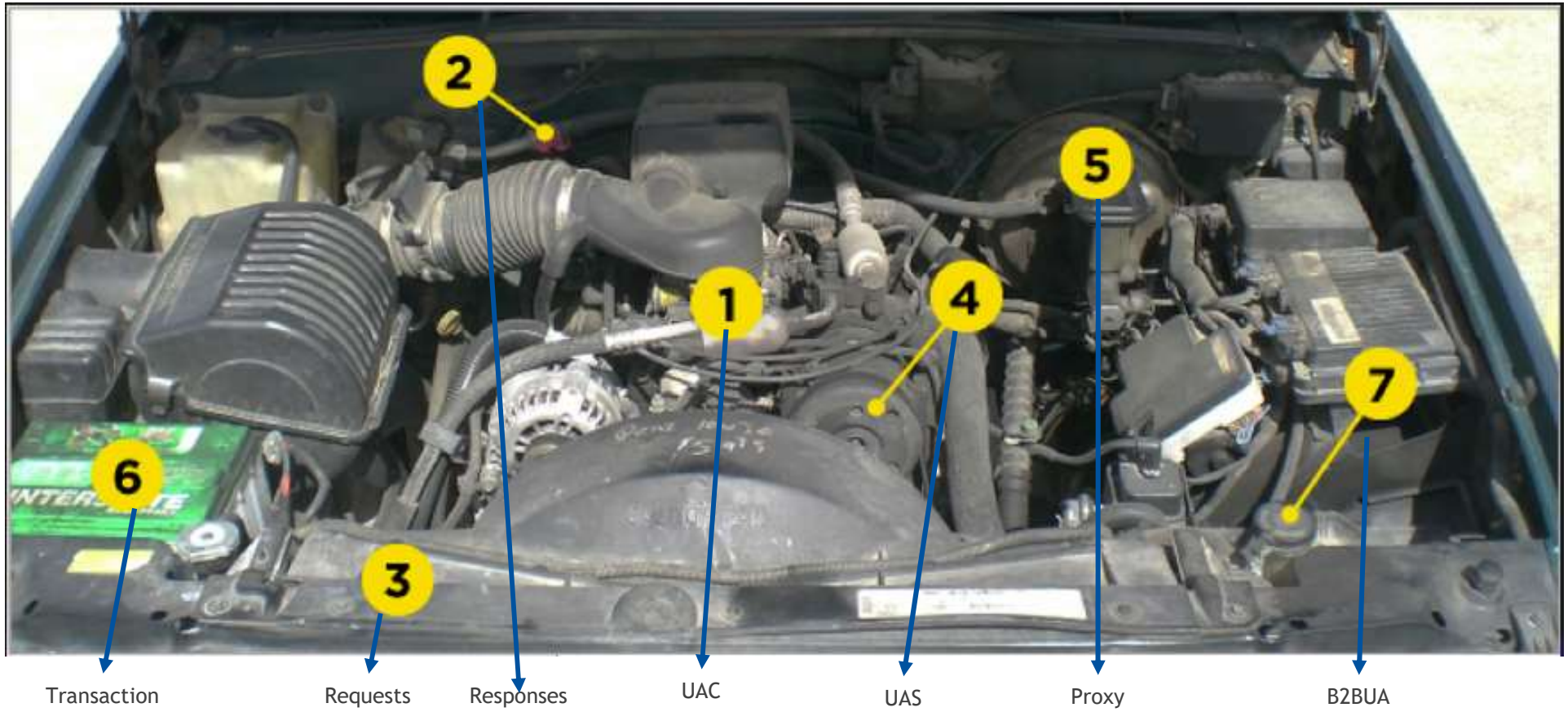


The Session Initiation Protocol (SIP) Stack: A look under the hood of VoIP

UniForum Chicago
The International Association of Open Systems Professionals

Vijay K. Gurbani, Ph.D. | Feb 22, 2018

NOKIA

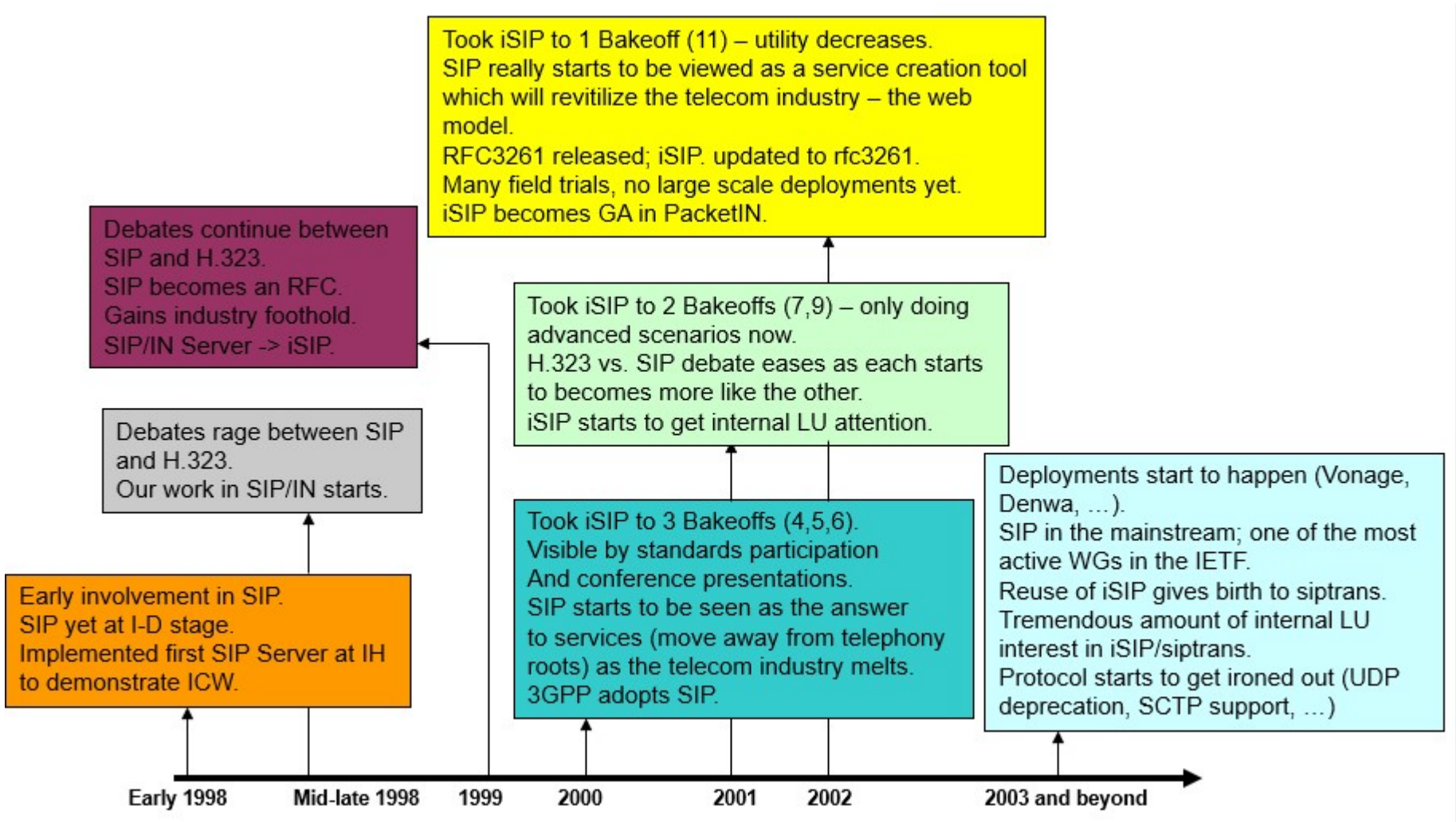
SIP: Brief history

- 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.
  - March 1999: RFC 2543 published, revised as RFC 3261 in June 2002.
  - 1999 – 2000 3GPP/IMS adopt SIP as the standard signaling protocol in IMS.
  - H.323 starts to loose steam.

