

DIME Working Group
Internet-Draft
Expires: January 29, 2009

T. Tsou
Huawei
V. Fajardo
TARI
J. Korhonen
TeliaSonera
T. Asveren
Sonus
July 29, 2008

Diameter Routing Extensions
draft-tsou-dime-base-routing-ext-04

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of 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 January 29, 2009.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

This document describes two(2) extensions to the current diameter routing scheme. The first extension describes an explicit routing mechanism that MAY be employed by Diameter nodes to allow specific stateful Diameter proxies to remain in the path of all messages exchanges constituting a Diameter session. The second extension describes a realm based redirection scheme as an alternative to host based redirection described in [[RFC3588](#)].

Table of Contents

1.	Introduction	3
1.1.	Diameter Explicit Routing	3
1.2.	Workarounds	5
1.2.1.	Consistent Next-Hop Routing	5
1.2.2.	Service Access Point Proxying	5
2.	Terminology	9
3.	Diameter Explicit Routing (ER)	10
3.1.	Originating a request (ER-Originator)	10
3.2.	Relaying and Proxying Requests (ER-Proxy)	12
3.3.	Receiving Requests (ER-Destination)	13
3.4.	Diameter answer processing	14
3.5.	Failover and Failback Considerations	14
3.6.	Explicit-Path-Record AVP	15
3.6.1.	Proxy-Realm AVP	15
3.7.	Explicit-Path AVP	16
3.8.	Error Handling	16
3.9.	Example Message Flows	17
4.	Redirect Realm Indication	20
4.1.	Redirect-Realm AVP	21
5.	RADIUS/Diameter Protocol Interactions	22
6.	IANA Considerations	23
7.	Security Considerations	24
8.	Acknowledgements	25
9.	Normative References	26
	Authors' Addresses	27
	Intellectual Property and Copyright Statements	28

1. Introduction

The following sections provides an overview of the routing extensions proposed in this document.

1.1. Diameter Explicit Routing

In [[RFC3588](#)], routing of request messages from source to the destination is based solely on the routing decision made by each node along the path. In a topology where multiple paths are possible from source to destination, it is not guaranteed that all messages constituting a session will take the same path. For a proxy node residing along a path that maintains stateful information for a session, it is desirable that it remains in the routing path of all message exchanges of that a session.

In general, a session that is comprised of multiple message exchanges and requires intermediary proxy functions will require explicit routing for all request messages within that session. An example of a stateful proxies are in the WLAN 3GPP IP access [[TS23.234](#)]. The WLAN Access Network (WLAN AN) can use Diameter EAP with the 3GPP AAA server or proxy for authentication & authorization. In the roaming case, the WLAN AN is communicating with a 3GPP AAA Proxy in the visited network over the Wa or the Wm reference points. The 3GPP AAA proxy is then connected to the 3GPP Server in the home network over the Wd reference point. The 3GPP AAA Proxy among its many functions will enforce local policies on access based on agreement with the 3GPP Home Network and with the WLAN operator either over the Wa or the Wg references points. It will also send per user charging information for the session to the Offline Charging system. This necessitates that the proxy maintains the session state information and hence it needs to remain in-path for the entire session.

Given that there are cases where a stateful proxies need to be in the routing path of a session, a generic description of the problem is shown in Figure 1. In this scenario there is a relay in the visited network (Relay1) and two(2) proxies in the home network (Proxy1 and Proxy2). Relay1 is connected to Proxy1 and Proxy2 for scalability and/or redundancy. If a session is composed of several request/answer exchanges it is possible that each request of the session takes different paths towards the Home Server. As an example, if Relay1 can route messages via Proxy1 or Proxy2 based on some policy independent of the session then the first message of the session can take the path Client->Relay1->Proxy1->Home Server while subsequent message can take the path Client->Relay1->Proxy2->Home Server. In this case if Proxy1 is stateful then it expects to process not only the first message but subsequent request as well.

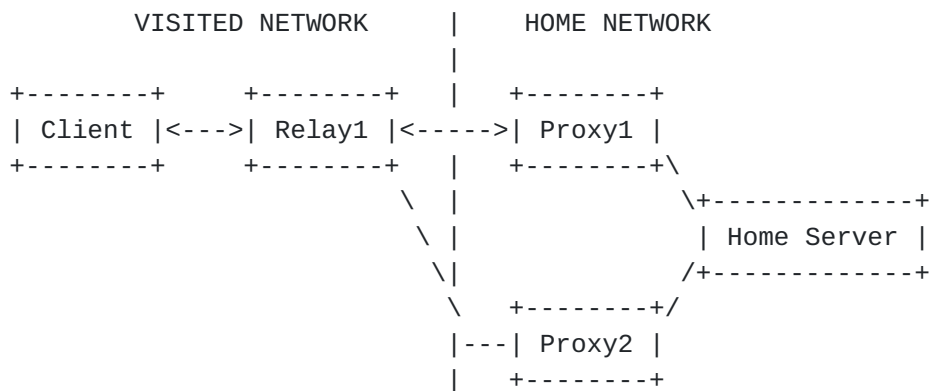


Figure 1: Generic Stateful Proxy Problem

In larger deployments, the issue can be aggravated when there are a greater number of proxy nodes in both visited and home networks in Figure 1. Further escalation of the problem occurs if the deployment adds stateless relays preceding any of the proxy nodes in Figure 1.

In [RFC3588], it is possible to use static routing between the source and the proxy to ensure all message exchanges traverses the proxy in question. However, static routing in general, introduces many limitations.

