Network Working Group
INTERNET DRAFT
Category: Informational
Expires : Aug 10, 2004

Farid Adrangi (Ed.)
Intel Corporation
Feb 10, 2004

Mediating Network Discovery and Selection
draft-adrangi-eap-network-Discovery-and-Selection-01.txt

Status of this Memo

Abstract

This document proposes a solution for Service Network discovery and selection that could be implemented within the existing EAP specification framework. The purpose of Service Network discovery and selection here is to help a WLAN client using EAP for authentication to decide whether or not to connect to a WLAN Access Network, and help it select the most appropriate Mediating Network as a next hop for routing AAA packets in roaming situations where the WLAN Access Network has agreements with more than one Mediating Network affiliated with the clientÆs Home Service Network.

The proposed solution has 3 components: a delivery mechanism for conveying Access Network and Service Network Information to a WLAN client, a data model/syntax for structuring the information in a generic manner, and a mechansim by which the WLAN client can

indicate its selection to the WLAN Access Network.

Table of Contents

1. Introduction

Wireless LAN (WLAN) Access Networks are being deployed in public places such as airports, hotels, shopping malls, and coffee shops. A Public WLAN (PWLAN) Access Network typically consists of three key components that work together to provide authorized users with a wireless access to the Internet or to services offered/authorized by their Service Network providers (e.g., WISP, 3GPP, or 3GPP2 type Service Networks). The three components are: the Access Points (AP), the PWLAN AAA server, and the Access Router which links the PWLAN Access Network to the services network (i.e., Internet and/or operatorÆs core IP network).

A PWLAN Access Network MAY have a direct or an indirect (i.e., via a mediator) relationship with 1 or more Service Networks (e.g., WISP, 3GPP, or 3GPP2). Figure 1 illustrates a PWLAN Access Network that has roaming agreements with three Mediating Networks (i.e., öRoaming Partnerö or öBrokerö or öVisited Service Networkö - hereafter these terms are used interchangeably to mean a Mediating Network in this document). As the figure shows, Mediating Networks 1 and 2 have relationships with Home Service Network A; Mediating Network 3 has relationship with Home Service Network B. The figure also shows a direct relationship between the PWLAN Access Network and Home Service Network B.

