SIP CLF Problem Statement
Draft-ietf-sipclf-problem-statement-03
(V. K. Gurbani, E. Burger, T. Anjali, H. Abdelnur, and O. Festor)

Presenter: Vijay K. Gurbani
IETF 78, Maastricht, Netherlands
July 26, 2010
Changes since -0{1,2}

• Minor changes:
  • Incorporated pending reviews done by John Elwell, Cullen Jennings and recent review of -02 by Peter Musgrave (thanks!)
  • Typos, etc.
The (Updated) Data Model

- Timestamp
- Size of message
- Message type (Request or response)
- Directionality (received or sent)
- Source-IP:port:xport
- Dest-IP:port:xport
- Server-txn
- Client-txn
- From
- To
- Method
- Call-ID
- Cseq
- R-URI
- Status
- Body
- Ordered list of other SIP fields
The Data Model

- The data model applies to all SIP entities:
  - UAC
  - UAS
  - Proxy
  - B2BUA (degenerate case of a Proxy)
  - Registrar/Redirect servers (special cases of UAS)
The (Updated) Data Model

- In -0{1,2} different SIP entities logged different data model elements depending on their role (UAC, UAS, etc.) and directionality (request, response.)

- Now all SIP entities create a canonical log entry with the following mandatory elements:

  Record size, Timestamp, Message type, Directionality, Cseq, R-URI, Destination:port:xport, Source:port:xport, To, From, Call-ID, Status, Server-Txn, Client-Txn
The (Updated) Data Model

Table summarizes how mandatory fields are handled:

R: implies that the field is logged when a request is handled by that SIP entity.

r: implies that the field is logged when a response is handled by that SIP entity.

-: implies that the field is not applicable to that SIP entity.

<table>
<thead>
<tr>
<th></th>
<th>UAC</th>
<th>UAS</th>
<th>UAS-half</th>
<th>UAC-half</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
</tr>
<tr>
<td>SIP CLF record size</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
</tr>
<tr>
<td>Message type</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
</tr>
<tr>
<td>Directionality</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
</tr>
<tr>
<td>CSeq</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
</tr>
<tr>
<td>R-URI</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
</tr>
<tr>
<td>Destination:port:xport</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
</tr>
<tr>
<td>Source:port:xport</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
</tr>
<tr>
<td>To</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
</tr>
<tr>
<td>From</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
</tr>
<tr>
<td>Call-ID</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
</tr>
<tr>
<td>Status</td>
<td>r</td>
<td>r</td>
<td>r</td>
<td>r</td>
</tr>
<tr>
<td>Server-Txn</td>
<td>-</td>
<td>R,r</td>
<td>R,r</td>
<td>R,r</td>
</tr>
<tr>
<td>Client-Txn</td>
<td>R,r</td>
<td>-</td>
<td>r</td>
<td>R,r</td>
</tr>
</tbody>
</table>

SIP CLF fields logged per entity
Example

Direct call from Alice to Bob (PoV: Alice's UAC)

<allOneLine>
103 1275930743.699 R s INVITE-32 sip:bob@bob1.example.net
203.0.113.1:5060:udp 198.51.100.1:5060:udp
sip:bob@example.net sip:alice@example.com;tag=76yhh
f82-d4-f7@example.com - - c-l-xt6
</allOneLine>

<allOneLine>
175 1275930745.002 r r INVITE-32 - 198.51.100.1:5060:udp
203.0.113.1:5060:udp sip:bob@example.net;tag=b-in6-1u
sip:alice@example.com;tag=76yhh f82-d4-f7@example.com
180 - c-l-xt6
</allOneLine>

<allOneLine>
175 1275930746.100 r r INVITE-32 - 198.51.100.1:5060:udp
203.0.113.1:5060:udp sip:bob@example.net;tag=b-in6-1u
sip:alice@example.com;tag=76yhh f82-d4-f7@example.com
200 - c.l-xt6
</allOneLine>

<allOneLine>
193 1275930746.120 R s ACK-32 sip:bob@bob1.example.net
203.0.113.1:5060:udp 190.51.100.1:5060:udp
sip:bob@example.net;tag=b-in6-1u
sip:alice@example.com;tag=76yhh f82-d4-f7@example.com
- - c-l-xt6
</allOneLine>

Record size, Timestamp, Message type, Directionality, Cseq, R-URI,
Destination:port:xport, Source:port:xport, To, From, Call-ID, Status, Server-Txn,
Client-Txn

More complex examples in the draft.
Open issues and next step

- No unknown open issues.
- 1 known open issue: Volume analysis (see http://www.ietf.org/mail-archive/web/sip-clf/current/msg00123.html).
- Do we need to include such analysis?
- Next steps: Besides above open issue, the draft is ready to be moved forward.
- Thanks!