DIME
Internet-Draft
Intended status: Informational
Expires: April 26, 2012

M. Jones
Bridgewater Systems
October 24, 2011

Diameter Group Signaling
draft-jones-diameter-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 in order 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

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on April 26, 2012.

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 in order 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 one 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 the 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.

Editor's Note: It is FFS whether this document should define a default permission model limiting removal of a session from a group. For example, 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.

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	BASR 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 BASA with Result-Code = SUCCESS, Send BSTR.	Discon
Open	BASR received with Session-Group-Action = PER_GROUPS, session is assigned to received group(s) and client will comply with request to end the session	Send BASA with Result-Code = SUCCESS, Send BSTR per group	Discon
Open	BASR received with Session-Group-Action = PER_SESSION, session is assigned to	Send BASA with Result-Code = SUCCESS,	Discon

	received group(s) and client will comply with request to end the session	Send STR per session	
Open	BASR received, client will not comply with request to end all session in received group(s)	Send BASA with Result-Code != SUCCESS	Open
Discon	BSTA Received	Discon. user/device	Idle
Open	BRAR received with Session-Group-Action = ALL_GROUPS, session is assigned to received group(s) and client will perform subsequent re-auth	Send BRAA, Send service specific group re-auth req	Pending
Open	BRAR received with Session-Group-Action = PER_GROUP, session is assigned to received group(s) and client will perform subsequent re-auth	Send BRAA, Send service specific group re-auth req per group	Pending
Open	BRAR received with Session-Group-Action = PER_SESSION, session is assigned to received group(s) and client will perform subsequent re-auth	Send BRAA, Send service specific re-auth req per session	Pending
Open	BRAR received and client will not perform subsequent re-auth	Send BRAA 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 BASR	Discon
Discon	BASA received	Cleanup	Idle
Any	BSTR received	Send BSTA, Cleanup	Idle
Open	Server wants to reauth group(s)	Send BRAR	Pending
Pending	BRAA received with Result-Code = SUCCESS	Update session(s)	Open
Pending	BRAA 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

4.1.2. Server Initiated Group Re-auth

TODO: rules/restrictions governing group re-auth

4.1.3. Session Group Termination

TODO: rules/restrictions governing session group termination

4.1.4. Aborting a Group of Sessions

TODO: rules/restrictions governing aborting groups of session

4.2. Commands

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 }
              [ User-Name ]
              [ 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.

[Editor's Note: Move these detailed behaviour requirements to earlier section?]

A successful GRAA message MUST be followed by an application-specific authentication and/or authorization message. The Group-Action AVP in the Group-Re-Auth-Request indicates whether a single exchange, per-group or per-session is required.

If the peer receiving the GRAR has no active sessions which are assigned to the groups listed in the Session-Group-Id AVPs, it MUST return a GRAA with the Result-Code set to TBD.

The Session-Group-Id AVPs in the GRAA indicate the groups for which the GRAR receiver has active sessions assigned to those groups.

```
      <GRAA>  ::= < Diameter Header: TBD, PXY >
                  * { Session-Group-Id }
                    { Result-Code }
                    { Origin-Host }
                    { Origin-Realm }
                    [ User-Name ]
                    [ 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 }
              [ User-Name ]
              [ 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.

Upon sending or receipt of the GSTA, the Diameter Server MUST release

all resources for all sessions belonging to the groups indicated by the Session-Group-Id AVP. Any intermediate server in the Proxy-Chain MAY also release any resources, if necessary.

```
<GSTA>  ::= < Diameter Header: TBD, PXY >
            * { Session-Group-Id }
              { Result-Code }
              { Origin-Host }
              { Origin-Realm }
              [ User-Name ]
            * [ 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 }
              [ User-Name ]
              [ 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.

If the sessions identified by Session-Group-Id in the GASR were successfully terminated, Result-Code is set to DIAMETER_SUCCESS. If the session is not currently active, Result-Code is set to DIAMETER_UNKNOWN_SESSION_ID. If the access device does not stop the session for any other reason, Result-Code is set to DIAMETER_UNABLE_TO_COMPLY.

[Editor's Note: Move these detailed behaviour requirements to earlier section.]

A successful GASA message MUST be followed by one or more STR or GSTR to the authorizing server. The Group-Action AVP in the Group-Abort-Session-Request indicates whether a GSTR per group of sessions, a GSTR per group or an STR per session is required.

If the peer receiving the GASR has no active sessions which are assigned the groups listed in the Session-Group-Id AVPs, it MUST return a GASA with the Result-Code set to TBD.

The Session-Group-Id AVPs in the GASA indicate the groups for which the GASR receiver has active sessions assigned to those groups.

```
      <GASA>  ::= < Diameter Header: TBD, PXY >
                  * { Session-Group-Id }
                    { Result-Code }
                    { Origin-Host }
                    { Origin-Realm }
                    [ User-Name ]
                    [ 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			
Attribute Name	AVP Code	Value Type	MUST	MAY	SHOULD NOT	MUST 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

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
Bridgewater Systems

Email: mark@azu.ca