



EAP  
Internet-Draft  
Expires: January 10, 2005

W. Groeting  
S. Berg  
M. Ness  
H. Tschofenig  
Siemens AG  
July 12, 2004

Network Selection Implementation Results  
draft-groeting-eap-netselection-results-00

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/lid-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 January 10, 2005.

Copyright Notice

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

Abstract

This document aims to highlight implementation results on network discovery as well as some new ideas for its extension. The implementation is based on the draft on mediating network discovery, a mechanism that enables a mobile node to discover roaming partners of an access network via EAP. The concept allows automatic network selection of end hosts, based on additional parameters, hence reducing interacting with the user. This document should also open a

Internet-Draft

Network Selection Implementation Results

July 2004

discussion on the need on network capability mechanisms.

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction . . . . .</a>	<a href="#">3</a>
<a href="#">1.1</a>	<a href="#">Terminology . . . . .</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Concept Aspects . . . . .</a>	<a href="#">5</a>
<a href="#">2.1</a>	<a href="#">Why has EAP been proposed to exchange this type of information . . . . .</a>	<a href="#">5</a>
<a href="#">2.2</a>	<a href="#">Information from the Access Network . . . . .</a>	<a href="#">6</a>
<a href="#">2.2.1</a>	<a href="#">Roaming Agreements . . . . .</a>	<a href="#">6</a>
<a href="#">2.2.2</a>	<a href="#">Cost of network resource usage . . . . .</a>	<a href="#">7</a>
<a href="#">2.2.3</a>	<a href="#">Quality of Services . . . . .</a>	<a href="#">7</a>
<a href="#">2.2.4</a>	<a href="#">Authorisation Information . . . . .</a>	<a href="#">7</a>
<a href="#">2.2.5</a>	<a href="#">Privacy Policy . . . . .</a>	<a href="#">8</a>
<a href="#">2.2.6</a>	<a href="#">Middlebox Devices . . . . .</a>	<a href="#">8</a>
<a href="#">3.</a>	<a href="#">Implementation Aspects and Test Environment . . . . .</a>	<a href="#">9</a>
<a href="#">3.1</a>	<a href="#">Design of Information transmitted . . . . .</a>	<a href="#">10</a>
<a href="#">3.2</a>	<a href="#">Implementation at the AAA-Server . . . . .</a>	<a href="#">11</a>
<a href="#">3.3</a>	<a href="#">Implementation at the Supplicant . . . . .</a>	<a href="#">13</a>
<a href="#">3.4</a>	<a href="#">Test Platform . . . . .</a>	<a href="#">14</a>
<a href="#">3.4.1</a>	<a href="#">FreeRADIUS . . . . .</a>	<a href="#">14</a>
<a href="#">3.4.2</a>	<a href="#">Xsupplicant . . . . .</a>	<a href="#">15</a>
<a href="#">3.4.3</a>	<a href="#">Challenges . . . . .</a>	<a href="#">15</a>
<a href="#">4.</a>	<a href="#">Security Considerations . . . . .</a>	<a href="#">16</a>
<a href="#">5.</a>	<a href="#">Conclusion . . . . .</a>	<a href="#">20</a>
<a href="#">6.</a>	<a href="#">Acknowledgement . . . . .</a>	<a href="#">21</a>
<a href="#">7.</a>	<a href="#">References . . . . .</a>	<a href="#">22</a>
<a href="#">7.1</a>	<a href="#">Normative References . . . . .</a>	<a href="#">22</a>
<a href="#">7.2</a>	<a href="#">Informative References . . . . .</a>	<a href="#">22</a>
	<a href="#">Authors' Addresses . . . . .</a>	<a href="#">24</a>
<a href="#">A.</a>	<a href="#">Cost Attribute . . . . .</a>	<a href="#">25</a>
<a href="#">A.1</a>	<a href="#">Cost-Header Attribute . . . . .</a>	<a href="#">25</a>
<a href="#">A.2</a>	<a href="#">Cost-Unit SubAttribute . . . . .</a>	<a href="#">26</a>
<a href="#">A.3</a>	<a href="#">Example . . . . .</a>	<a href="#">27</a>
<a href="#">B.</a>	<a href="#">QoS Attribute . . . . .</a>	<a href="#">29</a>
<a href="#">B.1</a>	<a href="#">UMTS QoS-Classes . . . . .</a>	<a href="#">29</a>
<a href="#">B.2</a>	<a href="#">QoS-Header Attribute . . . . .</a>	<a href="#">29</a>
<a href="#">B.3</a>	<a href="#">Example . . . . .</a>	<a href="#">30</a>
	<a href="#">Intellectual Property and Copyright Statements . . . . .</a>	<a href="#">31</a>

## 1. Introduction

Wireless LANs (WLAN) are receiving more attention as a complementary technology to 3G and there is an ever increasing number of hotspot deployments in areas such as airports and hotels. Currently, these hotspots are managed by Wireless ISP (WISP) operators that do not have an existing cellular subscriber base. Soon, WISP will provide WLAN access to a multiple number of mobile network providers.

To support the selection of a Roaming enabled WISP, the mechanism for mediating network discovery, as described in [[I-D.adrangi-eap-network-discovery](#)], can be used. This document highlights some implementation aspects of this draft and discusses some extensions to it. These parameters could be, e.g., cost and quality of service information. These parameters allow the end host to make a more intelligent network selection decision.

The objectives of the draft are to show the need for and the advantages of network discovery. It is primarily intended to trigger a discussion on a scalable network discovery mechanism, which will support end hosts regarding appropriate network selection.

As the discussion has already been started within different organizations like 3GPP and IEEE, a discussion on the information transmitted as well as the mechanism itself needs to take place. The authors would like to forward the discussion within the IETF by presenting some implementation findings and some ideas on not yet solved open issues.

