Netext
Internet-Draft
Intended status: Informational
Expires: January 17, 2013

Ravi. Valmikam
Unaffiliated
Rajeev. Koodli
Cisco Systems
July 16, 2012

EAP Attributes for WiFi - EPC Integration
draft-ietf-netext-wifi-epc-eap-attributes-01

Abstract

With WiFi beginning to establishing itself as a trusted access network for service providers, it has become important to provide functions commonly available in 3G and 4G networks in WiFi access networks. Such functions include Access Point Name (APN) Selection, multiple Packet Data Network (PDN) connections and seamless mobility between WiFi and 3G/4G networks.

EAP/AKA (and EAP/AKA') is standardized by 3GPP as the access authentication protocol for trusted access networks. This IETF specification is required for mobile devices to access the 3GPP Evolved Packet Core (EPC) networks. This document defines a few new EAP attributes and procedures to provide the above-mentioned functions in trusted WiFi access networks.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 17, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

The convergence of multiple access technologies is becoming more reality now than ever. Specifically, WiFi has emerged as a trusted access technology for mobile service providers. It has become important to provide certain functions in WiFi which are commonly supported in licensed-spectrum networks such as 3G and 4G networks. This draft specifies a few new EAP attributes and procedures for a Mobile Node (MN) to interact with the network to support some of the functions (see below). These new attributes serve as a trigger for network nodes to undertake the relevant mobility operations. For instance, when the Mobile Node indicates and the network agrees for a new IP session (i.e., a new APN in 3GPP), the corresponding attribute (defined below) can act as a trigger for the Mobile Anchor Gateway (MAG) to initiate a new mobility session with the Local Mobility Anchor (LMA).

The 3GPP networks support many functions that are not commonly implemented in a WiFi network. This draft specifically addresses the following functions and specifies methods to implement them using EAP-AKA' [RFC5448] and EAP-AKA [RFC4187]. Since the attributes share the same IANA registry, the methods are applicable to EAP-AKA', EAP-AKA and EAP-SIM [RFC4186], and with appropriate extensions, are possibly applicable for other EAP methods as well.

The following sections will focus on implementation of the following functions in the context of a 802.1X/EAP based WiFi network.

- o APN Selection
- o Multiple APN Connectivity
- o WiFi to 3G/4G (UTRAN/EUTRAN) mobility

EAP [RFC3748] is widely deployed in access networks to authenticate the user during network attach, and periodically afterwards. Apart from being an authentication mechanism, EAP provides a conduit to propagate information between a MN and network elements such as a WiFi Access Controller. Each of the addressed functions is described in detail below.

1.1. APN Selection

The 3GPP networks support the concept of an APN (Access Point Name). This is defined in [GPRS]. Each APN is an independent IP network with it's own set of IP services. When the MN attaches to the network, it may select a specific APN to receive desired services. For example, to receive generic internet services, user device may select APN "Internet" and to receive IMS voice services, it may select APN "IMSvoice".

In a WiFi access scenario, a MN needs a way of sending the desired APN name to the network. This draft specifies a method to propagate the APN information via EAP.

1.2. Multiple APN Connectivity

As an extension of APN Selection, a MN may choose to connect to multiple IP networks simultaneously. 3GPP provides this feature via Additional PDP contexts or Additional PDN connections. The 3GPP defines extensive set of signaling procedures to implement these features. In a WiFi network, a MN connects to the first APN via DHCPv4 or IPv6 Router Solicitation. For subsequent APN connections, a procedure is needed to request the network and propagate necessary information.

1.3. WiFi to EUTRAN mobility

When operating in a multi-access network, a MN may want to gracefully handover it's IP attachment from one access to another. For instance, a MN connected to 3GPP EUTRAN network may choose to move its connectivity to a trusted WiFi network. Alternatively, the MN may choose to connect from both the access technologies simultaneously, and maintain two independent IP attachments. To implement these scenarios, the MN needs a way to indicate seamless handover as well as a means to correlate the UTRAN/EUTRAN session with the new WiFi session. This draft specifies a method to propagate EUTRAN session identification (GUTI) to the network via EAP. This helps the network to correlate the sessions between the two RAN technologies and implement a handover.

