SIP/VoIP Technology

PATRIK FÄLTSTRÖM

<paf@cisco.com>

SIP-details based on a presentation by James M. Polk

Session Agenda

- SIP Refresher
- SIP Standards Efforts
- SIP Working Efforts
- SIP Summary
- Reachability

Session Agenda

- SIP Refresher
- SIP Standards Efforts
- SIP Working Efforts
- SIP Summary
- Reachability

SIP Refresher

- **The Session Initiation Protocol (SIP) is an application layer control (signaling) protocol for:**
  - **creating**
  - **modifying and**
  - **terminating**

  multimedia sessions with one or more participants

SIP Refresher (Cont.)

- SIP was originally a multicast session set-up protocol for the I2 (mid-late 90s)
  - then someone figured out it was good for unicast
- First Standardized in March 1999 in RFC 2543
- Revised Standard in May 2002 in RFC 3261, with
  - 22 Standards Track Extension RFCs
  - 21 Working Group Internet Drafts, and
    - > 50 individual IDs that are not WG items (yet)

SIP Refresher (Cont.)

SIP sessions include:

- Internet multimedia conferences
- Internet telephone calls
- Internet Video sessions and
- multimedia distribution

SIP Refresher (Cont.)

SIP members can:

- communicate via:
  - unicast
  - multicast
  - via a mesh of unicast relations or
  - a combination of these
- in IPv4 and IPv6 environments using:
  - UDP
  - TCP
  - SCTP or
  - TLS over TCP

SIP Refresher (Cont.)

SIP components include:

- User Agents (UAs)
- Gateways
- Registrar Servers
- Proxy Servers
- Redirect Servers

SIP Addressing

- **Fully-Qualified Domain Names**

  sip:jdoe.cisco.com

- **SMTP-style Domain Names [RFC 2368]**

  sip:jdoe@cisco.com

- **E.164 style addresses [RFC 2806]**

  sip:14085551234@gateway.com; user=phone

  user=phone means this is a gateway

  (gateway.com is the FQDN of the egress IP gateway)

- **Mixed addresses**

  sip:14085551234@10.1.1.1; user=phone

  sip:jdoe@10.1.1.1

Session Agenda

- SIP Refresher
- SIP Standards Efforts
- SIP Working Efforts
- SIP Summary
- Reachability

SIP Standards Efforts

- SIP Methods
- SIP Headers
- SIP Message Bodies (MIME and SDP)
- NAT/Firewall traversal
- SIP Security (Digest, TLS, IPsec, S/MIME, NAI)

SIP Methods

- Register
- Invite
- ACK
- BYE
- Cancel
- Options
- PRACK
- Subscribe
- Notify
- Message
- INFO
- Update
- Refer

SIP Methods: REGISTER

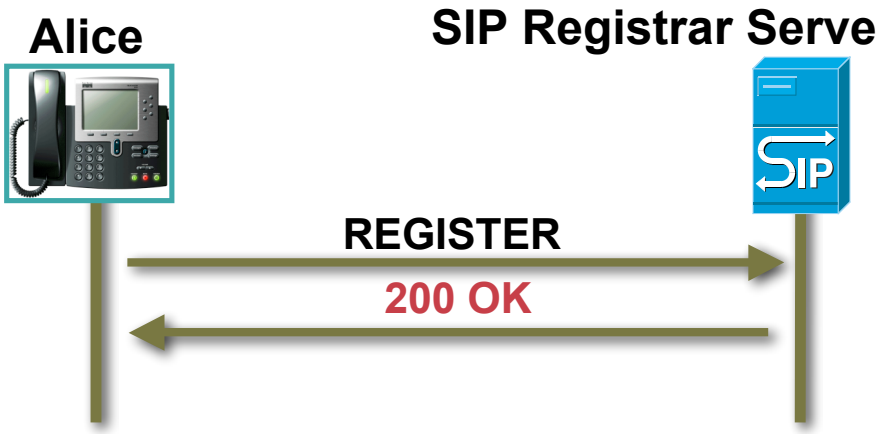

```
REGISTER sip:atlanta.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bk2l55n1
To: Alice <sip:alice@atlanta.com>
From: Alice <sip:alice@atlanta.com>;tag=283074
Call-ID: a84b4g96te10@pc33.atlanta.com
CSeq: 31862 REGISTER
Contact: <sip:alice@10.1.3.33>
Expires: 21600
Content-Length: 0
```

REGISTER - Binds a SIP URI (called an Address of Record (AOR)) with a contact name in a location service

- Enables UAs to receive SIP messages
- Registrations represent a dynamic piece of state maintained in a network

- **UAs can use three ways to determine the address to which to send registrations:**
  - Configuration
  - Address-of-Record
  - Multicast [224.0.1.75]

SIP Methods: REGISTER




```
SIP/2.0 200 OK
Via: SIP/2.0/TCP server19.atlanta.com
 ;branch=z9hG4bk2l55n1; received=10.1.3.33
To: Alice <sip:alice@atlanta.com>
From: server19.atlanta.com ;tag=283074
Call-ID: a84b4g96te10@pc33.atlanta.com
CSeq: 31862 REGISTER
Contact: <sip:alice@pc33.atlanta.com>
Contact: <sip:alice@cm9013.atlanta.com>
Expires: 3600
Contact-Length: 0
```

REGISTER - Binds a SIP URI (called an Address of Record (AOR)) with a contact name in a location service

- The 200 (OK) response from the registrar contains a list of Contact fields enumerating all current bindings
- Expires Header informs UA how long Registration lasts before a refresh is required
- Because devices can be “always on”, a domain can request that a SIP device re-authenticate to the domain