The draft is based on results of an implementation that covers one of the three options for mediating network discovery. Next to the mediating networks additional parameters have been defined and encoded as described within this document.

This document is structured as follows. [Section 2](#) covers the conceptual aspects and considered network information elements, followed by the implementation results in [section 3](#). [Section 4](#) covers the security considerations and finally a conclusion is given in [section 5](#). In the annex, some additional information on pricing and QoS issues is given.

## [1.1](#) Terminology

authenticator

The end of the link initiating EAP authentication. The term authenticator is used in [[IEEE-802.1X](#)], and has the same meaning in this document.

Groeting, et al.

Expires January 10, 2005

[Page 3]

---

Internet-Draft

Network Selection Implementation Results

July 2004

peer

The end of the link that responds to the authenticator. In [[IEEE-802.1X](#)], this end is known as the Supplicant.

Supplicant

The end of the link that responds to the authenticator in [[IEEE-802.1X](#)]. In this document, this end of the link is called the peer.

backend authentication server

A backend authentication server is an entity that provides an authentication service to an authenticator. When used, this server typically executes EAP methods for the authenticator. This terminology is also used in [[IEEE-802.1X](#)].

AAA

Authentication, Authorization, and Accounting. AAA protocols with EAP support include RADIUS and Diameter.

## 2. Concept Aspects

As the number of IEEE 802.11 wireless access networks proliferates, the support of roaming functionalities and thus the efficient exchange of mediating network information becomes more and more important [[I-D.adrangi-eap-network-discovery](#)]. Local WISPs are interested in offering their access points to a large number of users from other providers, and at the same time mobile operators are anxious to integrate WLAN access even through intermediary networks into their packet switched system.

To support more intelligent end host decisions, it seems to be beneficial to discover certain characteristics about the network up front during the association and authentication phase. Such information could include authentication models, roaming information, quality of service (see [Appendix B](#)) and cost parameters (see [Appendix A](#)).

### 2.1 Why has EAP been proposed to exchange this type of information

The IETF draft by Adrangi et al. [[I-D.adrangi-eap-network-discovery](#)] proposes a solution to transport mediating network information within the EAP protocol and thus enables 3GPP/WLAN interworking and roaming.

EAP is a generic container protocol that can - in theory - carry any information desired by the network (as long as both sides of the information exchange understand the information that they are receiving). It is an obvious choice for Layer 2 information exchange about network capabilities since it is highly likely that EAP will be implemented in both, the end host and the network. However, when EAP is used in this fashion (i.e., beyond its original intention) it is important to note that there are possible impacts on security, scalability and the EAP state machine.

One idea is to extend this mechanism to include extra data within Identity-Messages, e.g., requiring a certain bit rate or a certain quality of service. If information can be carried in identity messages, then the end host can make further decisions based on it, before the full authentication procedure has been completed (and hence probably before accounting has started). This is particularly useful for the case of cost and service availability information.

However, it needs to be taken into account that an EAP identity message, including any information carried within, is not protected. In addition, if the amount of exchanged information is too large then performance characteristics of EAP as an information transport protocol will become a limitation.

## [2.2](#) Information from the Access Network

The end host can retrieve information about the access network dynamically when it moves into coverage of that network. This information is retrieved via a link layer network capability discovery mechanism. Each piece of information may or may not have an effect on whether or not the end host attaches to and authenticates with that network.

As already proposed in [[I-D.adrangi-eap-network-discovery](#)] the discovery of roaming agreements and mediating networks is a valuable access network information. This can be extended by other access network information elements like costs and charging, quality of

service, authorization information, privacy policy and middlebox devices, which help the end host to make his attachment decision.

The information required within multimode end hosts to support efficient interface selection and network capability discovery algorithms are classified according their importance. Mandatory indicates that this should be included in near term implementations of the algorithms, optional indicates that the availability of this information improves the quality of the algorithm decisions, but is not vital to its operation.

The time of information discovery is classified related to the moment of association, i.e. the establishment of medium access control (MAC) transport services between access point/station (AP/STA), and authentication, the service used to establish the identity of one station as a member of the set of stations authorized to associate with another station [[IEEE-SPEC-99](#)].

The expected lifetime of the information, i.e. how frequently this information is updated and how persistent the information is within the end host, is characterized by the following categories:

Duration of session: the information is only valid for the lifetime of the session of an application with which it is associated

Duration of attach: the information is only valid for the lifetime of the interface attachment to that AN.

Inter-attach: the information is stored between attachments to an AN, but will timeout after some defined period.

### [2.2.1](#) Roaming Agreements

This information specifies what roaming agreements are in place in the network. It allows the mobile node to determine whether it can authenticate with the network, and which subscription credentials to

use.

Importance: Mandatory for authentication purpose

When discovered: Pre-authentication

How dynamic: Inter-attach

### [2.2.2](#) Cost of network resource usage

This information provides hints to the user device about the cost of using this network. It is useful to support mobile nodes that base network selection services on more complex policies based on user preferences, such as always use the cheapest. The cost information provided by the access network can be manifold. It includes information on the access network itself, cost information of roaming partners, different charging modes (per data, per time, per service, flat) and other information like the amount, currency, number of units, etc. The definition of an appropriate data format is subject of further investigation

Importance: Optional

When discovered: Preferably pre-authentication

How dynamic: Inter-attach

### [2.2.3](#) Quality of Services

Each network may support different levels of quality of service (e.g. there are four QoS classes in 3GPP) that can support different data rates. The multimode end host may be required to make decisions about whether or not to attach to a network based on what QoS can offer.

