Diameter Maintenance and Extensions   M. Jones
(DIME)   June 22, 2012
Internet-Draft
Intended status: Standards Track
Expires: December 24, 2012

Diameter Group Signaling
draft-ietf-dime-group-signaling-00.txt

Abstract

In large network deployments, a single Diameter peer can support over a million concurrent Diameter sessions. Recent use cases have revealed the need for Diameter peers to apply the same operation to a large group of Diameter sessions concurrently. The Diameter base protocol commands operate on a single session so these use cases could result in many thousands of command exchanges to enforce the same operation on each session in the group. In order to reduce signaling, it would be desirable to enable bulk operations on all (or part of) the sessions managed by a Diameter peer using a single or a few command exchanges. This document specifies the Diameter protocol extensions to achieve this signaling optimization.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

In large network deployments, a single Diameter peer can support over a million concurrent Diameter sessions. Recent use cases have revealed the need for Diameter peers to apply the same operation to a large group of Diameter sessions concurrently. For example, a policy decision point may need to modify the authorized quality of service for all active users having the same type of subscription. The Diameter base protocol commands operate on a single session so these use cases could result in many thousands of command exchanges to enforce the same operation on each session in the group. In order to reduce signaling, it would be desirable to enable bulk operations on all (or part of) the sessions managed by a Diameter peer using a single or a few command exchanges.

This document describes a mechanism for grouping Diameter sessions and performing re-authentication, re-authorization, termination and abortion of groups of sessions. This document does not define a new Diameter application. Instead it defines mechanisms, commands and AVPs that may be used by any Diameter application that requires management of groups of sessions.

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 RFC 2119 [RFC2119].

This document uses terminology defined [RFC3588].

3. Grouping User Sessions

Either Diameter peer may assign a session to a group. Diameter AAA applications typically assign client and server roles to the Diameter peers. In this document, a Diameter client is a node at the edge of the network that performs access control. A Diameter server is a node that performs authentication and/or authorization of the user.

3.1. Group assignment at session initiation

To assign a session to a group at session initiation, a Diameter client sends a service specific auth request, e.g. NASREQ AAR [RFC4005], containing zero or more client-assigned group identifiers. Assuming the user is successfully authenticated and/or authorized, the Diameter server responds with service-specific auth response, e.g. NASREQ AAA [RFC4005], containing both the client-assigned group identifiers and zero or more server-assigned group identifiers.

3.2. Mid-session group assignment modifications

Either Diameter peer may modify the group membership of an active Diameter session. A Diameter client MAY remove the group(s) assigned to the active session by the Diameter server and vice versa.

This document does not define a permission model that limits removal of a session from a group by the same peer that added the session to the group. However, applications which re-use the commands and methods defined in this document may impose their own permission model. For example, an application could require that the server MUST NOT remove a session from a group assigned by the client.

3.2.1. Client-initiated group assignment changes

To update the assigned groups mid-session, a Diameter client sends a service specific re-authorization request containing the updated list of group identifiers. Assuming the user is successfully authenticated and/or authorized, the Diameter server responds with a service-specific auth response containing the updated list of group identifiers received in the request.

3.2.2. Server-initiated group assignment changes

To update the assigned groups mid-session, a Diameter server sends a Re-authorization Request (RAR) message requesting re-authorization and the client responds with a Re-authorization Answer (RAA) message. The Diameter client sends a service specific re-authorization request containing the current list of group identifiers and the Diameter server responds with a service-specific auth response containing the

updated list of group identifiers.

3.3. Server Initiated Group Re-auth

This document defines a new Group-Re-Auth-Request/Answer (GRAR/ GRAA)command exchange which allows a server to initiate a re-authentication and/or re-authorization of all services that are assigned to one of the groups specified in the Session-Group-Id AVP in the request.

An access device that receives a Group-Re-Auth-Request(GRAR) message with Session-Group-Id equal to one of the group assigned to a currently active session MUST initiate the type of re-auth specified by the Re-Auth-Request-Type AVP in the manner specified by the Session-Group-Action AVP if the service supports this particular feature. Each Diameter application MUST state whether service-initiated group re-authentication and/or re-authorization is supported and which Session-Group-Action AVP values are supported for re-authorization.

The Session-Group-Action AVP specifies whether the server requires a re-authorization request per session, per group or for all groups. For a Re-Auth-Request-Type value of AUTHORIZE_AUTHENTICATE, the Session-Group-Action value MUST be PER_SESSION since re-authentication MUST be performed per user session.

