# Diameter User Session Update Procedure for Mobile Node’s Fast Handoff

**Yanqun Le, Qing Liu**
**Nokia Research Center, Beijing, 100013, P.R.China**
**Dan Forsberg**
**Nokia Research Center, Helsinki,**
**P.O.Box 407, FIN-00045 NOKIA GROUP, Finland**

## ABSTRACT

A mobile node (MN) may frequently change its access between different sub-domains or domains during a Diameter session. For many services, especially those real time services, it is significant to reduce the time for re-establishing the services in the new access router (AR), therefore the service states (e.g. AAA information) will be relocated to the new location rather than re-establishing the services from scratch. However, it will destroy the end-to-end Diameter user session. This paper proposes an efficient way to update the Diameter user session while the MN moves.

**Keywords:** AAA, Mobile Node, Access Router, AAA Server, anchor AAA Server

## I. INTRODUCTION

With the further development of the Internet and the telecommunication networks, today the end user can enjoy various kinds of services. And those service providers need a robust Authentication, Authorization and Accounting (AAA) protocol while providing services.

The Diameter base protocol is designed to provide an extensible AAA framework for services such as network access or IP mobility. Here we extend Diameter base protocol by two new messages in order to provide the user with session mobility for various services.

In Section 2 we review some AAA concepts, describe the Diameter user session and the demand of the session update procedure. Section 3 explains the basic idea of the session update procedure. Section 4 provides various session mobility scenarios. Section 5 discusses the advantages and the specific issues of the session update procedure.

## II. DIAMETER USER SESSION

Diameter is designed to be extensible. Its base protocol provides the basic functions of an AAA protocol, such as delivery of attribute value pairs (AVPs), capabilities negotiation and handling of user session, etc. In order to satisfy the need of various services, many applications are under development upon the Diameter base protocol.

An AAA infrastructure constructed by Diameter protocol consists of Diameter clients, Diameter agents and Diameter servers. The Diameter server authenticates the users, handles authorization requests and collects the information of resource usage.

### A. Diameter User Session

When a user requests the access to the network, the Diameter client, typically located within the access router (AR), issues an auth request to its local server. The request contains a Session-Id AVP, which will be used in subsequent messages (e.g. subsequent authorization, accounting, etc.) relating to the user's session. If it is a roaming user for the domain, the local server will forward the auth request to the user’s home AAA server (AAAH). The AAAH authorizes the user to use the network resources for the length of Session-Timeout, of which the client is notified by the auth answer. The Diameter user session between the AR and the AAAH lasts until session timeout or being stopped by Session Termination Request from the AR.

The AAAH generally maintains the identity of the original client of an active user session because this information is useful for the Diameter server to initiate a re-authentication and/or re-authorization service for the session (by Re-Auth-Request) or to abort the session (by Abort-Session-Request).

### B. Support of fast handoff

When the MN moves during a Diameter session, the relevant AAA parameters may be transferred during the handoff from its old access domain to the new one. There are several ways to transfer the AAA parameters, for example, by the context transfer process, or delivery by the MN. The relocation of AAA parameters can reduce the AAA signaling over the whole AAA infrastructure and therefore re-establish the authentication and authorization states in the new access domain quickly.

The Diameter client of the active Diameter session has changed during the fast handoff and the AAAH will not know the handoff until the MN re-authenticates. As the Destination-Host AVP within a request from the AAAH still has the value of the original Diameter client, the request will always be forwarded to the original client. Therefore, the request from the home domain cannot be executed timely and successfully, however, most of these requests are critical and may influence the authentication and/or authorization state. Therefore in order to support fast handoff better, there is a need of a Diameter session update procedure.

## III. DIAMETER SESSION UPDATE PROCEDURE

### A. Role of AAALs

The procedure introduces an anchor AAAL. AAAL, in comparison with AAAH, is the local Diameter server and acts as a Diameter proxy agent for the roaming node. AAAL makes policy decisions and forwards messages. In addition to the function of AAAL, the anchor AAAL, redirects the request from the home domain to the new AR.

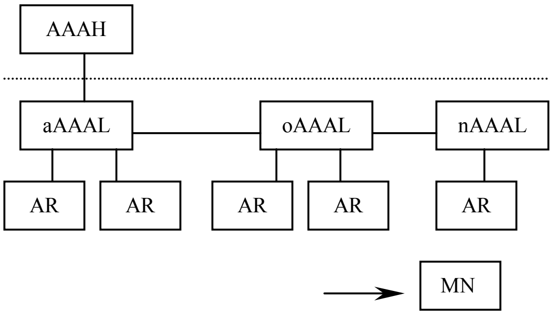

Fig.1 basic AAA infrastructure

aAAAL is the original AAAL where the initial auth request is forwarded towards the AAAH. nAAAL is the AAAL that is providing AAA service to the MN currently. oAAAL is the AAAL that has provided AAA service to the MN previously, may be the same as aAAAL.