2. Reference Architecture and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Protocol Overview

3.1. Brief Introduction to EAP

EAP is defined as a generic protocol in [RFC3748]. EAP, combined with one of the payload protocols such as EAP-AKA' [RFC5448] can accomplish several things in a network:

- Establish identity of the user (MN) to the network.
- Authenticate the user during the first attach with the help of an authentication center that securely maintains the user credentials. This process is called EAP Authentication.
- Re-authenticate the user periodically, but without the overhead of a round-trip to authentication center. This process is called EAP Fast Re-Authentication.

This draft makes use of the EAP Authentication procedure to implement the above-mentioned functions. The use of EAP Fast Re-Authentication procedure is for further study. Both the EAP Authentication and EAP Fast Re-Authentication procedures are specified for trusted access network use in 3GPP [3GPP-TS-33.402]

3.2. 802.11 Authentication using EAP over 802.1X

In a WiFi network, EAP is carried over the IEEE 802.1X Authentication protocol. The IEEE 802.1X Authentication is a transparent, payload-unaware mechanism to carry the authentication messages between the MN and the WiFi network elements.

EAP, on the other hand, has multiple purposes. Apart from it's core functions of communicating MN's identity to the network and proving MN's credentials, it also allows the MN to send arbitrary information elements to help establish the MN's IP session in the network. The following figure shows an example end-to-end EAP flow in the context of an IEEE 802.11 WiFi network.

