The Session Initiation Protocol (SIP) Stack: A look under the hood of VoIP

Vijay K. Gurbani, Ph.D. | Feb 22, 2018
SIP: Brief history

• Circa 1996
  - Session Invitation Protocol (SIP)
  - Simple Conference Invitation Protocol (SCIP)

• SIP + SCIP merged to form what we now know as the Session Initiation Protocol.

• Part of the pantheon of Internet Engineering Task Force (IETF) protocols:
  - SAP (Session Announcement Protocol)
  - SDP (Session Description Protocol)
  - RTP (Real-time Transport Protocol)
SIP: Brief history

• 1996 – 2002
  - H.323 dominates the VoIP landscape.
  - SIP is a relatively new entrant.
  - 1999 – 2000 3GPP/IMS adopt SIP as the standard signaling protocol in IMS.
  - H.323 starts to loose steam.
SIP: Brief timeline of my involvement

- Early involvement in SIP. SIP yet at I-D stage. Implemented first SIP Server at IH to demonstrate ICW.
- Debates continue between SIP and H.323. SIP becomes an RFC. Gains industry foothold. SIP/IN Server -> iSIP.
- Took iSIP to 1 Bakeoff (11) – utility decreases. SIP really starts to be viewed as a service creation tool which will revitalize the telecom industry – the web model. RFC3261 released; iSIP updated to rfc3261. Many field trials, no large scale deployments yet. iSIP becomes GA in PacketIN.
- Debates rage between SIP and H.323. Our work in SIP/IN starts.
- Took iSIP to 2 Bakeoffs (7,9) – only doing advanced scenarios now. H.323 vs. SIP debate eases as each starts to become more like the other. iSIP starts to get internal LU attention.
- Took iSIP to 3 Bakeoffs (4,5,6). Visible by standards participation. And conference presentations. SIP starts to be seen as the answer to services (move away from telephony roots) as the telecom industry melts. 3GPP adopts SIP.
- Deployments start to happen (Vonage, Denwa, ...). SIP in the mainstream; one of the most active WGs in the IETF. Reuse of iSIP gives birth to siptrans. Tremendous amount of internal LU interest in iSIP/siptrans. Protocol starts to get ironed out (UDP deprecation, SCTP support, …)
SIP: Basics

• Set up multimedia sessions
  - Voice, video, instant messaging, gaming, ...
• Renegotiate call parameters
• “Forking” of calls
• Terminate, transfer calls
• Call control (hold, forward, transfer, ...)
• Transport independent (TCP, UDP, TLS, DTLS, SCTP)
• RFC3261 SIP: Peer to peer
• IMS SIP: Centrally controlled
SIP Architecture: Peer-to-peer

Slide source: Prof. Henning Schulzrinne, Columbia University
SIP Architecture: Peer-to-peer

SIP architecture: carrier

Slide source: Prof. Henning Schulzrinne, Columbia University
SIP Addressing

• SIP addresses are URL’s

• Examples
  - sip:vijay.gurbani@nokia.com:5067
  - sip:vijay.gurbani:passwd@nokia.com

• To send a message, a SIP client can send it to a pre-configured proxy, or use DNS
  - Check for DNS SRV records
  - Then check for MX records
  - Finally, use an A record
SIP: Protocol components

• Clients
  - End systems
  - User Agent Client
    - Send SIP requests
  - User Agent Server
    - Listens for call requests
    - Prompts user or executes program to determine response

• Redirect Server
  - “Network” server; redirects users to try other server (user agent may act as redirect server)

• Proxy Server
  - “Network Server” Proxies request to another server (user agent also may do this)
  - Can “fork” request to multiple servers, creating a search tree

• Registrar
  - Accepts/stores/serves registration requests
  - May interfaces with a Location Service (LDAP, CORBA, RPC, carrier pigeons...)

• B2BUA
SIP: Protocol components
SIP Transactions

• SIP is an UTF-8 based request-reply protocol.

