Extensible Authentication Protocol
Working Group
Internet-Draft
Expires: December 16, 2004

F. Adrangi
V. Lortz
Intel Corporation
F. Bari
AT&T Wireless
P. Eronen
Nokia Research Center
M. Watson
Nortel

June 17, 2004

Mediating Network Discovery in the Extensible Authentication Protocol (EAP)
draft-adrangi-eap-network-discovery-01

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 16, 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document defines a mechanism to enable a wireless client to discover roaming partners of an access network over EAP. The purpose

is to help a wireless client select the most appropriate roaming partner as a next hop for routing of AAA packets. This solution is especially useful in roaming scenarios where the access network does not have a direct relationship with the wireless client's home network - i.e., when AAA packets can not be directly routed from access network to the home network.

Table of Contents

1. Introduction

In wireless network access, the high level network topology is comprised of access networks, mediating networks, and home networks as depicted in Figure 1. RADIUS [2] protocol has been assumed for AAA mediation between the access network and the home network although Diameter [3] could also be used instead of RADIUS without introducing significant architectural differences.

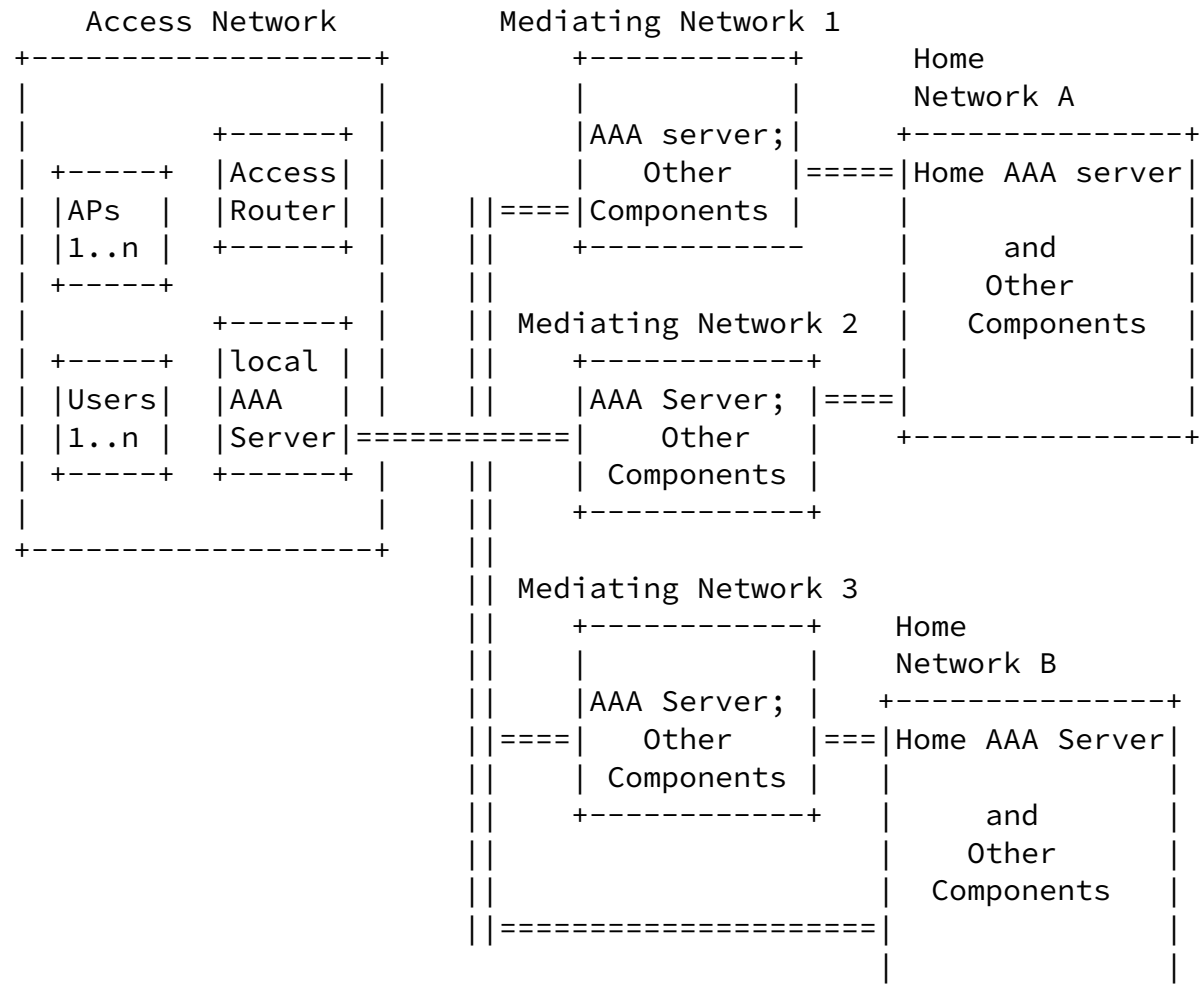


Figure 1. Network Access Arrangement.