RFC 3261

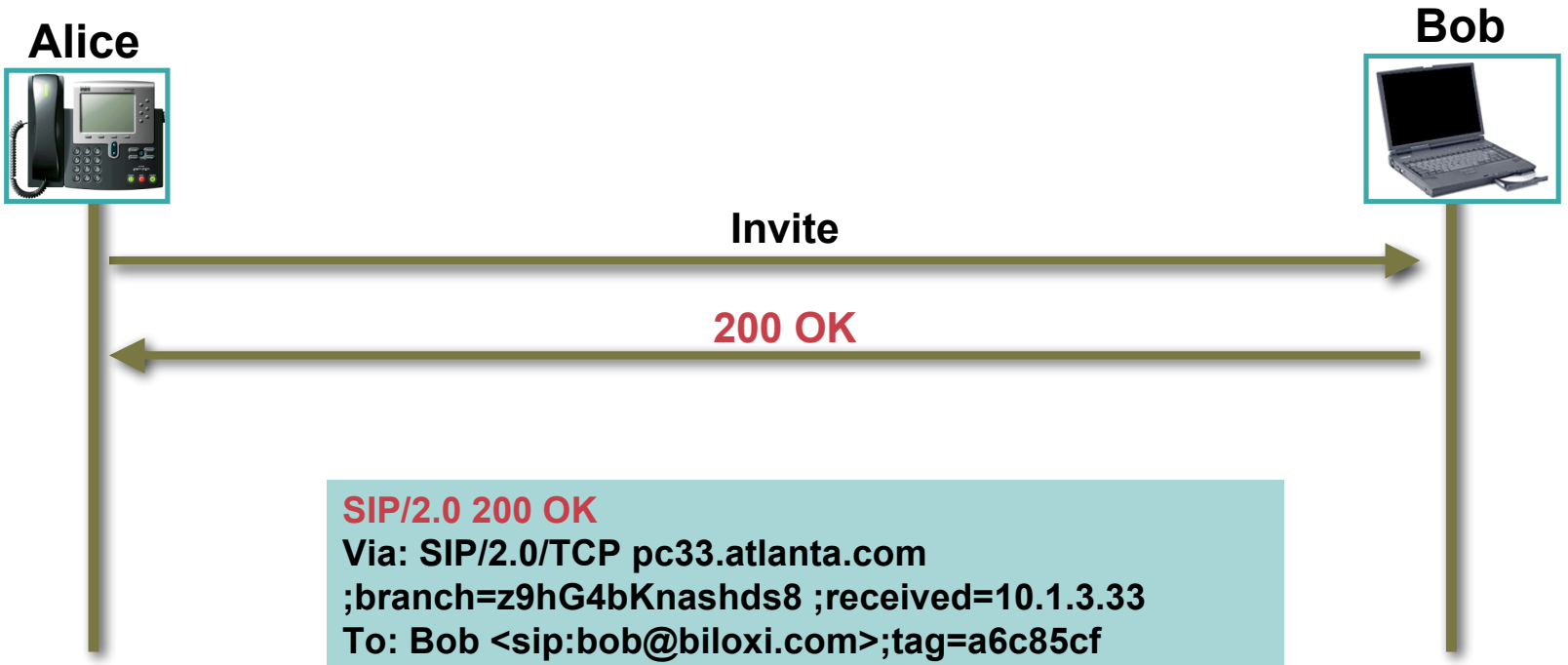
SIP Methods: INVITE, ACK and BYE

Cisco.com


```
INVITE sip:bob@192.168.10.20 SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

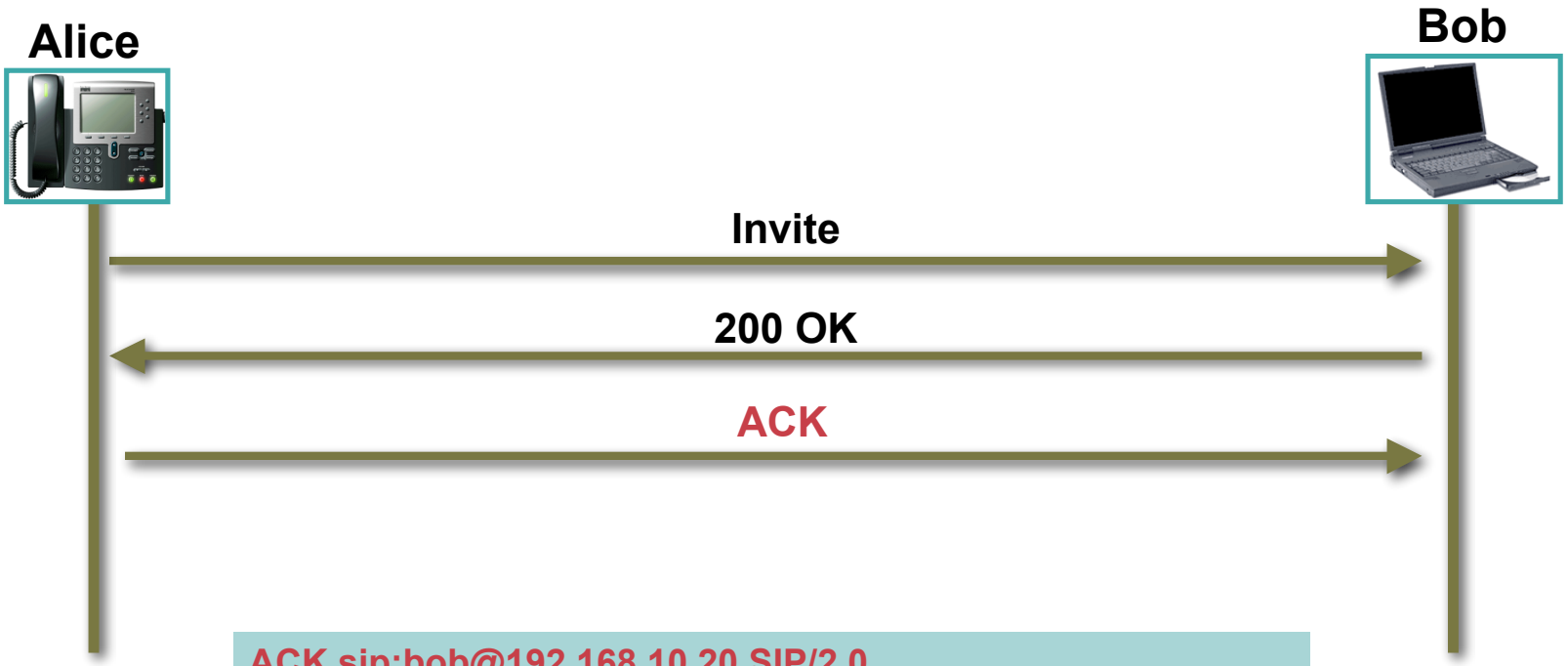
SIP Methods: INVITE, ACK and BYE



SIP/2.0 200 OK
Via: SIP/2.0/TCP pc33.atlanta.com
;branch=z9hG4bKnashds8 ;received=10.1.3.33
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:bob@192.168.10.20>
Content-Type: application/sdp
Content-Length: 131

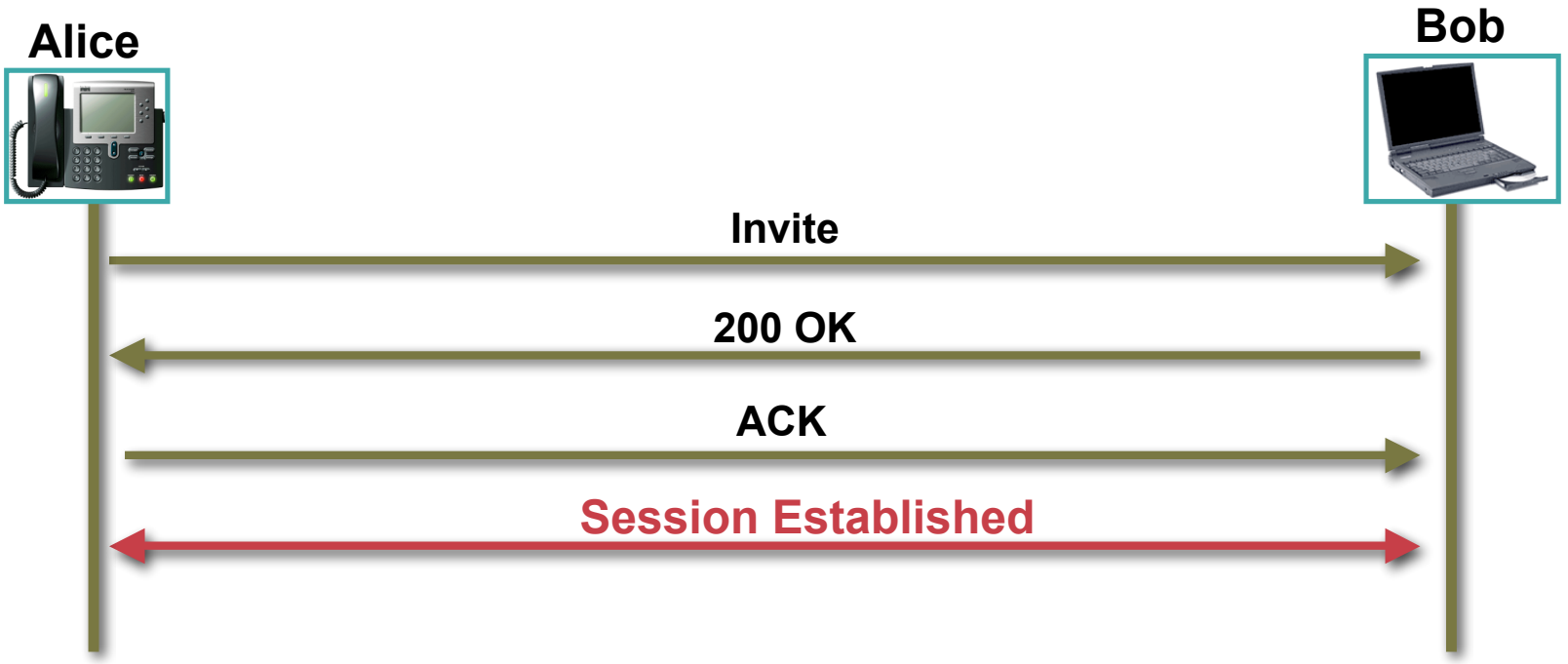
(Bob's SDP not shown)

SIP Methods: INVITE, ACK and BYE