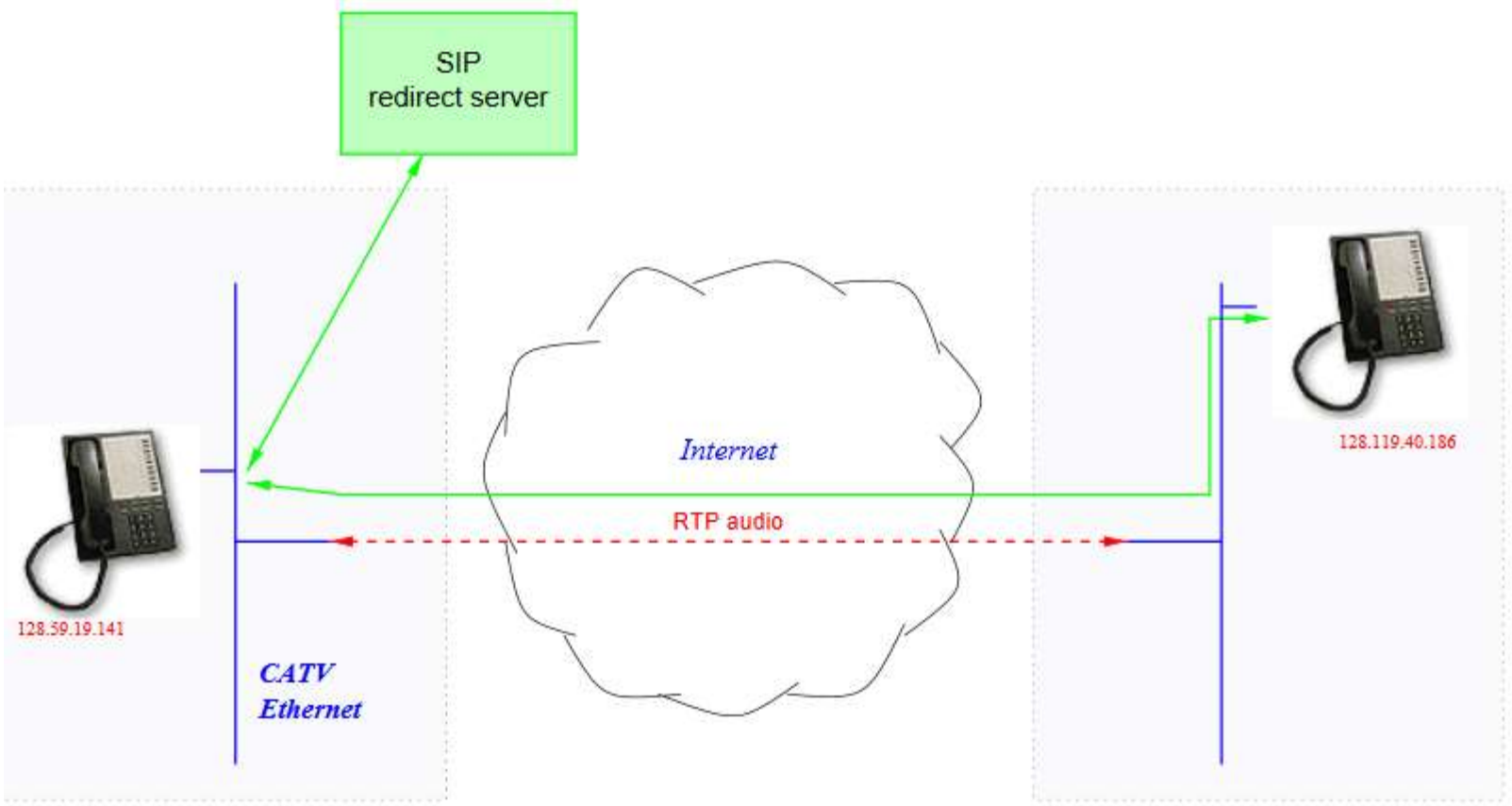
SIP: Brief timeline of my involvement



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

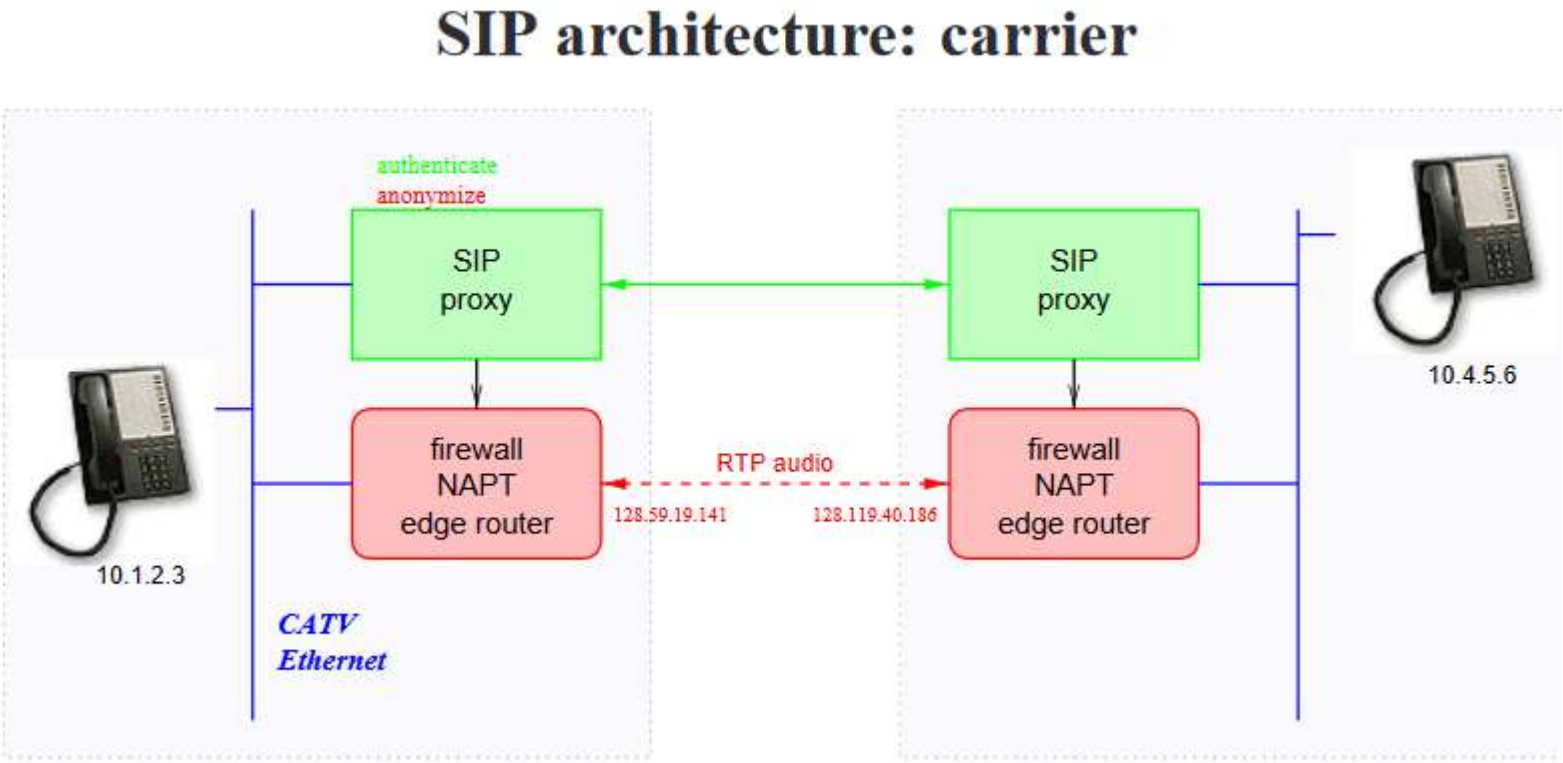
SIP Architecture: Peer-to-peer



Slide source: Prof. Henning Schulzrinne, Columbia University

