Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 14, 2011

B. Mongazon-Cazavet
Y. El Mghazli
Alcatel-Lucent Bell Labs

October 11, 2010

IP Connectivity modes Hint for EAP
draft-mongazon-emu-ip-modes-eap-00

Abstract

The Extensible Authentication Protocol (EAP) is defined in [RFC3748]. This document defines a mechanism that allows an access network to provide IP connectivity modes hints to an EAP peer -- the end of the link that responds to the authenticator. The purpose is to allow the EAP peer in executing in a reliable and efficient manner the IP connectivity step as soon as the authentication phase completes. This is useful in situations where a peer and the networks it visits support various IP connectivity modes. Without the hint, such a peer might fail or take some time to select a valid IP connectivity mode on the visited network. With the help of the hint, a visited network provides the peer with a list of supported IP connectivity modes and allows it to execute successfully the convenient IP connectivity as soon as the authentication is complete. The hint is particularly useful when users are performing vertical handovers through different network technologies such as wireless ones.

Requirements Language

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 RFC 2119 [RFC2119].

Status of this Memo

This Internet-Draft will expire on April 14, 2011.

Copyright Notice

Table of Contents

1. Introduction

Current wireless networks, such as IEEE 802.11, IEEE 802.16, 3GPP2 and 3GPP-LTE, provide IP connectivity over secured (authenticated/ encrypted) access to the network infrastructure. The Extensible Authentication Protocol (EAP), defined in [RFC3748], is used to authenticate users (EAP peers), grant or deny their entry to the wireless access network (EAP authenticator), and to generate Extensible Master Key for use by the EAP peers.

Once EAP authentication is complete, users continue with IP connectivity setup. Such a setup may vary depending on the network technology and architecture. In particular, there is no single nor common IP connectivity setup that would work for any wireless network. For example a network might support a regular DHCPv4 [RFC2131] connectivity while another would only support IPv6 connectivity using RS/RA [RFC4861] or DHCPv6 [RFC3315]. As a consequence, although EAP authentication might succeed, IP connectivity setup might either fail or lack of performance and efficiency due to the incompatibility or slow convergence between IP connectivity modes supported by the user terminal (EAP peer) on one hand and the network on the other hand (EAP authenticator). Such a drawback can be observed in vertical handover situations where a user terminal connects to a visited network that is of different kind than its usual home network.

This document defines a mechanism that allows the access network (EAP authenticator) to provide an EAP peer with IP connectivity modes hint, possibly including additional information and/or options related to an IP connectivity mode and key generation procedures. The IP connectivity modes information is sent to the EAP peer in an EAP-Request/Identity message by appending it after the displayable message and a NUL character. This mechanism may assist the peer in selecting the appropriate IP connectivity mode (and options) to ensure success and efficiency of IP connectivity setup including particular key generation procedures associated with each mode. If the IP connectivity modes information is present, the peer selects the mode among modes proposed by the access network and according to its local capabilities. If the peer does not find a supported or suited mode within the set proposed by the access network, it discards and log the event. If the peer finds an acceptable connectivity mode within the set proposed by the access network, it enters the selected mode procedure as soon as EAP authentication has complete. Should the selected connectivity mode fail, the peer might either retry it or use an alternate mode from the set proposed by the access network. Section 2 describes the required behavior of implementations, including the format for IP connectivity modes hint.

2. Implementation requirements

The EAP authenticator MAY send IP connectivity modes hint to the peer in the initial EAP-Request/Identity. If hint is not sent initially (such as when the EAP authenticator does not support this specification), then the EAP peer may select a default mode that is network or implementation dependent. If hint is sent, the EAP peer selects the most convenient mode according to its own criteria. Such criteria might be related to software capabilities of the user terminal and/or end-user requirements. EAP authenticators shall not propose in hint an IP connectivity mode that is not effectively supported by the network. Both EAP peer and authenticators might manage the supported connectivity modes in a dynamic manner. For example, user-terminal software supporting a particular IP connectivity mode might be loaded dynamically according to modes proposed by an authenticator. Similarly, authenticators might dynamically load software to handle a particular mode prior to advertise its support through the connectivity modes hint.