- o Static routing implies that all messages, regardless of session, will have to traverse the same proxy. This introduces a single point of failure in the routing path and affects any and all sessions regardless of whether the session is of interest to the proxy.
- o It compromises failover procedure in the node adjacent to the proxy and preceding it in the request forwarding path. This becomes apparent if the adjacent node explicitly and statically routes only towards the proxy.
- o In the event of more complex topologies where multiple proxies are traversed between source and destination, the administrative burden of static configuration along the path may be considerable.
- o No provision for load balancing as all the nodes in the path will be subjected to static routing.

Considering these limitations, an alternative and more dynamic method of establishing an explicit route is proposed.

1.2. Workarounds

This section describes two methods, which can be used to provide a workaround for the problem described above. These methods are relying on existing Diameter base protocol functionality and should not be considered as a normative part of this document.

1.2.1. Consistent Next-Hop Routing

If all entities in the signaling path are session stateful, they can select the same next-hop entity, when routing requests for a particular session.

It should be noted that Diameter Base Protocol does not mandate that all requests for the same session need to be routed to the same intermediary next-hop, even if a Diameter node has that capability.

1.2.2. Service Access Point Proxying

If a stateful intermediary node wants to stay in the message path during the whole session for a specific service, it may advertise itself as the entity providing that service.

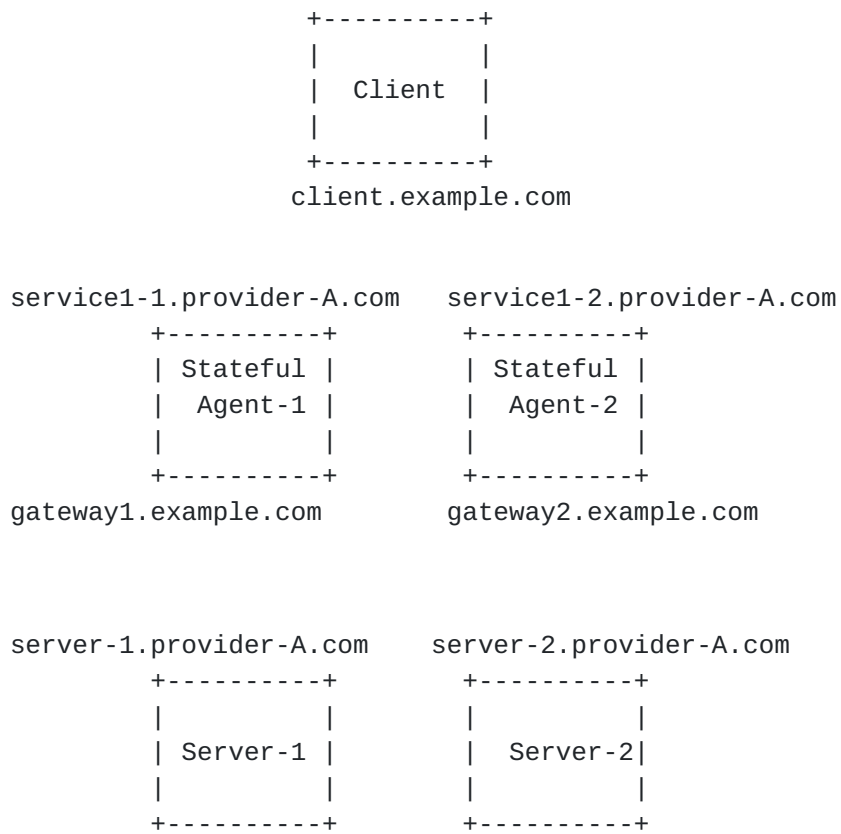


Figure 2: Addresses used for Service Access Point Proxying

An intermediary, proxying the Service Access Point would terminate the session from client side and initiate a corresponding session to the server. Values for certain fields could be reused for this second session depending on the service message flow. For example, the same Session-Id AVP value could be used for both of these sessions. If the message flow does not contain requests from server to client, Origin-Host AVP value could be directly copied as well.