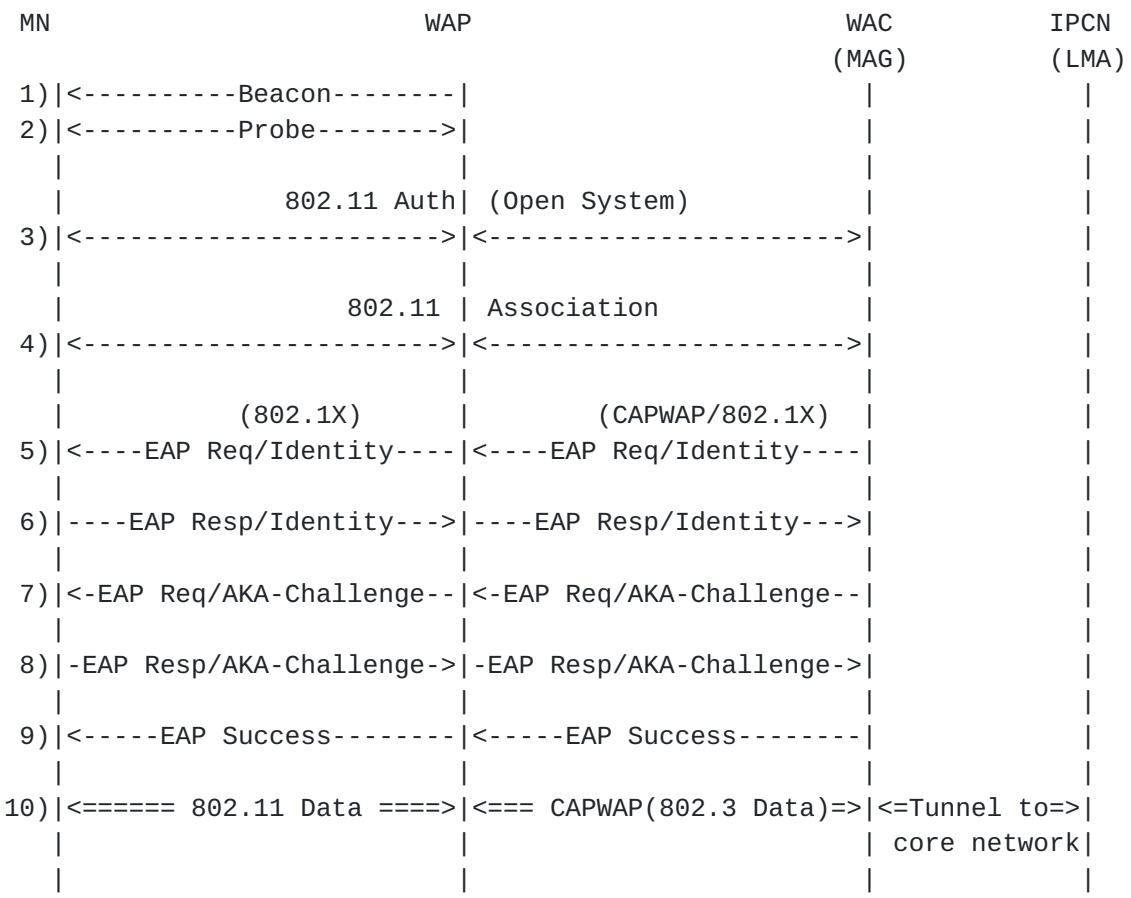

Figure 1: Example EAP Deployment

Legend:

- MN: Mobile Node
- WAP: WiFi Access Point
- WAC: WiFi Access Controller. In a PMIPv6-deployed network, hosts the MAG functionality or is assumed to have a suitable interface to the MAG. In the following, we simply use "WAC" notation. The MAG functionality within the WAC (or within the WiFi access network), or a suitable interface to MAG is assumed for PMIPv6 deployments.
- IPCN: IP Core Network. This includes the LMA function. It generically also includes the AAA server function.
-
- NOTE: The figure shows separate WiFi Access Point and WiFi Access Controller, following the split-MAC model of CAPWAP [RFC5415]. A particular deployment may have the two functions within a single node.

Call Flow Description:

1. MN detects a beacon from a WAP in the vicinity
2. MN probes the WAP to determine suitability to attach (Verify SSID list, authentication type and so on)
3. MN initiates the IEEE 802.11 Authentication with the WiFi network. In WPA/WPA2 mode, this is an open authentication without any security credential verification.
4. MN initiates 802.11 Association with the WiFi network.
5. WiFi network initiates 802.1X/EAP Authentication procedures by sending EAP Request/Identity
6. MN responds with it's permanent or temporary identity
7. WiFi network challenges the MN to prove it's credentials by sending EAP Request/AKA-Challenge
8. MN calculates the security digest and responds with EAP Response/AKA-Challenge
9. If authentication is successful, WiFi network responds to MN with EAP Success.
10. End-to-End data path is available for MN to start IP level activity (DHCPv4, IPv6 Router Solicitation etc.,)

4. Protocol Extensions

The following sections define the new EAP attributes and their usage.

4.1. APN Selection

In a WiFi network, a MN includes AT_VIRTUAL_NETWORK_ID attribute in EAP-Response/AKA-Challenge to indicate the desired APN identity for the first PDN connection.

If the MN does not include AT_VIRTUAL_NETWORK_ID attribute in EAP-Response/AKA-Challenge, the network may select an APN by other means. This selection mechanism is outside the scope of this draft.

4.2. WiFi to UTRAN/EUTRAN Mobility

When a multi-access MN enters a WiFi network, if MN intends to continue the IP session previously attached via UTRAN/EUTRAN, it shall include the following parameters in the EAP-Response/ AKA-Challenge.

- AT_HANDOVER_INDICATION : This attribute indicates to the network that MN intends to continue the IP session from UTRAN/EUTRAN. If a previous session can be located, network shall honor this request by connecting the WiFi access to the existing IP session.
- AT_HANDOVER_SESSION_ID: MN may use this attribute to identify the session on UTRAN/EUTRAN. If used, this attribute shall contain P-TMSI if the previous session was on UTRAN or shall contain

M-TMSI if the previous session was on EUTRAN. This attribute helps the network correlate the WiFi session to an existing UTRAN/ EUTRAN session.

5. Attribute Extensions

5.1. AT_VIRTUAL_NETWORK_ID

The AT_VIRTUAL_NETWORK_ID attribute identifies the virtual IP network that the MN intends to attach to. The implementation of the virtual network on the core network side is technology specific. For instance, in a 3GPP network, the virtual network is implemented based on the 3GPP APN primitive.

This attribute can be included in any of the EAP Request messages that are integrity protected, such as the EAP-Response/AKA-Challenge.