Importance: Optional, this is a useful hint, especially for handover scenarios

When discovered: Pre-authentication

How dynamic: Inter-attach

### [2.2.4](#) Authorisation Information

The AN will receive information from the home network about what the user is authorized to access and for how long. If this information can be transferred to the MT then it can be used to make informed decisions e.g. about interface selection - there is no point choosing to use an interface if it is about to become idle because the time for which it is authorized is nearly finished. It would also be useful for feedback to the user. As this information might belong to a particular user, it needs further investigation on how to secure such kind of information. A plain authorization information advertisement seems rather difficult to realize.

Importance: Optional  
When discovered: Pre-authentication  
How dynamic: Duration of Session

The functionality required to obtain this information is quite complex and does not yet exist so this information is considered to be optional at the moment.

#### [2.2.5](#) Privacy Policy

Access networks have the ability to monitor the users behaviors with regard to their application layer usage (e.g., HTTP or SIP) and to create user specific profiles. Many network access authentication protocols allow networks to learn the user identity since authentication and key exchange protocols which support user identity confidentiality are rarely used. The increasing deployment of location based services creates an additional privacy threat for end users. Similarly to the privacy initiatives in the web environment additional information about the privacy policy of an access network can be communicated. Such indication might reveal an end user that a particular network does not distribute location information to the user's home network during network access authentication, location information is not provided to third parties other than the network or that no application specific information is provided to third parties.

Importance: Optional  
When discovered: Pre-authentication  
How dynamic: Duration of attach

#### [2.2.6](#) Middlebox Devices

There are several types of applications that do not operate well if there is a NAT or firewall between communicating hosts/servers. Some examples of such applications are games, VoIP applications, H323/SIP, some instant message applications, and quality of service signaling protocols such as RSVP.

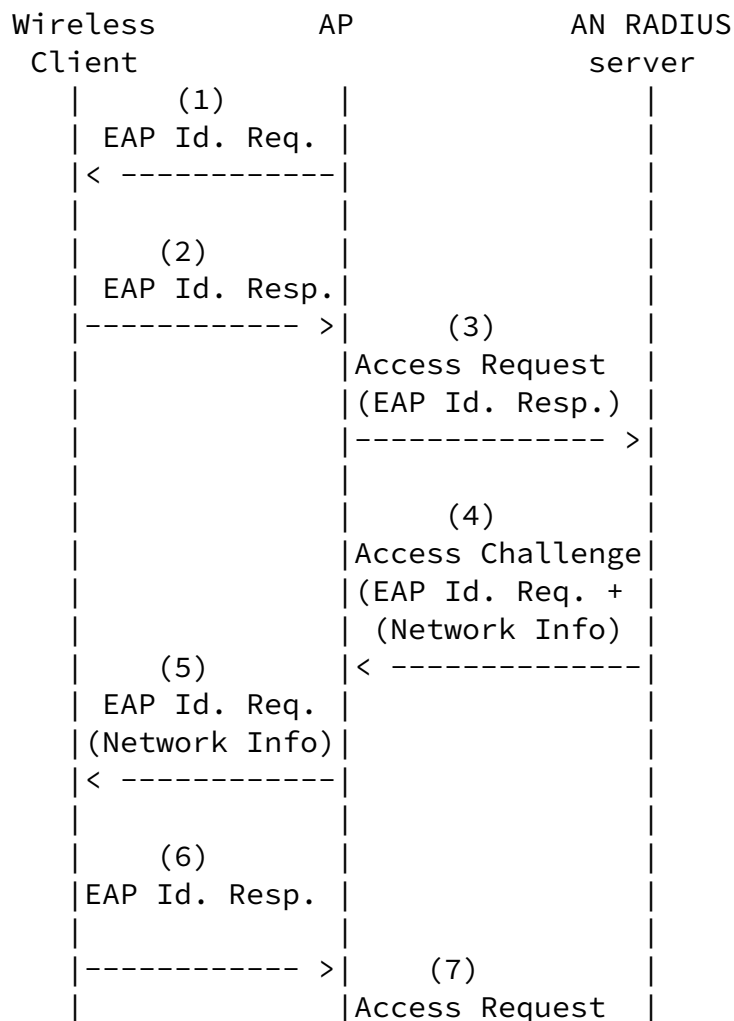
Consequently, the end host may need to know whether there are any middlebox devices, e.g. firewalls and NATs present in the AN in case the user wants to use applications that have a problem with them. A network without a middlebox device would be preferable.

Importance: Optional  
When discovered: Pre-authentication  
How dynamic: Duration of attach

### 3. Implementation Aspects and Test Environment

In Section 3 of [[I-D.adrangi-eap-network-discovery](#)] three options for delivering mediating network information with EAP are proposed. Each of these options uses a Identity-Request to submit this information. Only option 3 can be implemented without any modification of the AP and with every AP which is IEEE 802.1x enabled. Option 3 uses only the AAA server to transmit information to the end host (i.e., supplicant) rather than a modified access point. Hence, the authors think that this approach works for most existing systems. Lower effort and costs of implementation and better backwards compatibility are the reasons to favor this option for an implementation.

Figure 1 demonstrates the information exchange between supplicant, AP and AAA server when implementing the preferred solution:



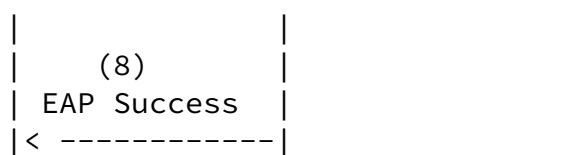
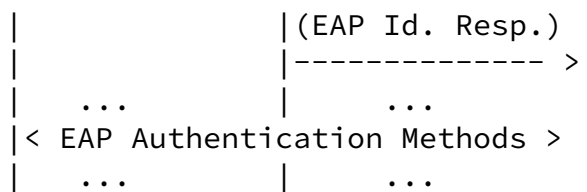


Figure 1: Option 3: Use a subsequent EAP-Identity Request issued by the access network RADIUS server

Based on this model the following subchapters explain the implementation in a working test environment.