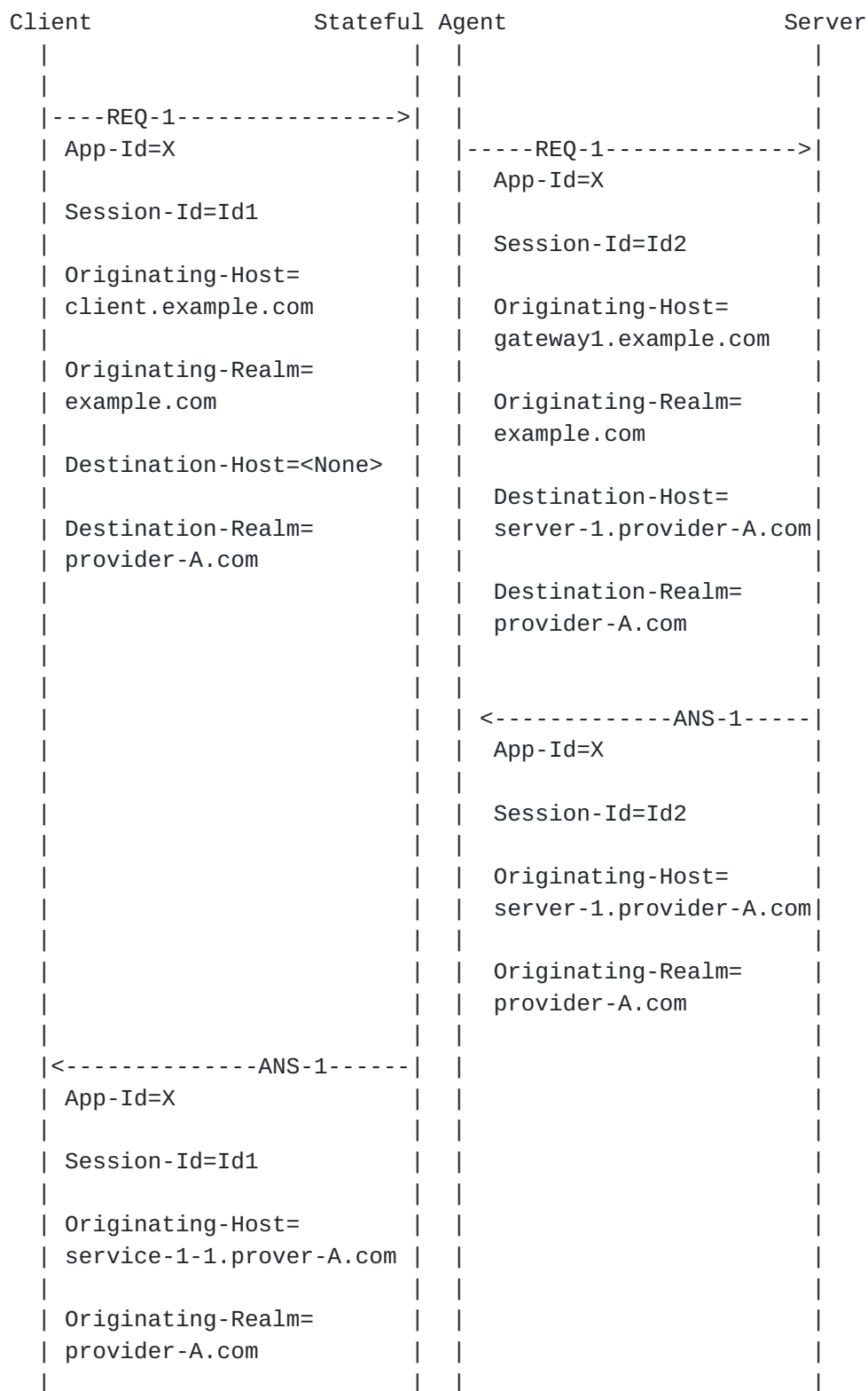


Figure 3: Messages used for Service Access Point Proxying

This approach requires that stateful agent provides service access point proxying for all service/domain combinations by advertising a different Diameter identity and may not scale well if the number of such combinations is high. Stateful agent should perform all Diameter endpoint procedures, e.g. duplicate detection. Furthermore, if end-to-end security is desired, either the stateful agent needs to have enough logic to proxy the end-to-end security service as well or this model should not be used.

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](#)].

The following terms defines the functionality and participants of the routing extensions described in this document.

ER

Diameter explicit routing scheme.

ER-Originator

A diameter node initiating a session and sending the requests. The originator can be any diameter node sending a request, i.e. client, server or proxy capable of initiating sessions. The originator is also capable of participating in explicit routing.

AAA Relays

Diameter nodes in between the proxies, originator or receiver. These nodes represent existing diameter agents and proxies that do not participate in an ER and do not recognize Explicit-Path AVPs.

ER-Proxy

Diameter proxies participating in an ER and is capable of processing Explicit-Path AVPs.

ER-Destination

Diameter node which will ultimately consume the request sent by an ER-Originator. The receiver is capable of participating in an ER.

3. Diameter Explicit Routing (ER)

This section outlines a Diameter ER mechanism by which ER participants can remain in the path of all request messages for a specific session. A new Explicit-Path AVP has been defined to allow diameter nodes participating in an ER to manipulate the Destination-Host and/or Destination-Realm AVP of request messages.

The following sections describe the extensions to the request routing in [RFC3588] to implement the ER mechanism. The proposed extensions utilized existing routing strategies in [RFC3588] and do not mandate modifications to it. The scheme also differs from existing strict source routing scheme where all hops in the path to have to participate. In the ER mechanism, only diameter nodes interested in participating in the ER scheme will be involved in it.

3.1. Originating a request (ER-Originator)

A diameter node acting as an ER-Originator for a particular session MUST maintain a local cache which enumerates all the diameter identities of the ER-Proxies that the request messages MUST traverse along the path to the ER-Destination. The identity of a diameter node is defined in [RFC3588]. The local cache may also include the nodes realm. The data structure of the cache is left up to the implementation and should persist as part of the session attributes or properties.

A ER-Originator sending request messages MUST add a Explicit-Path AVP to these requests. The contents of the cache SHOULD be used to populate the Explicit-Path AVP where each cached entry is represented by Explicit-Path-Record AVP. ER-Proxies along the path of the request message MUST review the contents of the Explicit-Path AVP and make routing adjustments based on records it contains. An example of the message flow is shown in [Section 3.9](#). Note that the ER-Originator can be any diameter node, i.e. client, server or proxy.

The ER-Proxy identities enumerated in the local cache SHOULD be maintained in the same order as they are traversed along the request routing path from the originator to destination. The same ordering should also exist in the enumeration of Explicit-Path-Records representing each ER-Proxy identity in the Explicit-Path AVP.

The ER-Originator can populate the cache either by pre-configuring its contents or by using the first request message of the session to gather identities of participating ER-Proxies along the routing path. The later scheme is known as Explicit-Path discovery. The contents of the cache can be pre-configured if the ER-Originator has explicit knowledge of the ER-Proxy(ies) the request messages has to traverse

otherwise it can use Explicit-Path discovery. It is recommended that Explicit-Path discovery is used whenever possible since pre-configuration is less flexible by nature.