NOKIA

SIP Architecture: Peer-to-peer



Slide source: Prof. Henning Schulzrinne, Columbia University

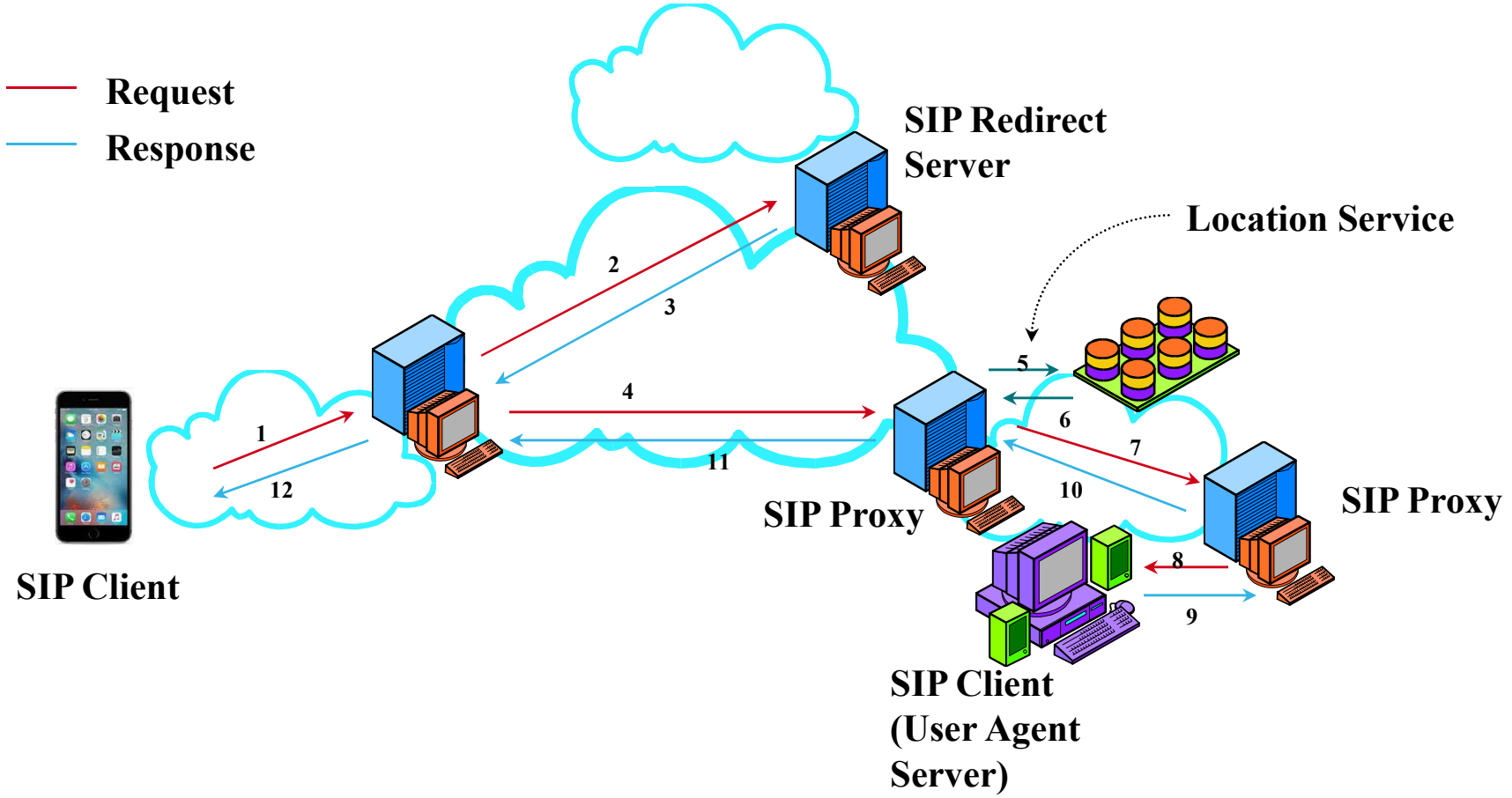
SIP Addressing

- 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:

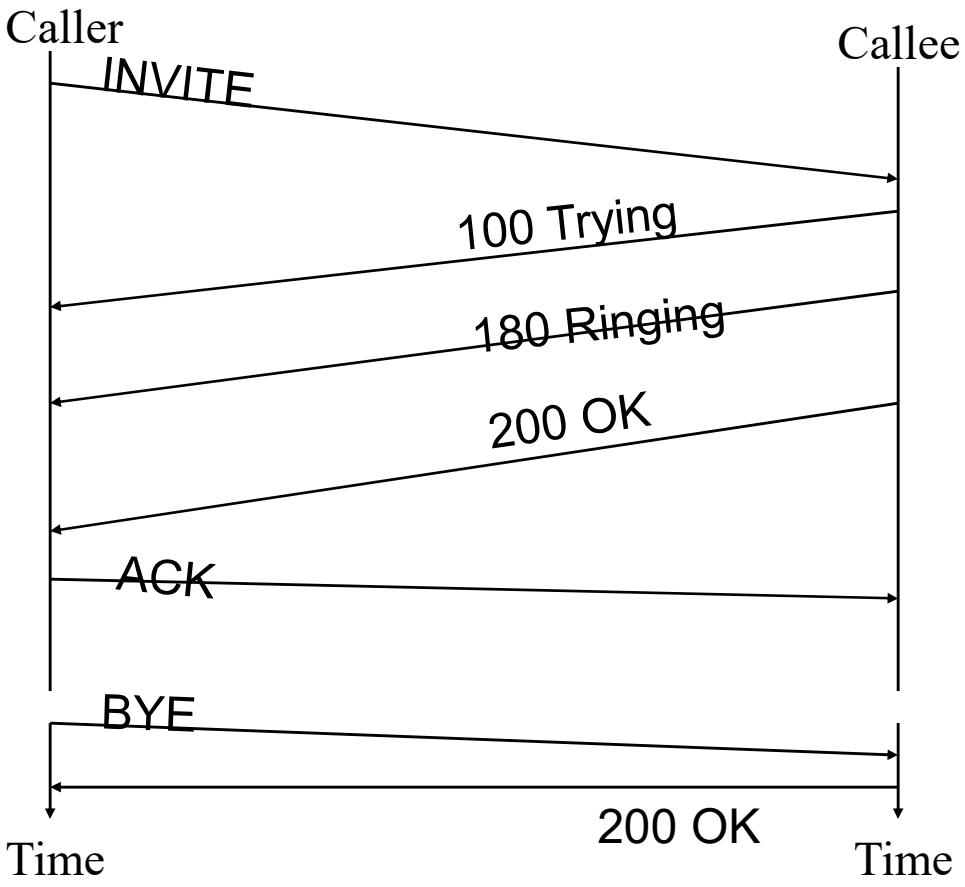
```
1-xx: Informational     2-xx: Successful          3-xx: Redirection
100 Trying              200 OK                    300 Multiple Choices
180 Ringing                                       301 Moved Temporarily
...                                               ...

4-xx: Request Failure   5-xx: Server Failure      6-xx: Global Failure