```
ACK sip:bob@192.168.10.20 SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com;branch=z9hG4bKnashds8
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 ACK
Content-Length: 0
```

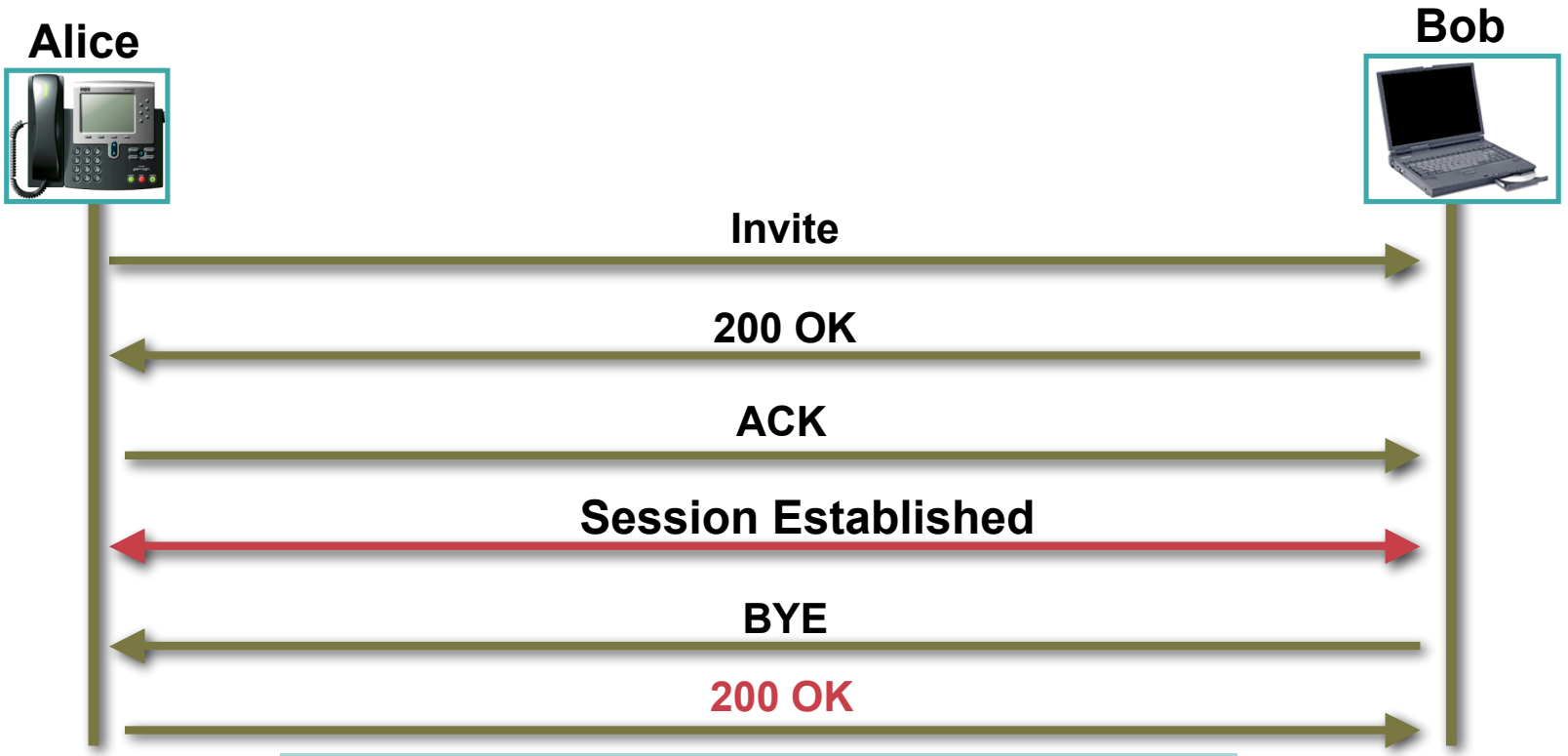
SIP Methods: INVITE, ACK and BYE



SIP Methods: INVITE, ACK and BYE

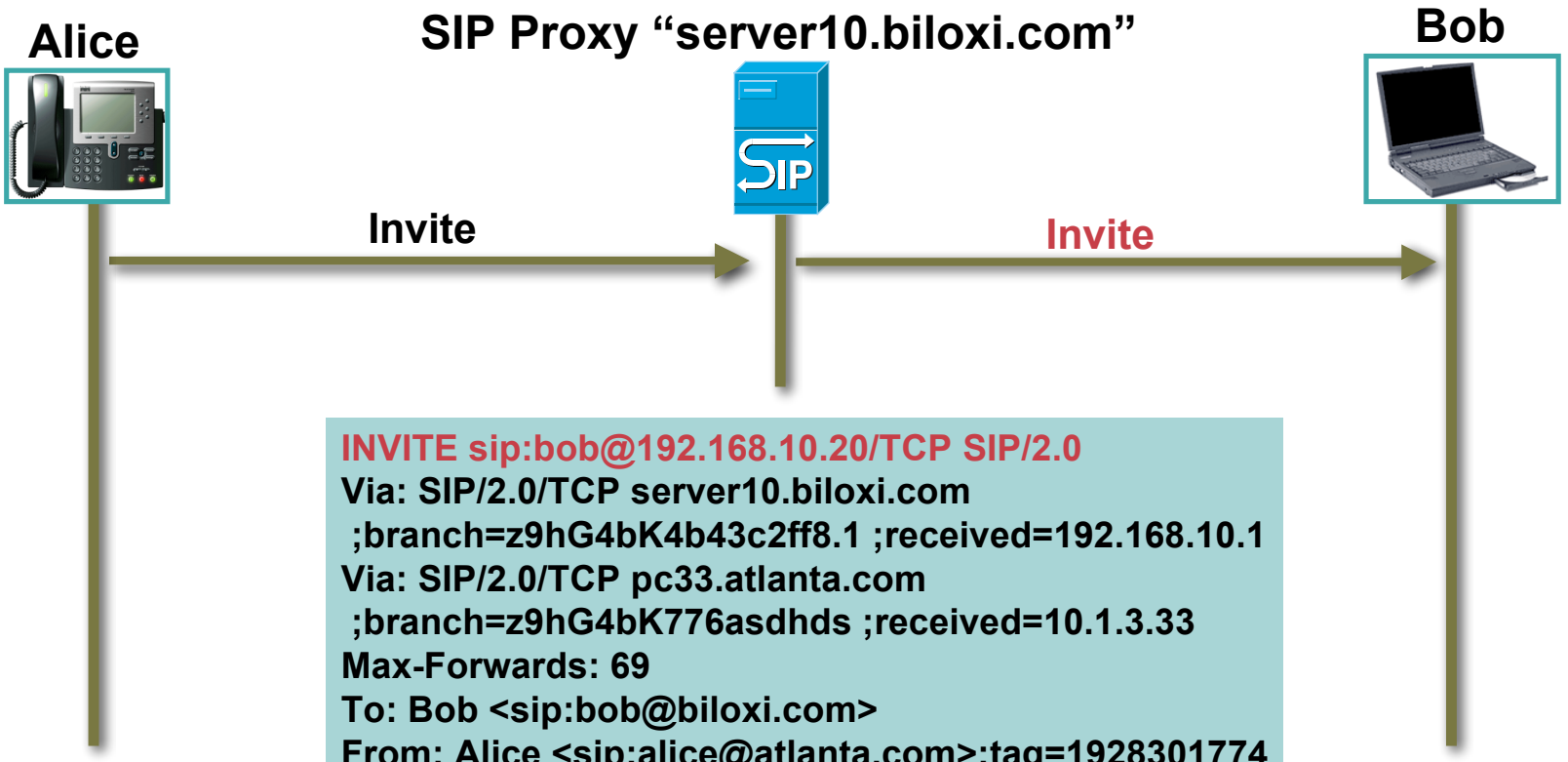

```
BYE sip:alice@pc33.atlanta.com SIP/2.0
Via: SIP/2.0/TCP 10.1.3.33;branch=z9hG4bKnashds8
Max-Forwards: 70
From: Bob <sip:bob@biloxi.com>;tag=a6c85cf
To: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 231 BYE
Content-Length: 0
```

SIP Methods: INVITE, ACK and BYE




```
SIP/2.0 200 OK
Via: SIP/2.0/TCP 192.168.10.20
From: Alice <sip:alice@atlanta.com>;tag=1928301774
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
Call-ID: a84b4c76e66710
CSeq: 231 BYE
Content-Length: 0
```

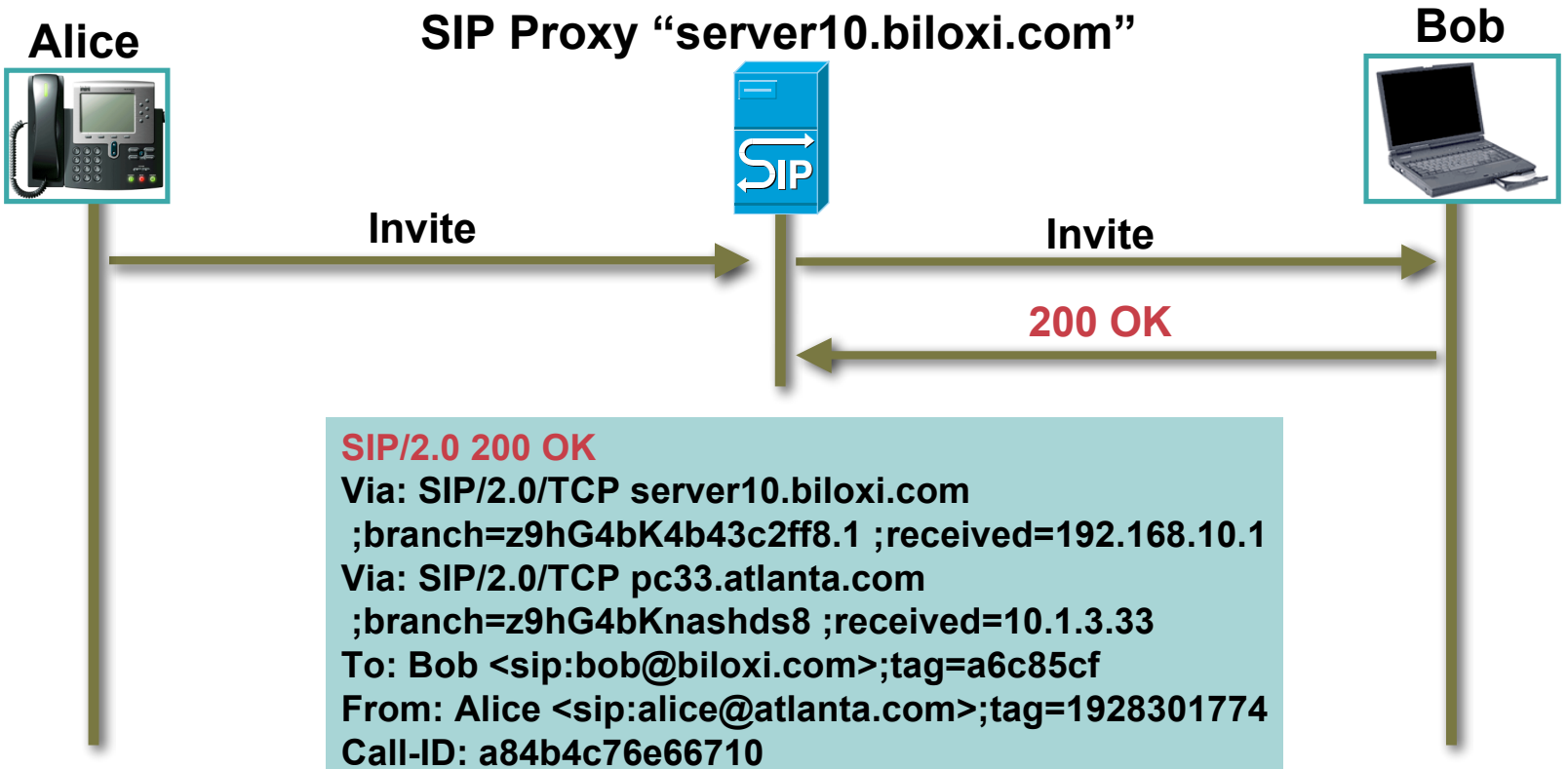
SIP Methods: INVITE, ACK and BYE w/Proxy




