Diameter Maintenance and
Extensions (DIME)
Internet-Draft
Intended status: Standards Track
Expires: April 30, 2009

J. Korhonen (ed.)
TeliaSonera
M. Jones
Bridgewater Systems
L. Morand
Orange Labs
T. Tsou
Huawei

October 27, 2008

Diameter User-Name and Realm Based Request Routing Clarifications
draft-korhonen-dime-nai-routing-02.txt

Status of this Memo

Copyright Notice

Abstract

This specification clarifies the Diameter realm based request routing. We focus on the case where a Network Access Identifier in the User-Name AVP is used to populate the Destination-Realm AVP and

the Network Access Identifier contains more than one realm. This particular case is possible when the Network Access Identifier decoration is used to force a routing of request messages through a predefined list of realms. However, this functionality is not unambiguously specified in the Diameter Base Protocol specification.

Table of Contents

1. Introduction

This specification clarifies the Diameter realm based request routing defined in RFC 3588 [1]. We focus on the case where the Network Access Identifier (NAI) [2] in the User-Name AVP is used to populate the Destination-Realm AVP and the NAI contains more than one realm. This particular case is possible when the NAI decoration is used to force a routing of request messages through a predefined list of realms.

According to the Diameter request routing processing rules in RFC 3588, the request originator may populate the Destination-Realm AVP with the realm part of the NAI available in the User-Name AVP. Unfortunately, there is no unambiguous mandatory language in RFC 3588 how Diameter agents participating to the request routing should update the Destination-Realm AVP at each realm.

This specification presents both the issue regarding to the Diameter realm based request routing with NAI decoration and also a solution for the problem. The solution would only apply to Diameter Base Protocol implementations that take the solution presented in this specification into account. The solution, however, is fully backwards compatible with the RFC 3588 Diameter Base Protocol.

2. Terminology and Abbreviations

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 [3].

Network Access Identifier (NAI):

> The Network Access Identifier (NAI) is the user identity submitted by the client during access authentication. In roaming, the purpose of the NAI is to identify the user as well as to assist in the routing of the authentication request.

Decorated NAI:

> A NAI specifying a source route. See Section 2.7 of RFC 4282 for more information.

Network Access Provider (NAP):

> A business entity that provides network access infrastructure to one or more realms. A NAP infrastructure constitutes of one or more NASes.

Network Access Server (NAS):

The device that peers connect to in order to obtain access to the network.

3. Problem Overview

The Diameter Base Protocol RFC 3588 Section 6.1 defines the request routing in detail. This specification concerns only those cases where a Destination-Realm AVP is included in a request message. A Diameter peer originating a request message MAY retrieve the realm information from the User-Name AVP and use that realm to populate the Destination-Realm AVP. The User-Name AVP is in form of a NAI (in this case a NAI with the realm part). The realm based request routing, as described in RFC 3588, does not discuss how to handle Decorated NAIs. The original NAI RFC 2486 [4] that RFC 3588 references to, does not defined how to construct a NAI with multiple realms. Since then RFC 2486 has been obsoleted by RFC 4282 which in turn defines how to construct Decorated NAIs.

Decorated NAIs are used to force routing of messages through a predefined list of realms and in that way force certain inter-realm roaming arrangements, see Section 2.7. of RFC 4282 [2]. For example, a terminal (e.g., a mobile host) may learn based on some application or implementation specific manner that its network access authentication signaling must traverse through certain realms in order to reach the home realm. In this case the terminal would decorate its NAI during the network access authentication with the list of intermediating realms and the home realm. As a result, the network access server (NAS) and intermediating Diameter agents would make sure that all subsequent request messages traverse through the desired realms as long as the request messages contain the User-Name AVP with a Decorated NAI.

NAI Decoration has previously been used, for example, in RADIUS [5] based roaming networks using RFC 2486 NAIs in a proprietary manner. There is a need to replicate the same NAI based routing enforcement functionality also in Diameter based roaming networks. There are also publicly available specifications (e.g., see [6], [7] and [8]) that assume NAI Decoration based request routing enforcement is fully supported by RFC 3588. The same assumption is carried over to NASREQ [9] and EAP [10] Diameter applications.