In roaming situations, EAP authentication exchanges [5] will be carried out between the wireless client in the access network and an AAA server in the home network directly when the two networks have a direct roaming relationship. However when a wireless client roams to an access network that it does not recognize and which does not have a direct roaming relationship with its home network, the AAA packets have to be routed through a mediating AAA network to the home network. For inter operator settlement reasons, it is necessary to select the best mediating network. For instance, in Figure 2, access

through the Mediating Network 1 may be cheaper for isp1 user, than if Mediating Network 2 is used. However this decision can not be made by the access network as it would be unaware of the roaming agreements of mediating networks 1 and 2 with the isp1. For this reason, it is desirable for the wireless client to know which mediating networks are available through an access network, and influence the decision of using the desired mediating network.

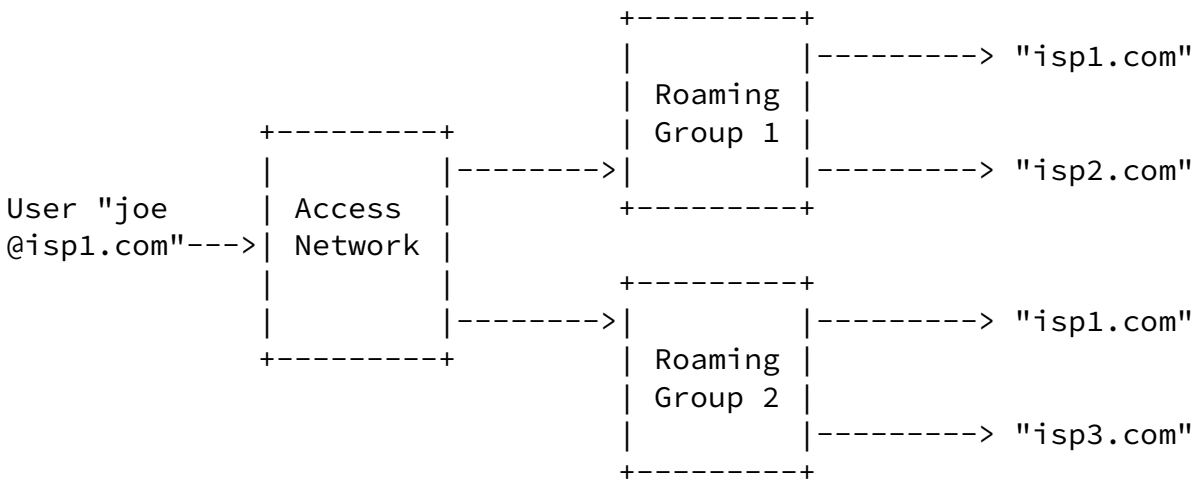


Figure 2: Ambiguous AAA routing

Influencing the mediating network selection problem can be divided into three sub-problems as follows:

1. A syntax by which mediating network information can be represented.

2. A delivery mechanism by which mediating network information is conveyed to a wireless client.

3. A general mechanism by which a wireless client's selection can be conveyed to the access network.

Section 2.7 of [6] discusses the conditions upon which NAIs can be used to affect AAA routing, i.e., problem 3 above. Problems 1 and 2 are discussed in this document.

1.1 Applicability

Although the proposed solution here is discussed in the context of public 802.11 access network deployment, it is applicable to other public wireless access networks where the wireless clients use the EAP specification framework [5] for authentication, and they present their identity to the network in NAI [6] format.

1.2 Terminology

Network Access Identifier (NAI)
: An identifier that represents a wireless client or user identity. The basic structure of a NAI is user@realm, where the realm part of the NAI indicates the domain responsible for interpretation and resolution of the user name. Please See [6] for more details on NAI format.

Access Point (AP)
: A station that provides access to the distribution services via the wireless medium for associated Stations.

RADIUS server
: This is a server which provides for authentication/ authorization via the protocol described in [2].