### [3.1](#) Design of Information transmitted

Beneath the definition of a Netinfo-Packet, which offers the possibility to check if the Data field in an EAP packet is used for network information, the syntax for the network information has to be defined, too.

In [[I-D.adrangi-eap-network-discovery](#)] the following syntax is proposed: network-info = attribute "=" value. for just transmitting the names of the mediating networks, this syntax is useful. When offering e.g. six attributes about three mediating networks there occurs a problem with the space available in the EAP packet. A solution to that problem is to send the network information in a defined order, seperated with a defined delimiter. Figure 2 is a possible way to transmit information about: the name of the mediating network, the cost of the mediating network, roaming agreements, quality of service , middlebox information and authorisation information (in this exemplary for three mediating networks):

MN1	MN2	MN3
C1	C2	C3
RA1	RA2	RA3
QS1	QS2	QS3
MI1	MI2	MI3
AI1	AI2	AI3
PP1	PP2	PP3

MN: Mediating Network

C: Cost

RA: Roaming Agreements

QS: Quality of Service

MI: Middlebox Information

AI: Authorisation Information

PP: Privacy Policy

Figure 2: Matrix for Network Information

Converted into a string this data looks like (used "," as delimiter between attributes and ";" as delimiter between values):

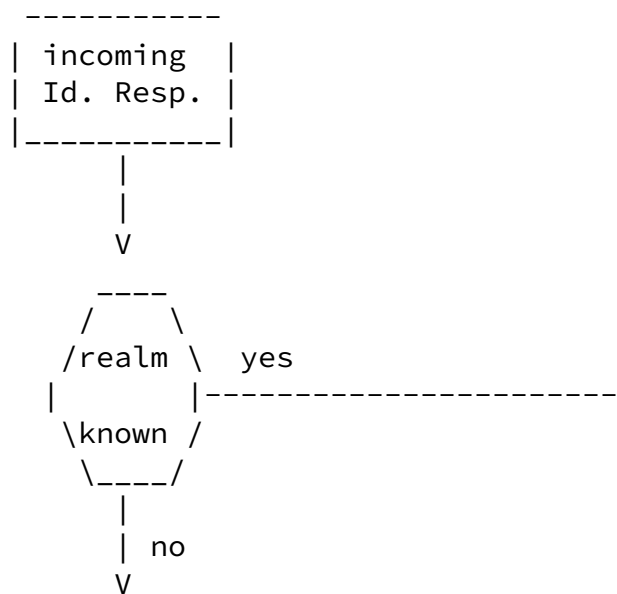
```
network-information=MN1;MN2;MN3,Cost1;Cost2;Cost3,  
RA1;RA2;RA3,QS1;QS2;QS3,MI1;MI2;MI3,AI1;AI2;AI3,PP1;PP2;PP3
```

Beneath the benefit of saving valuable space in the EAP packet this syntax has one disadvantage: to interpret the data on supplicant side correct, from all mediating networks all parameters have to be transmitted. If none of the mediating networks offers a specific parameter, this parameter has to be transmitted as a NULL.

### [3.2](#) Implementation at the AAA-Server

In an authentication process the AAA-Server normally receives an Access Request/Identity-Response which is sent by the supplicant and passed through by AP. As response to this message the AAA-Server has

to react with an Access Challenge including the start sequence for the chosen EAP authentication method. At this point we have to intervene and query which packet to send now. Figure 3 shows the possible decisions:



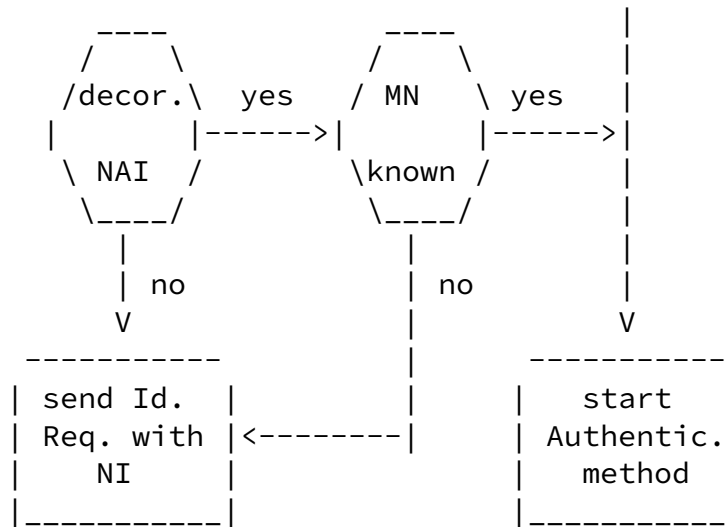


Figure 3: Decision on incoming Identity-Response

There are three queries to be done for knowing, how to react on an incoming Identity-Response:

- o Check if the realm submitted with the username is known
- o Check if the username includes a decorated-nai
- o Check if the mediating network submitted with the decorated-nai is known

If any of this queries can be answered with "yes" the normal authentication process can be started. Otherwise an Access Challenge including an EAP Identity-Request which submits mediating network information has to be sent [[I-D.adrangi-eap-network-discovery](#)].

One thing missing in this behaviour model is the reaction on an Identity-Response which arrives the second time - without having changed anything in username attribute. For this reason a counter has to be inserted into FreeRADIUS-code which makes it possible to check for packets who are arriving more than one time. As proposed in [[I-D.adrangi-eap-network-discovery](#)] the AAA-Server has to handle these packets based on the local routing policy. In fact the AAA-Server SHOULD discard these packets and send an EAP Failure packet which stops the authentication process.

This proceeding modifies the AAA-Server that way, that he is still able to handle authentication request from unmodified supplicants (they only have send a valid realm or mediating network). Also supplicants which send an Identity-Response including a valid decorated-nai directly, do not have to receive an additional Identity-Request because they already chose the mediating network.