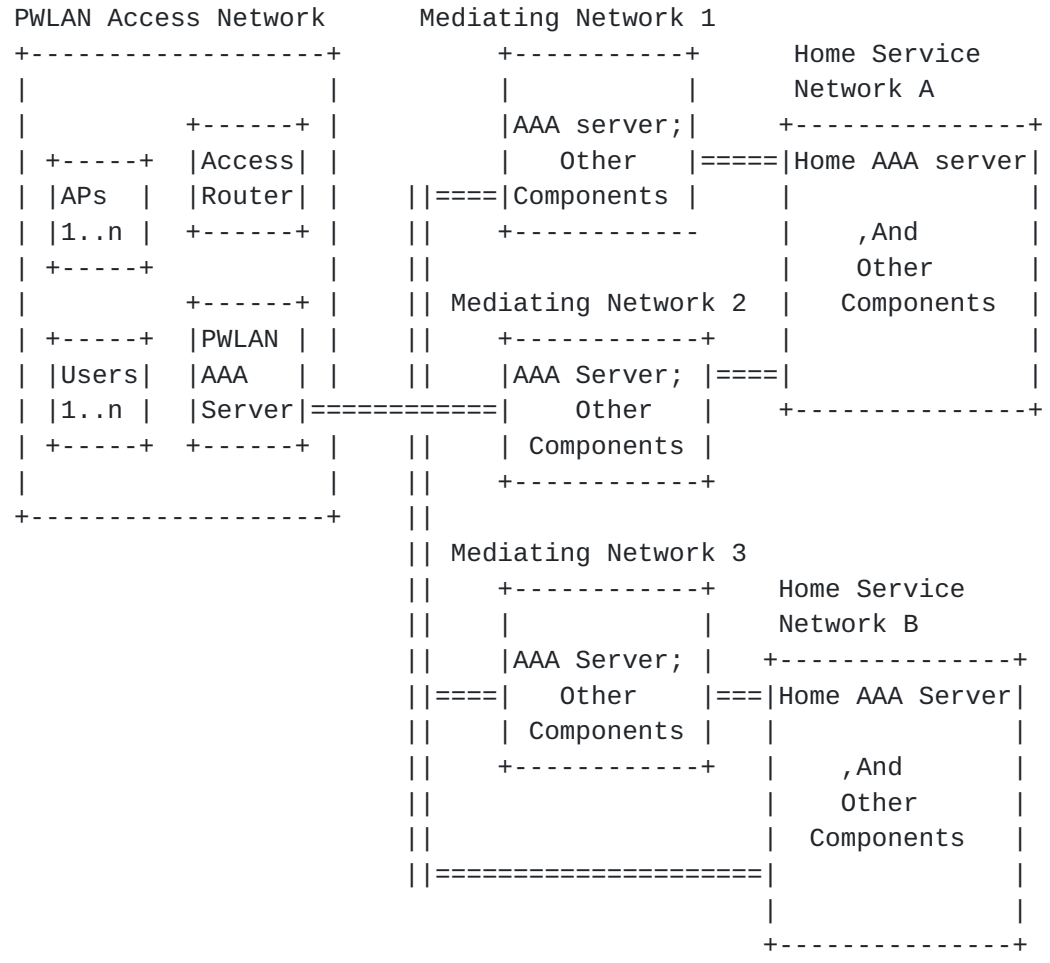


Figure 1 : WLAN Roaming Network Architecture with AAA mediation

To be specific, hereafter, RADIUS [1] protocol is assumed for AAA mediation between the PWLAN Access Network and the Home Service Provider. Diameter [2] could also be used instead of RADIUS without introducing significant architectural differences.

1.1 Authentication Message Flow

This section provides an overview of authentication exchanges between a WLAN client and a Home Service Provider.

In roaming situations, authentication exchanges are carried out between a WLAN client in a PWLAN AN and a RADIUS server in a Home

Service Network through 1 or more RADIUS proxies/servers located in the PWLAN Access Network and the Mediating Networks as shown in Figure 2. During the authentication phase, EAP messages are encapsulated using a mechanism such as EAPOL (EAP over LAN) between the WLAN client and the AP and re-encapsulated in RADIUS messages (referred to as the öEAP over RADIUSö [4]) from the AP to the home RADIUS server in the Home Service Network.

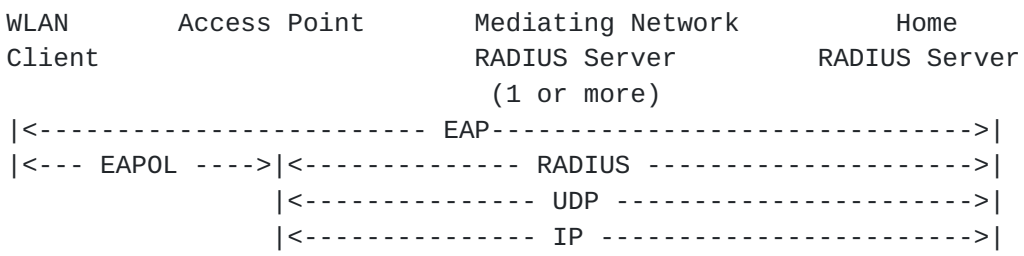


Figure 2 û EAP-based Authentication Message Flow

1.2 Problem Statement

In roaming situations where a WLAN Access Network has agreements with more than one Mediating Network affiliated with a WLAN clientÆs Home Service Network, the WLAN client SHOULD be able to influence the selection of the desired Mediating Network through which authentication packets SHOULD be routed through. The WLAN client may prefer one Mediating Network over another for charging, Quality of Service (QoS), or other reasons. The WLAN client may also decide to not connect to the WLAN Access Network due to the absence of a desired Mediating Network.

Influencing the Mediating Network selection problem can be divided into three sub-problems as follows:

1) A delivery mechanism by which Network Information is conveyed to a WLAN client.

2) A general data model and syntax by which Network Information is structured for unambiguous interpretation by the WLAN client.

3) A general mechanism by which a WLAN clientÆs selection can be conveyed to the WLAN Access Network.

1.3 Rationale for the Proposed Solution

Several solution alternatives were considered for Network Discovery and Selection. The fundamental difference among them is the type of bearer that they use to convey Network Information

to a WLAN client. This section articulates the rationale for using EAP as a mechanism / bearer for Network Discovery and

Selection by describing why the competing solution alternatives are undesirable.

[Competing Solution Alternative 1]

It is possible for a WLAN client to derive Network Information from the Broadcast SSID or other such information. However, this requires having structured SSID values with a standardized namespace which will break backwards compatibility, since deployed PWLAN networks may not be in a position to change the SSID used. Also private WLAN SSIDs could overlap with the standardized namespace making it inefficient.

Note that the SSIDs can be broadcasted as the identities of the Mediating Networks which eliminates the need for having structure SSID values with a standardized namespace. However, this will require APs to support broadcast of multiple SSIDs which is not an IEEE standard. Furthermore, the capability for broadcasting multiple SSIDs may have some scalability implications.

[Competing Solution Alternative 2]

It is possible to convey Network Information in Access Point (AP) broadcasts (e.g., beacon frames) to a WLAN client. However, this is undesirable because of the high frequency (i.e., every 100-400ms) of these broadcast frames and the incurred traffic overhead which would adversely impact the PWLAN performance. Furthermore, this is not backward-compatible with existing PWLAN deployments as it requires firmware/hardware changes to the APs.

[Competing Solution Alternative 3]

It is possible for a WLAN client to do active scanning wherein the WLAN client would send a probe request with a specific SSID and the Access Point would respond with the Network Information. However, this will require changes to the APs to support administrating and delivering Network Information, hence it is not backward-compatible with currently deployed PWLAN networks. It will also require changes to network software layers on the client to propagate the information up to the appropriate layer.