Explicit-Path discovery can be used if the identities of the ER-Proxies proxies are not known or if there are several ER capable proxies (a cluster of proxies) that can be dynamically chosen based on other routing policies. In Explicit-Path discovery, the cache of the ER-originator is initially empty. When the ER-Originator sends the first request message of a session, the Explicit-Path AVP will contain only a Explicit-Path-Record with the identity and/or the realm of the ER-Originator. The Destination-Host and/or Destination-Realm AVPs of the request message is set to the identity and/or the realm of the ER-Destination respectively as specified in [\[RFC3588\]](#). It should be noted that ER-Originator initial request message routing steps and the Destination-Realm population MAY be affected by the User-Name AVP NAI decoration [\[RFC4282\]](#). The NAI decoration is a form of request message source routing and defines realms that the request message MUST traverse through before routing towards the ER-Destination. Diameter nodes participating to the request message routing must examine and process the User-Name AVP, and modify the Destination-Realm AVP accordingly as long as there are realms left in the decorated NAI. The NAI decoration based source routing does not affect the Explicit-Path discovery as defined in this document.

As the request message is received and processed by an ER-Proxy, the ER-Proxy MUST append a new Explicit-Path-Record containing its own identity and/or realm to the Explicit-Path AVP prior to forwarding the message. Subsequent ER-Proxies along the path that wishes to participate in the ER MUST also append their own Explicit-Path-Record in the same manner ([Section 3.2](#)). When the request reaches the ER-Destination, it MUST append its a new Explicit-Path-Record to the Explicit-Path AVP in a similar manner. The ER-Destination MUST also copy the resulting Explicit-Path AVP to the answer message ([Section 3.3](#)). Once the answer message reaches the ER-Originator, the Explicit-Path AVP will contain several Explicit-Path-Records containing its the ER-Originator identity, the identities of all participating ER-Proxies and the identity of the ER-Destination. The ER-Originator SHOULD then populate its local cache with the contents of the Explicit-Path AVP.

If the answer message does not contain a Explicit-Path AVP or the Result-Code AVP is set to DIAMETER_ER_NOT_AVAILABLE [Section 3.8](#), it is an indication to the ER-Originator that the destination of the request does not support ER and that the ER-Originator SHOULD avoid sending a Explicit-Path AVP in subsequent request messages.

If after performing Explicit-Path discovery and the Explicit-Path AVP

in the answer message contains only the Explicit-Path-Record of the ER-Originator and ER-Destination then this SHOULD be an indication to the ER-Originator that there are no diameter proxies capable of participating in an ER along the path and that the ER-Originator MAY avoid sending a Explicit-Path AVP in subsequent request messages. Certain failover situations MAY cause this indication as described in [Section 3.5](#). In such cases, the situation maybe transient and subsequent Explicit-Path discovery in succeeding sessions may find participating proxies. It is left up to the ER-Originator to decide if subsequent Explicit-Path discovery should be attempted in succeeding sessions.

Once the ER-Originator's local cache has been populated, whether pre-configured or through Explicit-Path discovery, all request messages for the session MUST include the Explicit-Path AVP using the contents of the local cache. The Explicit-Path AVP MUST contain the Explicit-Path-Records of all the nodes enumerated in its cache except its own. The identities enumerated in the Explicit-Path AVP MUST appear in the order they will be traversed in the routing path. The last entry in the Explicit-Path AVP MUST be the Explicit-Path-Record of the ER-Destination. In addition, the value of the Destination-Host and/or Destination-Realm AVPs of the request messages MUST be set to the value of the Proxy-Host and/or Proxy-Realm of the first Explicit-Path-Record AVP present in the Explicit-Path AVP. This ensures that the ER-Originator as well as any AAA relays in between the ER-Originator and the first ER-Proxy will route the message towards the first ER-Proxy as specified in [\[RFC3588\]](#). Subsequent actions taken by the first ER-Proxy upon receipt of the message is described in [Section 3.2](#) and will mimic a similar action.

Answer messages received by the ER-Originator to subsequent request messages after the ER path has been established SHOULD not have a Explicit-Path AVP. Otherwise, this SHOULD be considered a suspect condition that maybe caused by a mis-behaving ER participant. It is left up to the ER-Originator to continue using ER scheme when such condition arises or attempt another Explicit-Path discovery on subsequent sessions.

[3.2](#). Relaying and Proxying Requests (ER-Proxy)

The basic action taken by an ER-Proxy upon receiving a request is to check whether explicit routing is supported in the request and if so, check whether it is already a participant in explicit routing for the said request. Being an existing participant would require the ER-Proxy to pop/remove the Explicit-Path-Record AVP pertaining to itself in the Explicit-Path AVP and then use the next Explicit-Path-Record AVP for subsequent routing. Details of this operation are as follows.

An ER-Proxy is not required to keep local state or cache state regarding the explicit routing procedure. However, it MUST check whether an incoming request contains a Explicit-Path AVP. If an incoming request does not contain a Explicit-Path AVP then it MUST process and forward the request as specified in [\[RFC3588\]](#). If the incoming request contains a Explicit-Path AVP, it MUST check whether its identity is present in the Explicit-Path AVP. Determining whether its identity is present can be done by matching its identity to the Proxy-Host AVPs contained in each Explicit-Path-Record. If its identity is not present and it wishes to participate in explicit routing, it MUST append a new Explicit-Path-Record in the Explicit-Path AVP prior to forwarding the request. The new Explicit-Path-Record MUST be added as the last AVP in the Explicit-Path AVP and MUST contain at the least a Proxy-Host AVP set to the proxies identity. This scenario is part of the Explicit-Path discovery scheme in [Section 3.1](#).