For Session-Group-Action values of PER_GROUP or ALL_GROUPS, the re-authorization is accomplished with an application-specifc group re-authorization command exchange. This command exchange as well as any limitations on which aspects of the service can be modified during a re-authorization MUST be defined by the Diameter application.

If the client is able to perform the requested re-authentication and/or re-authentication for the sessions assigned to the group(s) specified in the GRAR, it shall return a GRAA command with the Result-Code AVP set to DIAMETER_SUCCESS and Session-Group-Id AVP(s) indicating the groups for which the GRAR receiver has active sessions assigned. If there are no sessions assigned to the group(s) specified in the GRAR, the Result-Code is set to DIAMETER_UNKNOWN_SESSION_ID. If the client is unable to perform the requested re-authentication and/or re-authentication, the Result-Code is set to DIAMETER_UNABLE_TO_COMPLY.

```
    Diameter                                               Diameter
     Client                                                 Server
       |                                                      |
    (1)+-------------Svc-Specific-Auth-Request--------------->|
       |                  Session-Id=ABC                      |
       |                                                      |
    (2)|<------------Svc-Specific-Auth-Answer-----------------+
       |       Session-Id=ABC; Session-Group-Id=XYZ           |
       |                                                      |
    (3)+-------------Svc-Specific-Auth-Request--------------->|
       |                  Session-Id=DEF                      |
       |                                                      |
    (4)|<------------Svc-Specific-Auth-Answer-----------------+
       |       Session-Id=DEF; Session-Group-Id=XYZ           |
       |                                                      |
    (5)|<--------------Group-Re-Auth-Request------------------+
       | Session-Group-Id=XYZ; Session-Group-Action=PER_GROUP |
       |        Re-Auth_Request-Type=AUTHORIZE_ONLY           |
       |                                                      |
    (6)+---------------Group-Re-Auth-Answer------------------>|
       |                                                      |
    (7)+----------Svc-Specific-Group-Auth-Request------------>|
       |                Session-Group-Id=XYZ                  |
       |                                                      |
    (8)|<---------Svc-Specific-Group-Auth-Answer--------------+
       |           Updated Service Specific AVPs              |
       |                                                      |
```

Figure 1: Example: Group Re-authorization

In the example above, the Diameter server authorizes two sessions (ABC and DEF) and assigns them to a group named XYZ (Session-Group-Id=XYZ in steps 2 and 4). Some time later, an event occurs on the Diameter server which requires it to change one or more of the service parameters for the sessions assigned to group XYZ. The Diameter server sends a Group-Re-Auth-Request (step 5) specifying the impacted group (Session-Group-Id=XYZ) must be re-authorized (Re-Auth-Request-Type=AUTHORIZE_ONLY) with a single re-authorize command per group (Session-Group-Action=PER_GROUP). The Diameter client acknowledges the request (step 6) and issues a service-specific group authorization request to retrieve the updated service parameters (step 7).

3.4. Session Group Termination

This document defines a new Group-Session-Termination-Request/Answer (GSTR/GSTA) command exchange which allows a client to communicate to the server the termination of all sessions that are assigned to one

of the groups specified in the Session-Group-Id AVP in the request. The termination of a group of sessions could occur as a result of a local action or in reponse to a request to abort one or more groups of sessions.

FFS: When a client sends an GSTR to a server indicating termination of a specific group, is it indicating termination of the sessions that the server authorized and that are assigned to the specified group? Or does imply termination of all sessions on the client that are assigned to the specified group?

Upon receipt of the GSTR, the Diameter Server MUST release all resources for the sessions assigned to the group(s) specified in the Session-Group-Id AVP and return a GSTA with the Result-Code set to DIAMETER_SUCCESS to acknowledge the successful termination. If there are no sessions assigned to the group(s) specified in the GSTR, the Result-Code is set to DIAMETER_UNKNOWN_SESSION_ID. If the server is unable to perform the session termination, the Result-Code is set to DIAMETER_UNABLE_TO_COMPLY.

3.5. Aborting a Group of Sessions

This document defines a new Group-Abort-Session-Request/Answer (GASR/ GASA)command exchange which allows a server to request the termination of all sessions that are assigned to one of the groups specified in the Session-Group-Id AVP in the request.

A client that receives an GASR with Session-Group-Id equal to a group assigned to a currently active session MAY stop the session. Whether the client stops the session or not is implementation- and/or configuration-dependent. For example, a client may honor GASRs from certain agents only. In any case, the client MUST respond with an Group-Abort-Session-Answer, including a Result-Code AVP to indicate what action it took.

