is Routing policy for a specific APN, which is the policy used by MAPCON. It supports simultaneous connection to multiple PDNs from both 3GPP and non-3GPP networks. The second is Routing policy for IP flow mobility, which is the policy used by IFOM. It supports simultaneous connection to the same PDN from both 3GPP and non-3GPP networks. In this case, DSMIPv6 must be installed in the UE.

In addition to the above policies, ANDSF also has a function for managing a list of access networks available in the vicinity of the UE (Discovery information). It has functions for storing and managing status reports (UE Location and Profile) from the UE.

The policy and UE information are managed in units called Management Objects (MO) regulated by OMA-DM. The MO data uses an XML format tree structure standardized by 3GPP TS24.312.

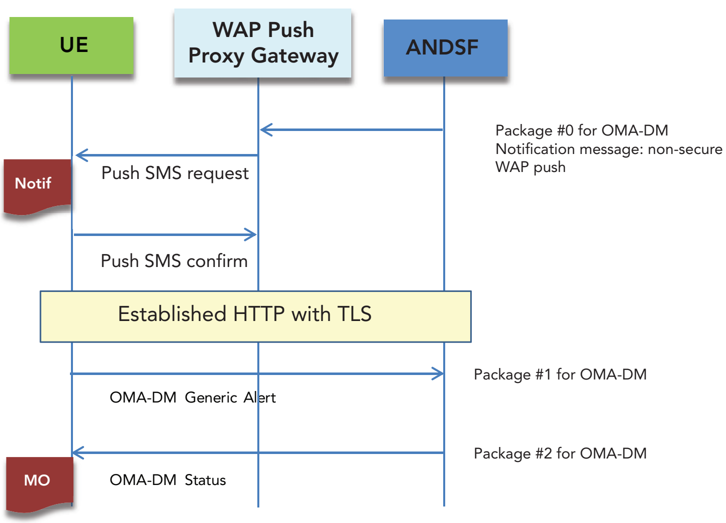
ANDSF has a function for distributing the above-described MO to the UE. The MO is delivered to the UE at the IP level via an interface called the S14 interface. Two distribution methods are defined: 1. The Pull model which distributes the MO in response to a UE request; and 2. The Push model which distributes the MO from the ANDSF autonomously. These distribution methods are implemented using the OMA-DM protocol.

In the Pull model, the MO is distributed using HTTPS. Although 3GPP TS24.302 has no security related specification, TLS1.1 and TLS1.2 are recommended for the OMA-DM protocol. The UE can request distribution of all the ISMP, ISRP, and Discovery information, or of any combination thereof.

Several methods are described for the Push model.

The first method is to send messages including GBA (Generic Bootstrapping Architecture) push information using WAP push method. Second is to send the MO using SMS method. Last is to send the Notification message defined by OMA-DM protocol using WAP push. The GBA push is used for distribution via 3GPP networks.

The following shows an example of the push model sequence using WAP push of the Notification message.