However, if the ER-Proxy does not wish to participate in the ER, it SHOULD not modify the Explicit-Path AVP and simply forward the request as specified in [\[RFC3588\]](#) using the existing value of Destination-Host and/or Destination-Realm AVP. The same scenario applies to non ER-proxies and relays that do not support ER and do not recognize Explicit-Path AVP.

If the identity of the ER-Proxy is present in the Explicit-Path AVP, then it MUST be the first Explicit-Path-Record in the AVP otherwise, this SHOULD be considered an error and an answer message with the e-bit set and the Result-Code set to DIAMETER_INVALID_PROXY_PATH_STACK must be sent back to the ER-Originator [Section 3.8](#). If the identity of the ER-Proxy matches the first Explicit-Path-Record, the ER-Proxy MUST remove this record from Explicit-Path AVP and set the Destination-Host and/or Destination-Realm AVP to the next Explicit-Path-Record present in the Explicit-Path AVP. Setting the Destination-Host and/or Destination-Realm AVP will ensure that the ER-Proxy as well as all AAA relays in between the current ER-Proxy and the next ER-Proxy enumerated in the Explicit-Path AVP will route the message towards the next ER-Proxy. The process of removing the ER-Proxies record is synonymous to removing an entry in a stack represented by the Explicit-Path AVP. Note that in the case of the ER-Destination, the Explicit-Path AVP MUST be empty once its own record is removed [Section 3.3](#). Note also that the behavior specified above applies to a diameter node acting as a relay agent and participates in the ER scheme.

[3.3](#). Receiving Requests (ER-Destination)

A diameter node that locally processes request sent by the ER-Originator [Section 3.1](#) and is able to support ER MUST check for the

presence of a Explicit-Path AVP in the request message. If an incoming request does not contain a Explicit-Path AVP then it is an indication that messages belonging to this session will not use ER. It SHOULD process the request for local consumption and formulate an answer message as specified in [\[RFC3588\]](#). If the incoming request contains a Explicit-Path AVP, it MUST check whether its identity is present in the Explicit-Path AVP. If its identity is not present in the Explicit-Path and it wishes to participate in the ER, it MUST append its a new Explicit-Path-Record in the Explicit-Path AVP. The new Explicit-Path-Record MUST contain at the least a Proxy-Host AVP set to the ER-Destinations identity. The ER-Destination MUST then copy the resulting Explicit-Path AVP in the subsequent answer message. This scenario is part of the proxy path discovery scheme in [Section 3.1](#). However, if the ER-Destination supports ER but does not wish to or cannot participate, it MAY send a Result-Code AVP set to DIAMETER_ER_NOT_AVAILABLE as defined in [Section 3.8](#). The ER-Destination SHOULD not include any Explicit-Path AVP in the subsequent answer. The same scenario applies to ER-destinations that does not support ER and do not recognize Explicit-Path AVP and is a hint to the ER-Originator that the destination does not support ER.

If the identity of the ER-Destination matches a record in the Explicit-Path AVP, then it MUST be the only Explicit-Path-Record present in the Explicit-Path AVP otherwise, this SHOULD be considered an error and an answer message with the e-bit set and the Result-Code set to DIAMETER_INVALID_PROXY_PATH_STACK MUST be sent back to the ER-Originator [Section 3.8](#). If the identity of the of the ER-Destination matches the only existing Explicit-Path-Record, then this is an indication of a successful ER. The ER-Destination SHOULD NOT copy the Explicit-Path AVP into the subsequent answer message.

[3.4.](#) Diameter answer processing

The diameter nodes participating in ER do not require special handling or routing of answer messages. Answer messages SHOULD be processed normally as specified in [\[RFC3588\]](#). However, a diameter node acting an ER-Destination MUST formulate a proper Explicit-Path AVP in answer messages as described in [Section 3.3](#).

[3.5.](#) Failover and Failback Considerations

In the event that failover occurs in a diameter node preceding an ER-Proxy and the ER-Proxy is a likely target of a Explicit-Path discovery, it is possible that the Explicit-Path AVP will not include the targeted ER-Proxy if the initial request involved in the Explicit-Path discovery is re-routed away from the ER-Proxy. In the case that there is no other ER-Proxy along the re-routed path, it is also possible that the resulting answer message will have a Explicit-

Path AVP that contains only the Explicit-Route-Record of the ER-Originator and the ER-Destination indicating that there is no ER support found in diameter nodes along the path. It is left to the ER-Originator to continue with processing of the request without ER support or abandon the transaction. The ER-Originator SHOULD not attempt to perform Explicit-Path discovery in subsequent request messages of the session in such cases so as to protect against fallback conditions where an ER-Proxy may suddenly appear in the path and attempts to add a new Explicit-Path-Record for request messages other than the initial request. However, based on certain policy, it is also possible for the ER-Originator to attempt Explicit-Path discovery in subsequent sessions.

If a failover occurs in diameter node preceding an ER-Proxy when the ER path is already established, it is possible that an `DIAMETER_UNABLE_TO_DELIVER` error will be received by the ER-Originator if there no other alternative path towards the ER-proxy. In such a case, it is left to the ER-Originator to handle the error as specified in diameter application or in [\[RFC3588\]](#).