[Competing Solution Alternative 4]

It is possible for a WLAN client to have a local database mapping SSIDs to Mediating Network names, where it is not

necessary to change SSIDs. However, this will have the same problems as the alternative 1. Furthermore, it will require

storage space for the database, and a mechanism for updating it.

Having described the disadvantages of the competing solution alternatives, this document proposes a solution that uses EAP as a mechanism for conveying Network Information to a WLAN client. And, the rationale for this as follows:

- o The proposed solution is backward-compatible with existing PWLAN deployments.
- o The proposed solution does not introduce a new protocol standard, or require any significant protocol changes to existing protocol standards.
- o The proposed solution can be implemented without impacting existing APs deployed in PWLAN networks.
- o The proposed solution does not negatively impact the performance of PWLAN networks.

1.4 Applicability of the Proposed Solution

The solution can be deployed in any wireless access network architecture where the clients use the existing EAP specification framework [9] for authentication, and they present their identity to the network in NAI [5][10] format.

1.5 Requirements language

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. 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].

1.6 Terminology

Access Network (AN)
: The PWLAN hotspot network that provides wireless connectivity to the Internet for WLAN clients (or stations) present in the local access area. This MAY be in a separate security and routing domain with respect to the Home Service Network or a Mediating Network.

Home Service Network (HSN)
: The network providing the service and therefore maintaining the direct relationship to the user/subscriber of the WLAN

service. All AAA functions are ultimately performed by the HSN.

Visited Service Network (VSN)
The Service network providing service in the local geographical region to roaming customers of another HSN. Such networks may act as Mediating Networks to the roaming clients.

Mediating Network (MN)
The network responsible for mediation between a PWLAN Access Network and a Home Service Network. They could be AAA brokers or Visited Service Networks.

Network Information (NI)
Network-related information pertaining to a PWLAN network (e.g., location information such as country, state, city, location ID, and etc.) and its roaming partners (e.g., a list of övisited networksö that the PWLAN has agreements with).

Network Access Identifier (NAI)
An identifier that represents a 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. See [5][10] for more details on NAI format.

Decorated NAI
A valid NAI with additional information influencing the routing choice of the next Mediating Network to the PWLAN AAA server as describe in this document. It may include information for several Mediating Networks to be indicated on the route to the Home Service Network.

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

RADIUS server
öThis is a server which provides for authentication/authorization via the protocol described in [1], and for accounting as described in [6].ö It is deployed in the PWLAN AN, MN, and HSN.

Service Set Identifier (SSID)
öan identifier attached to packets sent over the wireless LAN that functions as a öpasswordö for joining a particular radio network.ö

2. Proposed Solution

The EAP-Identity request message is used to deliver Network

Information (structured by a general data model/syntax) to a WLAN client. Upon receipt of the information, the WLAN client then MAY influence the selection of an MN which has a direct relationship

with the PWLAN AN for routing RADIUS packets through to the HSN. This is achieved by sending a Decorated NAI in the Type-Data field of the EAP-Identity Response. As specified in [4], the PWLAN AP then encapsulates the EAP-Response within an EAP-Message attribute and sends it to the PWLAN RADIUS server within a RADIUS Access-Request packet. It also copies the contents of the Type-Data field of the EAP-Response (i.e., the Decorated NAI) into the User-Name attribute.

When a PWLAN RADIUS server receives a RADIUS Access-Request packet containing a Decorated NAI which does not specify an MN recognized by the PWLAN AN as the next hop for routing the RADIUS packet, the PWLAN RADIUS server SHOULD route the RADIUS packet based on its local routing policy.

The solution is comprised of three components: the delivery mechanism for conveying the information to a WLAN client, the data model / syntax for structuring the information, and the NAI decoration for indicating the selected MN. The following sections describe each solution component in details.

2.1 Delivery Mechanism

The EAP specification [3] describes the use of the Type-Data field in an EAP-Identity Request for a displayable message terminated by a null. It also suggests that additional data (with format currently undefined) can be placed after the null character.

Network Information MUST be placed after the null character in the Type-Data field. The portion of the field prior to the null MAY contain zero or more bytes (depending on whether or not there is a displayable message). There are three possible options of delivering Network Information to a WLAN client by using an EAP-Identity Request. These options are:

1) Use the Initial EAP-Identity Request issued by the PWLAN AP.

2) Use the initial EAP-Identity Request issued by the PWLAN RADIUS server.