```
INVITE sip:bob@192.168.10.20/TCP SIP/2.0
Via: SIP/2.0/TCP server10.biloxi.com
 ;branch=z9hG4bK4b43c2ff8.1 ;received=192.168.10.1
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bK776asdhds ;received=10.1.3.33
Max-Forwards: 69
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

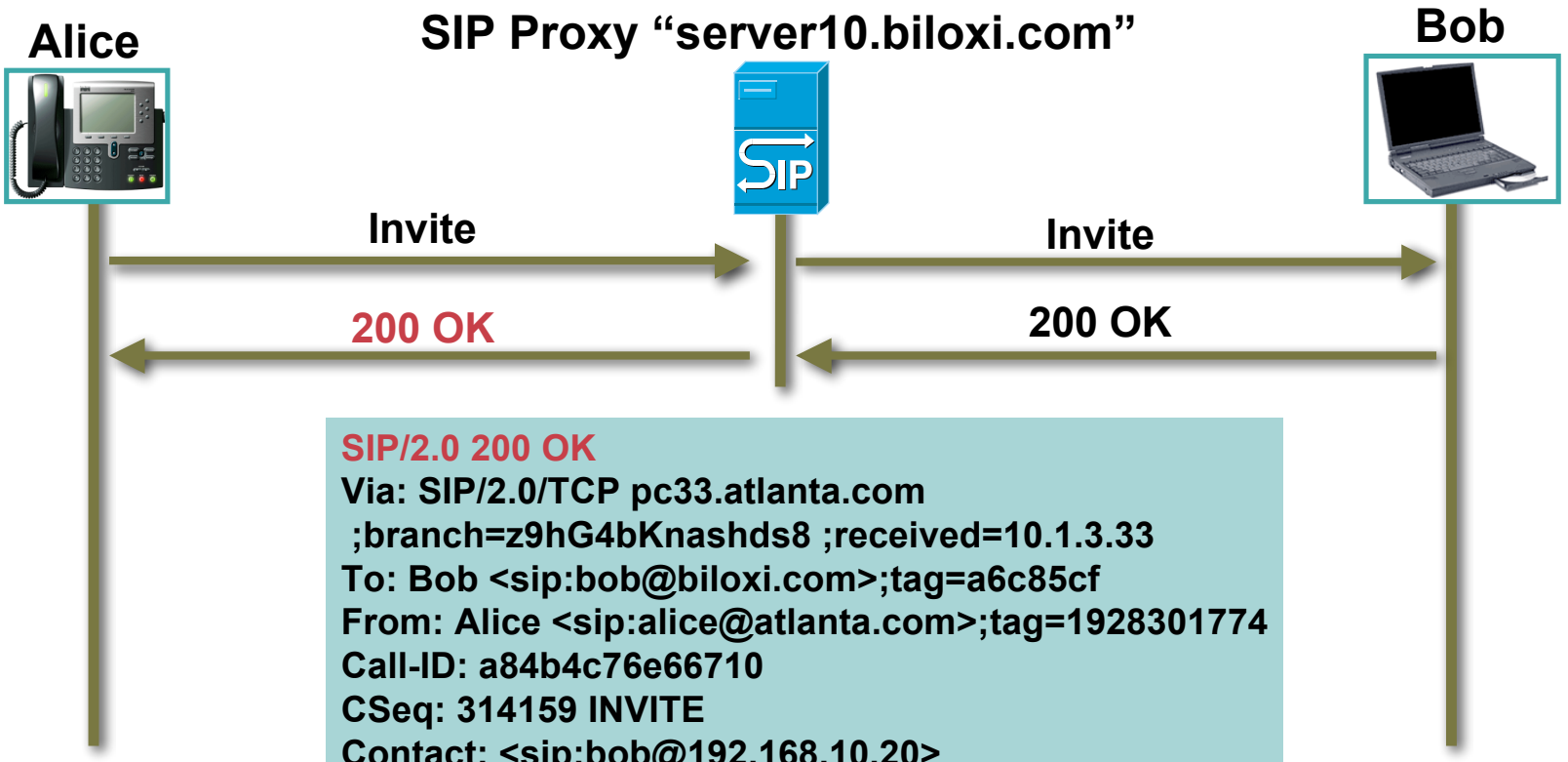
SIP Methods: INVITE, ACK and BYE w/Proxy



SIP/2.0 200 OK
Via: SIP/2.0/TCP server10.biloxi.com
;branch=z9hG4bK4b43c2ff8.1 ;received=192.168.10.1
Via: SIP/2.0/TCP pc33.atlanta.com
;branch=z9hG4bKnashds8 ;received=10.1.3.33
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:bob@192.168.10.20>
Content-Type: application/sdp
Content-Length: 131

(Bob's SDP not shown)

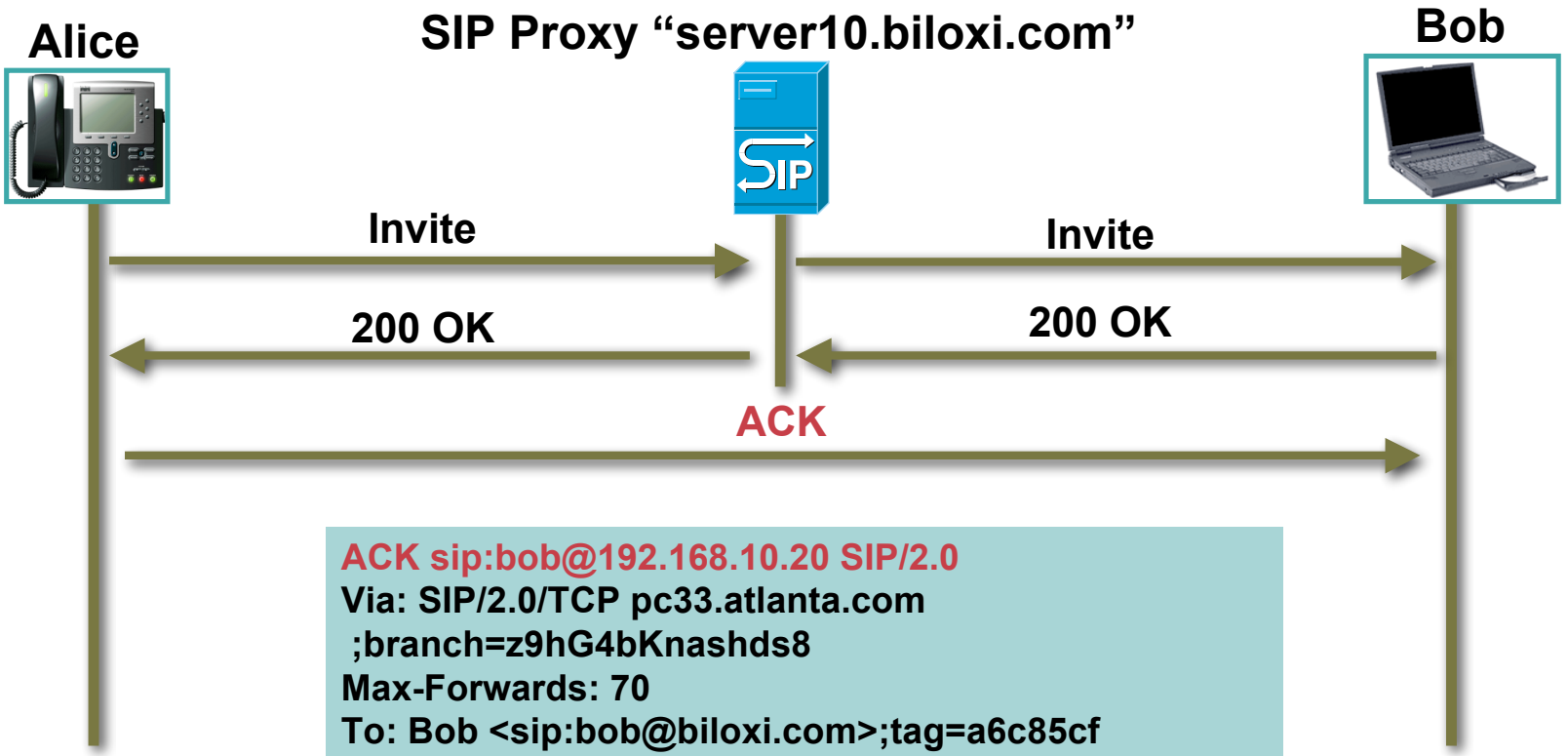
SIP Methods: INVITE, ACK and BYE w/Proxy