Figure 1 illustrates an example deployment scenario where Decorated NAIs would be used to force a certain route through desired realms. A roaming terminal (e.g., a mobile host) discovers a number of

Network Access Providers (NAP): NAP A and NAP B. None of the NAPs are able to provide direct connectivity to roaming terminals home realm (i.e. Realm-H). However, the roaming terminal learns, somehow, that NAP B is able to provide connectivity to the Realm-H through the Realm-X (i.e. the visited realm from the roaming terminal point of view). During the network access authentication, the roaming terminal would decorate its NAI as Realm-H!username@Realm-X. The roaming terminal has also an alternative route to its home realm through NAP A, Realm-Z and Realm-X. If the roaming terminal were to choose to use NAP A, then it would decorate its NAI as Realm-X!Realm-H!username@Realm-Z. Diameter agents should now be able to route the request message through desired realms using the Decorated NAI originally found in the User-Name AVP.

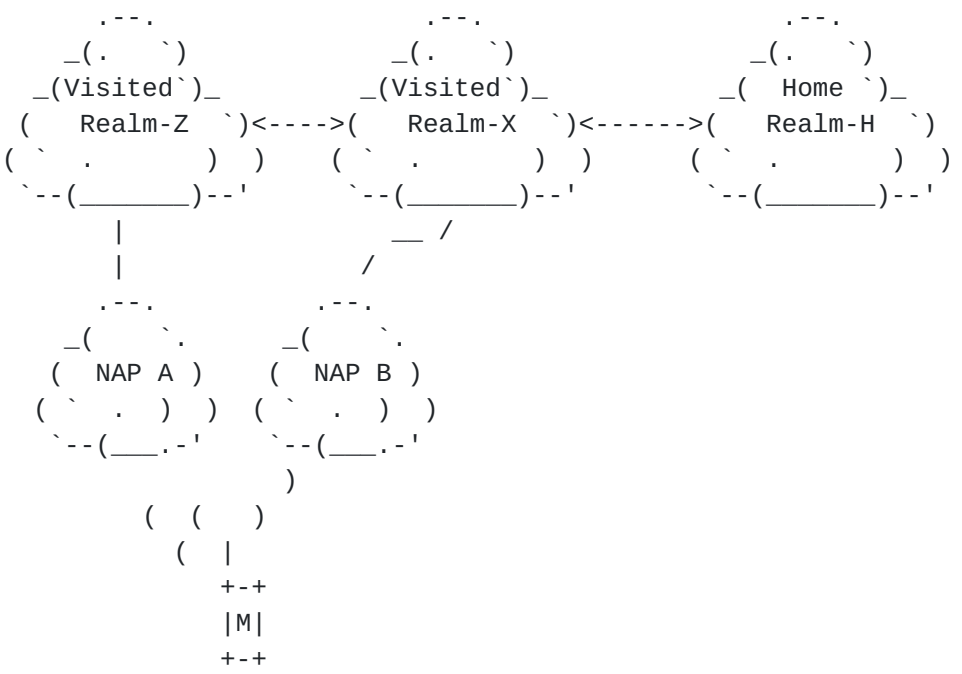

Figure 1: Example roaming scenario with intermediating realms. The mobile host authenticates to the home realm through one or more visited realms.

NAI Decoration is not limited to the network access authentication and authorization procedures. It can be used with any Diameter application whose commands are proxiable and include the User-Name AVP with a NAI. Generally NAI Decoration can be used to force a certain route for all request messages at a realm granularity.

As a problem summary we have two main issues:

- Updating both Destination-Realm and User-Name AVPs based on the Decorated NAI extracted from the User-Name AVP. The update would be done by intermediating Diameter agents that participate to realm based request routing. Specifically, this would concern Diameter proxies.

- How Diameter agents could implement the handling of the NAI Decoration based routing enforcement in a way that is still backwards compatible with RFC 3588.

RFC 5113 [11] Section 2.3 also discusses NAI decoration related issues with EAP [12] in general.

4. Solution Overview

This specification defines a solution for Diameter realm based request routing with routing enforcement using the User-Name AVP NAI Decoration. Diameter proxy agent implementations can claim compliance using the solution described in this specification.

4.1. Interpretation of Decorated NAIs

Implementations compliant to this specification MUST have an uniform way of interpreting decorated NAIs. That is, in the case of decoration, the character '!' is used to separate realms in the list of decorated realms in the NAI (as shown in examples in [2]).

4.2. Enhanced Request Routing Solution

When a Diameter agent receives a request message containing a Destination-Realm AVP with a realm that the agent is configured to process locally (and in the case of proxies the Diameter application is locally supported), it MUST do the following further processing before handling the message locally:

- If the User-Name AVP is available in the request message, then the Diameter agent MUST inspect whether the User-Name AVP contains a Decorated NAI. If the NAI is not decorated then the Diameter agent proceeds with a normal RFC 3588 message processing.