3.6. Explicit-Path-Record AVP

The Explicit-Path-Record AVP (AVP Code TBD) is of type Group. The identity added in this AVP MUST be the same as the one advertised by a diameter node in the Origin-Host during the Capabilities Exchange messages. Proxy-Host is as defined in [\[RFC3588\]](#).

```
Explicit-Path-Record ::= < AVP Header: TBD >
                        { Proxy-Host }
                        [ Proxy-Realm ]
                        * [ AVP ]
```

Figure 4: Explicit-Path-Record AVP

This AVP MAY be sent with the default AVP flags settings defined in Sec 4.1 of [\[RFC3588\]](#) where 'M' bit MUST be set and 'V' bit MUST NOT be set. If the 'M' bit is set then the recommendations in Sec 4.1 of [\[RFC3588\]](#) regarding preservation of interoperability SHOULD be followed.

3.6.1. Proxy-Realm AVP

The Proxy-Realm AVP (AVP Code TBD) is of type DiameterIdentity, and contains the realm the ER node inserting the record. This AVP is used in conjunction with Proxy-Host AVP.

It is recommended that the Proxy-Host AVP is present and used to uniquely identify an ER-Proxy within the AAA realm being traversed by

a request. Otherwise, ER will need to rely on realm routing. Realm routing would require a well known topology for ER scheme to work properly since the hostname of the proxy is not specified. In such a case, the Proxy-Realm AVP MUST be present and is used to identify the ER-Proxy of the realm.

When a Proxy-Host AVP is present in the Explicit-Path-Record AVP, the realm name included in the hostname MUST correspond to the identity present of the Proxy-Realm AVP.

3.7. Explicit-Path AVP

The Explicit-Path AVP (AVP Code TBD) is of type Group. This AVP SHOULD be present in all request and answer messages performing ER.

```
Explicit-Path ::= < AVP Header: XXX >
                1* [ Explicit-Path-Record ]
                *  [ AVP ]
```

Figure 5: Explicit-Path AVP

This AVP MAY be sent with the default AVP flags settings defined in Sec 4.1 of [\[RFC3588\]](#) where 'M' bit MUST be set and 'V' bit MUST NOT be set. If the 'M' bit is set then the recommendations in Sec 4.1 of [\[RFC3588\]](#) regarding preservation of interoperability SHOULD be followed.

3.8. Error Handling

The following are error conditions that are possible with ER. These errors fall within the Protocol Error category SHOULD be treated on a per-hop basis, and Diameter proxies MAY attempt to correct the error, if it is possible. Note that these and only these errors MUST only be used in answer messages whose 'E' bit is set.

DIAMETER_INVALID_PROXY_PATH_STACK

A request message received by an ER-Proxy or ER-Destination after an ER path has been established has the first or only Explicit-Path-Record AVP not matching the ER-Proxy or the ER-Destinations identity. The same error applies to ER-Destinations receiving a Explicit-Path-AVP containing more than one Explicit-Path-Record or a Explicit-Path-AVP with only on Explicit-Path-Record not matching its own identity.

This error value SHOULD be considered a protocol failure. Diameter nodes sending this error indication MUST have the e-bit set in the answer message and MUST conform to [Section 7.2](#) of

[[RFC3588](#)].

DIAMETER_ER_NOT_AVAILABLE

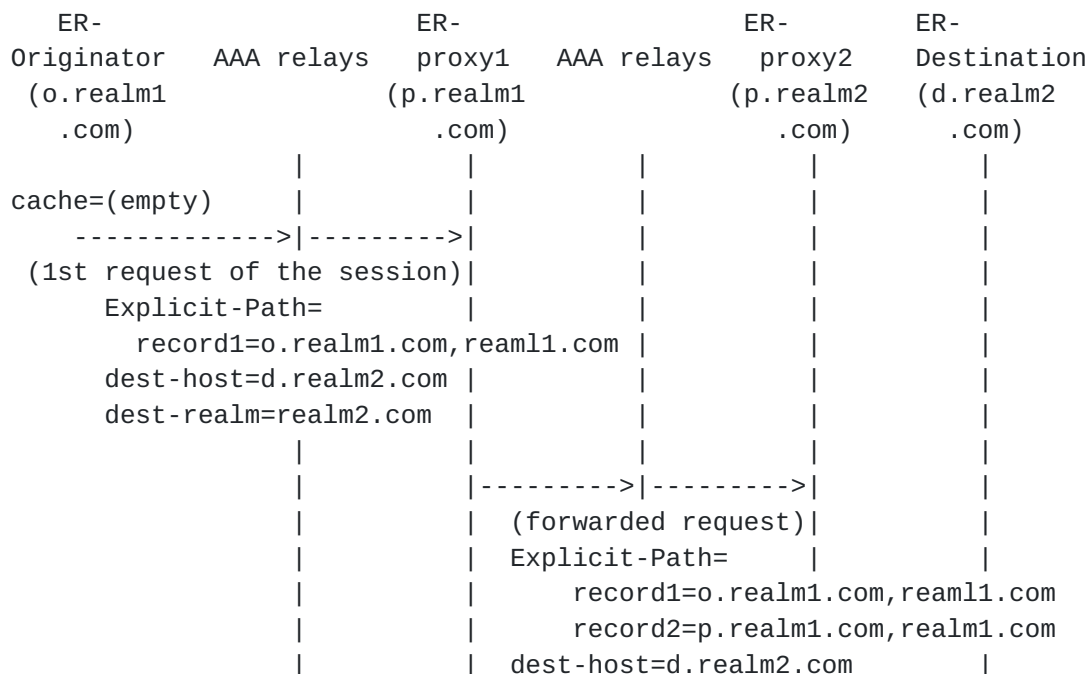
An ER-Destination which supports ER routing but is unable to comply for unknown reasons MAY send an answer message with the Result-Code AVP set to this error code. This error value SHOULD be considered a transient failure indicating that subsequent ER attempts MAY succeed.

3.9. Example Message Flows

The example presented here illustrates the flow of Diameter messages with the typical attributes present in the ER scenario.