As noted in [RFC3748], Section 3.1, the minimum EAP MTU size is 1020 octets. EAP does not support fragmentation of EAP-Request/Identity messages, so the maximum length of the IP connectivity modes hint is limited by the link MTU.

2.1. Packet Format

The IP connectivity modes hint information is placed after the displayable string and a NUL-character in the EAP-Request/Identity. The following ABNF [RFC5234] defines an IPmodes attribute for presenting the IP connectivity modes hint information. The attribute's value consists of a set of predefined IP connectivity mode names separated by a semicolon. The predefined names set can be extended in future release of the draft to adapt to new network protocols and architecture.

```
identity-request-data = [ displayable-string ] %x00 [ IP-modes ]

displayable-string = *CHAR

IP-modes = "IPmodes=" mode-list
mode-list = mode / ( mode-list ";" mode )
mode = "pmip4-ietf"  / "pmip6-ietf"  / "mip4-ietf"   /
       "mip6-ietf"   / "dsmip6-ietf" / "pmip4-wimax" /
       "pmip6-wimax" / "mip4-wimax"  / "mip6-wimax"  /
       "mip4-3gpp2"  / "mip6-3gpp2"  / "mip4-lte"    /
       "dsmip6-lte"
```

The "CHAR" rule is defined in [RFC 4234]

The current mode-list refers to IP connectivity procedures defined in separate standards as described in the list below.

- "pmip4-ietf" [RFC5563]
- "pmip6-ietf" [RFC5213]
- "mip4-ietf" [RFC3344]
- "mip6-ietf" [RFC3775]
- "dsmip6-ietf" [RFC5555]
- "pmip4-wimax" [WIMAX]
- "pmip6-wimax" [WIMAX]
- "mip4-wimax" [WIMAX]
- "mip6-wimax" [WIMAX]
- "mip4-3gpp2" [TGPP2-4]
- "mip6-3gpp2" [TGPP2-6]
- "mip4-lte" [LTE]
- "dsmip6-lte" [LTE]

3. Security Considerations

IP connectivity modes hint information refers to standard procedures supported by an EAP authenticator. References to standard procedures shall not be considered as a private information from authenticator point of view. Although it can reveal network capabilities to support a given standard, such a support is generally required and claimed depending on the network access. Thus the hint information should not be considered as compromising user nor network privacy.

4. Acknowledgements

The authors would especially like to thank Peretz Feder for reviewing the document in progress and suggesting improvements to it.

5. Normative References

[LTE] http://www.3gpp.org, "TS 33.402, Security aspects for non-3GPP access (Rel9)", December 2009.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

[RFC5563] Leung, K., Dommety, G., Yegani, P., and K. Chowdhury, "WiMAX Forum / 3GPP2 Proxy Mobile IPv4", RFC 5563, February 2010.

[TGPP2-4] www.3gpp2.org, "3GPP2 X.S0044-0 Version 1.0", September 2010.

[TGPP2-6] www.3gpp2.org, "3GPP2 X.S0047-0 Version 1.0", February 2009.

[WIMAX] WiMAX Forum, "WMF-T33-001-R015v01 Stage 3", November 2009.

Authors' Addresses

Mongazon-cazavet Bruno
Alcatel-Lucent Bell Labs
Centre de Villarceaux - Route de Nozay
Nozay, 91620
France

Email: bruno.mongazon-cazavet@alcatel-lucent.com

El Mghazli Yacine
Alcatel-Lucent Bell Labs
Centre de Villarceaux - Route de Nozay
Nozay, 91620
France

Email: yacine.el_mghazli@alcatel-lucent.com