### B. Commands and AVPs

Two new messages (Session-Update-Request and Session-Update-Answer) are also defined for the new AR to update the session information maintained in the anchor AAAL or the old AAAL.

1) Session-Update-Request

The Session-Update-Request (SUR), indicated by the Command-Code set to TBD, is sent by the access device or the Diameter client to inform the relevant Diameter Proxy that an authenticated and/or authorized session is being updated. Message Format:

```
<SUR> ::=    < Diameter Header: TBD, REQ, PXY >
               < Session-Id >
                { Origin-Host }
                { Origin-Realm }
                { Destination-Host }
                { Destination-Realm }
                { Auth-Application-Id }
                [ User-Name ]
                [ Anchor-AAA-Server ]
                [ New-AAA-Server ]
                [ Session-Update-Vector ]
                [ Origin-State-Id ]
               *[ Proxy-Info ]
               *[ Route-Record ]
               *[ AVP ]
```

2) Session-Update-Answer

The Session-Update-Answer (SUA), is sent by the Diameter Proxy to acknowledge the notification that the session has been updated. The Result-Code AVP MUST be present, and MAY contain an indication that an error occurred while servicing the SUR. Message Format:

```
<SUA> ::=     < Diameter Header: TBD, PXY >
              < Session-Id >
               { Result-Code }
               { Origin-Host }
               { Origin-Realm }
               [ User-Name ]
               [ Session-Info]
               [ New-AAA-Server ]
               [ Error-Message ]
               [ Error-Reporting-Host ]
             * [ Failed-AVP ]
               [ Origin-State-Id ]
             * [ Redirected-Host ]
               [ Redirected-Host-Usage ]
               [ Redirected-Max-Cache-Time ]
             * [ Proxy-Info ]
             * [ AVP ]
```

3) New AVPs

The Anchor-AAA-Server AVP is of type DiameterIdentity and contains the identity of the aAAAL.

The New-AAA-Server AVP is of type DiameterIdentity and contains the identity of the nAAAL in the foreign network.

The Session-Update-Vector AVP is of type Unsigned32 and is added with flag values set by the aAAAL or AAAH.

Flag values currently defined include:
1 Passed-Anchor-AAAL
2 Passed-AAAH

The Session-Info AVP is of type Grouped and contains the user session information maintained in the AAAL and need to be transferred to the new AAAL. The possible values of this AVP are for further study.

AVP Format

```
<Session-Info> ::= < AVP Header: TBD >
                   1* {AVP}
```

### C. Basic Procedure

AAAL generally maintains information of an active session and some of the information needs to be transferred to new AAAL inside one domain during MN's handoff. And the transfer between two different domains is for further study because it breaks the trust boundaries. The information that needs to be transferred is user profile related. Accounting data can be reported to the AAAH, but it can also be transferred to the new AAAL. Accounting related information includes interim interval and last event timestamp, etc.

Besides this information, aAAAL should also maintain the downstream node information, which is the next hop AAA node that the request message from AAAH aims to.

When MN changes its AR inside one AAAL, the new AR just sends SUR to the current AAAL, informing it to update the downstream node information from the old AR to the new AR.

When MN changes its AR between two AAALs, upon receipt of the AAA parameters, the new AR will send SUR through the nAAAL, optionally the oAAAL, to the aAAAL, informing the aAAAL to update the downstream node information from the oAAAL to the nAAAL. By the way, the other relevant user information can be transferred to the nAAAL by SUA message.

When the aAAAL receives a request from AAAH, it will forward the modified request to the nAAAL and nAAAL will forward it to the nAR.

If nAR re-initiates auth-request through a new AAAL, it becomes aAAAL for this extended session. The downstream node in the old aAAAL will be released by session timeout.

If AAAH receives a message from nAAAL that is different from aAAAL, it will update its pointer from aAAAL to nAAAL or from oAR to nAR based on the different implementation.

## IV. SESSION MOBILITY SCENARIOS

In order to explain the session update procedure more clearly, several representative session mobility scenarios and the complete procedure are illustrated here. From those scenarios, we can also get the reason why these new AVPs are defined.

As the operation of AR is almost the same in these scenarios, it will be summarized here first: after successful handoff, oAR will release session information and nAR will send SUR to oAAAL with Destination-Host set to oAAAL. If oAAAL doesn't equal to any of its local AAA servers, the request message should also include Anchor-AAA-Server AVP with the value of the aAAAL and New-AAA-Server AVP with the value of the nAAAL.

