

Internet Engineering Task Force (IETF)
Request for Comments: 7156
Category: Standards Track
ISSN: 2070-1721

G. Zorn
Network Zen
Q. Wu
Huawei
J. Korhonen
Broadcom
April 2014

Diameter Support for Proxy Mobile IPv6 Localized Routing

Abstract

In Proxy Mobile IPv6, packets received from a Mobile Node (MN) by the Mobile Access Gateway (MAG) to which it is attached are typically tunneled to a Local Mobility Anchor (LMA) for routing. The term "localized routing" refers to a method by which packets are routed directly between an MN's MAG and the MAG of its Correspondent Node (CN) without involving any LMA. In a Proxy Mobile IPv6 deployment, it may be desirable to control the establishment of localized routing sessions between two MAGs in a Proxy Mobile IPv6 domain by requiring that the session be authorized. This document specifies how to accomplish this using the Diameter protocol.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc7156>.

Copyright Notice

Copyright (c) 2014 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 (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Terminology	3
3. Solution Overview	3
4. Attribute Value Pair Used in This Document	4
4.1. User-Name AVP	5
4.2. PMIPv6-IPv4-Home-Address AVP	5
4.3. MIPv6-Home-Link-Prefix AVP	5
4.4. MIPv6-Feature-Vector AVP	5
5. Example Signaling Flows for Localized Routing Service Authorization	6
6. Security Considerations	9
7. IANA Considerations	10
8. Contributors	10
9. Acknowledgements	10
10. References	10
10.1. Normative References	10
10.2. Informative References	11

1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] allows the Mobile Access Gateway (MAG) to optimize media delivery by locally routing packets from a Mobile Node (MN) to a Correspondent Node (CN) that is locally attached to an access link connected to the same Mobile Access Gateway, avoiding tunneling them to the Mobile Node's Local Mobility Anchor (LMA). This is referred to as "local routing" in RFC 5213 [RFC5213]. However, this mechanism is not applicable to the typical scenarios in which the MN and CN are connected to different MAGs and are registered to the same LMA or different LMAs. [RFC6279] takes those typical scenarios into account and defines the problem statement for PMIPv6 localized routing. Based on the scenarios A11, A12, and A21 described in [RFC6279], [RFC6705] specifies the PMIPv6 localized routing protocol that is used to establish a localized routing path between two Mobile Access Gateways in a PMIPv6 domain.

This document describes Authentication, Authorization, and Accounting (AAA) support using Diameter [RFC6733] for the authorization procedure between the PMIPv6 mobility entities (MAG or LMA) and a AAA server within a Proxy Mobile IPv6 domain for localized routing in the scenarios A11, A12, and A21 described in [RFC6279].

2. Terminology

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. Solution Overview

This document addresses how to provide authorization information to the Mobile Node's MAG or LMA to enable localized routing and resolve the destination MN's MAG by means of interaction between the LMA and the AAA server. Figure 1 shows the reference architecture for Localized Routing Service Authorization. This reference architecture assumes that

- o If the MN and CN belong to different LMAs, the MN and CN should share the same MAG (i.e., scenario A12 described in [RFC6279]), e.g., MN1 and CN2 in Figure 1 are attached to MAG1 and belong to LMA1 and LMA2, respectively. Note that LMA1 and LMA2 in Figure 1 are in the same provider domain (as described in [RFC6279]).
- o If the MN and CN are attached to different MAGs, the MN and CN should belong to the same LMA (i.e., scenario A21 described in [RFC6279]); for example, MN1 and CN3 in Figure 1 are attached to MAG1 and MAG3, respectively, but belong to LMA1.

- o The MN and CN may belong to the same LMA and may be attached to the same MAG (i.e., scenario A11 described in [RFC6279]), e.g., MN1 and CN1 in Figure 1 are both attached to the MAG1 and belong to LMA1.
- o The MAG and LMA support Diameter client functionality.