2. Data Model

Mediating network information needs to be structured in a general

format and syntax so that the EAP client software can interpret it and behave accordingly. The syntax should have minimum overhead because the proposed delivery mechanism (i.e., EAP-Identity Request) doesn't support fragmentation and therefore size of the data is limited by the link layer MTU.

Mediating network information is placed after the displayable string and NULL in the EAP-Identity Request. It is structured as a set of comma-separated attribute names and values according to the following ABNF [1]:

```
identity-request-data = displayable-string [ %d0 network-info ]
displayable-string = *CHAR

network-info = attribute "=" value

attribute =  1*( ALPHA / "-" / "_" / DIGIT)

value = 1*( %x01-2B / %x2D-FF ) ; any non-null UTF-8 char except ","
```

The CHAR, DIGIT, ALPHA terminals are defined in [1].

Only one attribute is defined here, the NAIRealms attribute. The use of this facility for other purposes is discouraged due to the limited amount of space available in EAP packets.

The format and semantics of the NAIRealms attribute value are as follows:

```
value = Realm [ ";" Realm ]
```

Where the Realm is defined in [6].

An example "NAIRealms" attribute is shown below:

```
NAIRealms=anyisp.com;mnc123.mcc334.3gppnetwork.org
```

3. Delivery Mechanism

There are three possible options of delivering mediating network information to a wireless client by using an EAP-Identity Request. These options are:

Option 1 - Use the Initial EAP-Identity Request issued by the access network NAS

Mediating network information is pushed to a wireless client in the initial EAP-Identity Request issued by the AP.

Option 2 - Use the initial EAP-Identity Request issued by the access network RADIUS server

This is similar to Option 1, but the initial EAP-Identity Request is issued by the access network RADIUS Server instead. Once a wireless client associates with an access network AP using native IEEE 802.11 procedures, the AP sends an EAP-Start message [4] within a RADIUS Access-Request to trigger an EAP conversation initiated by the access network RADIUS server.

Option 3 - Use a subsequent EAP-Identity Request issued by the access network RADIUS server

Mediating network information is delivered to a wireless client in a subsequent EAP-Identity request, after the initial EAP-Identity Request/Response exchange, issued by by the access network RADIUS server.

4. Implementation Considerations

- In general, an option that requires changes only to a central AAA server is much preferred than a one that impacts a distributed set of

APs. The reasons for this preference include ease of operation and deployment, update costs, backwards compatibility and possible impact on current standards. Option 3 is therefore preferred as it does not require any changes to the AP. Option 2 is also equally desirable if the AP supports the EAP-Start message [4].

- In order for a wireless client software implementation to work with

all options transparently, the implementation MUST not require the arrival of mediating network information on a particular EAP-Identity Request (i.e., the initial or a subsequent Request). Access network operators therefore MAY choose to deploy any of the above delivery mechanism options in their network without losing interoperability. However, delivery mechanism options 2 and 3 are recommended as they are backward-compatible with the currently-deployed APs.

- When Option 3 is used, upon receipt of a RADIUS Access-Request packet containing the initial EAP-Identity Response, the access network RADIUS proxy/server MAY send an EAP-Identity Request containing mediating network information to the wireless client if it cannot route the RADIUS packet to the next AAA hop based on the realm portion (i.e., string after the @ sign) of the NAI in the RADIUS User-Name attribute. When a RADIUS Access-Request containing a subsequent EAP-Identity Response is received, if the RADIUS proxy/ server still cannot route the RADIUS packet to the next AAA hop based on the realm portion of the NAI, then it MUST discard the packet.

- The use of the mechanism described in this document SHOULD be reserved for situations where the WLAN client can not identify a direct route to its home network based on the available SSIDs in the hotspot.

5. IANA Considerations

This document does not define a new name space, therefore, there are no considerations for IANA.