Authentication and Security

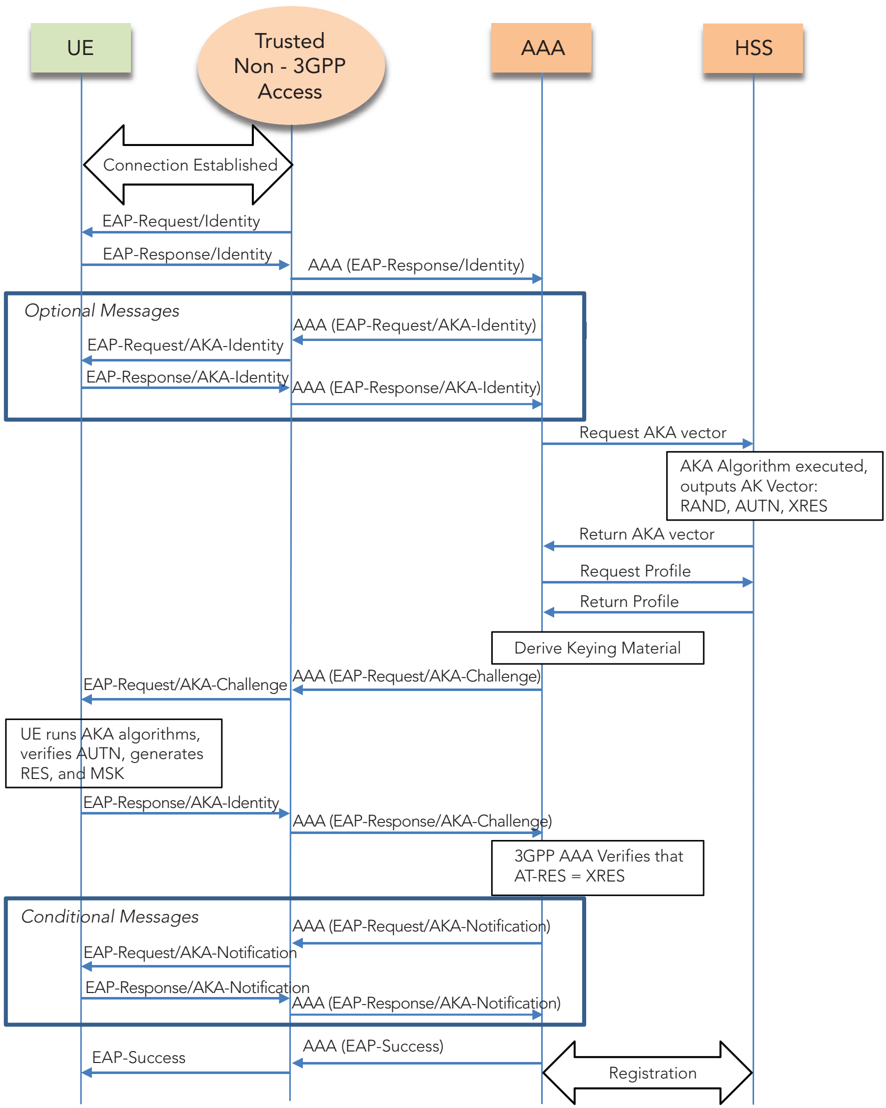
Trusted Access makes use of the EAP-SIM and EAP-AKA authentication methods for authenticating users using SIM card information, and supports simple, high-speed offloading to non-3GPP networks.

Untrusted Access supports secure communications using ePDG to provide access to carriers' networks via public networks. The two key technologies are authentication using EAP and secured communications using ePDG.

—EAP-SIM/EAP-AKA—

EAP-SIM/EAP-AKA are UE authentication methods using the UE SIM card that make use of the Extensible Authentication Protocol, which extends the older Point to Point Protocol standard used for wired network authentication. The UE sends the SIM card information to the trusted non-3GPP access AP and the AP queries the AAA server with Pass/Fail authentication (STa interface). The AAA server compares the query with the user information saved at HSS and returns the authentication result to the UE. The implementation of authentication functions EAP-SIM/EAP-AKA to the UE has been standardized by the TS22 GSMA.

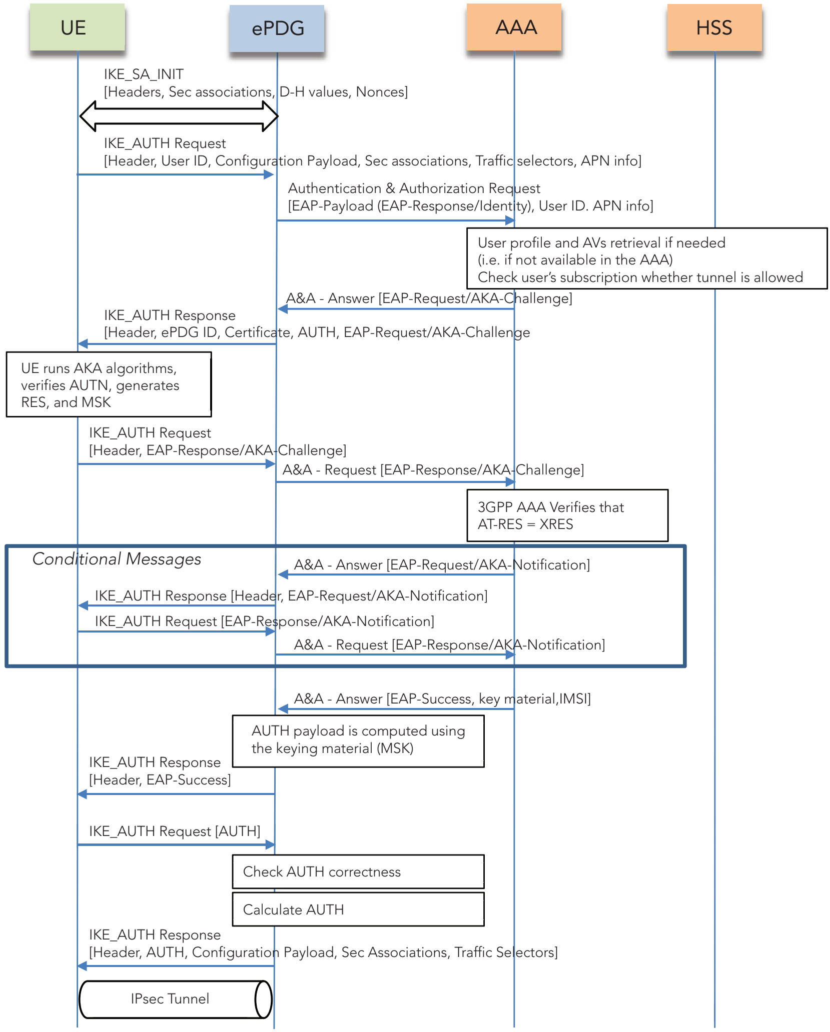
The following shows an example of the trusted non-3GPP access authentication sequence (EAP-AKA full authentication).