### 3.3 Implementation at the Supplicant

At supplicant side there is also one point where it makes most sense to implement a query when to send a decorated-nai. This is on every incoming Identity-Request. For example all incoming Identity-Requests could be checked for their size, and then be interpreted or not.

Next step is to validate the data which received. Therefore header information which came with the possible network information should be interpreted. Figure 4 shows the possible design of a Netinfo-Packet:

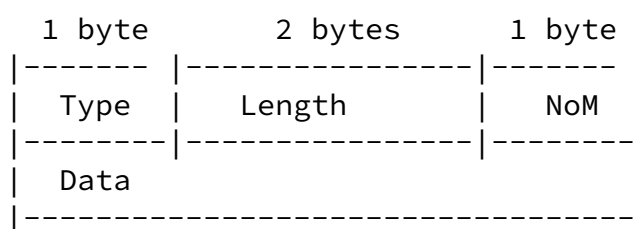


Figure 4: Design of a Netinfo-Packet

- o "Type" is a 1 byte long field which defines of which version the network information are (e.g.: Type 1 could only include information about the names of the mediating networks. Whereas Type 2 includes informations like e.g. costs, too).

- o "Length" is 2 bytes long and contains the length of the string included in the Data-field
- o "NoM" is also 1 byte long and defines the number of mediating networks, which are transmitted with that packet.
- o "Data" contains a string with the network information

After the correctness of the network information is confirmed, the data can be processed. Which data is exactly interpreted depends on

the preferences the user made, e.g. the setting "Always cheapest connected" may only interpret "cost" and leave the rest unregarded.

Of importance is only, that the algorithmus comes to a decision if to proceed authenticating to the access network and which mediating network to choose.

If it decides not to continue with authenticating process, the supplicant SHOULD send an EAP logoff packet. Else an Identity-Response has to be sent, which includes a decorated-nai as username. Part of this decorated-nai is the chosen mediating network.

### 3.4 Test Platform

To ensure that this approach described before is not only of theoretic nature it was necessary to build up a test system. This test platform consists of an AAA-Server, an AP and a supplicant. The following two subchapters give some hints on the installation, configuration and modification of these three network components.

The aim of this implementation was not to develop a product ready for market, but to point out that it is possible to realize the proposal suggested by Adrangi and in this draft. Hence the way for implementing was not to completly new develop all software, but to find the shortest way for realization. This recommends to use existing software, which is published under the GPL and therefore can be modified.

#### 3.4.1 FreeRADIUS

FreeRADIUS is an AAA-Server which was former developed as Cistron RADIUS server and is now the leading AAA-Server developed for Linux under the GPL. The sources are available for download at <http://www.freeradius.org/>.

FreeRADIUS has a module for EAP authentication. The sources for this module can be found in the directory src/modules/rlm\_eap/. All necessary modifications to FreeRADIUS has to be done in this directory.

#### 3.4.2 Xsupplicant

There are not many IEEE 802.1x implementations available for Linux right now. Xsupplicant seems to be the most popular at the moment. Xsupplicant is available for download at <http://www.open1x.org/>. It is also developed under GPL. Xsupplicant is not a full RADIUS-client, it is only ready for EAP authentication.

### 3.4.3 Challenges

While implementing one problem occurred: the second Identity-Response from Supplicant (which is the one with the Decorated-NAI inside) does not arrive at the AAA-Server. Because the packet leaves the Supplicant and cannot be discovered at the AAA-Server at all, the packet seems to get lost at the AP.

Analysis on the AP (via Telnet a lot of debugging on the AP is possible) resulted, that the Identity value of the Identity-Response is not the one expected by the AP. It looks like the AP does not store the Identity of the Identity-Request sent by the AAA-Server. When the Identity-Response to that request arrives at the AP the reaction is right: the message is blocked.

The solution is to prevent the AAA-Server from increasing the Identity value in the EAP packet, when sending the second Identity-Request. Hence it is sent with the same Identity like the original Identity-Request and the AP lets the Identity-Response to that packet pass.

#### 4. Security Considerations

[I-D.ietf-eap-netsel-problem] tries to classify the problem space of network selection:

Access Network discovery:

Access Network discovery is concerned about the selection of a particular network (if multiple access networks are available) based on a number of parameters. This section mainly focuses on the security implication of this particular aspect.

Identifier selection:

Identifier selection plays a role when an end user has more than one identifier to select from. The selected identifier might impact the selected roaming partner of the attached network and thus might have cost and performance implications. In some sense this is a policy-based routing mechanism with interesting impacts on the traditional Internet pricing where the edge pricing between neighboring networks was exercised. In more sophisticated scenarios one might imagine that IP packets are routed by the access network through different ISPs depending on some classifiers in the packet (such as DiffServ codepoints or particular destination IP addresses). The security properties are not well understood for these scenarios. As an example, one might consider a moving network which has to change its roaming partners over time based on mobility. How should the end host be notified about the possible implication on the cost? Should the user be re-authorized? How should the user be certain that such a provider change was actually necessary?

AAA routing:

After selecting a particular identifier, the NAI is used to route the AAA messages back to the home network (possibly via some intermediate brokers). No dynamic routing protocols are available for AAA routing and the selection of a particular route might have impacts on the price. This issue is mostly outside the scope of this document.

Payload routing:

As part of the authorization information provided by the home AAA server the routing and treatment of packets might be affected. The payload route binding problem refers to mismatch between the

routing of IP packet and the hinted (or offered) route. It needs to be studied whether this is truly a problem. This issue is

outside the scope of this document.