6. Security Considerations

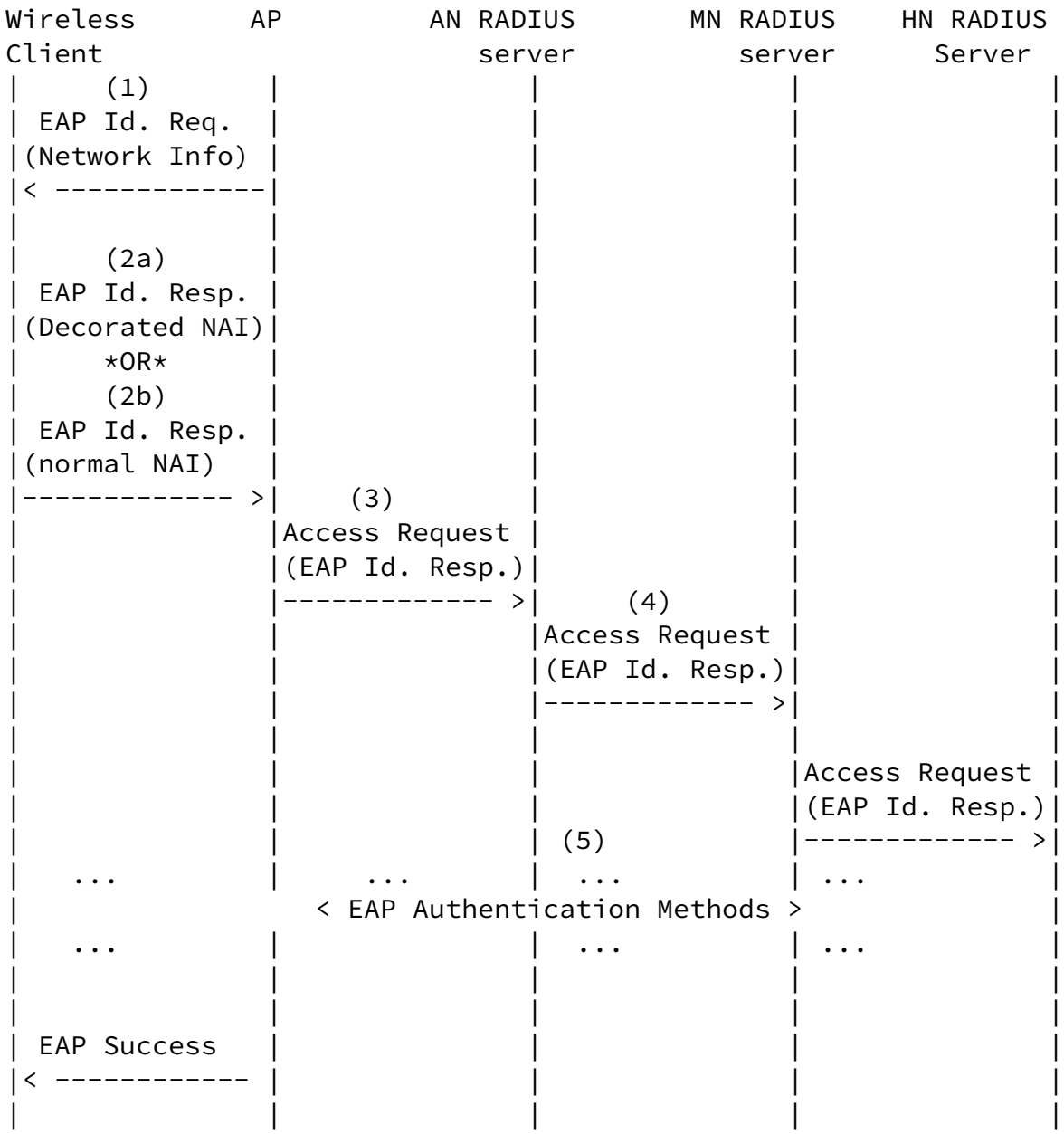
Mediating network information delivered inside an EAP-Identity Request before the user authenticates to the network. Therefore, it is considered as a hint in guiding the wireless client to select the desired mediating network through which the AAA packets should be routed.

It should also be noted that at least with some EAP methods, there is no way for the home network RADIUS server to verify that the mediating network used was actually the same one that the wireless client had requested.

7. Appendix

The railroad diagrams below illustrate conversations between a wireless client, AP, Access Network (AN) RADIUS proxy/server, Mediating Network (MN) RADIUS proxy/server, and Home Network (HN) RADIUS server for the three options described above.

Option 1 - Use the Initial EAP-Identity Request issued by the access network AP



The following describes each message flow in details.

