Diameter Maintenance and
Extensions (DIME)
Internet-Draft
Updates: 3588, 3588bis
(if approved)
Intended status: Standards Track
Expires: November 11, 2009

J. Korhonen, Ed.
Nokia Siemens Networks
M. Jones
Bridgewater Systems
L. Morand
Orange Labs
T. Tsou
Huawei

May 10, 2009

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

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

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

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

This Internet-Draft will expire on November 11, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This specification defines the behavior required of Diameter agents to route requests when the User-Name Attribute Value Pair contains a Network Access Identifier formatted with multiple realms. These multi-realm or "Decorated" Network Access Identifiers are used in order to force the routing of request messages through a predefined list of mediating realms.

Table of Contents

1. Introduction

This specification defines the behavior required of Diameter agents to route requests when the User-Name Attribute Value Pair (AVP) contains a Network Access Identifier (NAI) formatted with multiple realms (hereafter referred to as Decorated NAI). Decorated NAIs are used in order to force the routing of request messages through a predefined list of mediating realms. This specification does not define a new Diameter application but instead defines behaviour that would be common across all Diameter applications which require request routing based on Decorated NAI.

At the time of publication of the Diameter Base Protocol [RFC3588], the NAI definition was based on [RFC2486] in which a NAI could only contain a single realm. The NAI definition has since been updated in [RFC4282] to define Decorated NAIs that contain multiple realms. However, RFC 4282 does not define how the Decorated NAIs should be handled by Diameter agents so this specification was written to capture those requirements.

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].

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 containing multiple realms used to specify a source route and formatted according to Section 2.7 in RFC 4282.

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. In that case, the User-Name AVP is in form of a NAI including the realm part.

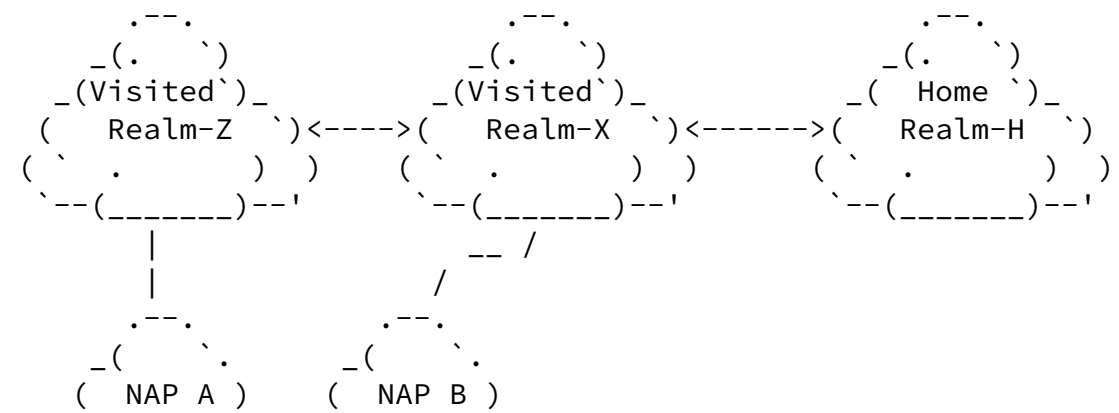
Decorated NAIs are used to force routing of messages through a predefined list of realms and in that way e.g., force certain inter-realm roaming arrangements, see Section 2.7. of RFC 4282. For example, a terminal (e.g. a mobile host) may learn based on some application or implementation specific manner 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 in RADIUS [RFC2865] 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 [3GPP.23.234], [3GPP.24.234], [3GPP.23.003], [3GPP.29.273] and [WiMAX]) that assume NAI decoration based request routing enforcement is fully supported by RFC 3588. The same assumption is carried over to NASREQ [RFC4005] and EAP [RFC4072] 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.



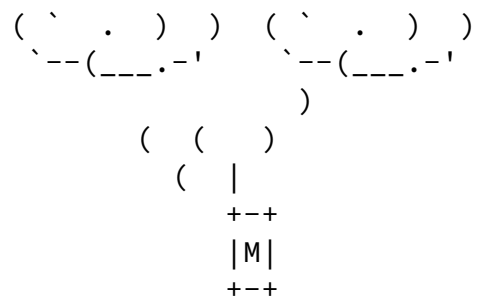


Figure 1: Example roaming scenario with intermediating realms. The mobile host authenticates to the home realm through one or more visited realms.

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, the 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.

[RFC5113] Section 2.3. also discusses NAI decoration related issues with EAP [RFC3748] 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 [RFC4282]).

4.2. Ensuring Backwards Compatibility

Implementations compliant to this specification MUST define a new Diameter application. This requirement is set to guarantee backwards compatibility with existing Diameter implementations, applications and deployments. Diameter agents not compliant with this specification will not advertise support for these new applications that implement the enhanced routing solution based on Decorated NAIs and will therefore be bypassed.

4.3. Enhanced Request Routing Solution

When a Diameter client originates a request message, the Destination-Realm AVP is populated with the realm part of the NAI available in the User-Name AVP (realm given after the '@' character of the NAI). The NAI in the User-Name AVP may or may not be decorated.

When a Diameter agent receives a request message containing the 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.

5. IANA Considerations

This specification has no actions to IANA.

6. Security Considerations

A malicious node initiating (or indirectly causing initiation of) a 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, Stefan Winter and Avi Lior for their detailed comments on this document.

Jouni Korhonen would like to thank TEKES WISEciti project for providing funding to work on this document while he was at TeliaSonera's employ.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

8.2. Informative References

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

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

[3GPP.24.234]
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.

[3GPP.29.273]
3GPP, "Evolved Packet System (EPS); 3GPP EPS AAA interfaces", 3GPP TS 29.273 8.1.0, March 2009.

[RFC2486] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[RFC4072] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[RFC5113] Arkko, J., Aboba, B., Korhonen, J., and F. Bari, "Network Discovery and Selection Problem", RFC 5113, January 2008.

[WiMAX] WiMAX Forum, "WiMAX Forum Network Architecture (Stage 2: Architecture Tenets, Reference Model and Reference Points)", Release 1 Version 1.2, January 2008.

Authors' Addresses

Jouni Korhonen (editor)
Nokia Siemens Networks
Linnoitustie 6
Espoo FIN-02600
Finland

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