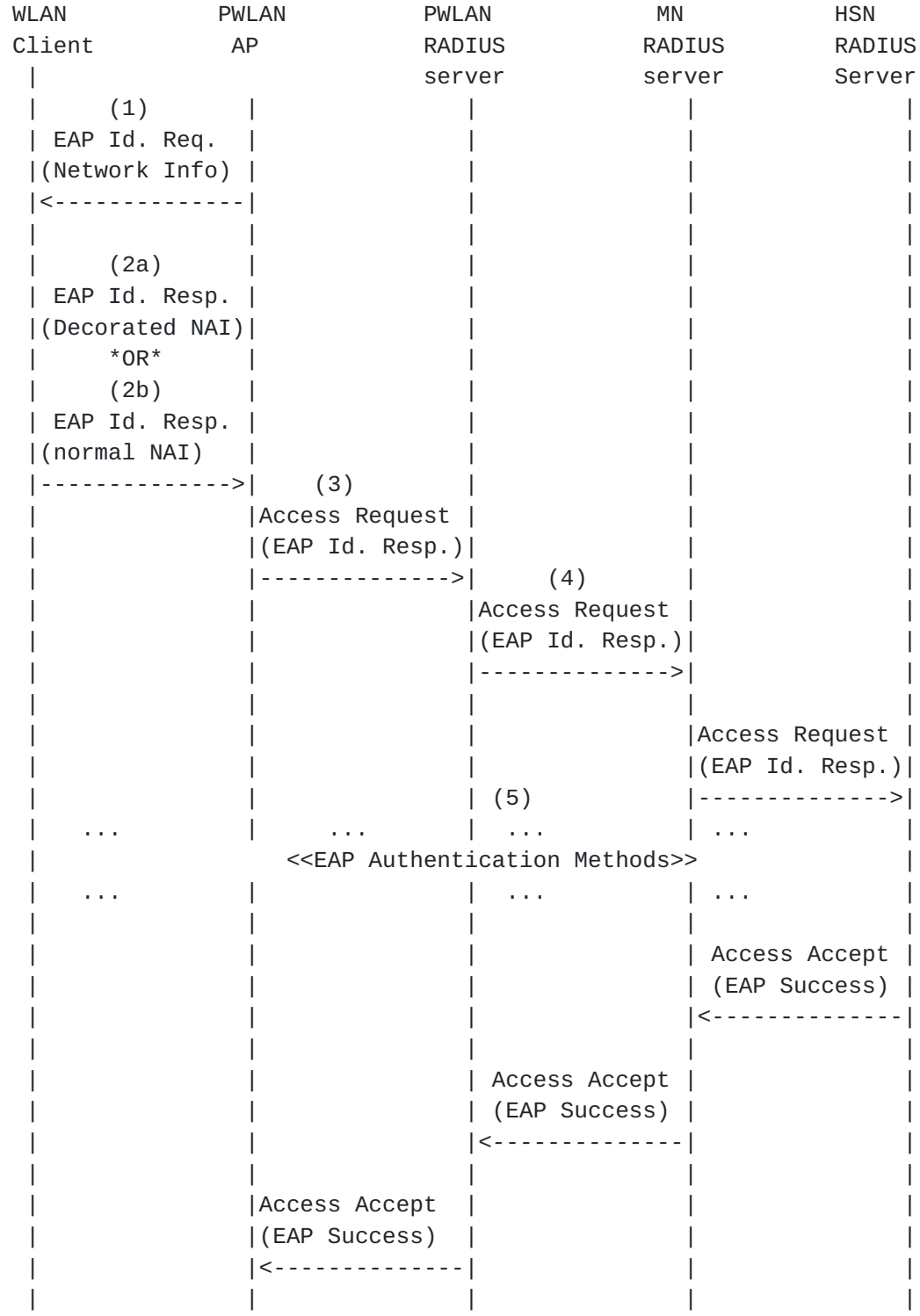
3) Use a subsequent EAP-Identity Request issued by the PWLAN RADIUS server.

Here we look at these three options with pros and cons of each.

[Option 1] Use the Initial EAP-Identity Request issued by the PWLAN AP

Network information is pushed to a WLAN Client in the initial EAP-Identity Request issued by the AP.

The message flow below illustrates conversations between an authenticating peer, AP, PWLAN AN RADIUS server, MN RADIUS server, and HSN RADIUS server. Where the AP sends an EAP-Request/Identity containing Network Information as the initial packet, the exchange appears as follows:




| EAP Success |
|<-------------- |

The following describes each message flow in details.

(1) The PWLAN AP sends the initial EAP-Identity Request containing Network Information the WLAN Client.

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

(2b) The WLAN client sends an EAP-Identity Response containing a normal NAI defined in [5][10] to the PWLAN AP.

(3) The PWLAN AP sends a RADIUS Access Request packet containing the EAP-Identity Response (as defined in [4]) to the PWLAN RADIUS server.

(4) The PWLAN RADIUS server processes the received Access-Request packet as specified in [4] and forwards it to the appropriate MN RADIUS server.

(5) The EAP Authentication continues as described in [4].

The following summarizes pros and cons of this option.

Pros:

- It does not introduce additional EAP messages

Cons:

- It requires modifications to APs, since most currently-deployed APs do not include support for administering and delivering Network Information in the EAP-Identity Request.

- It MAY require modification to the PWLAN RADIUS server for processing a Decorated NAI (many RADIUS servers already have this capability).