• A SIP transaction occurs between a SIP client and a SIP server and comprises all messages from the first request sent from the client to the server up to a final (non-1xx) response sent from the server to the client.
SIP Methods (Requests):

• INVITE
  - Invites a participant to a conference
  - Conference can be unicast, multicast, bridged, new or in existence

• BYE
  - Ends a client’s participation in a call

• CANCEL
  - Terminates a search

• OPTIONS
  - Queries a participant about their media capabilities, and finds them, but doesn’t invite

• ACK
  - For reliability and call acceptance

• REGISTER
  - Informs a SIP server about the location of a user
SIP Responses:

Divided into 6 classes:

1-xx: Informational
  100 Trying
  180 Ringing
...

2-xx: Successful
  200 OK

3-xx: Redirection
  300 Multiple Choices
  301 Moved Temporarily
...

4-xx: Request Failure
  400 Bad Request
  482 Loop Detected
...

5-xx: Server Failure
  500 Server Internal Error
  501 Not Implemented
...

6-xx: Global Failure
  603: Decline
  606: Not Acceptable
...

All 2xx, 3xx, 4xx, and 5xx responses are **FINAL** (terminates the SIP transaction).

A 1xx is a **PROVISIONAL** SIP response.
SIP Call Flow (Direct signaling between endpoints):

Notes:
- Caller media preferences specified in INVITE.
- 1xx responses are optional.
- Callee media preferences are specified in 200 OK.

IT TAKES ONLY 3 UDP PACKETS TO ESTABLISH A SIP SESSION!!
SIP Call Flow (Redirection):

Note:
- Media flows directly between the two endpoints.
SIP Call Flow (Proxy Server):

INVITE vkg@lucent.com

200 OK

ACK vkg@lucent.com

INVITE vkg@ihmain.ih.lucent.com

200 OK

ACK vkg@ihmain.ih.lucent.com
# SIP: A prototypical stack layering

<table>
<thead>
<tr>
<th>Stateless Proxy</th>
<th>Transaction User</th>
</tr>
</thead>
<tbody>
<tr>
<td>UAS</td>
<td>UAC</td>
</tr>
<tr>
<td>Redirect</td>
<td>Registrar</td>
</tr>
<tr>
<td>Transaction-Call-stateful Proxy</td>
<td>B2BUA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax/Encoding</th>
</tr>
</thead>
</table>
SIP on-the-wire representation:

Request from client to server (proxy)

```
INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b43
Max-Forwards: 70
Route: <sip:ss1.atlanta.example.com;lr>
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76s1
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:alice@client.atlanta.example.com;transport=tcp>
Content-Type: application/sdp
Content-Length: 151

v=0
o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
s=-
c=IN IP4 192.0.2.101
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```
SIP on-the-wire representation:

Request from client to server (proxy)

```
INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b43
Max-Forwards: 70
Route: <sip:ss1.atlanta.example.com;lr>
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76s1
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:alice@client.atlanta.example.com;transport=tcp>
Content-Type: application/sdp
Content-Length: 151

v=0
o=alice 2890844526 2890844526 IN IP4 client.atlanta.example.com
s=-
c=IN IP4 192.0.2.101
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

Response from server to client

```
SIP/2.0 100 Trying
Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9
;received=192.0.2.101
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76s1
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 2 INVITE
Content-Length: 0
```
SIP on the wire representation:

```
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9
     ;received=192.0.2.101
Record-Route: <sip:ss2.biloxi.example.com;lr>,
              <sip:ss1.atlanta.example.com;lr>
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76s1
To: Bob <sip:bob@biloxi.example.com>;tag=314159
Call-ID: 3848276298220188511@atlanta.example.com
Contact: <sip:bob@client.biloxi.example.com;transport=tcp>
CSeq: 2 INVITE
Content-Length: 0
```
SIP on the wire representation:

Response from server to client

SIP/2.0 180 Ringing
Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9
;received=192.0.2.101
Record-Route: <sip:ss2.biloxi.example.com;lr>,
    <sip:ss1.atlanta.example.com;lr>
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76s1
To: Bob <sip:bob@biloxi.example.com>;tag=314159
Call-ID: 3848276298220188511@atlanta.example.com
Contact: <sip:bob@client.biloxi.example.com;transport=tcp>
CSeq: 2 INVITE
Content-Length: 0