There is a risk that a large number of service providers with complex roaming agreements create a non-transparent service and cost-structure. In a traditional subscription-based scenario users are registered with their home networks and use this trust relationship to dynamically establish a financial settlement between the home and the visited network and required security associations (for example to provide link layer security between the end host and an entity in the visited network such as the access point). This is the typical AAA deployment scenario. In such a scenarios users do not learn the identity of the access network as part of a regular authentication and key exchange protocol message exchange. The usage of EAP the Extensible Authentication Protocol in IEEE 802.1x/IEEE 802.11i or also PANA never aimed to allow authentication of the access network to the end host. As such, the identity of the access network is not revealed (in a secure fashion). The user is therefore only authenticated to the home network (and hopefully vice versa). This design decision is also reflected in the choice of identifier space used in the WLAN IEEE 802.11 environment. The Service Set Identifier (SSID) does not mandate a structure and hence is not really suitable as an identifier to perform authentication and authorization. Overloading the SSID as an identifier to indicate particular services is attractive, but fails in most cases. In fact, most administrators of WLANs do not change the default SSID (see for example [\[Pri04\]](#) for a study about WLAN usage in London where approximately 40% of the access points are running their default SSID.) Such an approach makes the phone book (see [\[RFC3017\]](#)) approach (as an out-of-band mechanism to associate a particular service to an identifier) difficult to deploy. The approach of assisting with the selection of the appropriate certificate based on a list of SSIDs as described in [\[RFC3770\]](#) will also fail. Apart from this fact, the authentication and authorization message exchange between the end host and the home network is, for the subscription-based environment, required. Public key based authentication between the end host and the access network cannot replace the exchange between the end host and the home network due to the need for a financial compensation. Hence, authentication of the access network, if possible, could only aim to securely

exchange parameters between the end host and the visited network. This draft discusses some of these parameters or objects (such as cost or QoS parameters). Several approaches are possible to address the problem of protecting the distributed information.

First, the access network might "broadcast" (or distribute) information about the offered service (price, QoS, etc.). End hosts process this information automatically and make their decision. The access network might lie about the offered price (to the user) since

this information is not protected by any means. The access network provide could charge the user more than "agreed". It would be possible to verify the broadcasted information by utilizing the same mechanism as proposed with the 'lying NAS' problem. This mechanism requires that the distributed information can be securely exchanged between the EAP peer (end host) and the EAP server (user's home network) within an EAP method.

Second, the access network could be authenticated before user authentication takes place. This would allow to securely exchange parameters between the access network and the user and to even allow the user to provide more information about the offered services to the user. The following message exchange may be reasonable:

Alice wants to attach to one of the access networks found. She establishes a secure tunnel based on unilateral (network to user authentication). Then she would like to know what services are offered by this network. Subsequently, if she is happy about the offered price she decides to authenticate herself to the home network (by selecting a particular identifier and the corresponding credentials) to establish the necessary financial relationship between the home and the visited network.

This type of service is provided by today's hotspots with web interfaces. The usage of virtual access points or authentication at a higher layer (such as PANA) comes into mind when higher security other than packet filters are desired. This mechanism, however, requires user interaction and is therefore slow and error-prone. This process can of course be provided by protocols. Today there is no standardized protocol available which allows users to exchange information about offered and desired services, to communicate cost limits, to request cost information for network resources or to learn

already accumulated costs.

Authentication of the visited network requires some sort of server-side PKI which might not be available. Additionally, providing public key based authentication and the subsequent protocol exchange requires some time which causes delays during the network access procedure.

Even with the last approach it is still possible for the network to return incorrect charging information to the user's home network. Performing a higher number of re-authentication steps which are associated to a maximum amount each (similar to the idea proposed by micro-payment protocols) can help to give the user more control over his / her expenses.

Especially in roaming environments where an end host is likely to

have access to a large number of visited networks within a short time period cost control is even more complicated. User interaction might not be highly desirable. In fact these issues are a show-stopper for seamless mobility.

It might be worth mentioning that the issues and problems of cost control has already been identified in the NSIS working group some time ago in the context of Quality of Service signaling where the problems go beyond those described in this document (and with network selection as well).

As a summary, to provide a short-term solution the authors suggest to provide a mechanism to exchange information about the offered and the desired service between the end host and the access network. Subsequently, this information has to be repeated both in the EAP method and the AAA infrastructure to give the user and the home network the ability to detect fraud. This proposal has not been verified by the current implementation and hence needs further assessment.

## 5. Conclusion

This document presents some implementation results, which are considered to be suitable and useful for future implementations and extensions. The authors think that the mechanism proposed by [[I-D.adrangi-eap-network-discovery](#)] is suitable as network discovery for mediating network discovery. However, while implementing the proposed mechanism some irregularity towards the behavior of the Access point have been found and described. An implementation specific solution has been presented. Additional access network information elements like QoS and costs have been introduced, evaluated and implemented to prove the performance of the mechanism to convey network capabilities. The set of information identified is not considered as a complete approach and is mainly intended to trigger further discussion. The same holds for the exact data formats which are for further study. The security evaluation on network selection discovered some fields, which are not well understood so far and hence need further assessment. A proposal has

been given for an increased security level for network discovery.

The interoperability between unmodified and modified end hosts and AAA-Servers is given. AAA-Servers that are not modified do not send an additional Identity-Request, but directly authenticate the user. End hosts have to sent a valid Decorated-NAI from the beginning. Then the AAA-Server authenticates the end host without any new Identity-Request.

## [6.](#) Acknowledgement

The authors would like to thank Eleanor Hepworth, Dirk Kroeselberg and Stephen McCann for their comments.