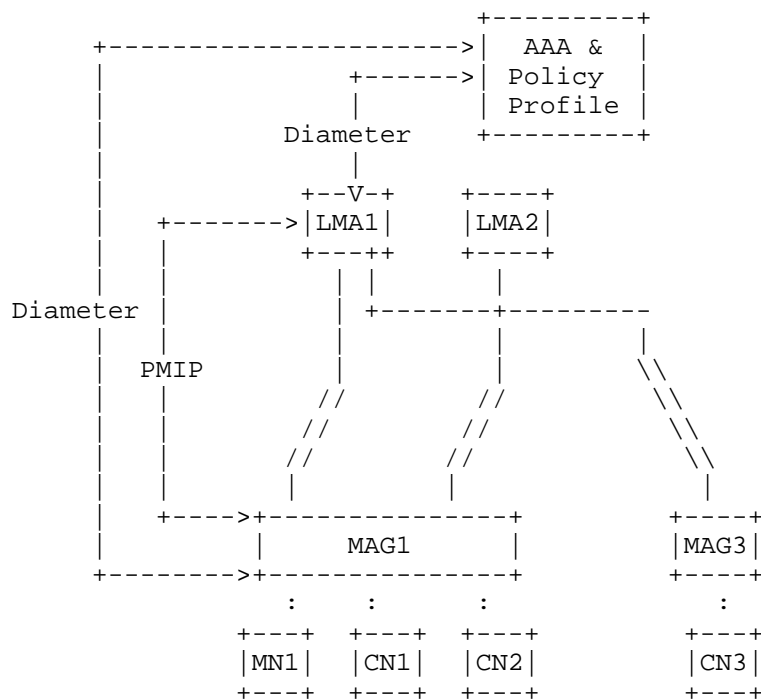


Figure 1: Localized Routing Service Authorization Reference Architecture

The interaction of the MAG and LMA with the AAA server according to the extension specified in this document is used to authorize the localized routing service.

4. Attribute Value Pair Used in This Document

This section describes Attribute Value Pairs (AVPs) and AVP values defined by this specification or reused from existing specifications in a PMIPv6-specific way.

4.1. User-Name AVP

The User-Name AVP (AVP Code 1) is defined in [RFC6733], Section 8.14. This AVP is used to carry the Mobile Node identifier (MN-Identifier) [RFC5213] in the Diameter AA-Request message [RFC7155] sent to the AAA server. The MN-Identifier is defined in PMIPv6 [RFC5213].

4.2. PMIPv6-IPv4-Home-Address AVP

The PMIPv6-IPv4-Home-Address AVP (AVP Code 505) is defined in [RFC5779], Section 5.2. This AVP is used to carry the Mobile Node's IPv4 home address (IPv4-MN-HoA) in the Diameter AA-Request message [RFC7155] sent to the AAA server. The IPv4-MN-HoA is defined in [RFC5844].

4.3. MIP6-Home-Link-Prefix AVP

The MIP6-Home-Link-Prefix AVP (AVP Code 125) is defined in [RFC5779], Section 5.3. This AVP is used to carry the Mobile Node's home network prefix (MN-HNP) in the Diameter AA-Request [RFC7155] sent to the AAA server.

4.4. MIP6-Feature-Vector AVP

The MIP6-Feature-Vector AVP is defined in [RFC5447] and contains a 64-bit flags field used to indicate supported capabilities to the AAA server. This document allocates a new capability flag bit according to the IANA rules in RFC 5447 [RFC5447].

INTER_MAG_ROUTING_SUPPORTED (0x0002000000000000)

When set, this flag indicates support or authorization of Direct routing of IP packets between MNs anchored to different MAGs without involving any LMA.

During the network access authentication and authorization procedure [RFC5779], this flag is set by the MAG or LMA in the MIP6-Feature-Vector AVP included in the request to indicate to the home AAA server (HAAA) that inter-MAG direct routing may be provided to the mobile node identified by the User-Name AVP. By setting the INTER_MAG_ROUTING_SUPPORTED flag in the response, the HAAA indicates to the MAG or LMA that direct routing of IP packets between this mobile node and another node anchored to a different MAG is authorized. The MAG and the LMA set also the INTER_MAG_ROUTING_SUPPORTED flag of the MIP6-Feature-Vector AVP in AA-R sent to the HAAA for requesting authorization of inter-MAG direct routing between the mobile nodes identified in the request by two distinct instances of the User-Name AVP. If this bit is set in

the returned MIP6-Feature-Vector AVP, the HAAA authorizes direct routing of packets between MNs anchored to different MAGs. When the `INTER_MAG_ROUTING_SUPPORTED` flag is cleared, either in request or response, it indicates that the procedures related to authorization of localized routing between MNs anchored to different MAGs is not supported or not authorized. MAG and LMA compliant to this specification MUST support this policy feature on a per-MN and per-subscription basis.