If the client is able to perform the requested termination of the sessions assigned to the group(s) specified in the GASR, it shall return a GASA command with the Result-Code AVP set to DIAMETER_SUCCESS and Session-Group-Id AVP(s) indicating the groups for which the GASR receiver has active sessions assigned. If there are no sessions assigned to the group(s) specified in the GASR, the Result-Code is set to DIAMETER_UNKNOWN_SESSION_ID. If the client is unable to perform the requested termination for any of the sessions, the Result-Code is set to DIAMETER_UNABLE_TO_COMPLY.

When a client terminates a session upon receipt of a Group-Abort-Session-Request, it MUST issue a session termination request to the Diameter server that authorized the service. The Session-Group-

Action AVP specifies whether the server requires a single session termination request per session (with STR message), per group (with GSTR message) or for all groups (with GSTR message).

```
    Diameter                                               Diameter
     Client                                                 Server
       |                                                      |
    (1)+-------------Svc-Specific-Auth-Request--------------->|
       |                  Session-Id=ABC                      |
       |                                                      |
    (2)|<------------Svc-Specific-Auth-Answer-----------------+
       |       Session-Id=ABC; Session-Group-Id=XYZ           |
       |                                                      |
    (3)+-------------Svc-Specific-Auth-Request--------------->|
       |                  Session-Id=DEF                      |
       |                                                      |
    (4)|<------------Svc-Specific-Auth-Answer-----------------+
       |       Session-Id=DEF; Session-Group-Id=XYZ           |
       |                                                      |
    (5)|<-----------Group-Abort-Session-Request---------------+
       | Session-Group-Id=XYZ; Session-Group-Action=PER_GROUP |
       |                                                      |
    (6)+------------Group-Abort-Session-Answer--------------->|
       |                                                      |
    (7)+---------Group-Session-Termination-Request----------->|
       |                Session-Group-Id=XYZ                  |
       |                                                      |
    (8)|<---------Group-Session-Termination-Answer------------+
       |                                                      |
```

Figure 2: Example: Aborting a Group of Sessions

In the example above, the Diameter server authorizes two sessions (ABC and DEF) and assigns them to a group named XYZ (Session-Group-Id=XYZ in steps 2 and 4). Some time later, an event occurs on the Diameter server which requires it to abort the sessions assigned to group XYZ. The Diameter server sends a Group-Abort-Session-Request (step 5) specifying the sessions assigned to the impacted group (Session-Group-Id=XYZ) are to be terminated and a single termination command is to be sent per impacted group (Session-Group-Action=PER_GROUP). The Diameter client acknowledges the request with a GASA (step 6) and issues a GSTR (step 7) command to release all resources for the sessions assigned to the group XYZ. The Diameter server acknowledges the termination with a GGSTA (Step 8).

4. Protocol Description

4.1. Session Management

4.1.1. Authorization Session State Machine

Section 8.1 in [RFC3588] defines a set of finite state machines, representing the life cycle of Diameter sessions, and which MUST be observed by all Diameter implementations that make use of the authentication and/or authorization portion of a Diameter application. This section defines the additional state transitions related to the processing of the new commands which may impact multiple sessions.

The group membership is session state and therefore only those state machines from [RFC3588] in which the server is maintaining session state are relevant in this document. As in [RFC3588], the term Service-Specific below refers to a message defined in a Diameter application (e.g., Mobile IPv4, NASREQ).

The following state machine is observed by a client when state is maintained on the server. State transitions which are unmodified from [RFC3588] are not repeated here.

CLIENT, STATEFUL

State	Event	Action	New State
Idle	Client or Device Requests access	Send service specific auth req optionally including groups	Pending
Open	GASR received with Session-Group-Action = ALL_GROUPS, session is assigned to received group(s) and client will comply with request to end the session	Send GASA with Result-Code = SUCCESS, Send GSTR.	Discon
Open	GASR received with Session-Group-Action = PER_GROUPS, session is assigned to	Send GASA with Result-Code = SUCCESS,	Discon