SIP/2.0 200 OK
Via: SIP/2.0/TCP pc33.atlanta.com
;branch=z9hG4bKnashds8 ;received=10.1.3.33
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:bob@192.168.10.20>
Content-Type: application/sdp
Content-Length: 131

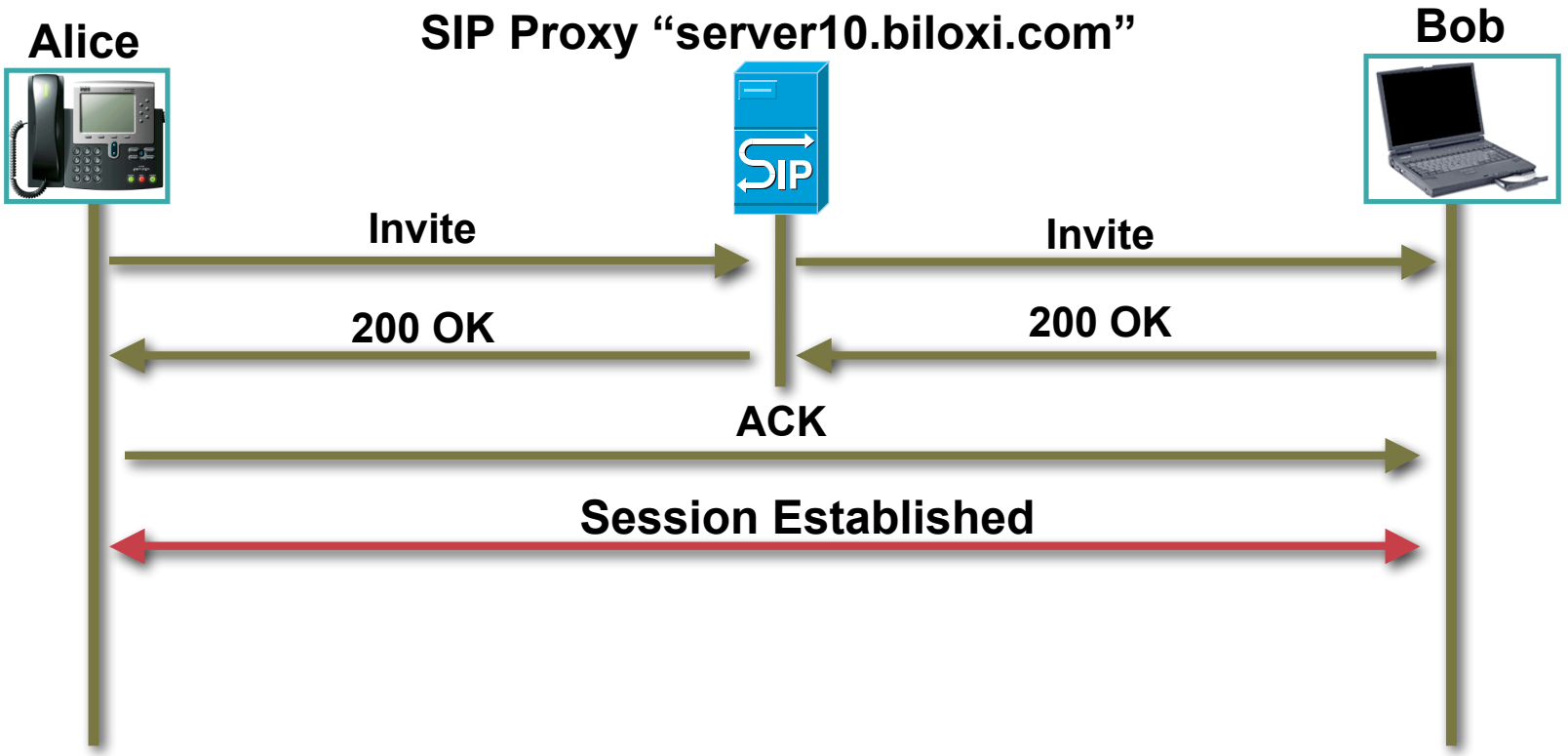
(Bob's SDP not shown)

SIP Methods: INVITE, ACK and BYE w/Proxy




```
ACK sip:bob@192.168.10.20 SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bKnashds8
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 ACK
Content-Length: 0
```

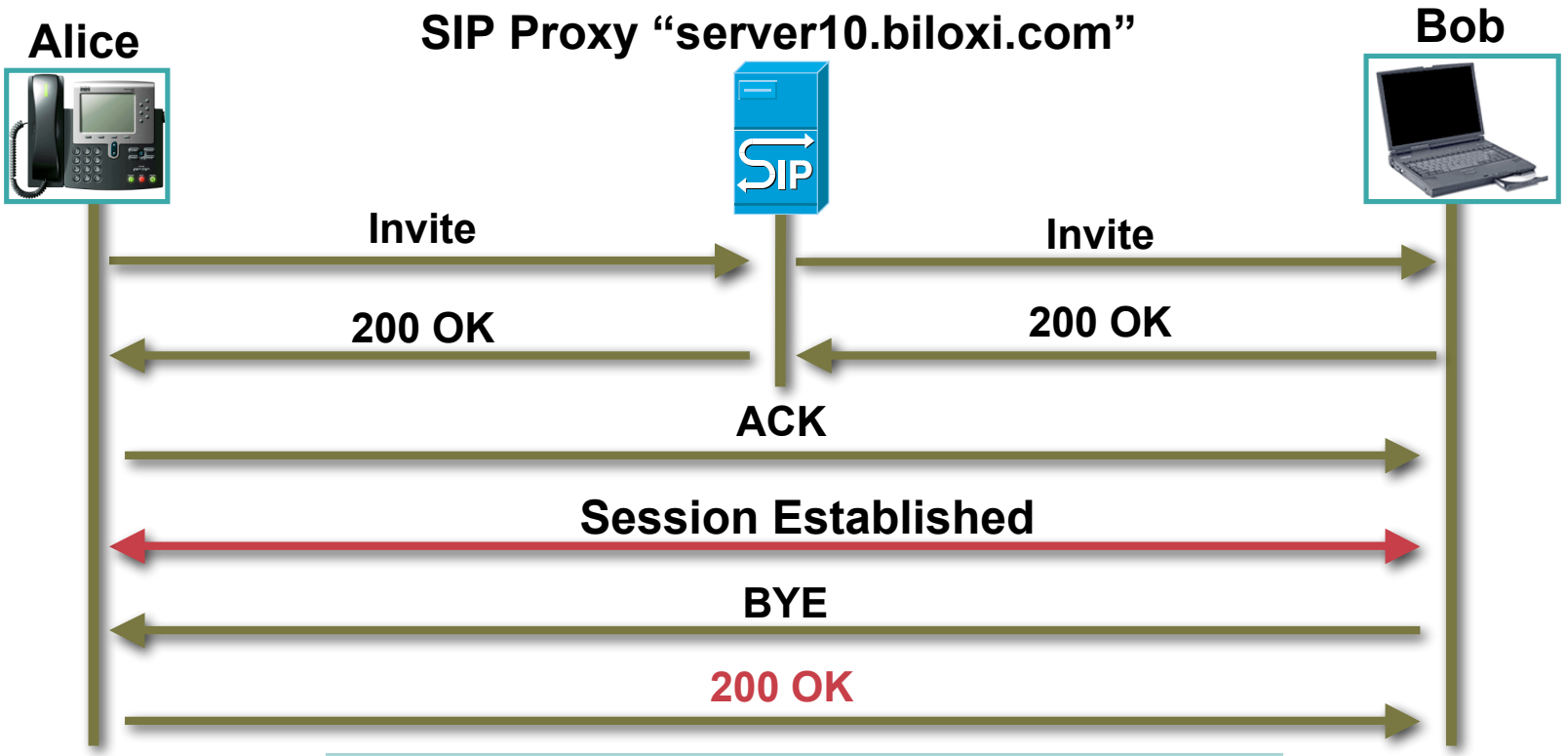
SIP Methods: INVITE, ACK and BYE w/Proxy