400 Bad Request         500 Server Internal Error 603: Decline
482 Loop Detected       501 Not Implemented       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):



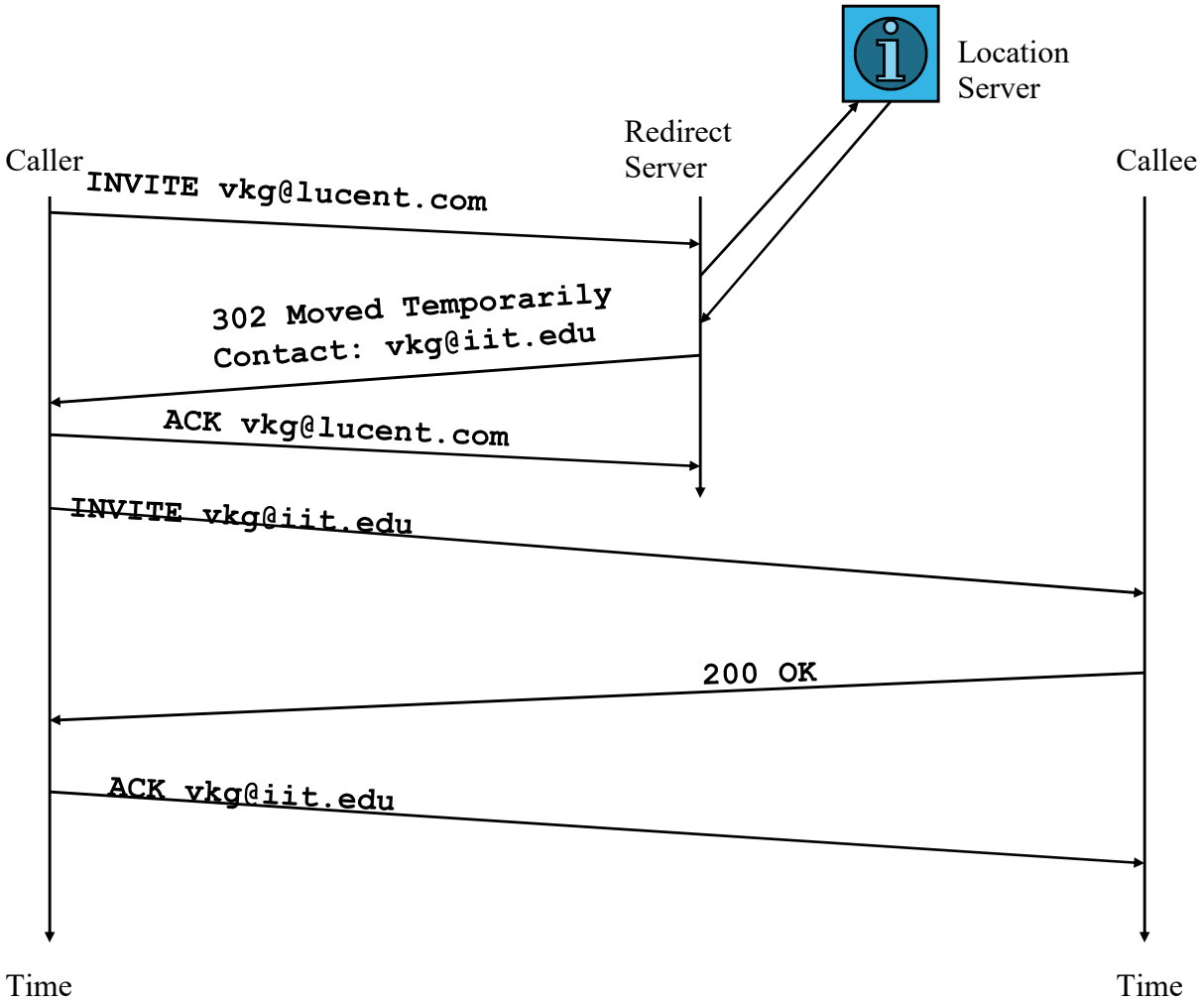
Notes:

- 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!!

NOKIA

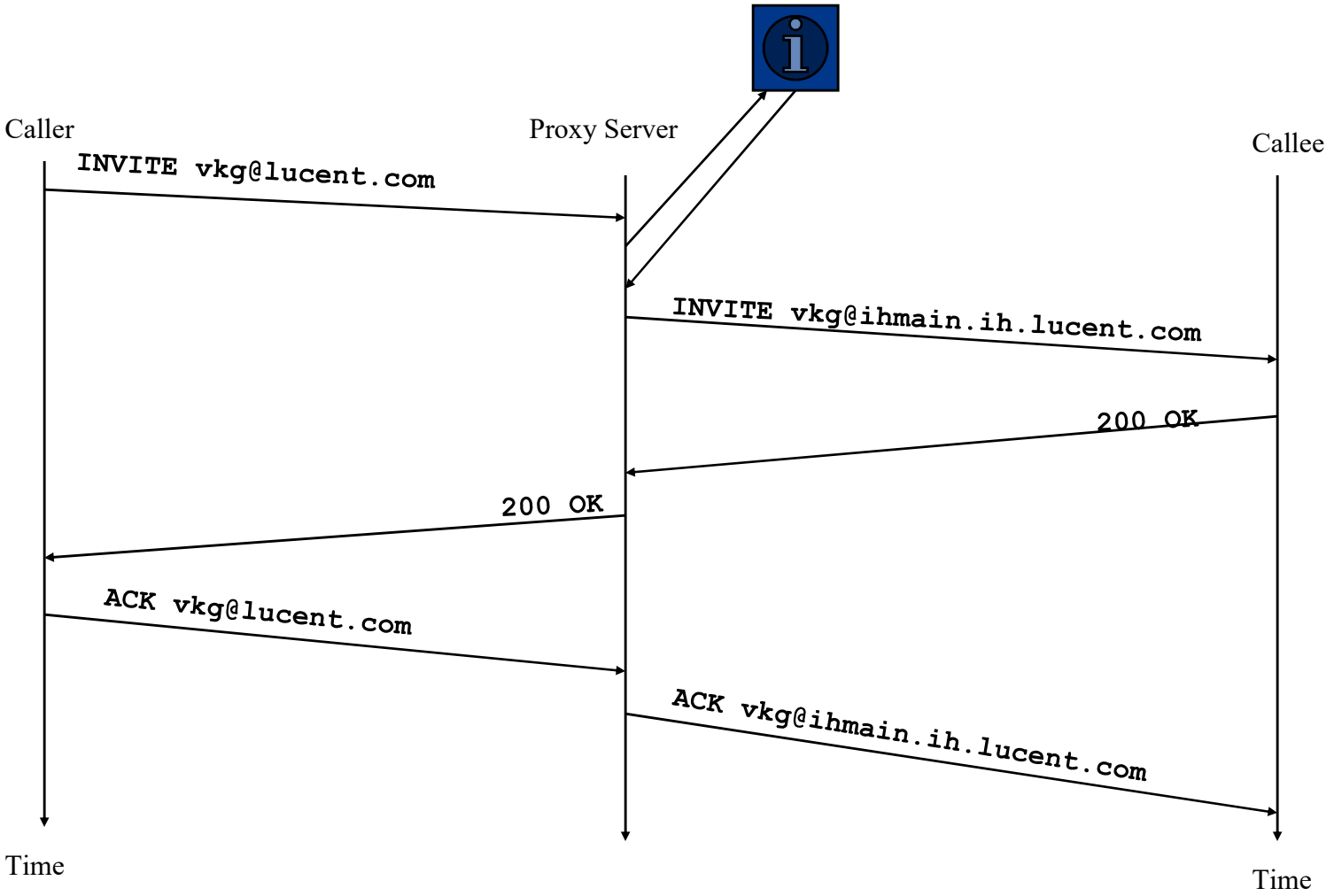
SIP Call Flow (Redirection):



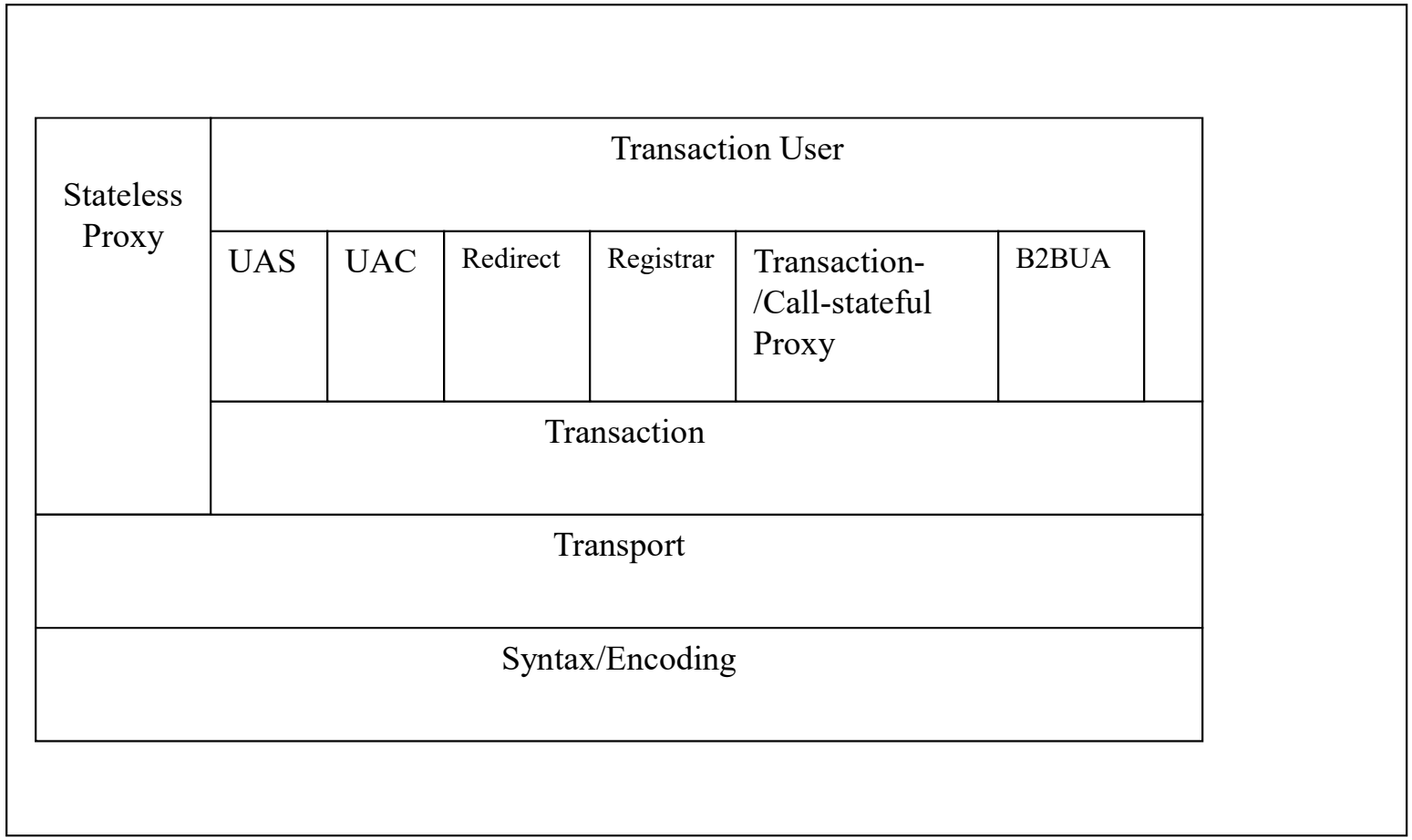
Note:

- Media flows directly between the two endpoints.

SIP Call Flow (Proxy Server):



SIP: A prototypical stack layering



NOKIA

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=9fxced76sl
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=9fxced76sl
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=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 2 INVITE
Content-Length: 0
```