	received group(s) and client will comply with request to end the session	Send GSTR per group	
Open	GASR received with Session-Group-Action = PER_SESSION, session is assigned to received group(s) and client will comply with request to end the session	Send GASA with Result-Code = SUCCESS, Send STR per session	Discon
Open	GASR received, client will not comply with request to end all session in received group(s)	Send GASA with Result-Code != SUCCESS	Open
Discon	GSTA Received	Discon. user/device	Idle
Open	GRAR received with Session-Group-Action = ALL_GROUPS, session is assigned to received group(s) and client will perform subsequent re-auth	Send GRAA, Send service specific group re-auth req	Pending
Open	GRAR received with Session-Group-Action = PER_GROUP, session is assigned to received group(s) and client will perform subsequent re-auth	Send GRAA, Send service specific group re-auth req per group	Pending
Open	GRAR received with Session-Group-Action = PER_SESSION, session is assigned to received group(s) and client will perform subsequent re-auth	Send GRAA, Send service specific re-auth req per session	Pending
Open	GRAR received and client will not perform subsequent re-auth	Send GRAA with Result-Code != SUCCESS,	Idle

		Discon. user/device	
Pending	Successful service-specific group re-authorization answer received.	Provide service	Open
Pending	Failed service-specific group re-authorization answer received.	Discon. user/device	Idle

The following state machine is observed by a server when it is maintaining state for the session. State transitions which are unmodified from [RFC3588] are not repeated here.

SERVER, STATEFUL

State	Event	Action	New State
Idle	Service-specific authorization request received, and user is authorized	Send successful service specific answer optionally including groups	Open
Open	Server wants to terminate group(s)	Send GASR	Discon
Discon	GASA received	Cleanup	Idle
Any	GSTR received	Send GSTA, Cleanup	Idle
Open	Server wants to reauth group(s)	Send GRAR	Pending
Pending	GRAA received with Result-Code = SUCCESS	Update session(s)	Open
Pending	GRAA received with Result-Code != SUCCESS	Cleanup session(s)	Idle
Open	Service-specific group re-authoization request received and user is authorized	Send successful service specific group re-auth answer	Open
Open	Service-specific group re-authorization request received and user is not authorized	Send failed service specific group re-auth answer, cleanup	Idle

4.2. Commands

Editor's Note: The content of this section does not represent working group consensus but rather the views of the draft author prior to (and post) adoption. Alternative methods for manipulating groups of sessions are being considered by the working group and this section may be heavily modified or removed in subsequent versions.

This specification extends the existing RAR, RAA, STR, STA, ASR and ASA command ABNFs.

4.2.1. Group-Re-Auth-Request

The Group-Re-Auth-Request (GRAR), indicated by the Command-Code set to TBD and the message flags' 'R' bit set, may be sent by any server to the access device that is providing session service, to request that one or more groups of users be re-authenticated and/or re-authorized.

```
      <GRAR>  ::= < Diameter Header: TBD, REQ, PXY >
                * { Session-Group-Id }
                  { Origin-Host }
                  { Origin-Realm }
                  { Destination-Realm }
                  { Destination-Host }
                  { Auth-Application-Id }
                  { Re-Auth-Request-Type }
                  [ Origin-State-Id ]
                * [ Proxy-Info ]
                * [ Route-Record ]
                  [ Session-Group-Action ]
                * [ AVP ]
```

4.2.2. Group-Re-Auth-Answer

The Group-Re-Auth-Answer (GRAA), indicated by the Command-Code set to TBD and the message flags' 'R' bit clear, is sent in response to the GRAR. The Result-Code AVP MUST be present, and indicates the disposition of the request.

```
         <GRAA>  ::= < Diameter Header: TBD, PXY >
                   * { Session-Group-Id }
                     { Result-Code }
                     { Origin-Host }
                     { Origin-Realm }
                     [ Origin-State-Id ]
                     [ Error-Message ]
                     [ Error-Reporting-Host ]
                   * [ Failed-AVP ]
                   * [ Redirect-Host ]
                     [ Redirect-Host-Usage ]
                     [ Redirect-Host-Cache-Time ]
                   * [ Proxy-Info ]
                   * [ AVP ]
```

4.2.3. Group-Session-Termination-Request

The Group-Session-Termination-Request (GSTR), indicated by the Command-Code set to TBD and the Command Flags' 'R' bit set, is sent by the access device to inform the Diameter Server that one or more groups of authenticated and/or authorized sessions are being terminated.

```
         <GSTR>  ::= < Diameter Header: TBD, REQ, PXY >
                   * { Session-Group-Id }
                     { Origin-Host }
                     { Origin-Realm }
                     { Destination-Realm }
                     { Auth-Application-Id }
                     { Termination-Cause }
                     [ Destination-Host ]
                   * [ Class ]
                     [ Origin-State-Id ]
                   * [ Proxy-Info ]
                   * [ Route-Record ]
                   * [ AVP ]
```