The ER-Originator in the example in below shows the use of Explicit-Path discovery with the first request. However, the ER-Originator may also use a pre-configure cache. The ER-Originator can be any diameter node sending a request, i.e. client, server or proxy. In this scenario, the local cache of the ER-Originator is initially empty.

The AAA relays in between the ER-Proxies, ER-Originator and ER-Destination may or may not be present and are shown here to depict routing paths that the requests may take prior to being processed by nodes participating in the ER scheme. The AAA relays also depicts existing diameter relays or proxies that do not recognize Explicit-Path AVPs and therefore do not participate in ER.



			dest-realm=realm2.com		
				----->	
				(forwarded request)	
				Explicit-Path=	
				record1=o.realm1.com,	
				realm1.com	
				record2=p.realm1.com,	
				realm1.com	
				record3=p.realm2.com,	
				realm2.com	
				dest-host=d.realm2.com	
				dest-realm=realm2.com	
cache=	<-----	<-----	<-----	<-----	
record1=o.realm1.com, realm1.com			(answer)		
record2=p.realm1.com, realm1.com			Explicit-Path=		
record3=p.realm2.com, realm2.com			record1=o.realm1.com, realm1.com		
record4=d.realm2.com, realm2.com			record2=p.realm1.com, realm1.com		
			record3=p.realm2.com, realm2.com		
			record4=d.realm2.com, realm2.com		
Note: An originator pre-configuring it's local cache can skip the exchange above and send the initial request as shown below					
-----> ----->					
(subsequent request of the session)					
Explicit-Path=					
record1=p.realm1.com, realm1.com					
record2=p.realm2.com, realm2.com					
record3=d.realm2.com, realm2.com					
dest-host=p.realm1.com					
dest-realm=realm1.com					
			-----> ----->		
			(forwarded request)		
			Explicit-Path=		
			record1=p.realm2.com, realm2.com		
			record2=d.realm2.com, realm2.com		
			dest-host=p.reaml2.com		
			dest-realm=realm2.com		
				----->	
			(forwarded request)		
			Explicit-Path		
			record1=d.realm2.com,		
			realm2.com		
			dest-host=d.realm2.com		

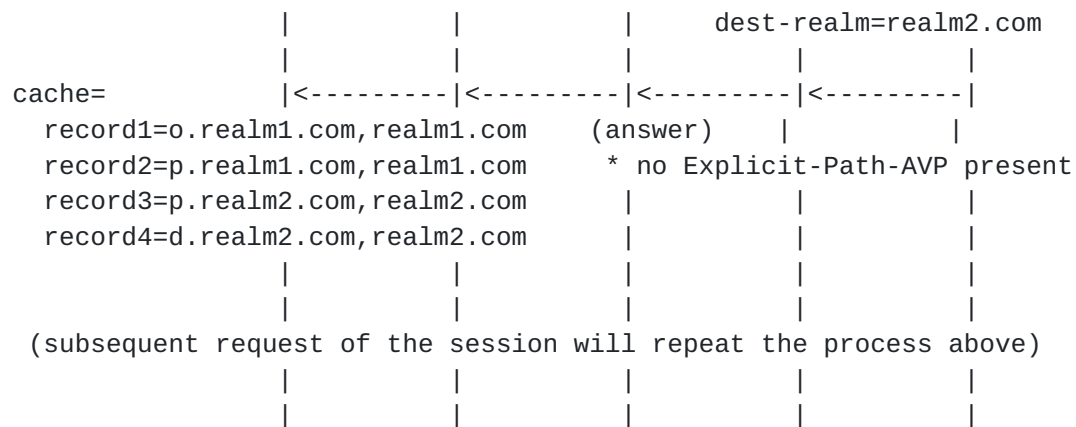


Figure 6: Example ER Message Flow

4. Redirect Realm Indication

A redirect agent MAY add a Redirect-Realm AVP to the redirect indication sent to the client. If the redirect agent has added a Redirect-Realm AVP to the indication, it MAY not add any Redirect-Host AVP to it.

The client receiving a redirect indication with a Redirect-Realm AVP MUST reconstruct the request using Redirect-Realm AVP as the Destination-Realm AVP. If one (or more) Redirect-Host AVP(s) are present in the indication, the client uses one of them as the Destination-Host AVP in the reconstructed request. The processing of this request at any Diameter node along the path will follow the Request forwarding/routing procedures described in [RFC3588], i.e. if the value in the Destination-Host AVP resolves to a peer to which the node can directly communicate, the request is forwarded to the peer, else the Destination-Realm AVP is used for request routing.