1. The AP sends the initial EAP-Identity Request containing mediating network information to the wireless client.

2. The wireless client sends an EAP-Identity Response containing a Decorated NAI indicating the selected MN to the AP. OR,

3. The wireless client sends an EAP-Identity Response containing a normal NAI (i.e., non-decorated)to the AP.

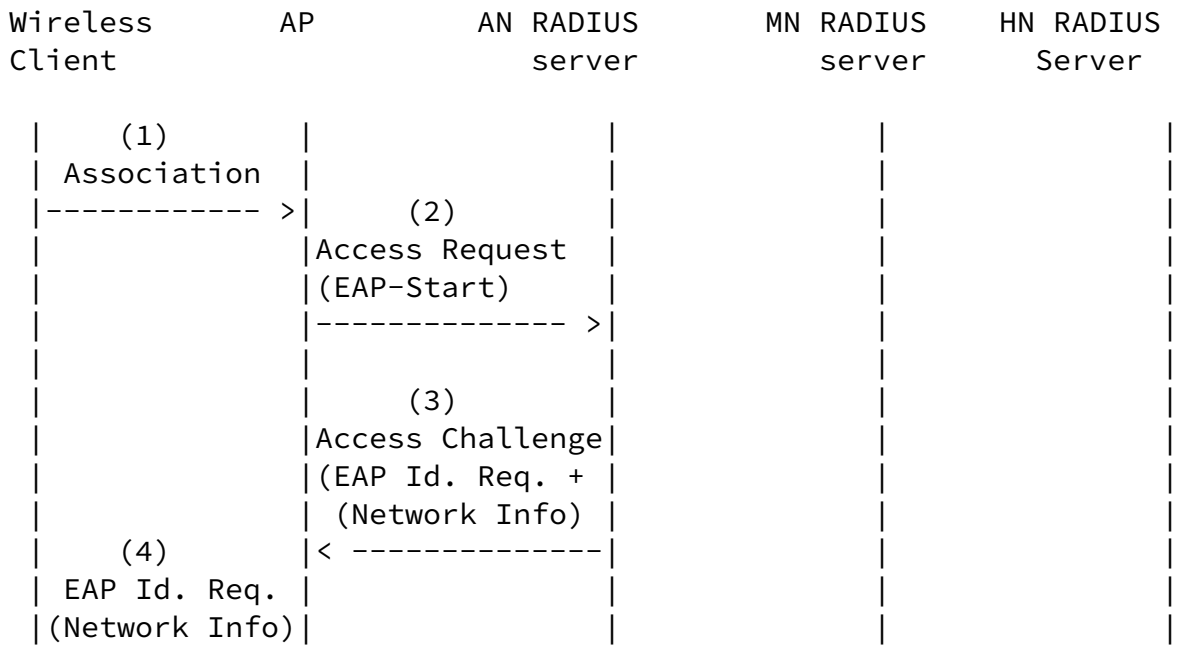
4. The AP sends a RADIUS Access Request packet containing the EAP-Identity Response to the access network RADIUS proxy/server as described in [4]. Please note that NAI in the EAP-Identity Response is copied to the RADIUS User-Name attribute in the Access-Request packet as per [4].