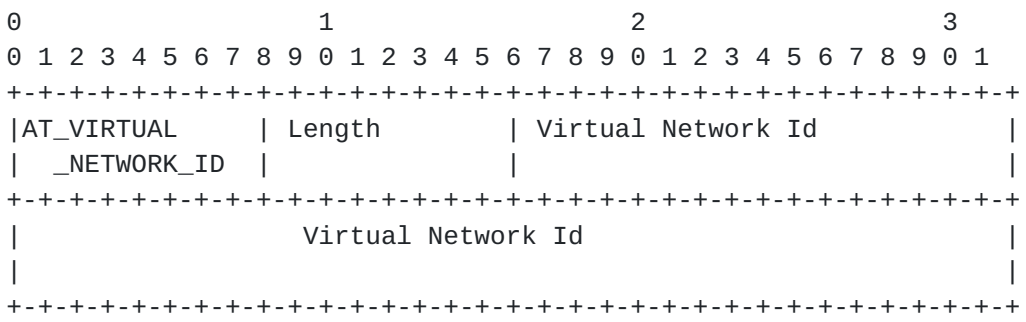

Figure 2: AT_VIRTUAL_NETWORK_ID EAP Attribute

Virtual Network Id:

An arbitrary octet string that identifies a virtual network in the access technology MN is attaching to. For instance, in 3GPP EUTRAN, this could be an APN.

5.2. AT_VIRTUAL_NETWORK_REQ

When MN intends to connect or disconnect from an APN, MN shall use this attribute to indicate the intent to the network.

This attribute can be included only in EAP-Response/Identity.

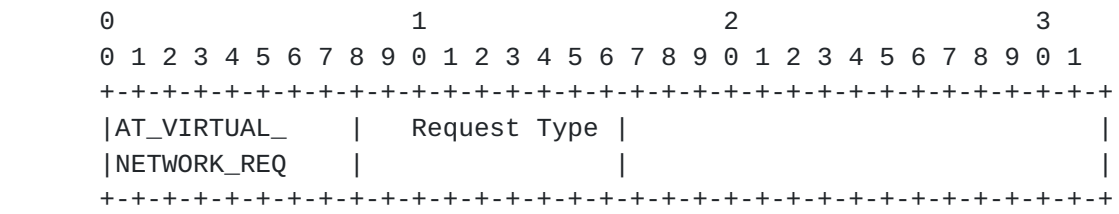

Figure 3: AT_VIRTUAL_NETWORK_REQ EAP Attribute

Request Type:

Request Type shall have one of the following values:

- 0 : Reserved
- 1 : Connect to an APN
- 2 : Disconnect from an APN

6. AT_HANDOVER_INDICATION

This attribute indicates a MN's handover intention of an existing IP attachment.

This attribute can be included in any of the EAP Request messages that are integrity protected, such as EAP-Response/AKA-Challenge.

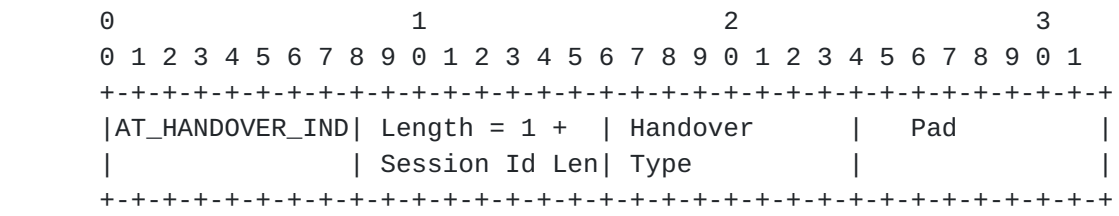

Figure 4: AT_HANDOVER_INDICATION EAP Attribute

Handover Type:

- 0 - MN has no intention of handing over an existing IP session, i.e., MN is requesting an independent IP session with the WiFi network without disrupting the IP session with the UTRAN/EUTRAN. In this case, no Session Id (Section 7) may be included.
- 1 - MN intends to handover an existing IP session. In this case, MN may include a Session Id (Section 7) to correlate this WiFi session with a UTRAN/EUTRAN session.