- It MAY introduce a contention problem if space in the Type-Data field has already been used up for other purposes.

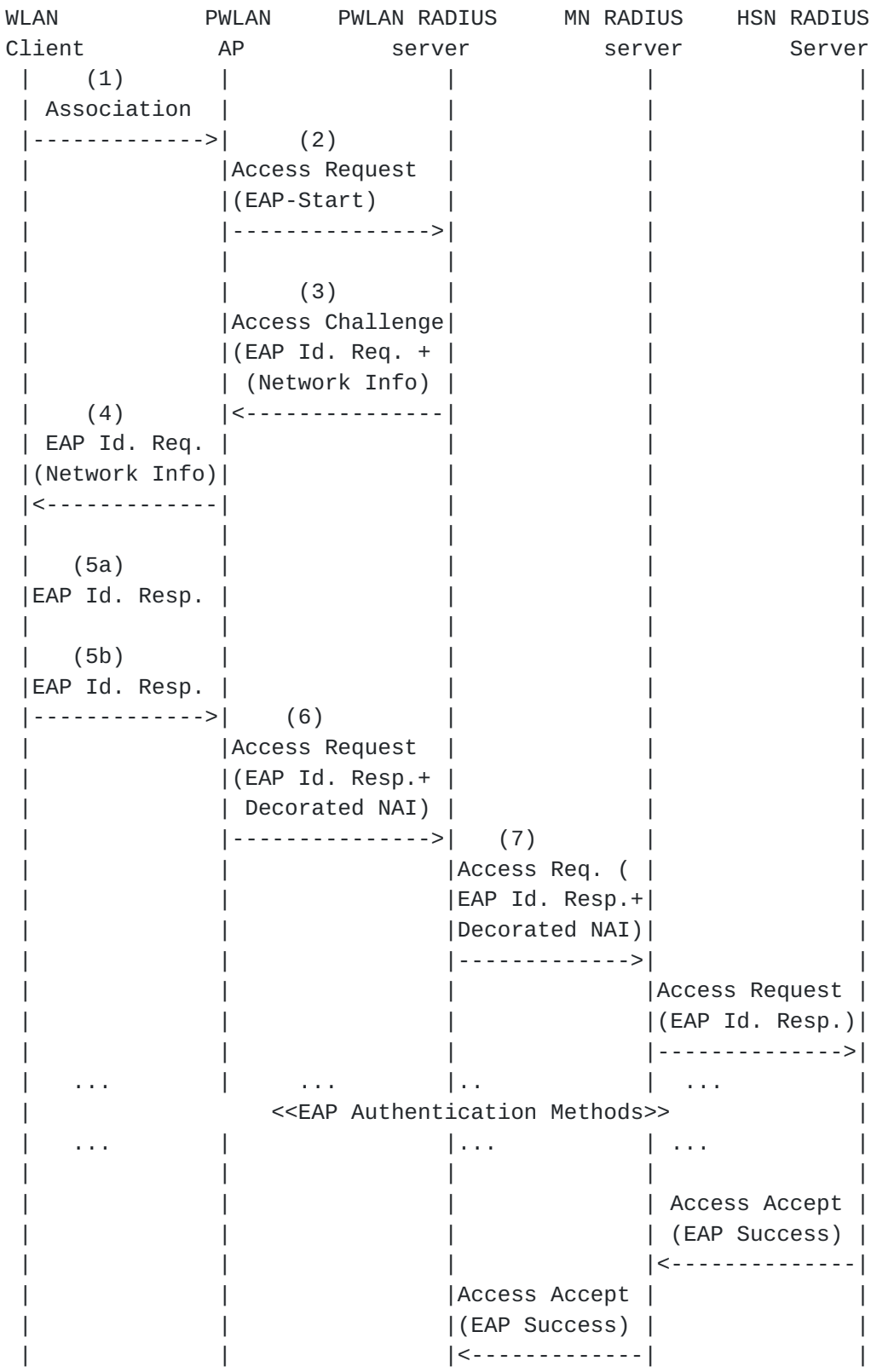
[Option 2] Use the initial EAP-Identity Request issued by the PWLAN RADIUS server

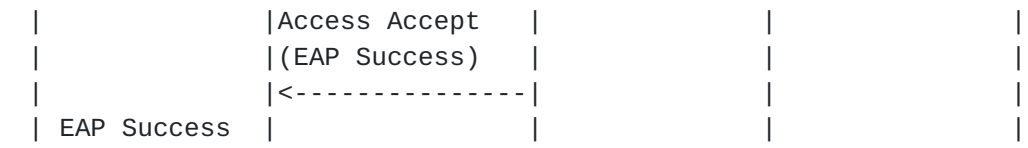
This is similar to Option 1, but the initial EAP-Identity Request is issued by the PWLAN RADIUS Server instead. Once a WLAN client associates with a PWLAN AP using native IEEE 802.11 procedures, the AP sends an EAP-Start message within a RADIUS Access-Request as defined in [4] to trigger an EAP conversation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

The message flow below illustrates conversations between an

authenticating peer, AP, PWLAN AN RADIUS server, MN RADIUS server, and HSN RADIUS server. Where the AP sends an EAP-

Request/Identity containing Network Information as the initial packet, the exchange appears as follows:




|Access Accept |
|(EAP Success) |
|<----------------|
| EAP Success |

The following describes each message flow in details.