SIP Methods: INVITE, ACK and BYE w/Proxy


```
BYE sip:alice@pc33.atlanta.com SIP/2.0
Via: SIP/2.0/TCP 10.1.3.33;branch=z9hG4bKnashds8
Max-Forwards: 70
From: Bob <sip:bob@biloxi.com>;tag=a6c85cf
To: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 231 BYE
Content-Length: 0
```

SIP Methods: INVITE, ACK and BYE w/Proxy




```
SIP/2.0 200 OK
Via: SIP/2.0/TCP 192.168.10.20
From: Alice <sip:alice@atlanta.com>;tag=1928301774
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
Call-ID: a84b4c76e66710
CSeq: 231 BYE
Content-Length: 0
```

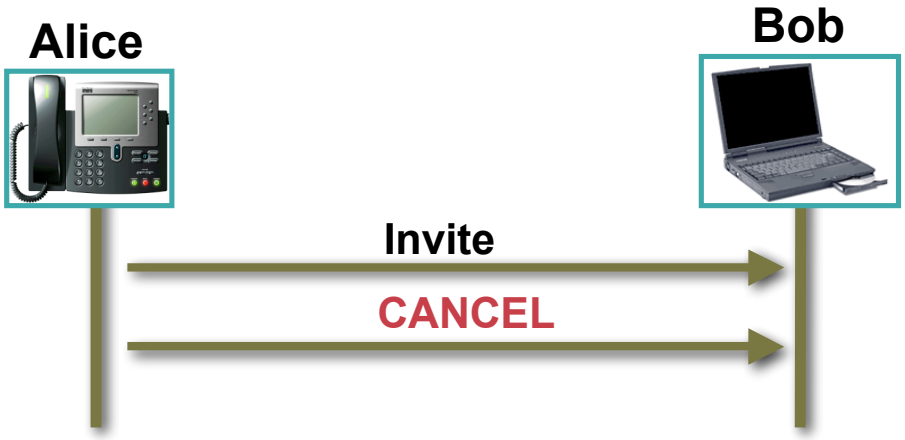
SIP Methods: CANCEL


```
INVITE sip:bob@192.168.10.20 SIP/2.0
Via: SIP/2.0/TCP 10.1.3.33
 ;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

CANCEL— discontinues pending requests; does not terminate sessions that have been accepted

SIP Methods: CANCEL

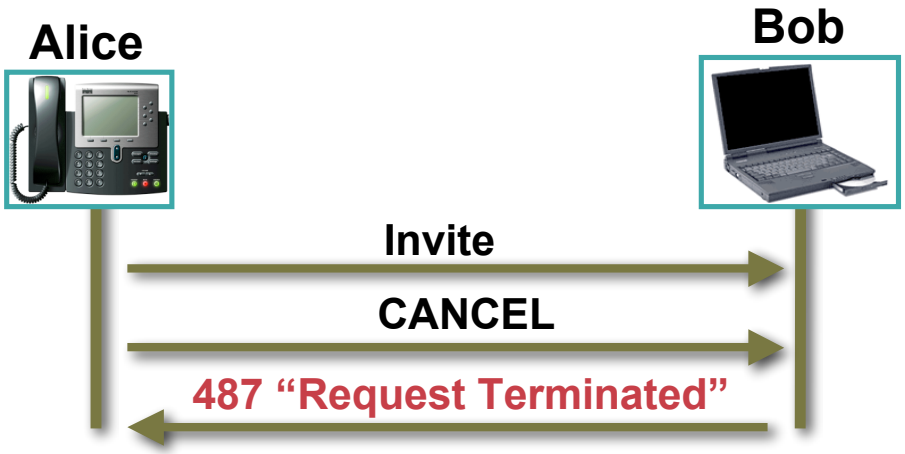



```
CANCEL sip:bob@192.168.10.20 SIP/2.0
Via: SIP/2.0/TCP 10.1.3.33
 ;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 10197 CANCEL
Contact: <sip:alice@atlanta.com>
Reason: SIP ;cause=486 ;text="Busy"
Content-Length: 0
```

CANCEL— discontinues pending requests; does not terminate sessions that have been accepted

- Reason Header will give the reason
- Here, the caller may have hung up to accept another call before the first was accepted

SIP Methods: CANCEL




```
SIP/2.0 487 Request Terminated
Via: SIP/2.0/TCP 10.1.3.33
From: Alice <sip:alice@atlanta.com>;tag=1928301774
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 10197 CANCEL
Content-Length: 0
```

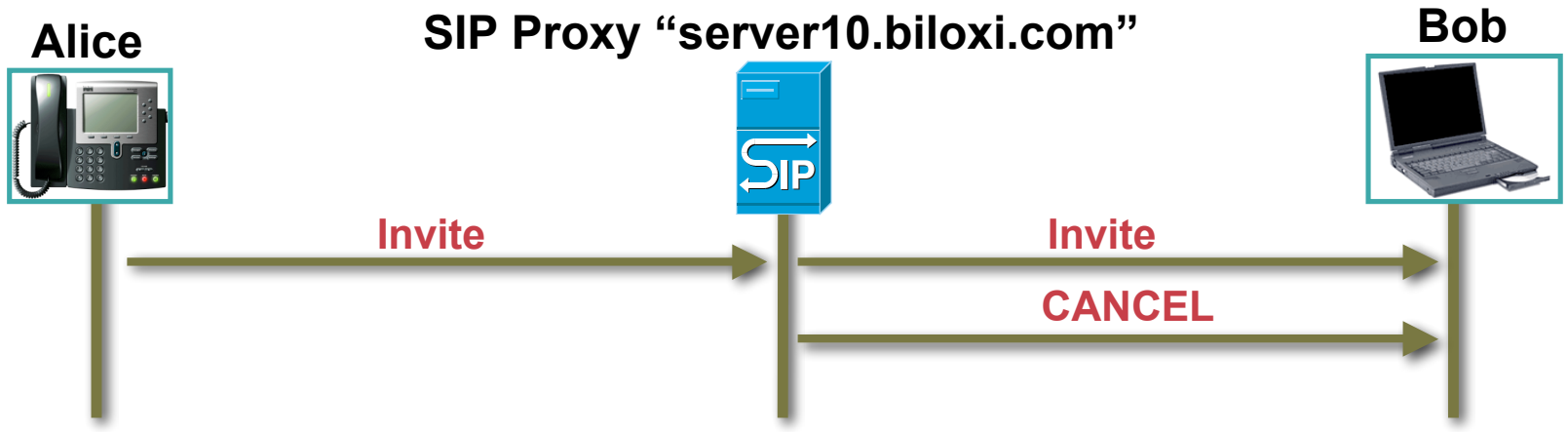
CANCEL— discontinues pending requests; does not terminate sessions that have been accepted

- **487 "Request Terminated is the proper Response to an INVITE Request**

RFC 3261

SIP Methods: CANCEL w/Proxy

Cisco.com

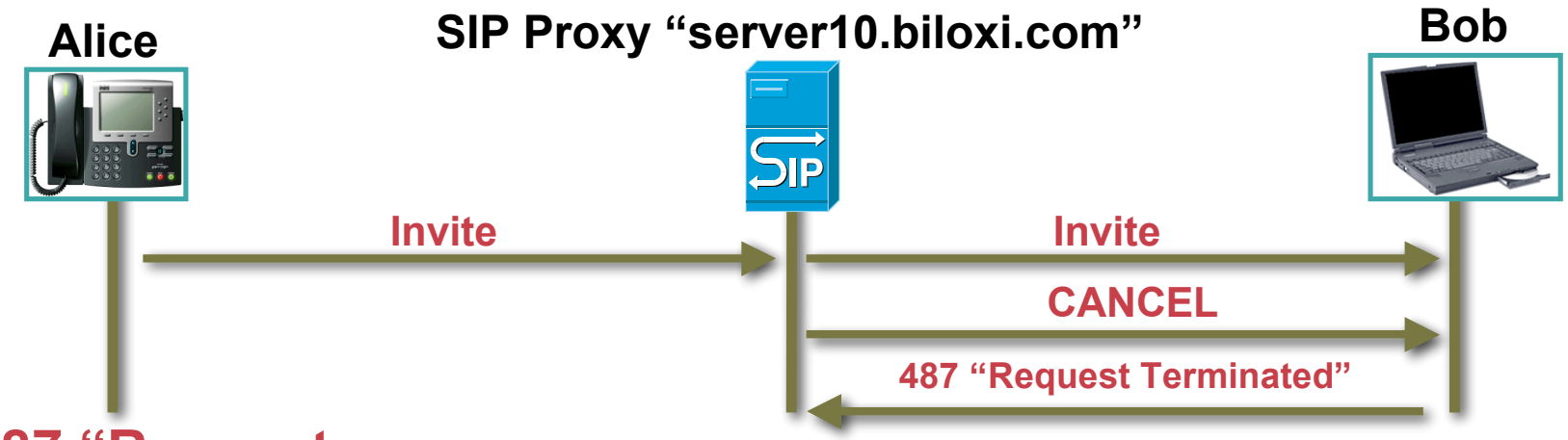


Why would a Proxy do a CANCEL by itself?

- A Sequential or concurrent forking cleanup, for example
- In this case, Proxy received 200 OK from another Forked INVITE