4.2.4. Group-Session-Termination-Answer

The Group-Session-Termination-Answer (GSTA), indicated by the Command-Code set to TBD and the message flags' 'R' bit clear, is sent by the Diameter Server to acknowledge the notification that one or more groups of session have been terminated. The Result-Code AVP MUST be present, and MAY contain an indication that an error occurred while servicing the GSTR.

```
      <GSTA>  ::= < Diameter Header: TBD, PXY >
                * { Session-Group-Id }
                  { Result-Code }
                  { Origin-Host }
                  { Origin-Realm }
                * [ Class ]
                  [ Error-Message ]
                  [ Error-Reporting-Host ]
                * [ Failed-AVP ]
                  [ Origin-State-Id ]
                * [ Redirect-Host ]
                  [ Redirect-Host-Usage ]
                  [ Redirect-Max-Cache-Time ]
                * [ Proxy-Info ]
                * [ AVP ]
```

4.2.5. Group-Abort-Session-Request

The Group-Abort-Session-Request (GASR), indicated by the Command-Code set to TBD and the message flags' 'R' bit set, may be sent by any server to the access device that is providing session service, to request that the sessions identified by the Session-Group-Id be stopped.

```
      <GASR>  ::= < Diameter Header: TBD, REQ, PXY >
                * { Session-Group-Id }
                  { Origin-Host }
                  { Origin-Realm }
                  { Destination-Realm }
                  { Destination-Host }
                  { Auth-Application-Id }
                  [ Origin-State-Id ]
                * [ Proxy-Info ]
                * [ Route-Record ]
                  [ Group-Action ]
                * [ AVP ]
```

4.2.6. Group-Abort-Session-Answer

The Group-Abort-Session-Answer (GASA), indicated by the Command-Code set to TBD and the message flags' 'R' bit clear, is sent in response to the GASR. The Result-Code AVP MUST be present, and indicates the disposition of the request.

```
         <GASA>  ::= < Diameter Header: TBD, PXY >
                   * { Session-Group-Id }
                     { Result-Code }
                     { Origin-Host }
                     { Origin-Realm }
                     [ Origin-State-Id ]
                     [ Error-Message ]
                     [ Error-Reporting-Host ]
                   * [ Failed-AVP ]
                   * [ Redirect-Host ]
                     [ Redirect-Host-Usage ]
                     [ Redirect-Max-Cache-Time ]
                   * [ Proxy-Info ]
                   * [ AVP ]
```

5. AVPs

			AVP Flag rules			
	AVP				SHOULD	MUST
Attribute Name	Code	Value Type	MUST	MAY	NOT	NOT
Session-Group-Id	TBD	OctetString		P		V
Session-Group-Action	TBD	Enumerated		P		V

AVPs for the Diameter Group Signaling

5.1. Session-Group-Id AVP

The Session-Group-Id AVP (AVP Code TBD) is of type OctetString and identifies a group of sessions. This uniqueness scope of this AVP is specified by the Diameter application which makes use of group signaling commands.

5.2. Session-Group-Action AVP

The Session-Group-Action AVP (AVP Code TBD) is of type Enumerated and specifies how the peer SHOULD issue follow up exchanges in response to a command which impacts mulitple sessions. The following values are supported:

ALL_GROUPS (0)
Follow up exchanges should be performed with a single message exchange for all impacted groups.

PER_GROUP (1)
Follow up exchanges should be performed with a message exchange for each impacted group.

PER_SESSION (2)
Follow up exchanges should be performed with a message exchange for each impacted session.

6. Result-Code AVP Values

This section defines new Result-Code [RFC3588] values that MUST be supported by all Diameter implementations that conform to this specification.

[Editor's Note: Group specific error values may need to be added here.]

7. IANA Considerations

This section contains the namespaces that have either been created in this specification or had their values assigned to existing namespaces managed by IANA.

7.1. Command Codes

This specification requires IANA to register the following new Commands from the Command Code namespace defined in [RFC3588].

- Group-Re-Auth-Request/Answer
- Group-Session-Termination-Request/Answer
- Group-Abort-Session-Request/Answer

The commands are defined in Section 4.2.

7.2. AVP Codes

This specification requires IANA to register the following new AVPs from the AVP Code namespace defined in [RFC3588].

- Session-Group-Id
- Session-Group-Action

The AVPs are defined in Section 5.

8. Security Considerations

TODO

9. Acknowledgments

10. 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.

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

Author's Address

Mark Jones

Email: mark@azu.ca