- If the User-Name AVP contains a Decorated NAI, then the Diameter agent MUST process the NAI as defined in RFC 4282 and update the value of the User-Name AVP accordingly. Furthermore, the Diameter agent MUST update the Destination-Realm AVP to match the new realm in the User-Name AVP.

o The request message is then sent to the next hop using the normal request routing rules as defined in RFC 3588.

Figure 2 illustrates an example of a roaming terminal originated signaling with the home realm (Realm-H) through a NAP and two intermediating realms (Realm-Z, Realm-X) before reaching the home realm (Realm-H). The example shows how the User-Name AVP and the Destination-Realm AVP change at each realm before reaching the final destination. If the signaling were originated from the NAS/NAP only, then the step 1) can be omitted.

```
1) Roaming Terminal -> NAS/NAP
       Identity/NAI = realm-X!realm-H!username@realm-Z

2) NAS/NAP -> Realm-Z
       User-Name = realm-X!realm-H!username@realm-Z
       Destination-Realm = realm-Z

3) Realm-Z -> realm-X
       User-Name = realm-H!username@realm-X
       Destination-Realm = realm-X

4) Realm-X -> Realm-H
       User-Name = username@realm-H
       Destination-Realm = realm-H
```

Figure 2: The roaming terminal decides that the Diameter messages must be routed via Realm-Z, Realm- X and Realm-H.

4.3. Backwards Compatibility Considerations

Obviously, the functionality described in Section 4.2 cannot be guaranteed to work with the existing implementations of RFC 3588 or any other strictly RFC 3588 compliant existing application (such as NASREQ and EAP). An incompliant implementation would automatically fall back to the normal RFC 3588 request routing behavior that, unfortunately, cannot offer desired enhanced request routing functionality. Therefore, it is RECOMMENDED that the solution defined in this specification is only applied to newly specified Diameter applications. A Diameter agent MAY implement the solution defined in this specification also for the existing application. A Diameter client SHOULD NOT assume the functionality described in Section 4.2 from Diameter applications that do not comply with this specification.

5. IANA Considerations

This specification has no actions to IANA.

6. Security Considerations

A malicious node initiating (or indirectly causing initiation of) Diameter request may purposely create malformed list of realms in the NAI. This may cause the routing of requests through realms that would normally have nothing to do with the initiated Diameter message exchange. Furthermore, a malformed list of realms may contain non-existing realms causing the routing of Diameter messages that cannot ultimately be routed anywhere. However, the request message might get routed several hops before such non-existent realms are discovered and thus creating unnecessary overhead to the routing system in general.

The NAI decoration is used in AAA infrastructures where the Diameter messages are transported between the NAS and the Diameter server via one or more AAA brokers or Diameter proxies. In this case the NAS to the Diameter server AAA communication rely on the security properties of the intermediate AAA brokers and Diameter proxies.

7. Acknowledgements

The authors would like to thank Victor Fajardo and Stefan Winter for their comments on this draft.

Jouni Korhonen would like to thank TEKES WISEciti project for providing funding to work on this document.

8. References

8.1. Normative References

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

[2] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

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

8.2. Informative References

[4] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

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

[6] 3GPP, "3GPP system to Wireless Local Area Network (WLAN) interworking; System description", 3GPP TS 23.234 6.10.0, October 2006.

[7] 3GPP, "3GPP system to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 3", 3GPP TS 24.234 6.7.0, October 2006.

[8] 3GPP, "Numbering, addressing and identification", 3GPP TS 23.003 3.15.0, October 2006.

[9] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[10] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[11] Arkko, J., Aboba, B., Korhonen, J., and F. Bari, "Network Discovery and Selection Problem", RFC 5113, January 2008.

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

Authors' Addresses

Jouni Korhonen
TeliaSonera

Email: jouni.nospam@gmail.com

Mark Jones
Bridgewater Systems
303 Terry Fox Drive
Ottawa, Ontario K2K 3J1
Canada

Email: Mark.Jones@bridgewatersystems.com

Lionel Morand
Orange Labs
38-40 rue du general Leclerc
Issy-moulineaux Cedex 9, 92794
France

Email: Lionel.morand@orange-ftgroup.com

Tina Tsou
Huawei
R&D Center, Huawei Technologies Co., Ltd
Bantian, Shenzhen
P.R. China

Email: tena@huawei.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).