5. Example Signaling Flows for Localized Routing Service Authorization

Localized Routing Service Authorization can happen during the network access authentication procedure [RFC5779] before localized routing is initialized. In this case, the preauthorized pairs of LMA / prefix sets can be downloaded to Proxy Mobile IPv6 entities during the procedure from [RFC5779]. Localized routing can be initiated once the destination of a received packet matches one or more of the prefixes received during the procedure from [RFC5779].

Figure 2 shows an example scenario in which MAG1 acts as a Diameter client, processing the data packet from MN1 to MN2 and requesting authorization of localized routing (i.e., MAG-Initiated LR authorization). In this example scenario, MN1 and MN2 are attached to the same MAG and anchored to the different LMAs (i.e., scenario A12 described in [RFC6279]). In this case, MAG1 knows that MN2 belongs to a different LMA (which can be determined by looking up the binding cache entries corresponding to MN1 and MN2 and comparing the addresses of LMA1 and LMA2). In order to set up a localized routing path with MAG2, MAG1 acts as Diameter client and sends an AA-Request message to the AAA server. The message contains an instance of the MIP6-Feature-Vector (MFV) AVP [RFC5447] with the `LOCAL_MAG_ROUTING_SUPPORTED` bit ([RFC5779], Section 5.5) set, two instances of the User-Name AVP [RFC6733] containing the identifiers of MN1 and MN2. In addition, the message may contain either:

- an instance of the MIP6-Home-Link-Prefix AVP [RFC5779] carrying the MN1's IPv4 address;
- an instance of the PMIPv6-IPv4-Home-Address AVP [RFC5779] carrying the MN1's home network prefix (MN-HNP).

The AAA server authorizes the localized routing service by checking if MN1 and MN2 are allowed to use localized routing. If so, the AAA server responds with a AAA message encapsulating an instance of the MIP6-Feature-Vector (MFV) AVP [RFC5447] with the `LOCAL_MAG_ROUTING_SUPPORTED` bit ([RFC5779], Section 5.5) set indicating that direct routing of IP packets between MNs anchored to the same MAG is authorized. MAG1 then knows that the localized

routing between MN1 and MN2 is allowed. Then, MAG1 sends the Request messages respectively to LMA1 and LMA2. The request message is the Localized Routing Initialization (LRI) message in Figure 2 and belongs to the Initial phase of the localized routing. LMA1 and LMA2 respond to MAG1 using the Localized Routing Acknowledge message (LRA in Figure 2) in accordance with [RFC6705].

In case of LRA_WAIT_TIME expiration [RFC6705], MAG1 should ask for authorization of localized routing again according to the procedure described above before the LRI is retransmitted up to a maximum of LRI_RETRIES.