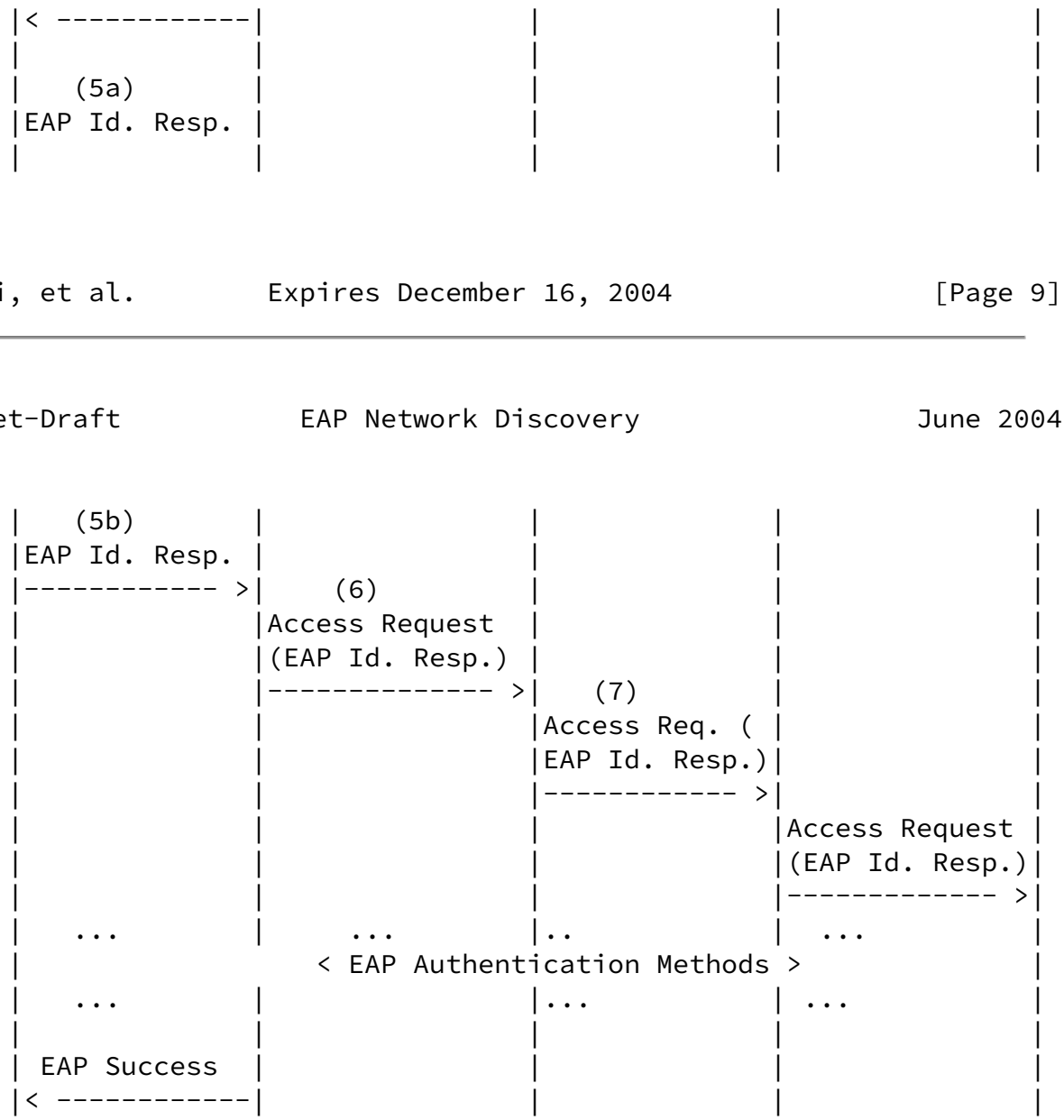
5. The access network RADIUS proxy/server forwards the received Access-Request packet to the next AAA hop based on the realm portion of the NAI in the RADIUS User-Name attribute.

6. The MN RADIUS proxy/server forwards the received Access-Request packet based on the NAI in the RADIUS User-Name attribute to the next AAA hop (i.e., HN RADIUS Server).

7. The EAP Authentication continues as described in [4].

Option 2 - Use the initial EAP-Identity Request issued by the access network RADIUS server.





The following describes each message flow in details.

1. The wireless client associates with the AP.

2. An EAP-Start message encapsulated within a RADIUS Access-Request sent to the access network RADIUS server.

3. The access network RADIUS server processes the received Access-Request message and initiates an EAP conversation by sending an EAP-Identity Request containing mediating network information encapsulated within a RADIUS Access-Challenge.

4. The AP extracts the EAP-Identity Request from the received Access-Challenge and sends it to the wireless client.

5. The wireless client sends an EAP-Identity Response containing its

decorated NAI indicating the selected MN to the AP. OR,

6. The wireless client sends an EAP-Identity Response containing a normal NAI (i.e., non-decorated) to the AP.

7. The AP sends a RADIUS Access-Request packet containing the EAP-Identity Response to the access network RADIUS server as described in [4]. Please note that NAI in the EAP-Identity Response is copied to the RADIUS User-Name attribute in the Access-Request packet as per [4].