(1) The WLAN client associates with the PWLAN AP.

(2) An EAP-Start message encapsulated within a RADIUS Access-Request sent to the PWLAN AN RADIUS server.

(3) The PWLAN RADIUS server processes the received Access-Request message and initiates an EAP conversation by sending an EAP-Identity Request encapsulated within a RADIUS Access-Challenge.

(4) The PWLAN AP extracts the EAP-Identity Request from the received Access-Challenge and sends it to the WLAN client.

(5a) The WLAN client sends an EAP-Identity Response containing a Decorated NAI indicating the selected MN to the PWLAN AP. OR,

(5b) The WLAN client sends an EAP-Identity Response containing a normal NAI [5][10] to the PWLAN AP.

(6) The PWLAN AP sends a RADIUS Access-Request packet containing the EAP Response (as defined in [4]) to the PWLAN RADIUS server.

(7) The PWLAN AN RADIUS server processes the received Access-Request packet and forwards it to the appropriate MN RADIUS server.

(8) The EAP Authentication continues as described in [4].

The following summarizes pros and cons of this option.

Pros:

- o It does not introduce additional EAP messages
- o It does not require any modifications to APs to include support for administrating and delivering Network Information.

Cons:

- o It may not be backwards compatible if currently deployed APs in PWLAN ANs do not support EAP-Start.
- o It MAY require modification to the PWLAN RADIUS server for processing a Decorated NAI (many RADIUS servers already have this capability).

- It MAY introduce a contention problem if space in the Type-Data field has already been used up for other purposes.

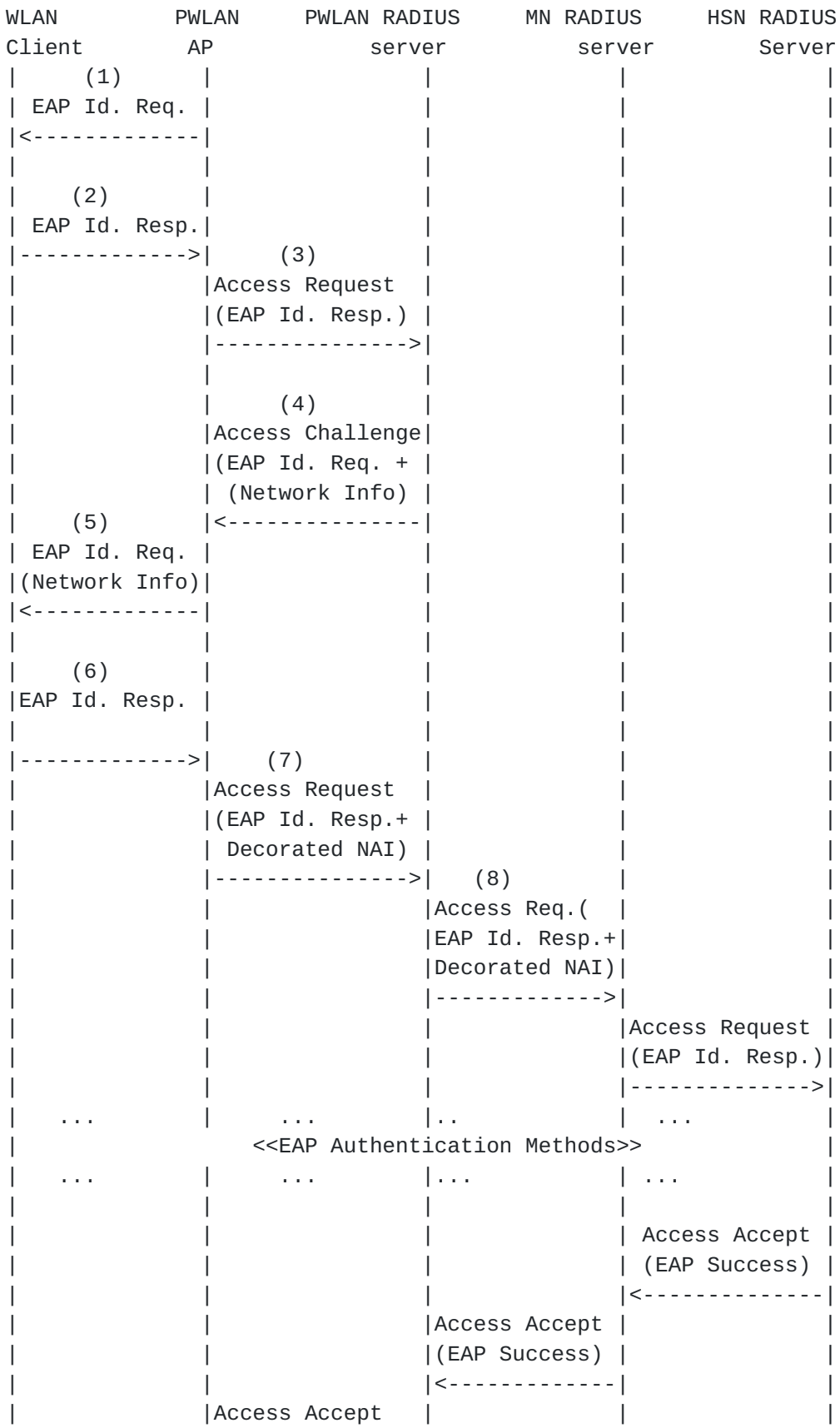
[Option 3] û Use a subsequent EAP-Identity Request issued by the PWLAN RADIUS server