Below are the different session mobility scenarios:

### A. Handoff inside one AAAL

The procedure applies to the scenario whether the handoff happens within aAAAL or not.

1. nAR sends SUR to the AAAL to update the downstream node to nAR. And the AAAL answers with SUA.

### B. Handoff from aAAAL (or oAAAL) to nAAAL

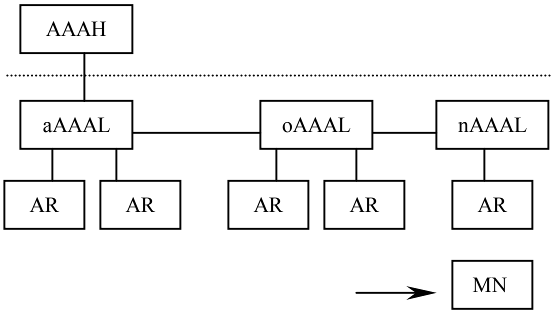

Fig. 2: Handoff from oAAAL to nAAAL

1. When SUR passes through nAAAL, the nAAAL will update its downstream node to the host in Origin-Host AVP, besides forwarding the message;

2. When oAAAL receives SUR, it compares local host with the value of Anchor-AAA-Server AVP. If they are different, the oAAAL should replace the Destination-Host AVP value with that of Anchor-AAA-Server AVP and send the request out;

3. When aAAAL receives SUR, it should update the downstream node to the value of New-AAA-Server AVP and send back Session-Update-Answer message. In addition, if there is user information maintained in the aAAAL, this information is encoded into a Session-Info AVP included as part of the SUA message. Once the AAA information is transferred, AAA server doesn't need to maintain it any longer;

4. If, otherwise, the user information is maintained in oAAAL, the information will be inserted into SUA message as a Session-Info AVP when the message is forwarded from oAAAL to nAAAL;

5. In the path of the SUA, if some AAAL detects that its local host name equals to the value of New-AAA-Server AVP in the message (i.e. it is nAAAL), it will extract the Session-Info AVP and save the user information locally.

### C. Handoff from oAAAL to aAAAL

It refers to the scenario when MN returns to the original sub-domain.

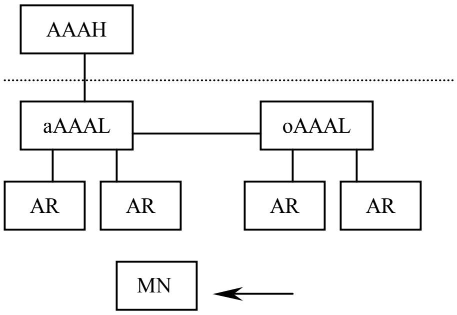

Fig. 3: Handoff from oAAAL to aAAAL

1. When SUR passes through nAAAL, the nAAAL will update its downstream node to the Origin-Host besides forwarding the message. If it discovers it is aAAAL, it must add Session-Update-Vector with Passed-Anchor-AAAL flag set to one before forwarding, in order to inform oAAAL that the message has passed aAAAL;

2. On receipt of SUR, since Passed-Anchor-AAAL flag is one in the message, oAAAL encodes the maintained user AAA into a Session-Info AVP included as part of the Session-Update-Answer message to be sent back;

3. In the path of the SUA, if some AAAL detects that its local host name equals to the value of New-AAA-Server AVP in the message (i.e. it is nAAAL), it will extract the Session-Info AVP and save the user information locally.

### D. Handoff from oAAAL to nAAAL, also aAAAL is in the middle of them.

Because the AR does not know if the route to oAAAL passes aAAAL, Destination-Host of SUR still points to oAAAL.

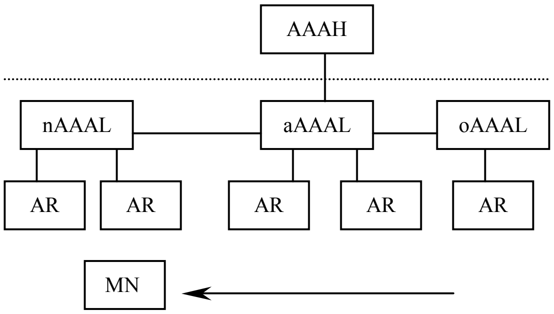

Fig 4: aAAAL between the handoff path

1. When SUR passes through nAAAL, the nAAAL will update its downstream node to the host in the Origin-Host AVP, besides forwarding the message;

2. When SUR passes through aAAAL, the aAAAL discovers that its local host doesn't equal to the value of New-AAA-Server, so it will update its downstream node to the New-AAA-Server. Also, it must add Session-Update-Vector with Passed-Anchor-AAAL flag set to one before forwarding the message;

3. On receipt of SUR, since Passed-Anchor-AAAL flag is one in the message, oAAAL encodes the maintained user AAA into a Session-Info AVP included as part of the Session-Update-Answer message to be sent back;

4. In the path of the SUA, if some AAAL detects that its local host name equals to the value of New-AAA-Server AVP in the message (i.e. it is nAAAL), it will extract the Session-Info AVP and save the user information locally.