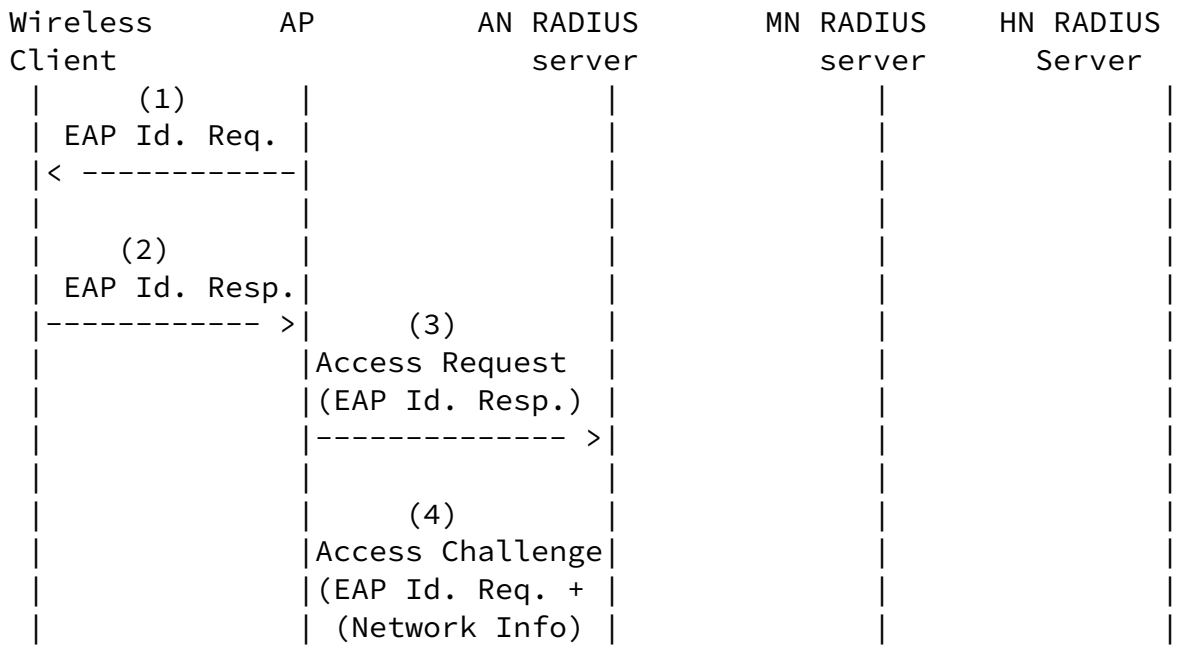
8. The access network RADIUS proxy/server forwards the received

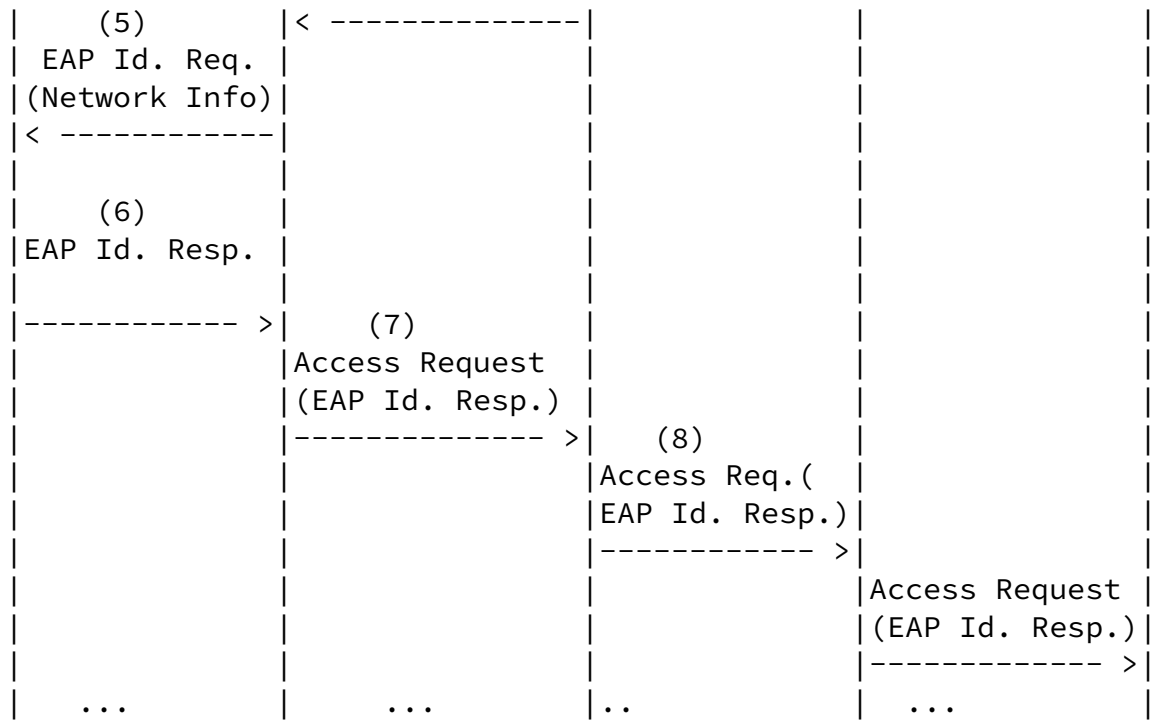
Access-Request packet to the next AAA hop based on the realm portion of the NAI in the RADIUS User-Name attribute.