NOKIA

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=9fxced76sl
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
```


NOKIA

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=9fxced76sl
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=9fxced76sl
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
o=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
```

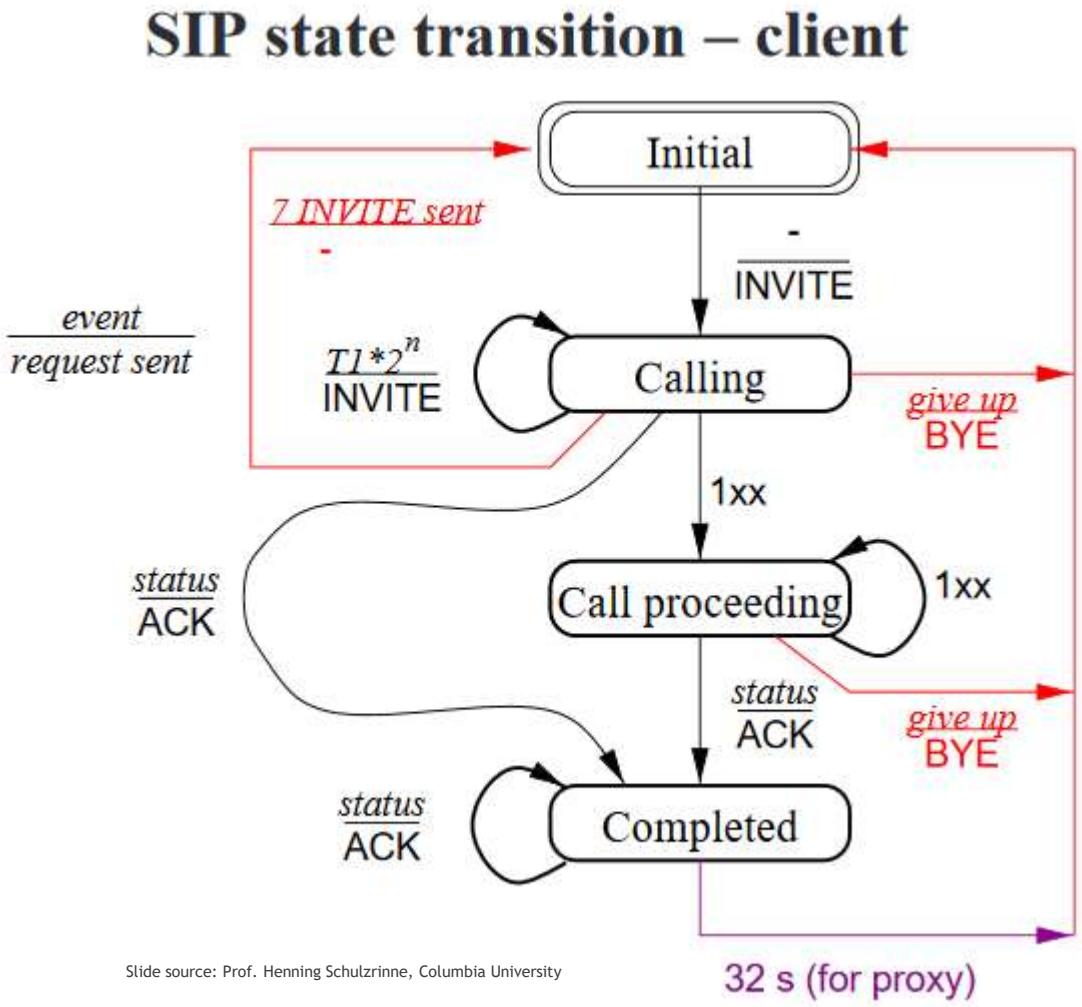
SIP on the wire representation:

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=9fxced76sl
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.