7. AT_HANDOVER_SESSION_ID

When MN intends to handover an earlier IP session to the current access network, it may propagate identity that can help identify the previous session from UTRAN/EUTRAN that MN intends to handover. This attribute is defined as a generic octet string. MN may include EUTRAN GUTI if the previous session was a EUTRAN session. If the previous session was a UTRAN session, MN may include UTRAN Global RNC ID (MCC, MNC, RNC Id) and P-TMSI concatenated as an octet string.

This attribute can be included in any of the EAP Request message that are integrity protected, such as EAP-Response/AKA-Challenge.

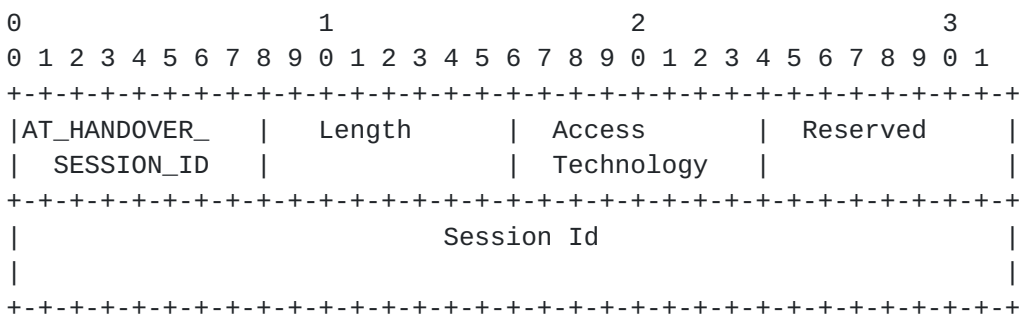

Figure 5: AT_HANDOVER_SESSION_ID EAP Attribute

Access Technology:

This field represents the RAN technology from which the MN is undergoing a handover.

- 0 - Reserved
- 1 - UTRAN
- 2 - EUTRAN

Session Id:

An arbitrary octet string that identifies the session in the source access technology. As defined at the begining of this section, the actual value is RAN technology dependent. For EUTRAN, the value is GUTI. For UTRAN, the value is Global RNC Id (6 bytes) followed by P-TMSI (4 bytes).

8. Security Considerations

This documents defines a new EAP attribute to extend the capability of EAP-AKA protocol as specified in Section 8.2 of RFC 4187 [RFC4187]. This attribute is passed from the MN to the AAA server.

The document does not specify any new messages or options to the EAP-AKA protocol.

9. IANA Considerations

This document defines four new non-skippable EAP attributes: the AT_VIRTUAL_NETWORK_ID (TBD by IANA), AT_VIRTUAL_NETWORK_REQ (TBD by IANA), AT_HANDOVER_INDICATION (TBD by IANA) and AT_HANDOVER_SESSION_ID (TBD by IANA). All these attributes need IANA assignment.

10. Informative References

[3GPP-TS-33.402] "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses, 3GPP TS 33.402 8.6.0, December 2009.", , <http://www.3gpp.org/ftp/Specs/html-info/33402.htm>.

[EPC] "General Packet Radio Service (GPRS);enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TS 23.401 8.8.0, December 2009.", , <http://www.3gpp.org/ftp/Specs/html-info/23401.htm>.

[GPRS] "General Packet Radio Service (GPRS); Service description; Stage 2, 3GPP TS 23.060, December 2006", , <http://www.3gpp.org/ftp/Specs/html-info/23060.htm>.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC3748, June 2004, <http://www.ietf.org/rfc/rfc3748.txt>.

[RFC4186] Haverinen, H. and J. Salowey, "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", RFC 4186, January 2006.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC4187, January 2006, <http://tools.ietf.org/html/rfc4187>.

[RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC5415, January 2009,

<http://www.ietf.org/rfc/rfc5415.txt>.

[RFC5448] Arkko, J., Lehtovirta, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", RFC 5448, May 2009.

Appendix A. Change Log

Revisions in descending chronological order

- o: Initial Draft
- o: v01: status to Informational, Updated References, Revised the Figure

Authors' Addresses

Ravi Valmikam
Unaffiliated
USA

Email: valmikam@gmail.com

Rajeev Koodli
Cisco Systems
USA

Email: rkoodli@cisco.com