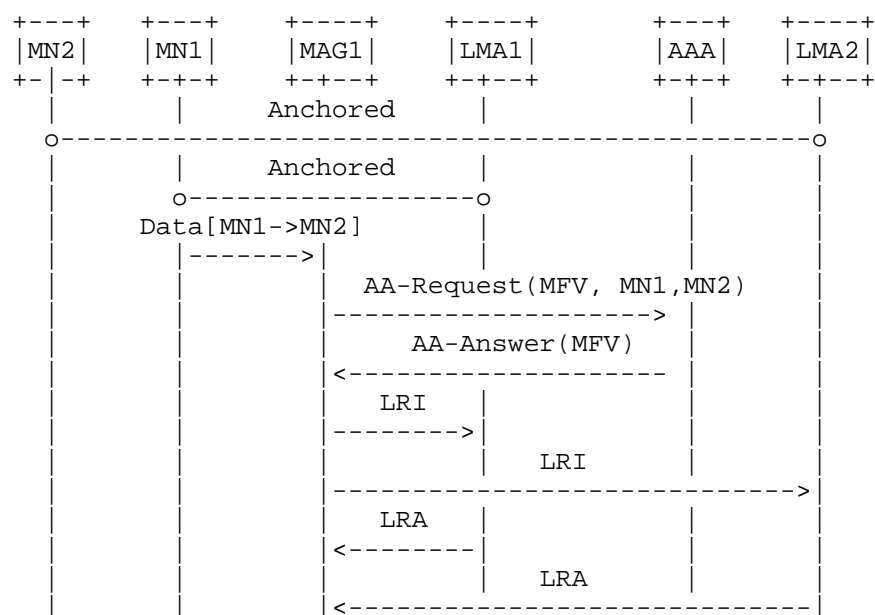


Figure 2: MAG-Initiated Localized Routing Authorization in A12

Figure 3 shows the second example scenario, in which LMA1 acts as a Diameter client, processing the data packet from MN2 to MN1 and requesting the authorization of localized routing. In this scenario, MN1 and MN2 are attached to a different MAG and anchored to the same LMA (i.e., A21 described in [RFC6279]), LMA knows that MN1 and MN2 belong to the same LMA (which can be determined by looking up the binding cache entries corresponding to MN1 and MN2 and comparing the addresses of the LMA corresponding to MN1 and LMA corresponding to MN2). In contrast with the signaling flow shown in Figure 2, it is LMA1 instead of MAG1 that initiates the setup of the localized routing path.

The Diameter client in LMA1 sends an AA-Request message to the AAA server. The message contains an instance of the MIP6-Feature-Vector (MFV) AVP [RFC5447] with the INTER_MAG_ROUTING_SUPPORTED bit (Section 4.5) set indicating direct routing of IP packets between MNs anchored to different MAGs is supported and two instances of the User-Name AVP [RFC6733] containing identifiers of MN1 and MN2. The AAA server authorizes the localized routing service by checking if MN1 and MN2 are allowed to use localized routing. If so, the AAA server responds with an AA-Answer message encapsulating an instance of the MIP6-Feature-Vector (MFV) AVP [RFC5447] with the INTER_MAG_ROUTING_SUPPORTED bit (Section 4.5) set indicating that direct routing of IP packets between MNs anchored to different MAGs is authorized. LMA1 then knows the localized routing is allowed. In a successful case, LMA1 responds to MAG1 in accordance with [RFC6705].

In the case of LRA_WAIT_TIME expiration [RFC6705], LMA1 should ask for authorization of localized routing again according to the procedure described above before the LRI is retransmitted up to a maximum of LRI_RETRIES.

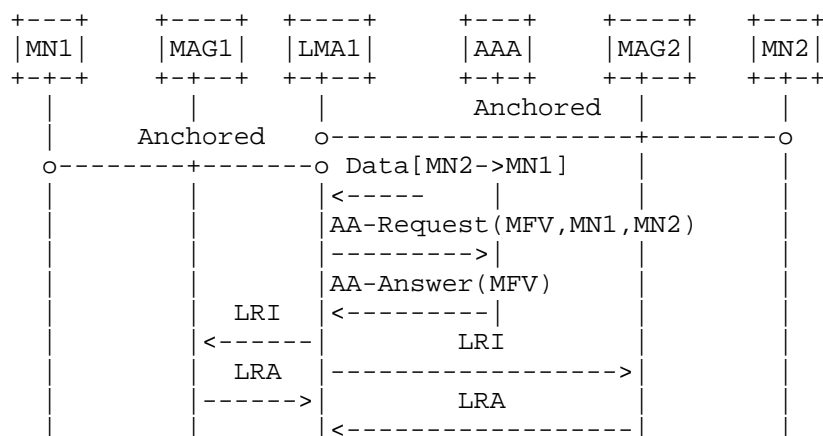


Figure 3: LMA-Initiated Localized Routing Authorization in A21

Figure 4 shows another example scenario, in which LMA1 acts as a Diameter client, processing the data packet from MN2 to MN1 and requesting the authorization of localized routing. In this scenario, MN1 and MN2 are attached to the same MAG and anchored to the same LMA (i.e., All described in [RFC6279]), the LMA knows that MN1 and MN2 belong to the same LMA (which can be determined by looking up the binding cache entries corresponding to MN1 and MN2 and comparing the addresses of LMA corresponding to MN1 and LMA corresponding to MN2).

The Diameter client in LMA1 sends an AA-Request message to the AAA server. The message contains an instance of the MIP6-Feature-Vector AVP [RFC5447] with the LOCAL_MAG_ROUTING_SUPPORTED bit set and two instances of the User-Name AVP [RFC6733] containing the identifiers MN1 and MN2. The AAA server authorizes the localized routing service by checking if MN1 and MN2 are allowed to use localized routing. If so, the AAA server responds with an AA-Answer message encapsulating an instance of the MIP6-Feature-Vector (MFV) AVP [RFC5447] with the LOCAL_MAG_ROUTING_SUPPORTED bit ([RFC5779], Section 5.5) set indicating that direct routing of IP packets between MNs anchored to the same MAG is authorized. LMA1 then knows the localized routing is allowed and responds to MAG1 for localized routing in accordance with [RFC6705].