—ePDG—

ePDG is a gateway for securing untrusted non-3GPP access on networks without security, such as public wireless LAN. An IPSec tunnel is created between the UE and ePDG for key exchange using IKEv2 to secure the mobile data using the IPsec tunnel. Compared to the older PDG standard defined by 3GPP TS23.234, ePDG has extended the CoA allocation when using the S2c interface and the terminal functions of PMIPv6 when using the S2b interface.

The following shows an example of the tunnel full authentication and authorization sequence.



Session Mobility

Two mechanisms are defined as methods for managing mobility between 3GPP and non-3GPP networks.

The first is Network Based Mobility (NBM). NBM runs independently on the network side and is a method for managing mobility between 3GPP and non-3GPP networks. The UE communicates with the network entity such as ePDG and P-GW using GTP or PMIPv6, supporting mobile data continuity when the mobile moves between 3GPP and non-3GPP networks.

The second is Host Based Mobility (HBM). HBM runs on the client UE and is a method for managing mobility. Secure communications are assured by allocating an IP address between PDN-GW and the UE using DSMIPv6, supporting mobile data continuity when the mobile moves between 3GPP and non-3GPP networks.

The above-described mobility management mechanisms are defined as Multi Access PDN Connectivity (MAPCON) and IP Flow Mobility (IFOM) in 3GPP TR23.861 Multi Access PDN connectivity and IP flow mobility. *3GPP Rel-12 discusses the related evolution of Network Based IP Flow Mobility (NBIFOM).

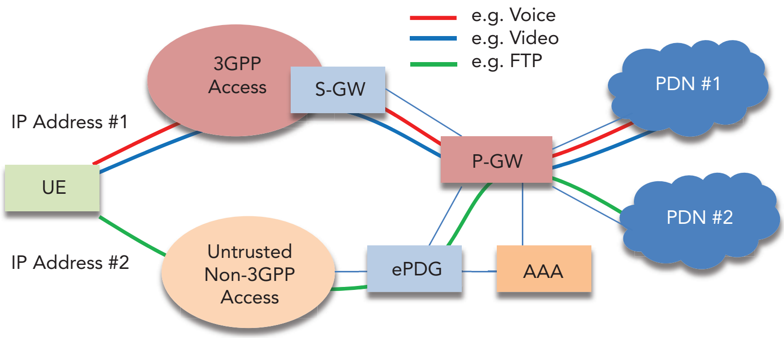
The mobility management mechanisms are the third key technology for Wi-Fi™ offloading.

Each is explained below.