## [7.](#) References

### [7.1](#) Normative References

- [I-D.adrangi-eap-network-discovery]  
Adrangi, F., Lortz, V., Bari, F., Eronen, P. and W. Watson, "Mediating Network Discovery in the Extensible Authentication Protocol (EAP)", [draft-adrangi-eap-network-discovery-01](#) (work in progress), June 2004, <reference.I-D.adrangi-eap-network-discovery.xml>.
- [I-D.ietf-eap-nettsel-problem]  
Arkko, J. and B. Aboba, "Network Discovery and Selection Problem", [draft-ietf-eap-nettsel-problem-00](#) (work in progress), January 2004, <reference.I-D.ietf-eap-nettsel-problem.xml>.
- [IEEE-802.1X]  
Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Port-Based Network Access Control", September 2001, <reference.IEEE-802.1X.xml>.

## [7.2](#) Informative References

- [3GPP TS23.107]  
3rd Generation Partnership Project, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture (Release 6)", Technical Specification 3GPP TS 23.107 V6.1.0 (2004-03), March 2004, <reference.3GPP TS23.107.xml>.
- [GRJK00] Gerke, J., Ritter, H., Schiller, J. and K. Wehrle, "Elements of an open framework for pricing in the future internet, in Proceedings of the Conference on Quality of future Internet Services (QofIS 2000), pages 300--311, Berlin", 2000, <reference.Paper.GRJK00>.
- [I-D.arkko-eap-service-identity-auth]  
Arkko, J. and P. Eronen, "Authenticated Service Identities for the Extensible Authentication Protocol (EAP)", [draft-arkko-eap-service-identity-auth-00](#) (work in progress), April 2004, <reference.I-D.arkko-eap-service-identity-auth.xml>.
- [I-D.caron-aaa-cost-advertisement]  
Caron, J., "AAA cost advertisement extensions",

[draft-caron-aaa-cost-advertisement-00](#) (work in progress),  
June 2002,  
<reference.I-D.caron-aaa-cost-advertisement.xml>.

[I-D.heckmann-tdp]

Heckmann, O., "Tariff Distribution Protocol (TDP)",  
[draft-heckmann-tdp-00](#) (work in progress), March 2002,  
<reference.I-D.heckmann-tdp.xml>.

[I-D.prasanna-bip]

Prasanna, R., "BIP: Billing Information Protocol",  
[draft-prasanna-bip-00](#) (work in progress), December 2002,  
<reference.I-D.prasanna-bip.xml>.

[I-D.tschofenig-eap-ikev2]

Tschofenig, H., Kroeselberg, D. and Y. Ohba, "EAP IKEv2  
Method (EAP-IKEv2)", [draft-tschofenig-eap-ikev2-02](#) (work  
in progress), October 2003,  
<reference.I-D.tschofenig-eap-ikev2.xml>.

[IEEE-SPEC-99]

Institute for Electric Engineers, "IEEE802.11 Spec 1999  
Edition", Technical Specification IEEE802.11 Spec 1999  
Edition, 1999, <reference.IEEE-SPEC-99.xml>.

[IS04217] International Organization for Standardization, "Codes for  
the representation of currencies and funds", ISO Standard  
4217, August 2001.

[KSS98] Karsten, M., Schmitt, J. and R. Steinmet, "An embedded  
charging approach for RSVP, in International Workshop on  
Quality of Service '98. Napa, California, USA", May 1998,  
<reference.Paper.KSS98>.

[ORW00] Oberle, V., Ritter, H. and K. Wehrle, "Bpp: A protocol for  
exchanging pricing information between autonomous systems,  
in Proceedings of HPSR 2001 (IEEE Workshop on  
High-Performance Switching and Routing), Dallas (USA)",  
May 2001, <reference.Paper.ORW00>.

[Pri04] Priest, J., "The State of Wireless London, available at  
'<http://www.spacestudios.org.uk/content/articles/461.pdf>'  
(July 2004)", March 2004.

[RFC3017] Riegel, M. and G. Zorn, "XML DTD for Roaming Access Phone  
Book", [RFC 3017](#), December 2000, <reference.RFC.3017.xml>.

Internet-Draft

Network Selection Implementation Results

July 2004

Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)", [RFC 3770](#), May 2004.

[RNAP] Wang, X. and H. Schulzrinne, "Rnap: A resource negotiation and pricing protocol, in International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV'99), pages 77--93, Basking Ridge, New Jersey", 1999, <reference.Paper.RNAP>.

#### Authors' Addresses

Wolfgang Groeting  
Siemens AG, ICM MP PD TI 2  
Frankenstrasse 2  
46395 Bocholt  
Germany

EMail: Wolfgang.Groeting@siemens.com

Stefan Berg  
Siemens AG, ICM MP PD TI 2  
Frankenstrasse 2  
46395 Bocholt  
Germany

EMail: Stefan.Berg@siemens.com

Malte Ness  
Siemens AG, ICM MP PD TI 2  
Frankenstrasse 2  
46395 Bocholt  
Germany

EMail: Malte.Ness@bch.siemens.de

Hannes Tschofenig  
 Siemens AG  
 Otto-Hahn-Ring 6  
 81739 Munich  
 Germany

EMail: Hannes.Tschofenig@siemens.com

Groeting, et al.

Expires January 10, 2005

[Page 24]

Internet-Draft

Network Selection Implementation Results

July 2004

## [Appendix A](#). Cost Attribute

To be more specific about the proposed attributes in [Section 2.2.2](#). In the past various drafts have proposed to include cost specific into protocols (such QoS signaling protocols, AAA protocols or SIP). The flexibility of the proposals varies a simple cost attribute, to complex formulas and even JAVA classes which allow sophisticated price calculation. From the investigated proposals (including TDP [[I-D.heckmann-tdp](#)], RNAP [[RNAP](#)], BIP [[I-D.prasanna-bip](#)], BPP [[GRJK00](#)] and [[ORW00](#)], [[KSS98](#)] ) [[I-D.caron-aaa-cost-advertisement](#)] was simple enough to be reused for our purpose.

We use the following attributes, Cost-Header attribute and one or more Cost-Unit subattribute for encoding this type of information.