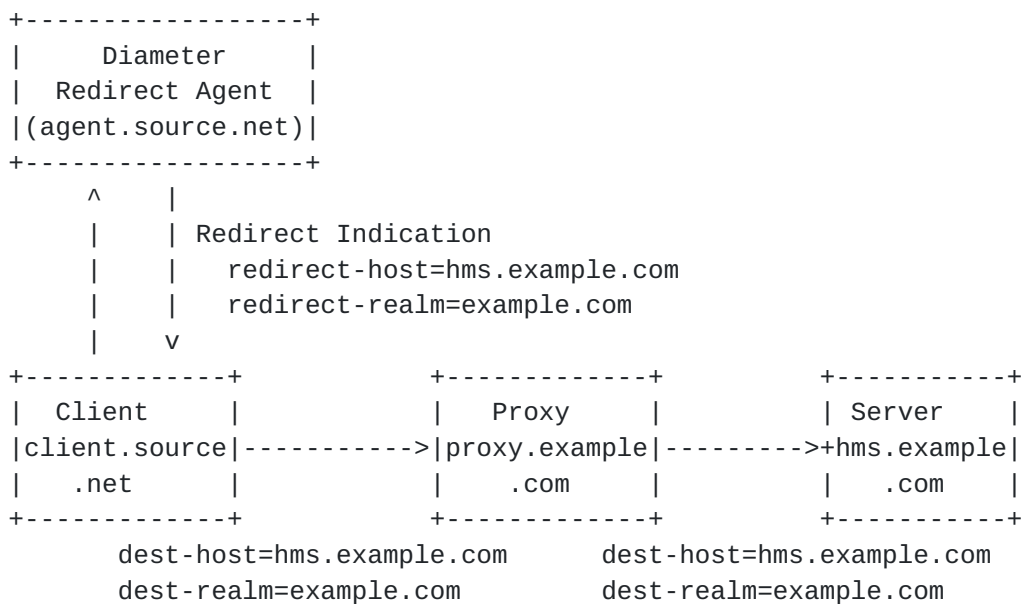


Figure 7: Redirection using host and realm information

In the figure above, the Redirect agent in realm source.net replies to the client request with a redirect indication having a Redirect-Host AVP set to "hms.example.com" and Redirect-Realm AVP set to "example.com". The client reconstructs the request and sets Destination-Host and/or Destination-Realm to the value of the Redirect-Host and/or Redirect-Realm AVP respectively. Since the client has no direct peer connection with the server, request routing is performed using realm routes [RFC3588]. In the scenario above, the request is routed to an in-bound proxy of the realm example.com. Since the proxy can directly communicate with the server, it forwards

the request using the Destination-Host AVP which was set to the servers identity (hms.example.com).

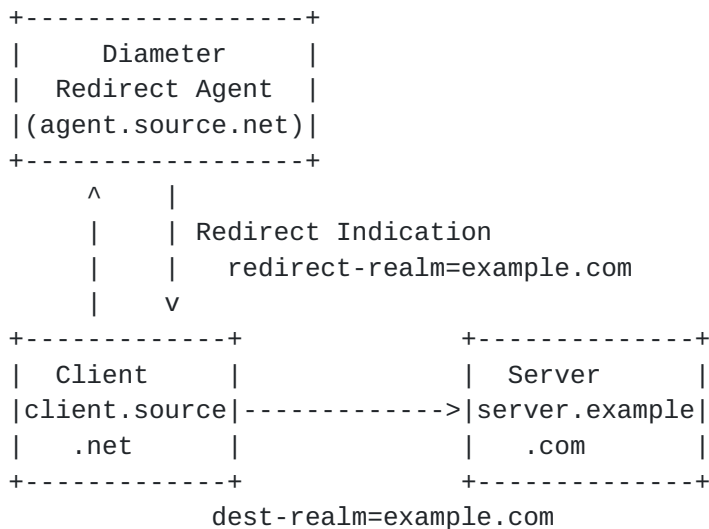


Figure 8: Redirection using only realm information

In the figure above, the Redirect agent in realm source.net replies to the client request with a redirect indication having Redirect-Realm AVP set to "example.com". The client reconstructs the request and sets the Destination-Realm AVP to the value of the Redirect-Realm AVP. The client follows realm routing procedures in [\[RFC3588\]](#) using the Destination-Realm AVP and routes the request to a server in the realm "example.com". Once the server receives the request, it can process it for local consumption since it is responsible for diameter request for that realm ([Section 2.7 of \[RFC3588\]](#)).

4.1. Redirect-Realm AVP

The Redirect-Realm AVP (AVP Code XXX_3) is of type DiameterIdentity. Only one instance of this AVP MAY be present if the answer message e-bit set and the Result-Code AVP is set to DIAMETER_REDIRECT_INDICATION.

5. RADIUS/Diameter Protocol Interactions

No actions need to be taken with regards to RADIUS/Diameter interaction. The routing extensions introduced by this document is transparent to any translation gateway and relevant only to diameter routing. The assumption is that if there is a RADIUS proxy chain between Diameter translation agents the route between translation agents remains stable during the session and does not cause an invalidation of the proxy path stack.

6. IANA Considerations

IANA is to assign new AVP codes for the following AVPs discussed in this document: Explicit-Path, Explicit-Path-Record and Proxy-Realm AVP.

7. Security Considerations

This document does not contain a security protocol; it describes extensions to the existing Diameter protocol. All security issues of DIAMETER protocol must be considered in implementing this specification. These extension does not add any unique concerns.

8. Acknowledgements

The author gratefully acknowledges the contributions of: Avi Lior, Tolga Asveren, Tony Zhang, Rajith R.

9. 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.
- [TS23.234] 3GPP, "3GPP system to Wireless Local Area Network (WLAN) interworking; System description", 3GPP TS 23.234 Version 7.4.0 2006.

Authors' Addresses

Tina Tsou
Huawei Technologies
Bantian, Longgang District
Shenzhen, 518129
China

Phone:
Email: tena@huawei.com

Victor Fajardo
Toshiba America Research, Inc.
1 Telcordia Drive
Piscataway, NJ 08854
USA

Phone: +1 732 699 5368
Email: vfajardo@tari.toshiba.com

Jouni Korhonen
TeliaSonera Corporation.
P.O.Box 970
FIN-00051 Sonera
Finland

Email: jouni.korhonen@teliasonera.com

Tolga Asveren
Sonus Networks
4400 Route 9 South
Freehold, NJ 07728
USA

Email: tasveren@sonusnet.com

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

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.

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, THE IETF TRUST 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.

Intellectual Property

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.

Acknowledgment

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