### E. MN returns to its home domain

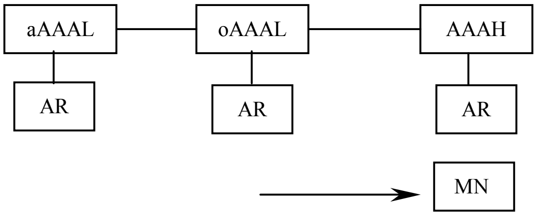

Fig. 5: MN returns to home domain

It means that nAAAL is AAAH.

1. When SUR passes through nAAAL, the AAAH will add Session-Update-Vector AVP with Passed-AAAH flag set to one, in order to inform aAAAL that the message has passed AAAH;

2. When oAAAL receives SUR, it compares local host with the value of Anchor-AAA-Server AVP. If they are different, the oAAAL should replace the Destination-Host AVP value with that of Anchor-AAA-Server AVP and send the request out;

3. When aAAAL receives SUR, as the Passed-AAAH flag is one, whether to transfer the maintained user information is application specific. After SUA is sent, it will free the relevant information of the session;

4. If the user information is maintained in oAAAL, whether to transfer the maintained user information is application specific too.

### F. Race Scenario

Race scenario refers to the situation when oAR receives a request from AAAL (possibly originally from AAAH) for a session that has moved to nAR. When a diameter message is heading for the MN's access router, at the same time the MN is changing its AR, the diameter message will be answered with errors if it reached the oAR when MN had already changed to the nAR. This happens when SUR message has not yet been processed. oAR answers with Result-Code set to DIAMETER_UNKNOWN_SESSION_ ID.

When AAAL receives an answer with the Result-Code AVP set to DIAMETER_UNKNOWN_SESSION_ID from a downstream AR (oAR) or AAAL, it will wait for SUR message with the matching Session-Id AVP for a certain period of time, meanwhile holding the answer. After the matching SUR has been received and neither of the flags of Session-Update-Vector AVP is set, AAAL will re-send the request to the nAR or AAAL and free the answer, Otherwise it will just forward this answer.

### G. Re-direct request message from AAAH

There have been two request messages defined in the Diameter base protocol that will be sent from the AAAH, that is, Re-Auth-Request (RAR) or Abort-Session-Request (ASR).

When AAAL receives a request message from the MN's AAAH, the request will be forwarded according to the downstream node value maintained in the AAAL. It should forward the message after replacing the value of Destination-Host AVP with its saved downstream node of this session. When AAAL receives a request forwarded from another AAAL, the same procedure should be applied.

Upon the receipt of the answer (e.g. RAA or ASA) for the request, it will release the maintained AAA information after the answer is sent out.

The re-auth request or STR should be delivered as that defined in Diameter base protocol.

## V. CONCLUSION

While a user is roaming, the current domain may be far away in most cases from the user's home domain in terms of the signaling transmission time. In the proposed session update procedure, since the new AR only needs to notify the AAAL rather than the AAAH of the handoff, the request/answer round-trip delay and the number of signaling messages between domains can be reduced greatly. Even if the MN returns to its home domain, this procedure is also applicable.

Other session information can also be transferred between AAALs accordingly while the user moves. In addition, it can be used to all Diameter applications to support session mobility, since it is implemented in the session layer of the Diameter protocol.

There is one requirement of the session update procedure, that is, the request from the AAAH should go through the aAAAL. But it is not difficult to achieve.

In order to know the exact performance improvement of fast handoff by the introduction of the procedure, we will implement and further study on it.

## REFERENCES

[1] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, A. Rubens, **Diameter Base Protocol**, draft-ietf-aaa-diameter-17.txt, Internet Draft, Oct. 2002.

[2] P. Calhoun, T. Johansson, C. Perkins, **Diameter Mobile IPv4 Application**, draft-ietf-aaa-diameter-mobileip-13.txt, Internet Draft, Oct. 2002.

[3] J. Kempf, **Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network**, RFC3374, Sept. 2002.

[4] D. Forsberg, R. Koodli, C. Perkins, **Context Relocation of AAA Parameters in IP Networks**, draft-forsberg-seamoby-aaa-relocate-01.txt, work in progress.