—MAPCON—

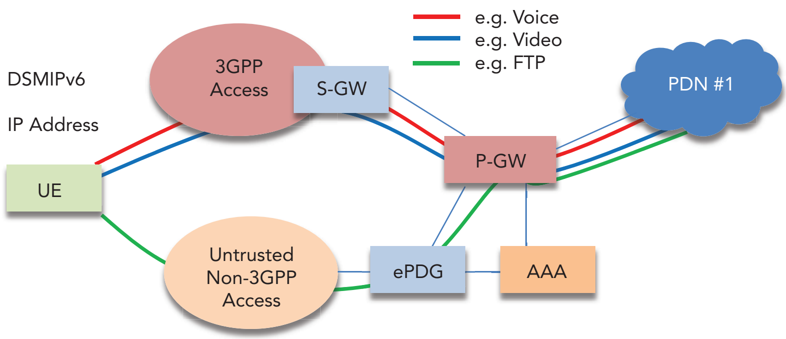
MAPCON is a method for managing mobility by managing multiple PDN connections when the UE itself has multiple IP addresses. With MAPCON, the UE achieves simultaneous connections to 3GPP and Wi-Fi networks (non-3GPP networks). In concrete terms, a PDN connection (session with anchor P-GW) is established for each 3GPP and Wi-Fi™ network and the mobility data is divided for communications simultaneously between the different networks. For example, downloading large files using FTP is handled via the Wi-Fi™ network while voice calls using VoLTE and video calls are handled via the 3GPP network. Using MAPCON, offloading can be achieved relatively easily, instead of requiring the UE to support multiple client-based mobility management like DSMIPv6.

Each is explained below.



—IFOM—

IFOM is a mobility management method that connects 3GPP and non-3GPP networks to the same PDN and maintains the connection while managing the mobility data in flow units. Using IFOM, both 3GPP and non-3GPP networks can be connected simultaneously using DSMIPv6 to offload mobile data for each flow. The 3GPP and non-3GPP networks establish a connection to the same PDN (session with anchor P-GW) and the mobile data is distributed in flow units for each different network. By using DSMIPv6 IP address processing, the session can be maintained without knowledge of the different network paths. In the same way as MAPCON, downloading large files using FTP is performed via the Wi-Fi™ network while voice calls using VoLTE and video calls are handled via the 3GPP network.



Wi-Fi™ Offload Test

When testing UEs supporting Wi-Fi™ Offload, consideration must be given to starting from the PHY and MAC layers specified by IEEE802.11, such as modulation (OFDM) for IEEE802.11n/11ac, and the TRx technology (MIMO). QoS scheduling and IEEE802.11ac throughput measurements may be necessary.

These PHY and MAC layer tests are in most cases used by chipset vendors, in the development phase of devices supporting Wi-Fi™, or at the final production line test; the Wi-Fi™ Alliance, etc., also offers verification test arrangements. For smartphone devices supporting Wi-Fi™, the PHY and MAC layer tests are extremely important. At Anritsu, we have developed the MT8870A Universal Wireless Test Set with MU887000A TRx Test Module, MX8870xxA Measurement Software, and MV8870xxA Waveform File to meet the need for an all-in-one measurement solution for evaluating the TRx characteristics of multi-system wireless modules, such as wireless LAN and mobile communications systems.

Visit the following URL for information on MT8870A related products.

http://www.anritsu.com/en-GB/Products-Solutions/Products/MT8870A.aspx

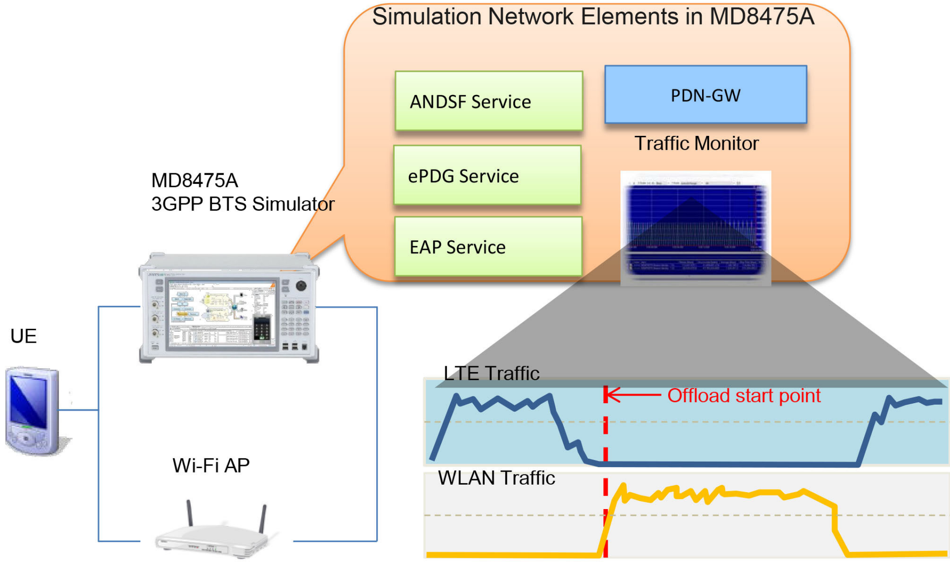
Seen from the perspective of Wi-Fi™ Offload at the 3GPP network side, besides the simple IEEE802.11 tests described above, there is a need for tests of the previously described key technology functions as well as usability. In addition, terminal operation using ANDSF will need to be verified along with 3GPP network-side switch timing, throughput, and video/voice traffic continuity.