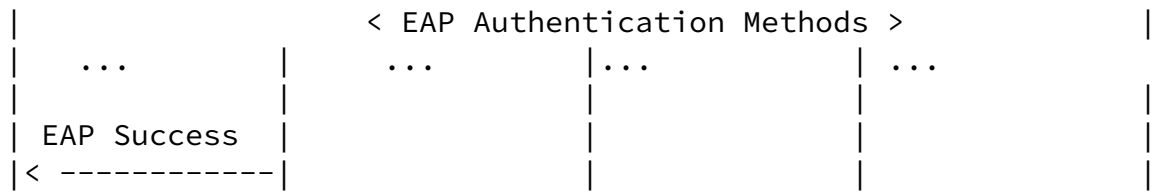
9. The MN RADIUS proxy/server forwards the received Access-Request packet based on the NAI in the RADIUS User-Name attribute to the next AAA hop (i.e., HN RADIUS Server).

10. The EAP Authentication continues as described in [4].

Option 3 - Use a subsequent EAP-Identity Request issued by the access network RADIUS server







The following describes each message flow in details.

1. The access network AP issues an EAP-Identity Request to a wireless client

2. The wireless client replies with an EAP-Identity Response containing a normal NAI (i.e., non-decorated), or perhaps a Decorated NAI [6] based on the mediating network information cached from the most recent authentication session to the access network.

3. The AP creates a RADIUS Access-Request packet encapsulating the EAP-Identity Response and sends it to the access network RADIUS server.

4. The access network RADIUS proxy/server sends a RADIUS

Access-Challenge packet encapsulating an EAP-Identity Request containing mediating network information. Or, the step 8 is executed if the access network proxy/server can route the packet based on the realm portion of the NAI in the RADIUS User-Name attribute to the next AAA hop.

5. The access network AP forwards the EAP-Identity Request containing the mediating network information to the wireless client.

6. The wireless client replies with an EAP-Identity Response containing a Decorated NAI indicating the preferred MN. Wireless client can still send an undecorated NAI to the RADIUS proxy/ server, if it is a legacy client. It should also be noted that the wireless client may also decide not to connect to the access network in the absence of the desired MN in the received MN information in step (4).

7. The access network AP forwards the EAP-Identity Response to the access network RADIUS server over RADIUS protocol.

8. The access network RADIUS proxy/server forwards the received Access Request to the appropriate MN RADIUS server based on the realm portion of the NAI in the RADIUS User-Name attribute.

9. The MN RADIUS proxy/server forwards the received Access-Request

packet based on the NAI in the RADIUS User-Name attribute to the next AAA hop (i.e., HN RADIUS Server). The EAP Authentication continues as described in [4].

8. Acknowledgement

The authors would specially like to thank Jari Arkko (of Ericsson) for his help in scoping the problem, for reviewing the draft work in progress and for suggesting improvements to it.

The authors would also like to acknowledge and thank Jari Arkko (of Ericson), Bernard Aboba (of Microsoft), Adrian Buckley (of RIM), Blair Bullock (of iPass) , Jose Puthenkulam (of Intel), Johanna Wild (of Motorola), Joe Salowey (of Cisco), Marco Spini (of Telecom

Italia), Simone Ruffino (of Telecom Italia) and Mark Grayson (of Cisco)for their support, feedback and guidance during the various stages of this work.

9. References

9.1 Normative References

[1] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[2] Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[3] Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[4] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[5] Blunk, L., "Extensible Authentication Protocol (EAP)", draft-ietf-eap-rfc2284bis-09 (work in progress), February 2004.

[6] Aboba, B., "The Network Access Identifier", draft-arkko-roamops-rfc2486bis-00 (work in progress), February 2004.

9.2 Informative References

Authors' Addresses

Farid Adrangi
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro OR
USA

Phone: +1 503-712-1791
EMail: farid.adrangi@intel.com

Victor Lortz
Intel Corporation
2111 N.E. 25th Avenue
Hillsboro OR
USA

Phone: +1 503-264-3253
EMail: victor.lortz@intel.com

Farooq Bari
AT&T Wireless
7277 164th Avenue N.E.
Redmond WA
USA

Phone: +1 425-580-5526
EMail: Farooq.bari@attws.com

Pasi Eronen
Nokia Research Center
P.O. Box 407
FIN-0005 Nokia Group
Finland

EMail: pasi.eronen@nokia.com

Mark Watson
Nortel
2221, Lakeside Blvd
Richardson TX
USA

EMail: mwatson@nortel.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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 independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.