```
CANCEL sip:bob@192.168.10.20/TCP SIP/2.0
Via: SIP/2.0/TCP server10.biloxi.com
 ;branch=z9hG4bK4b43c2ff8.1 ;received=192.168.10.1
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Server10 <sip:server10.biloxi.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 6187 CANCEL
Contact: <sip:server10.biloxi.com>
Reason: SIP ;cause=200 ;text=”call completed elsewhere”
Content-Length: 0
```

SIP Methods: CANCEL w/Proxy



- **487 "Request Terminated" is immediately sent by Bob's UA to cancel this INVITE Request**
- **If Bob's UA had already sent a 200 OK prior to receiving the CANCEL, the CANCEL would be ignored**

```
SIP/2.0 487 Request Terminated
Via: SIP/2.0/TCP 192.168.10.20
From: Alice <sip:alice@atlanta.com>;tag=1928301774
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 6187 CANCEL
Content-Length: 0
```

SIP Methods: OPTIONS

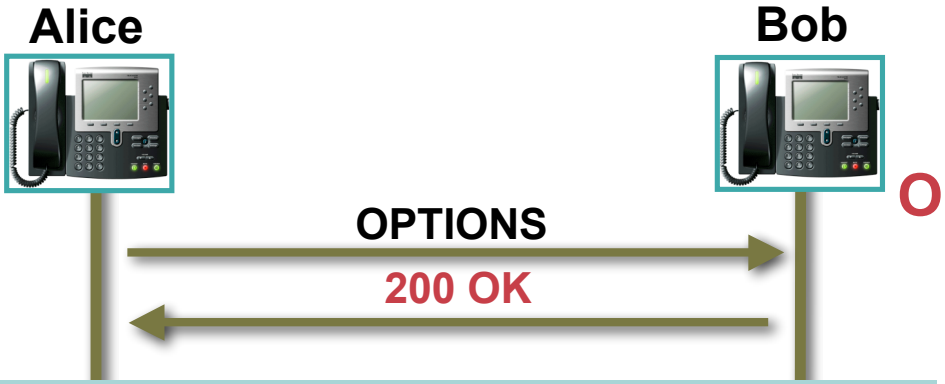

```
OPTIONS sip:bob@192.168.10.20 SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bK77i832k9 ;received=10.1.3.33
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e6Kr456@pc33.atlanta.com
CSeq: 22757 OPTIONS
Contact: <sip:alice@pc33.atlanta.com>
Accept: application/sdp
Content-Length: 0
```

OPTIONS—enables queries of the capabilities of UASs or servers

- Allows a UAC to discover the supported:
  - methods,
  - content types,
  - extensions,
  - codecs,
  - etc.

  without "ringing" the other party

SIP Methods: OPTIONS



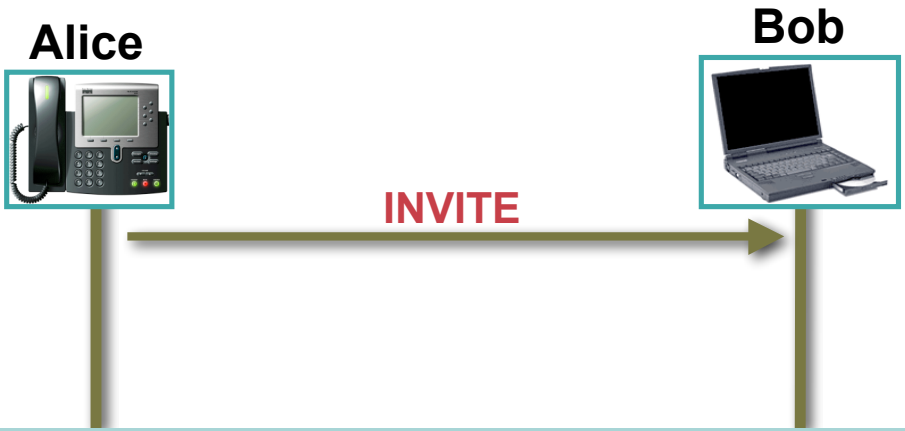
SIP/2.0 200 OK
Via: SIP/2.0/TCP sip:alice@atlanta.com
;branch=z9hG4bK77i832k9 ;received=10.1.3.33
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e6Kr456@pc33.atlanta.com
CSeq: 22757 OPTIONS
Contact: <sip:bob@biloxi.com>
Contact: <mailto:bob@biloxi.com>
Allow: INVITE, ACK, OPTIONS, BYE, CANCEL, REFER
Accept: application/sdp
Accept-language: en
Content-Type: application/sdp
Content-Length: 274

(Bob's SDP indicating those parameters not shown)

OPTIONS—enables queries of the capabilities of UASs or servers

- 200 OK provides all:
  - Contacts known
  - Methods supported
  - Language supported
  - Message Body type
- A 486 "Busy Here" is returned if the UA is not ready to accept a new Request

SIP Methods: PRACK




```
INVITE sip:bob@192.168.10.20 SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bK776asdhds ;received=10.1.3.33
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Requires: 100rel
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

PRACK- a reliable provisional response

- purpose is to acknowledge progress information on a requesting process
- The INVITE Includes a Requires header stipulating the UAC wants a reliable provisional response

SIP Methods: PRACK

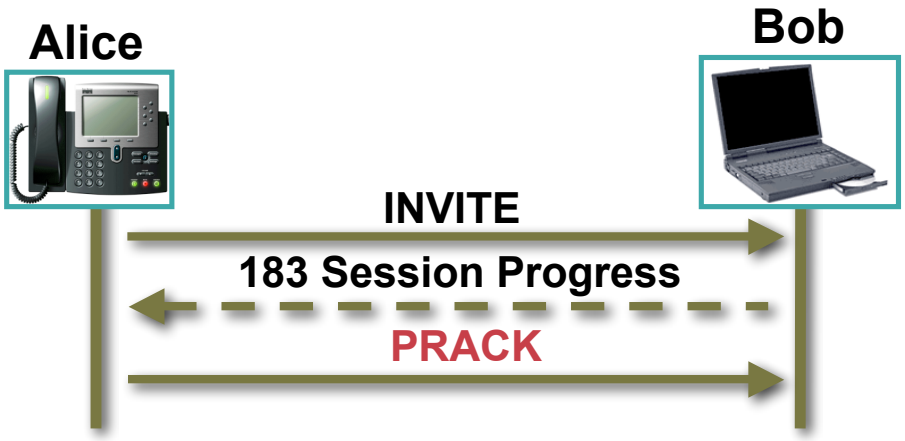

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bK776asdhds
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
RSeq: 813520
Contact: <sip:alice@pc33.atlanta.com>
Content-Type:  application/sdp
Content-Length: 235

(Bob's (different) SDP not shown)
```

PRACK- a reliable provisional response

- Includes an RSeq header, which is the sequence number of the reliable message to be generated by the UAC
- Why is this exchange necessary?
  - Perhaps to ensure some condition is met before the UAs transmit media (see Preconditions section)

SIP Methods: PRACK

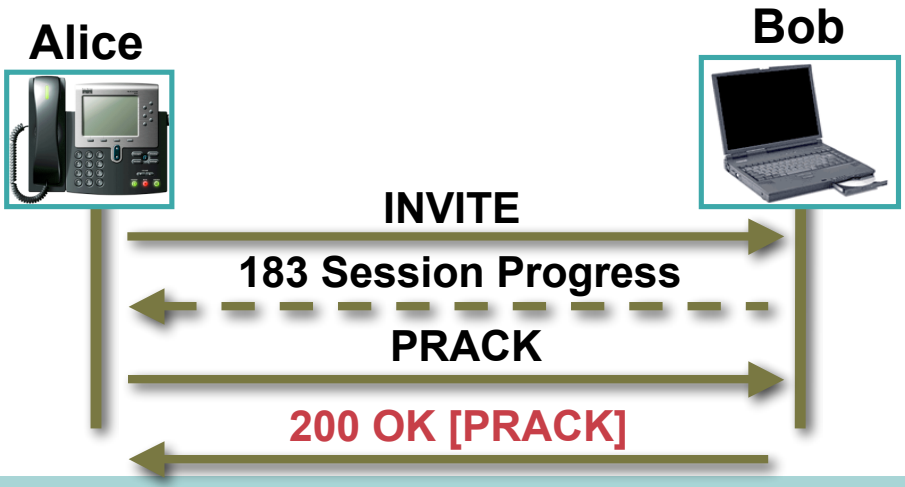