Not surprisingly, this test environment is complex with contents covering a lot of ground. For example, at switching from a 3GPP network to Wi-Fi™ while monitoring mobile data traffic, the IPsec tunneling function must be verified and then the return to the 3GPP network side during a video call, etc., must be tested too. It may also be necessary to reproduce scheduling errors that should not be generated on an actual live network. A simulation environment is needed to create the complex test cases for an environment with these types of 3GPP and Wi-Fi™ network interactions.

The following explains a test solution from the Wi-Fi™ Offload perspective.

Solution Overview

Test Environment



Visit the following URL for details about the MD8475A Signalling Tester (BTS Tester).

http://www.anritsu.com/en-GB/Products-Solutions/Products/MD8475A.aspx

EAP Service: Simulates EAP-SIM/AKA authentication server function.

This provides an EAP authentication server running on the MD8475A to execute UE function tests at trusted non-3GPP access by performing EAP over RADIUS communications (EAP-SIM/EAP-AKA) between AP and the EAP authentication server.

ANDSF Service: Simulates ANDSF policy delivery server function

This provides the ANDSF function running on the MD8475A to execute UE function tests after ANDSF delivery by delivering the policy to the UE.

ePDG Service: Simulates ePDG server function

This provides the ePDG server running on the MD8475A to execute UE function tests at untrusted non-3GPP access by performing IPsec communications and key exchange between the UE and ePDG.

PDN-GW WLAN Traffic monitor: Simulates PDN-GW function

This distributes and monitors data communications between the servers and UE. Additionally, it authenticates data access by bearers in the PHY layer to verify switching between 3GPP and Wi-Fi™.

Test Cases

The previously explained test environment can be broadly into three types of test cases. The first is functional tests. This test case tests authentication functions at access as well as basic functions like policy delivery using ANDSF. The second is connectivity tests. This test case tests connectivity between 3GPP and Wi-Fi™ networks as well as mobile data traffic continuity. The third is composite tests. This test case tests the validity of various services provided on 3GPP and Wi-Fi™ networks concurrently.

Assuring UE QoS requires execution of quality checks by using each of these test cases to generate specific phenomena, such as abnormal sequences, that cannot be generated on actual live networks.

Examples of each test case are listed below.

Category	Item	Test case
Functional test	Authentication by trusted WLAN Access. (EAP Option)	Full authentication sequence (EAP-AKA/SIM Basic)
		Full authentication sequence (EAP-AKA/SIM Client error)
		Full authentication sequence (EAP-AKA/SIM Server error)
		Fast re-authentication sequence (EAP-AKA/SIM Normal)
		Fast re-authentication sequence (EAP-AKA/SIM Client error)
	Authentication by untrusted WLAN Access. (ePDG Option)	Full authentication sequence (Basic)
		Full authentication sequence (Rekeying)
		Full authentication sequence (Dead Peer Detection)
		Full authentication sequence (Auth error)

	ANDSF	Authentication of the ANDSF-Delivery
		UE operation check after delivery all MO (Management Object)
		UE operation check after delivery just ISMP Policy
		UE operation check after delivery just Discovery
		UE operation check after delivery just ISRP Policy
		Confirm of the alert message (Location / Profile)
Connectivity Test	3GPP - WLAN	3GPP -> trusted WLAN (not deliver ANDSF)
		3GPP -> untrusted WLAN (not deliver ANDSF)
		3GPP -> trusted WLAN (deliver ANDSF)
		3GPP -> untrusted WLAN (deliver ANDSF)
		trusted WLAN -> 3GPP (not deliver ANDSF)
		untrusted WLAN -> 3GPP (not deliver ANDSF)
		trusted WLAN -> 3GPP (deliver ANDSF)
		untrusted WLAN -> 3GPP (deliver ANDSF)
	Data communication	Confirmation of Web browsing via trusted WLAN
		Confirmation of Web browsing via untrusted WLAN
		Confirmation of Voice call via trusted WLAN
		Confirmation of Voice call via untrusted WLAN
		Confirmation of Video call via trusted WLAN
		Confirmation of Video call via untrusted WLAN
		Measurement Throughput (Downstream)
		Measurement Throughput (Upstream)
Composite Test	Concurrent access of WLAN and 3GPP (during data communication) e.g. FTP, Web browsing, during movie playback	During data communication on WLAN, Voice call from 3GPP side
		During data communication on WLAN, Voice incoming call from 3GPP side
		During data communication on WLAN, Video call from 3GPP side