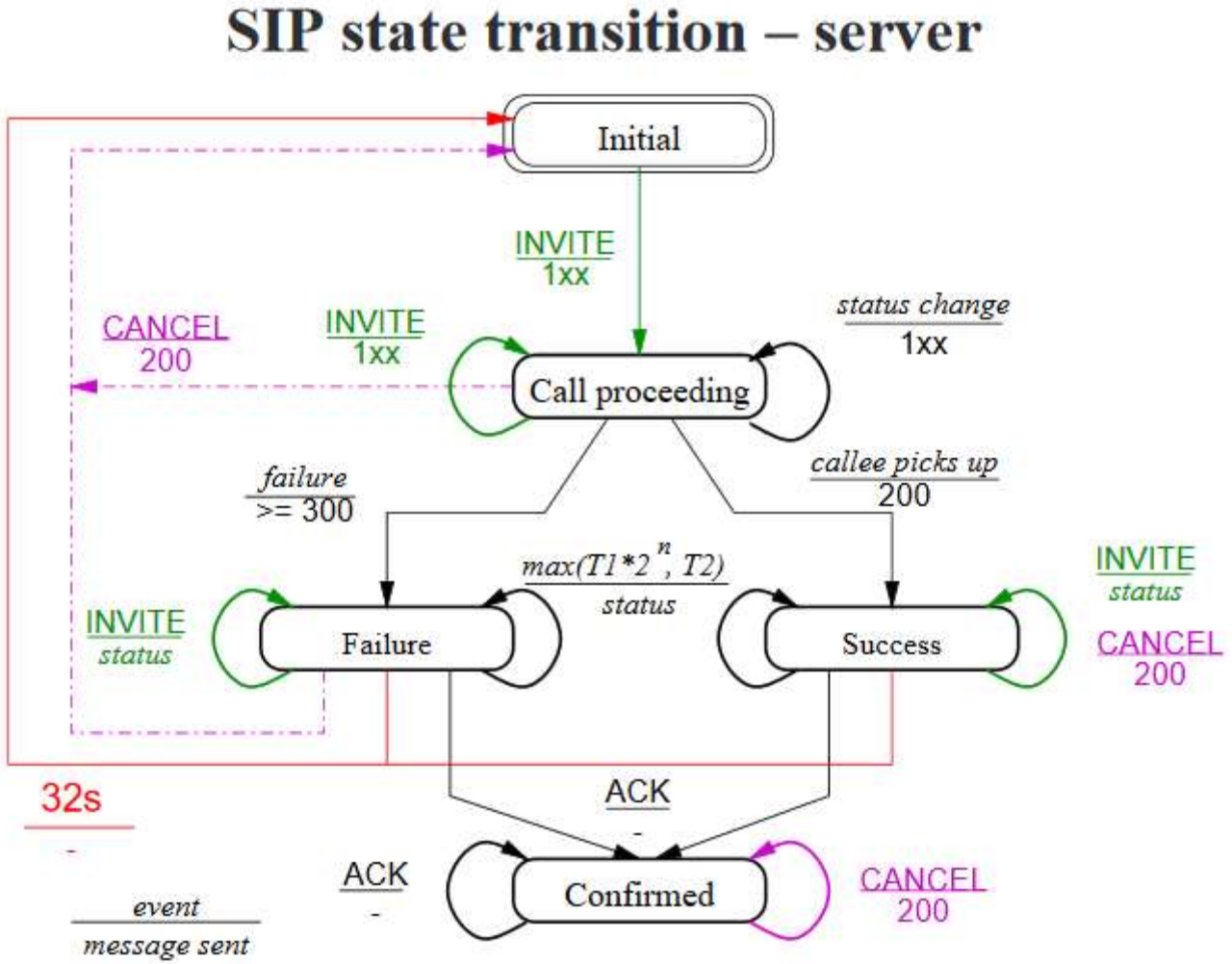
SIP state machines



Slide source: Prof. Henning Schulzrinne, Columbia University

NOKIA

SIP state machines



Slide source: Prof. Henning Schulzrinne, Columbia University

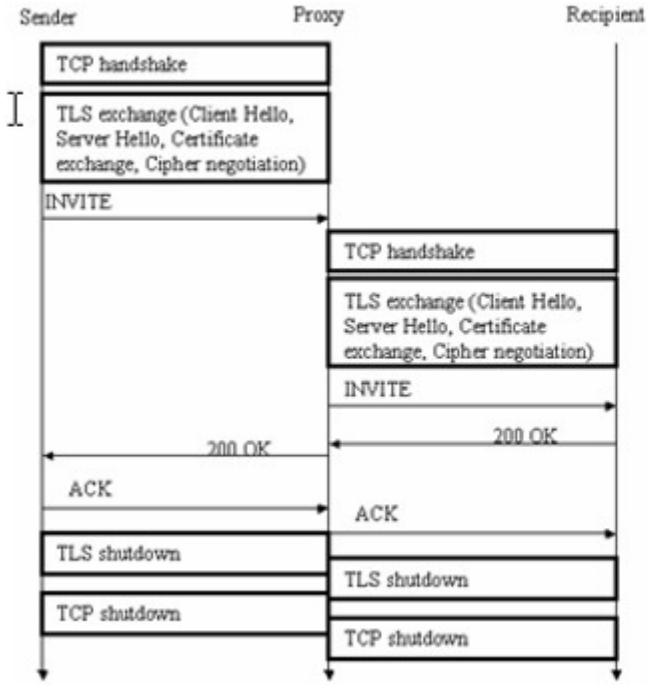
SIP: The specifications

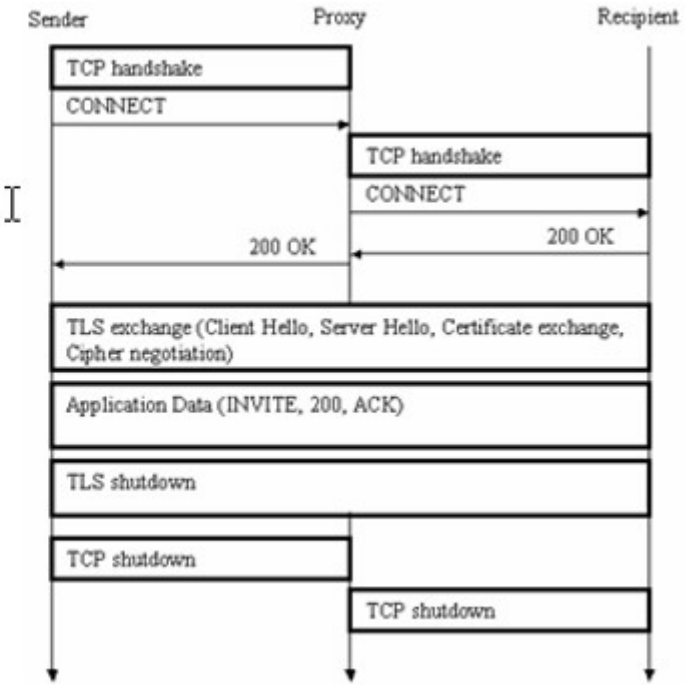
- Core SIP protocol
  - RFCs 3261, 3263 (Locating Servers), 3264 (Offer/Answer model), 3265 (Event Notification framework, or pub/sub), …
- Public-Switched Telephone Network interworking
  - RFCs 2848 (PINT: use SIP to invoke services in PSTN), 3910 (SPIRITS: allows a PSTN switch to ask IP element how 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

Gurbani, V.K., Willis, D., and Audet, F., "Cryptographically Transparent Session Initiation Protocol (SIP) Proxies," *Proceedings of the 2007 IEEE International Conference on Communications (ICC)*, pp. 1185-1190, June 2007, Glasgow, UK





SIP Esoterica

Mitigating Mimicry Attacks in the Session Initiation Protocol

Marchal, S., Mehta, A., Gurbani, V.K., Ho, T.K., State, R. and Sancier-Barbosa, F., "Mitigating mimicry attacks against the Session Initiation Protocol (SIP)," In *IEEE Transactions on Network and Service Management (TNSM)*, pp. 467-482, 12(3), 2015

```
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=tstsip 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 - - - -
```

```
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
Conta ct: <sip:alice@10.111.64.160:5099>;q=0.5
Max-Forwards: 55
Vi a: 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=tstsip 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 - - - -
```


NOKIA

SIP: Time to say BYE

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