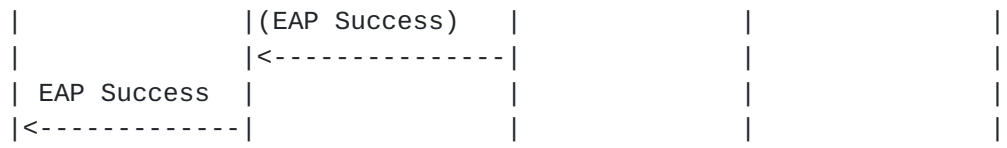
Network Information is delivered to a WLAN Client in a subsequent EAP-Identity request after the initial EAP-Identity Request/Response exchange.

Upon receipt of a RADIUS Access-Request packet containing the initial EAP-Identity Response, the PWLAN RADIUS server MAY send an EAP-Identity Request containing Network Information to the WLAN client if the Response does not already contain a Decorated NAI which specifies an MN recognized by the PWLAN AN as the next hop for routing the RADIUS packet.

When a RADIUS Access-Request containing a subsequent EAP-Identity Response is received, if the User-Name attribute contains a normal NAI [5][10] then the PWLAN server MUST route the RADIUS packet based on its local routing policy as usual.

The protocol message flow below illustrates conversations between an authenticating peer, AP, PWLAN RADIUS server, MN RADIUS server, and HSN RADIUS server. Where the AP sends an EAP-Request/Identity containing Network Information as the initial packet, the exchange appears as follows:


WLAN Client
PWLAN AP
PWLAN RADIUS server
MN RADIUS server
HSN RADIUS Server
(1)
EAP Id. Req.
(2)
EAP Id. Resp.
(3)
Access Request
(EAP Id. Resp.)
(4)
Access Challenge
(EAP Id. Req. +
(Network Info)
(5)
EAP Id. Req.
(Network Info)
(6)
EAP Id. Resp.
(7)
Access Request
(EAP Id. Resp.+
Decorated NAI)
(8)
Access Req.(
EAP Id. Resp.+
Decorated NAI)
Access Request
(EAP Id. Resp.)
...
<<EAP Authentication Methods>>
Access Accept
(EAP Success)
Access Accept
(EAP Success)
Access Accept


|(EAP Success)
EAP Success

The following describes each message flow in details.

(1) The PWLAN AP issues an EAP-Identity Request to a WLAN Client

(2) The WLAN Client replies with an EAP-Identity Response containing a normal NAI, or perhaps a Decorated NAI based on the Network Information cached from the most recent authentication session to the PWLAN AN.

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

(4) The PWLAN RADIUS server sends a RADIUS Access-Challenge packet encapsulating an EAP-Identity Request containing Network Information. Or, the step 8 is executed if the Response does already contain a Decorated NAI which specifies an MN recognized by the PWLAN.

(5) The PWLAN AP forwards the EAP-Identity Request containing the network information to the WLAN Client.

(6) The WLAN Client replies with an EAP-Identity Response containing a Decorated NAI indicating the preferred MN.

(7) The AP forwards the EAP-Identity Response to the PWLAN RADIUS server over RADIUS protocol.

(8) The PWLAN RADIUS server processes the received Access-Request message containing a normal or a Decorated NAI and forwards it to the appropriate MN RADIUS server.

(9) The EAP Authentication continues as described in [4].

The following summarizes pros and cons of this option.

Pros:

- It does not require any modifications to existing APs
- It uses a dedicated EAP-Identity Request for delivering Network Information and hence no contention problem for using the space in the Type-Data field.

Cons:

- It introduces an extra EAP-Identity Request/Response pair
- It requires software upgrades to the PWLAN RADIUS server

In the above options, if the HSN RADIUS server uses an updated User-Name attribute, for example, in RADIUS Access-Challenge and

Access-Accept packets, then this SHOULD be used in subsequent RADIUS message flows between AP and Home RADIUS Server.

In order for a WLAN client software implementation to work with all options transparently, the implementation MUST not expect the arrival of Network Information on a particular EAP-Identity Request (i.e., the initial or a subsequent Request). PWLAN AN operators therefore MAY choose to deploy any of the above delivery mechanism options in their network without risking the interoperability. However, this document recommends deploying delivery mechanism options 2 and 3 as they are backward-compatible with the currently deployed APs.