		During data communication on WLAN, Voice call from 3GPP side
		During data communication on WLAN, Voice incoming call from 3GPP side
		During data communication on WLAN, Video call from 3GPP side
		During data communication on WLAN, Video incoming call from 3GPP side
		During data communication on 3GPP, Voice call from WLAN side
		During data communication on 3GPP, Voice incoming call from WLAN side
		During data communication on 3GPP, Video call from WLAN side
		During data communication on 3GPP, Video incoming call from WLAN side
		During data communication on WLAN, send SMS from 3GPP side
		During data communication on WLAN, receive SMS from 3GPP side
		During data communication on 3GPP, send SMS from WLAN side
		During data communication on 3GPP, receive SMS from WLAN side
	During voice calling Also includes emergency call	During voice calling on WLAN, Voice call from 3GPP side
		During voice calling on WLAN, Voice incoming call from 3GPP side
		During voice calling on WLAN, Video call from 3GPP side
		During voice calling on WLAN, Video incoming call from 3GPP side
		During voice calling on 3GPP, Voice call from WLAN side
		During voice calling on 3GPP, Voice incoming call from WLAN side
		During voice calling on 3GPP, Video call from WLAN side

		During voice calling on 3GPP, Video incoming call from WLAN side
		During voice calling on WLAN, send SMS from 3GPP side
		During voice calling on WLAN, receive SMS from 3GPP side
		During voice calling on 3GPP, send SMS from WLAN side
		During voice calling on 3GPP, receive SMS from WLAN side
	During video calling	During video calling on WLAN, video call from 3GPP side
		During video calling on WLAN, video incoming call from 3GPP side
		During video calling on WLAN, Video call from 3GPP side
		During video calling on WLAN, Video incoming call from 3GPP side
		During video calling on 3GPP, video call from WLAN side
		During video calling on 3GPP, video incoming call from WLAN side
		During video calling on 3GPP, Video call from WLAN side

Conclusion

Carriers and UE vendors are positively supporting Wi-Fi™ Offload due to its many advantages, such as reduced network loads and high-speed communications. On the other hand, implementation of Wi-Fi™ Offload requires careful consideration of many important themes, including prevention of Wi-Fi™ interference, output tuning, etc.

However, in the future, the importance of offloading to non-3GPP networks will not change and is likely to become increasingly important. Not only mobile data will be offloaded, but it also seems likely that new composite services such as O2O (Online To Offline) will be implemented increasingly in the coming so-called “big data age”. This guide outlines some of the important elements and key technologies in achieving these composite services fusing mobile and fixed-line communications.

Anritsu is using its specialist knowledge and experience in 3GPP and Wi-Fi™ networks to help support evaluation and debugging of UE Wi-Fi™ Offload technology and bring these services to markets as smoothly as possible.

Abbreviations

The abbreviations in this guide are listed below:

AAA – Authentication, Authorization and Accounting

AKA – Authentication and Key Agreement

ANDSF – Access Network Discovery and Selection Function

AP – Access Point

DHCP – Dynamic Host Configuration Protocol

DM – Device Management

DNS – Domain Name System

DPD – Dead Peer Detection

DSMIPv6 – Dual-Stack MIPv6

EAP – Extensible Authentication Protocol

ePDG – Evolved Packet Data Gateway

GW – Gateway

HBM – Host-based Mobility

IFOM - IP Flow Mobility

IKEv2 – Internet Key Exchange version 2

ISMP – Inter-System Mobility Policies

IPMS – IP Mobility Mode Selection

ISRP – Inter-System Routing Policies

MAPCON – Multi Access PDN Connectivity

MIPv6 – Mobile IP version 6

MO – Management Object

NBM – Network based mobility management

OMA – Open Mobile Alliance

PDN – Packet Data Network

PSK – Pre-Shared Key

RADIUS – Remote Authentication Dial In User Service

TLS – Transport layer Security

UE – User Equipment

WAP – Wireless Application Protocol

Wi-Fi – Wireless Fidelity

WLAN – Wireless Local Area Network

References

RFC4186	Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)
RFC4187	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
RFC3748	Extensible Authentication Protocol (EAP)
RFC2865	Remote Authentication Dial In User Service (RADIUS)
RFC3579	RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)
3GPP TS33.102	3G Security; Security architecture
3GPP TS34.108	Common test environments for User Equipment (UE); Conformance testing
3GPP TS35.205	3G Security; Specification of the MILENAGE Algorithm Set
3GPP TS 23.234	3GPP system to Wireless Local Area Network (WLAN) interworking; System description
3GPP TS 23.402	Architecture enhancements for Non-3GPP accesses
3GPP TS 33.402	3GPP System Architecture Evolution (SAE); Security aspects of Non-3GPP accesses
3GPP TS 33.234	3G Security; Wireless Local Area Network (WLAN) interworking security
3GPP TS 33.310	Network Domain Security (NDS); Authentication Framework (AF)
3GPP TS 24.302	Access to the 3GPP Evolved Packet Core (EPC) via Non-3GPP access networks; Stage 3
3GPP TS 34.108	Common test environments for User Equipment (UE); Conformance testing
RFC 4306	Internet Key Exchange (IKEv2) Protocol
RFC 5996	Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 4555	IKEv2 Mobility and Multihoming Protocol (MOBIKE)
RFC 4187	Extensible Authentication Protocol Method for 3rd Generation
3GPP TS23.402 V12.0.0	Technical Specification Group Services and System Aspects; Architecture enhancements for Non-3GPP accesses (Release 12)
3GPP TS24.302 V12.0.0	Technical Specification Group Core Network and Terminals; Access to the 3GPP Evolved Packet Core (EPC) via Non-3GPP access networks; Stage 3 (Release 12)
3GPP TS24.312 V12.0.0	Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO) (Release 12)

3GPP TS33.223 V11.0.0	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function
3GPP TS33.402 V11.4.0	3GPP System Architecture Evolution (SAE); Security aspects of Non-3GPP accesses
OMA-RD-DM-V1_3-20120306-C	OMA Device Management Requirements V1.3
OMA-TS-DM_Protocol-V1_3-20121009-C	OMA Device Management Protocol V1.3
OMA-TS-DM_RepPro-V1_3-20130422-C	OMA Device Management Representation Protocol V1.3
OMA-TS-DM_StdObj-V1_3-20121009-C	OMA Device Management Standard Object V1.3
OMA-TS-DM_Notification-V1_3-20130422-C	OMA Device Management Notification Initiated Session V1.3
OMA-TS-DM_PushBinding-V1_3-20120306-C	OMA Device Management Push Binding V1.3
OMA-TS-DM_HTTPBinding-V1_3-20120306-C	OMA Device Management HTTP Binding V1.3A
OMA-TS-DM_Security-V1_3-20120306-C	OMA Device Management Security V1.3
OMA-TS-DM_TND-V1_3-20121213-C	OMA Device Management Tree and Descriptions V1.3
WAP-250-PushArch Overview-20010703-a	WAP Push Architectural Overview Version 03-Jul-2001
WAP-247-PAP-20010429-a	Push Access Protocol Version 29-Apr-2001
WAP-249-PPGService-20010713-a	Push Proxy Gateway Service Version 13-Jul-2001
WAP-235-PushOTA-20010425-a	Push OTA Protocol Version 25-April-2001
3GPP TS23.402 V12.0.0	Technical Specification Group Services and System Aspects; Architecture enhancements for Non-3GPP accesses (Release 12)
3GPP TS33.223 V11.0.0	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function
3GPP TS33.402 V11.4.0	3GPP System Architecture Evolution (SAE); Security aspects of Non-3GPP accesses
OMA-RD-DM-V1_3-20120306-C	OMA Device Management Requirements V1.3

Specifications are subject to change without notice.