In the case of LRA_WAIT_TIME expiration [RFC6705], LMA1 should ask for authorization of localized routing again according to the procedure described above before the LRI is retransmitted up to a maximum of LRI_RETRIES.

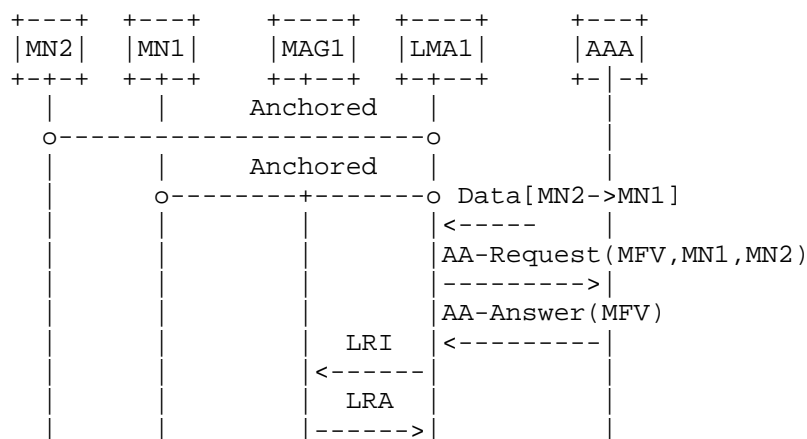


Figure 4: LMA-Initiated Localized Routing Authorization in All

6. Security Considerations

The security considerations for the Diameter Network Access Server Requirements (NASREQ) [RFC7155] and Diameter Proxy Mobile IPv6 [RFC5779] applications are also applicable to this document.

The service authorization solicited by the MAG or the LMA relies upon the existing trust relationship between the MAG/LMA and the AAA server.

An authorized MAG could, in principle, track the movement of any participating mobile nodes at the level of the MAG to which they are anchored. If such a MAG were compromised, or under the control of a bad actor, then such tracking could represent a privacy breach for the set of tracked mobile nodes. In such a case, the traffic pattern from the compromised MAG might be notable, so monitoring for, e.g., excessive queries from MAGs, might be worthwhile.

7. IANA Considerations

This specification defines a new value in the "Mobility Capability Registry" [RFC5447] for use with the MIP6-Feature-Vector AVP: INTER_MAG_ROUTING_SUPPORTED (see Section 4.4).

8. Contributors

Paulo Loureiro, Jinwei Xia and Yungui Wang all contributed to early versions of this document.

9. Acknowledgements

The authors would like to thank Lionel Morand, Marco Liebsch, Carlos Jesus Bernardos Cano, Dan Romascanu, Elwyn Davies, Basavaraj Patil, Ralph Droms, Stephen Farrel, Robert Sparks, Benoit Claise, and Abhay Roy for their valuable comments and suggestions on this document.

10. References

10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5447] Korhonen, J., Bournelle, J., Tschofenig, H., Perkins, C., and K. Chowdhury, "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction", RFC 5447, February 2009.
- [RFC5779] Korhonen, J., Bournelle, J., Chowdhury, K., Muhanna, A., and U. Meyer, "Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server", RFC 5779, February 2010.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

- [RFC6705] Krishnan, S., Koodli, R., Loureiro, P., Wu, Q., and A. Dutta, "Localized Routing for Proxy Mobile IPv6", RFC 6705, September 2012.
- [RFC6733] Fajardo, V., Arkko, J., Loughney, J., and G. Zorn, "Diameter Base Protocol", RFC 6733, October 2012.
- [RFC7155] Zorn, G., Ed., "Diameter Network Access Server Application", RFC 7155, April 2014.

10.2. Informative References

- [RFC6279] Liebsch, M., Jeong, S., and Q. Wu, "Proxy Mobile IPv6 (PMIPv6) Localized Routing Problem Statement", RFC 6279, June 2011.

Authors' Addresses

Glen Zorn
Network Zen
227/358 Thanon Sanphawut
Bang Na, Bangkok 10260
Thailand

Phone: +66 (0) 87-040-4617
EMail: glenzorn@gmail.com

Qin Wu
Huawei Technologies Co., Ltd.
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012
China

Phone: +86-25-56623633
EMail: bill.wu@huawei.com

Jouni Korhonen
Broadcom
Porkkalankatu 24
FIN-00180 Helsinki
Finland

EMail: jouni.nospam@gmail.com