2.2 Data Model / Syntax

Network Information needs to be structured in a general format and syntax so that the WLAN 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.

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 following an optional prefix and values according to the following ABNF [7].

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

network-info = item ["," item ]
item = attribute "=" value

attribute = [prefix] 1*( ALPHA / "-" / "_" / DIGIT)
prefix = 1* alphanum ö:ö

value = 1*( 0x01-2B / 0x2D-FF ) ; any non-null UTF-8 char except
","
```

The intent of prefixes is to define a namespace to avoid collision where private attribute names (i.e., not registered with IANA) are used. Either Attribute names or their prefixes MUST be registered with IANA [8]. The content of an attribute MUST NOT contain a comma (ö,ö). The exact format and semantics of the content of an attribute MUST be specified in the definition of the attribute. Examples of prefixed and non-prefixed attribute names are: 3GPP:HotSpotInfo, NAIRealms.

2.3 NAI Decoration

The WLAN client using EAP specifies the preferred MN for routing AAA packets by decorating the NAI that would use a mediating realm, instead of the WLAN clientÆs home realm, in the EAP-Identity Response. The NAI decoration is a representation of a NAI in accordance to the guidelines specified in [5][10] for routing AAA transactions to the userÆs home realm when the home realm is only reachable via another mediating realm. For example, given a userÆs NAI öuser@homerealmö, the NAI can be represented as öhomerealm!user@mediating-netö.

3. Attribute Definitions

This section lists definitions of 1 or more EAP Network Information attribute(s).

3.1 NAIRealms

It defines a Network Information attribute for specifying a list of NAI realms corresponding to MNs that are recognized by the PWLAN AN.

Attribute name: öNAIRealmsö

Attribute value:

NAIRealms-value = Realm [ö;ö Realm]

```
Realm = *( domainlabel "." ) toplabel
domainlabel    =  alphanum *( alphanum / "-" )
toplabel         =  ALPHA *alphanum
```

The öNAIRealmsö attribute lists MN names that are recognized by the PWLAN AN.

An example öNAIRealmsö attribute is shown below:

NAIRealms=ipass.com;mnc123.mcc334.3gppnetwork.org

4. IANA Considerations

This section provides guidance to the Internet Assigned Numbers Authority (IANA) regarding registration of a new namespace for the EAP Network Information attributes or prefixes, in accordance with [7]. The initial attribute(s) are listed in Section 3. New

attributes or prefixes are assigned using the First Come Fist Served policy defined in [8].

Requests for new attribute names MUST be accompanied by a reference to a publicly available description of the attribute value syntax and semantics.

5. Security Considerations

Network Information delivered inside an EAP-Identity Request is considered as a hint in guiding the WLAN Client to select the desired MN. It SHOULD be treated similarly to the SSID in beacon broadcast: subject to modification and spoofing.

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

6. Contributors

This document is a joint work of the contributing authors (in alphabetical order):

- Farid Adrangi (Intel)
- Farooq Bari (AT&T Wireless)
- Adrian Buckley (Rim)
- Blair Bullock (iPass)
- Pasi Eronen (Nokia)
- Mark Grayson (Cisco)
- Victor Lortz (Intel)
- Jose Puthenkulam (Intel)
- Joe Salowey (Cisco)
- Marco Spini (Telecom Italia)
- Mark Watson (Nortel)
- Johanna Wild (Motorola)

7. Acknowledgements

The authors would like to thank Bernard Aboba (of Microsoft), and Jari Arkko (of Ericsson), Jesse Walker (of Intel), Prakash Iyer (of Intel), Dj Johnston (of Intel), Serge Manning (of Sprint), Ed Van Horne (of Cisco), Antonio Ascolese (of Telecom Italia), Simone Ruffino (Telecom Italia), Luca Dell'uomo (of Telecom Italia), Luciana Costa (of Telecom Italia), Basavaraj Patil (of Nokia) for their feedback and guidance.

8. References

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

June 2000.

[2] Calhoun, P., "Diameter Base Protocol",
draft-ietf-aaa-diameter-17 (work in progress), January 2003.

[3] Blunk, L. and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[4] Aboba, B. and P. Calhoun, "RADIUS Support for Extensible Authentication Protocol (EAP)", Internet draft (work in progress), RFC 3579, September 2003.

[5] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC

2486, January 1999.

[6] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

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

[8] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[9] Blunk, L., "Extensible Authentication Protocol (EAP)", draft-ietf-eap-rfc2284bis-04 (work in progress), June 2003.

[10] Arkko, Jari, "The Network Access Identifier", RFC

2486bis,
Feburary 2004.

Authors Æ Addresses

Farid Adrangi

Intel Corporation
Email: farid.adrangi@intel.com
Phone:+1 503-712-1791

Full Copyright Statement

Acknowledgement

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