● **United States**
Anritsu Company
1155 East Collins Blvd., Suite 100, Richardson,
TX 75081, U.S.A.
Toll Free: 1-800-267-4878
Phone: +1-972-644-1777
Fax: +1-972-671-1877

● **Canada**
Anritsu Electronics Ltd.
700 Silver Seven Road, Suite 120, Kanata,
Ontario K2V 1C3, Canada
Phone: +1-613-591-2003
Fax: +1-613-591-1006

● **Brazil**
Anritsu Eletrônica Ltda.
Praça Amadeu Amaral, 27 - 1 Andar
01327-010 - Bela Vista - São Paulo - SP - Brazil
Phone: +55-11-3283-2511
Fax: +55-11-3288-6940

● **Mexico**
Anritsu Company, S.A. de C.V.
Av. Ejército Nacional No. 579 Piso 9, Col. Granada
11520 México, D.F., México
Phone: +52-55-1101-2370
Fax: +52-55-5254-3147

● **United Kingdom**
Anritsu EMEA Ltd.
200 Capability Green, Luton, Bedfordshire, LU1 3LU, U.K.
Phone: +44-1582-433200
Fax: +44-1582-731303

● **France**
Anritsu S.A.
12 avenue du Québec, Bâtiment Iris 1- Silic 612,
91140 VILLEBON SUR YVETTE, France
Phone: +33-1-60-92-15-50
Fax: +33-1-64-46-10-65

● **Germany**
Anritsu GmbH
Nemetschek Haus, Konrad-Zuse-Platz 1
81829 München, Germany
Phone: +49-89-442308-0
Fax: +49-89-442308-55

● **Italy**
Anritsu S.r.l.
Via Elio Vittorini 129, 00144 Roma, Italy
Phone: +39-6-509-9711
Fax: +39-6-502-2425

● **Sweden**
Anritsu AB
Kistagången 20B, 164 40 KISTA, Sweden
Phone: +46-8-534-707-00
Fax: +46-8-534-707-30

● **Finland**
Anritsu AB
Teknobulevardi 3-5, FI-01530 VANTAA, Finland
Phone: +358-20-741-8100
Fax: +358-20-741-8111

● **Denmark**
Anritsu A/S (Service Assurance)
Anritsu AB (Test & Measurement)
Kay Fiskers Plads 9, 2300 Copenhagen S, Denmark
Phone: +45-7211-2200
Fax: +45-7211-2210

● **Russia**
Anritsu EMEA Ltd.
Representation Office in Russia
Tverskaya str. 16/2, bld. 1, 7th floor.
Russia, 125009, Moscow
Phone: +7-495-363-1694
Fax: +7-495-935-8962

● **United Arab Emirates**
Anritsu EMEA Ltd.
Dubai Liaison Office
P O Box 500413 - Dubai Internet City
Al Thuraya Building, Tower 1, Suit 701, 7th Floor
Dubai, United Arab Emirates
Phone: +971-4-3670352
Fax: +971-4-3688460

● **India**
Anritsu India Private Limited
2nd & 3rd Floor, #837/1, Binnamangla 1st Stage,
Indiranagar, 100ft Road, Bangalore - 560038, India
Phone: +91-80-4058-1300
Fax: +91-80-4058-1301

● **Singapore**
Anritsu Pte. Ltd.
11 Chang Charn Road, #04-01, Shriro House
Singapore 159640
Phone: +65-6282-2400
Fax: +65-6282-2533

● **P.R. China (Shanghai)**
Anritsu (China) Co., Ltd.
Room 2701-2705, Tower A,
New Caohejing International Business Center
No. 391 Gui Ping Road Shanghai, 200233, P.R. China
Phone: +86-21-6237-0898
Fax: +86-21-6237-0899

● **P.R. China (Hong Kong)**
Anritsu Company Ltd.
Unit 1006-7, 10/F., Greenfield Tower, Concordia Plaza,
No. 1 Science Museum Road, Tsim Sha Tsui East,
Kowloon, Hong Kong, P.R. China
Phone: +852-2301-4980
Fax: +852-2301-3545

● **Japan**
Anritsu Corporation
8-5, Tamura-cho, Atsugi-shi, Kanagawa, 243-0016 Japan
Phone: +81-46-296-1221
Fax: +81-46-296-1238

● **Korea**
Anritsu Corporation, Ltd.
5FL, 235 Pangyoyeok-ro, Bundang-gu, Seongnam-si,
Gyeonggi-do, 463-400 Korea,
Phone: +82-31-696-7750
Fax: +82-31-696-7751

● **Australia**
Anritsu Pty. Ltd.
Unit 21/270 Ferntree Gully Road, Notting Hill,
Victoria 3168, Australia
Phone: +61-3-9558-8177
Fax: +61-3-9558-8255

● **Taiwan**
Anritsu Company Inc.
7F, No. 316, Sec. 1, NeiHu Rd., Taipei 114, Taiwan
Phone: +886-2-8751-1816
Fax: +886-2-8751-1817

1309

Please Contact:

Issue 2, 09/2013