SIP/2.0 200 OK
Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74bf9
;received=192.0.2.101
Record-Route: <sip:ss2.biloxi.example.com;lr>,
    <sip:ss1.atlanta.example.com;lr>
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76s1
To: Bob <sip:bob@biloxi.example.com>;tag=314159
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 2 INVITE
Contact: <sip:bob@client.biloxi.example.com;transport=tcp>
Content-Type: application/sdp
Content-Length: 147

v=0
c=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com
s=--
c=IN IP4 192.0.2.201
t=0 0
m=audio 3456 RTP/AVP 0
a=rtpmap:0 PCMU/8000
SIP on the wire representation:

Request from client to server (proxy)

ACK sip:bob@client.biloxi.example.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.example.com:5060;branch=z9hG4bK74b76
Max-Forwards: 70
Route: <sip:ss1.atlanta.example.com;lr>,
      <sip:ss2.biloxi.example.com;lr>
From: Alice <sip:alice@atlanta.example.com>;tag=9fxced76s1
To: Bob <sip:bob@biloxi.example.com>;tag=314159
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 2 ACK
Content-Length: 0

The session is now established and can be changed using a re-INVITE or torn down using a BYE. The re-INVITE and BYE can be issued by either side.
SIP state machines

SIP state transition – client

Slide source: Prof. Henning Schulzrinne, Columbia University
SIP state machines

SIP state transition – server

- Initial
  - INVITE 1xx
  - CANCEL 200
  - INVITE 1xx

- Call proceeding
  - CANCEL 200
  - max(T1*2^n, T2)
  - Failure
    - failure >= 300
  - Success
    - callee picks up 200
    - status change 1xx
  - ACK
    - event
    - message sent
    - ACK
    - Confirmed
    - CANCEL 200

Slide source: Prof. Henning Schulzrinne, Columbia University
SIP: The specifications

• Core SIP protocol
  - RFCs 3261, 3263 (Locating Servers), 3264 (Offer/Answer model), 3265 (Event Notification framework, or pub/sub), ...

• Public-Switched Telephone Network interworking
  - RFCs 2848 (PINT: use SIP to invoke services in PSTN), 3910 (SPIRITS: allows a PSTN switch to ask IP element how to proceed, ICW), 3398 (ISUP to SIP), 3960 (Early media), ...

• NAT traversal
  - RFCs 5245 (ICE), 5626 (Outbound, reaching UAs behind NATs), ...
SIP Esoterica

Cryptographically Transparent SIP Proxies

Mitigating Mimicry Attacks in the Session Initiation Protocol


INVITE sip:+16305551212@gl07b.example.com SIP/2.0
Session-Expires: 1800
Min-SE: 300
Allow-Events: calling-name,presence,reg
Allow: INVITE,ACK,CANCEL,BYE,OPTIONS,INFO,REGISTER,UPDATE
    NOTIFY, SUBSCRIBE, MESSAGE, REFER, PUBLISH
User-Agent: tstsip, version feat442.pl
Supported: HistInfo,path,timer
Expires: 600000
Contact: <sip:alice@10.111.64.160:5099>;q=0.5
Max-Forwards: 55
Via: SIP/2.0/UDP 10.111.64.160:5099;branch=z9hG4bK-12911-0-478
CSeq: 477 INVITE
To: Called Test 13 <sip:+16305551212@gl07b.example.com>
From: Alice W<sip:+alice@gl07b.example.com>;tag=Orig-475
Call-id: Default_Label-12911-1254978872-0000012@0
v:SIP/2.0/UDP 10.111.64.100:5060;branch=z9hG4bK-otag-991
Route: <sip:pcgw-stdn.imsgroup.gl07b.example.com:5062;lr;bidx=0>
Route: <sip:scsf.imsgroup.example.com:5060;lr;ottag=ue>
Content-Type: application/SDP
Content-Length: 284

v=0
o=tstsipUser12 12911 476 IN IP4 9.0.0.12
s=tstisp offer Default_Label
c=IN IP4 9.0.0.12
t=0 0
m=audio 10000 RTP/AVP 0 8 101
b=AS:64
a=rtpmap:0 PCMU/8000/1
a=rtpmap:8 PCMA/8000/1
a=rtpmap:101 telephone-event/8000/1
a=fmtp:101 0-15
a=sendrecv
a=silenceSupp:off - - - -
SIP: Time to say BYE

Questions, comments, and feedback!
vijay.gurbani@nokia.com