### [A.1](#) Cost-Header Attribute

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
Type										Length										Decimals										No-of-AVPs									
Currency-Code																														...									

Type:

To Be Assigned by IANA

Length:

Indicates the length of this header attribute in bytes.

No-of-AVPs (6 bits):

This field points to the number of Cost-Unit attributes following the header attribute.

Decimals (10 bits)

Indicates where to place the comment in all subsequent units. For example, if Decimals is set to 2 then a value of 199 means 1.99. The value of '0' indicates that no decimal should set. The value should be read as it is.

Currency-Code (3 - 6 Bytes):

The value field of the Currency-Code attribute is of type "string" and indicates the currency to be applied to the Cost value as indicated by the Cost attribute. The string value for a single currency is defined in ISO 4217.

## [A.2](#) Cost-Unit SubAttribute

The Cost-Header attribute, described in [Appendix A.1](#), is followed by one or more Cost-Unit subattributes.

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
SubType										Quantity										Repeat ...																			
Repeat										Amount																													

### SubType:

- 1 Time-based chargig: billing is based on duration in seconds
- 2 Volume-based charging: billing is based on total bytes

### Quantity:

Quantity is the number of seconds or bytes that this amount will cover. 0 means none, and all ones means unlimited.

### Repeat:

Repeat is the number of times this unit will be repeated before moving on to the next one. 0 means unlimited.

### Amount:

Amount is the amount of money that should be billed. The value stored here should be divided by  $10^{\text{decimals}}$  to get the number of

currency units.

### [A.3](#) Example

To express the network cost for 10 EUR (independent of the time) the following payload has to be transmitted.

Cost-Header AVP:

Type = IANA assigned  
Length = 5  
Decimals = 0  
No-of-AVPs = 1  
Currency-Code = EUR (3 bytes)

Cost-Unit:

SubType = 1 (Time-based charging)  
Quantity = all ones (means unlimited)  
Repeat = 0 (unlimited)  
Amount = 10

More complex, non-linear pricing schemes can also be expressed by listing several Cost-Unit attributes. For example, to express a pricing policy where 2 EUR are charged for the first 30 minutes and then 0.02 EUR for every further minute.

Cost-Header AVP:

Type = IANA assigned  
Length = 5  
Decimals = 2  
No-of-AVPs = 2  
Currency-Code = EUR (3 bytes)

Cost-Unit:

SubType = 1 (Time-based charging)  
Quantity = 1800 (60 \* 30 minutes)

Repeat = 0 (no repeat)  
Amount = 200

Cost-Unit:

SubType = 1 (Time-based charging)  
Quantity = 60 (60 seconds)  
Repeat = 0 (unlimited)  
Amount = 2

The transport of these attributes within RADIUS or Diameter and via an EAP protocol (see an example in [[I-D.tschofenig-eap-ikev2](#)] and the generalized version in [[I-D.arkko-eap-service-identity-auth](#)]) are not described in this document.

## [Appendix B](#). QoS Attribute

In [Section 2.2.4](#), it was proposed to indicate supported QoS classes. To be more specific, the UMTS classes, defined in [3GPP TS23.107], could be used.

## [B.1](#) UMTS QoS-Classes

There are four different QoS classes defined in [3GPP TS23.107]:

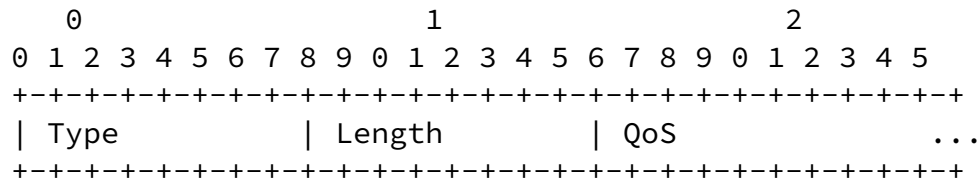
- conversational class
- streaming class
- interactive class
- background class

The main distinguishing factor between these QoS classes is how delay sensitive the traffic is: Conversational class is meant for traffic which is very delay sensitive while Background class is the most delay insensitive traffic class.

Conversational and Streaming classes are mainly intended to be used to carry real-time traffic flows. The main divider between them is how delay sensitive the traffic is. Conversational real-time services, like video telephony, are the most delay sensitive applications and those data streams should be carried in Conversational class.

Interactive class and Background are mainly meant to be used by traditional Internet applications like WWW, Email, Telnet, FTP and News. Due to looser delay requirements, compare to conversational and streaming classes, both provide better error rate by means of channel coding and retransmission. The main difference between Interactive and Background class is that Interactive class is mainly used by interactive applications, e.g. interactive Email or interactive Web browsing, while Background class is meant for background traffic, e.g. background download of Emails or background file downloading. Responsiveness of the interactive applications is ensured by separating interactive and background applications. Traffic in the Interactive class has higher priority in scheduling than Background class traffic, so background applications use transmission resources only when interactive applications do not need them. This is very important in wireless environment where the bandwidth is low compared to fixed networks.

## [B.2](#) QoS-Header Attribute



Type:

To Be Assigned by IANA

Length:

Indicates the length of this header attribute in bytes.

QoS:

This field contains the supported QoS classes

Bit1 - conversational

Bit2 - streaming

Bit3 - interactive

Bit4 - background

Bit5 (and following) - tbd

### B.3 Example

To express the network supports UMTS QoS classes `interactive` and `background` the following payload has to be transmitted:

QoS-Header:

Type = IANA assigned

Length = 4

QoS = 0011

A network supports exclusively real time services and indicates only UMTS QoS class «conversational»:

QoS-Header:

Type = IANA assigned

Length = 1

$$QoS = 1$$

---

Internet-Draft      Network Selection Implementation Results      July 2004

## 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](mailto: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.

Groeting, et al.

Expires January 10, 2005

[Page 31]