```
PRACK sip:bob@192.168.10.20 SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bK776asi98JK ;received=10.1.3.33
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159
RAck: 813520 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Length: 0
```

PRACK- a reliable provisional response

- sent by UAC after receiving a non-100 Provisional response to an INVITE Request and before the Final Acknowledgement message, but only if asked to within the INVITE
- MUST be sent if an INVITE contained a Require Header with a 100rel option tag
- Includes an RAck header with a matching value to the RSeq number from the 183 message as an acknowledgment of that message

SIP Methods: PRACK




```
SIP/2.0 200 OK sip:bob@192.168.10.20
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bK776asi98JK ;received=10.1.3.33
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 PRACK
Contact: <sip:alice@pc33.atlanta.com>
Content-Length: 0
```

PRACK- a reliable provisional response

- 200 OK to the PRACK is sent by the UAS
- Message flows never end with a PRACK or its 200 OK
  - Later examples will show this

RFC 3265&3680

SIP Methods: SUBSCRIBE & NOTIFY


```
SUBSCRIBE sip:alice@atlanta.com SIP/2.0
Via: SIP/2.0/TCP app_IM.atlanta.com
 ;branch=z9hG4bKnashds7
From: sip:app_IM.atlanta.com ;tag=123aa9
To: sip:alice@atlanta.com
Call-ID: 9987@app_IM.atlanta.com
CSeq: 9887 SUBSCRIBE
Contact: sip:app_IM.atlanta.com
Event: reg
Max-Forwards: 70
Expires: 21600
Accept: application/reginfo+xml
```

SUBSCRIBE - used to request asynchronous notification of an event or set of events at a later time

- method used to request current state and state updates from a remote node
- Expires header SHOULD be present in Request
- Requests MUST have exactly one Event Header value

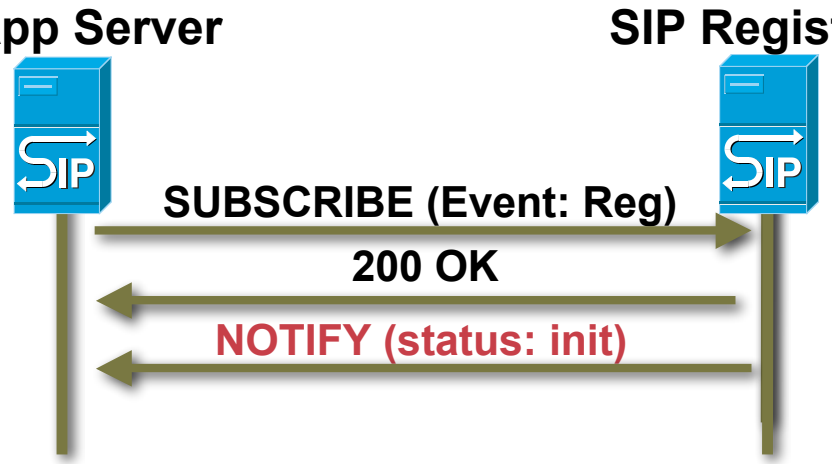
SIP Methods: SUBSCRIBE & NOTIFY

SIP/2.0 200 OK
Via: SIP/2.0/TCP app_IM.atlanta.com ;branch=z9hG4bKnashds7 ;received=10.1.3.2
From: sip:app_IM.atlanta.com ;tag=123aa9
To: sip:alice@atlanta.com ;tag=xyzygg
Call-ID: 9987@app_IM.atlanta.com
CSeq: 9987 SUBSCRIBE
Contact: sip:server19.atlanta.com
Expires: 3600

SUBSCRIBE - used to request asynchronous notification of an event or set of events at a later time

- **Expires header MUST be present in Response**
- **200-class responses indicate that the subscription has been accepted, and that a NOTIFY will be sent immediately**

SIP Methods: SUBSCRIBE & NOTIFY



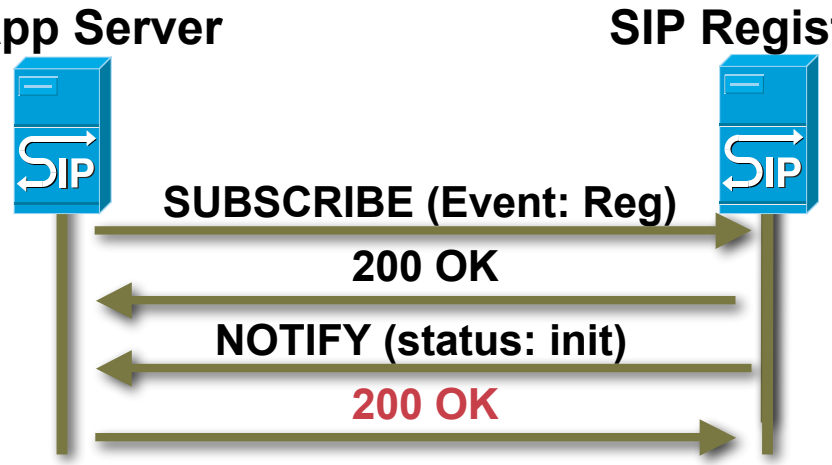
NOTIFY sip:app_IM.atlanta.com SIP/2.0
Via: SIP/2.0/TCP server1.atlanta.com
;branch=z9hG4bKnasaii
From: sip:alice@atlanta.com ;tag=xyzygg
To: sip:app_IM.atlanta.com ;tag=123aa9
Call-ID: 9987@app_IM.atlanta.com
CSeq: 1288 NOTIFY
Contact: sip:server19.atlanta.com
Event: reg
Max-Forwards: 70
Content-Type: application/reginfo+xml
Content-Length: 223

NOTIFY - used to notify a SIP node that an event which has been requested by an earlier SUBSCRIBE method has occurred

- NOTIFY is sent to inform subscribers of changes in state to which the subscriber has a subscription
- Event Header MUST match

```
<?xml version="1.0"?>
  <reginfo xmlns=
           "urn:ietf:params:xml:ns:reginfo"
           version="0" state="full">
    <registration aor="sip:alice@atlanta.com"
           id="a7" state="init" />
  </reginfo>
```

SIP Methods: SUBSCRIBE & NOTIFY



SIP/2.0 200 OK
Via: SIP/2.0/TCP server19.atlanta.com
;branch=z9hG4bKnasaii ;received=10.1.3.1
From: sip:app_IM.atlanta.com ;tag=123aa9
To: sip:alice@atlanta.com ;tag=xyzygg
Call-ID: 9987@app_IM.atlanta.com
CSeq: 1288 NOTIFY
Contact: sip:server1.atlanta.com
Content-Length: 0

NOTIFY - used to notify a SIP node that an event which has been requested by an earlier SUBSCRIBE method has occurred

- **sending a NOTIFY message to an unsuspecting node is invalid behavior, MUST receive a 481 "Subscription does not exist" response**

RFC 3265

SIP Methods: SUBSCRIBE & NOTIFY

Cisco.com

- SUBSCRIBE- 1) method used to request current state and state updates from a remote node
- 2) used to request asynchronous notification of an event or set of events at a later time
  - SUBSCRIBE requests SHOULD contain an "Expires" header which indicates the duration of the subscription
  - Subscriptions need to be refreshed periodically
  - 200-class responses to SUBSCRIBE requests also MUST contain an "Expires" header
  - Subscribers MUST include exactly one "Event" header in SUBSCRIBE requests, indicating to which event or class of events they are subscribing
  - SUBSCRIBE is a dialog-creating method
  - 200-class responses indicate that the subscription has been accepted, and that a NOTIFY will be sent immediately
  - a proxy wishes to see all of the SUBSCRIBE and NOTIFY requests for a given dialog, it MUST record-route the initial SUBSCRIBE and any dialog-establishing NOTIFY requests
  - SUBSCRIBE Events are IANA registered

RFC 3428

SIP Methods: MESSAGE

Cisco.com


```
MESSAGE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bK776asegma
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 22756 MESSAGE
Content-Type: text/plain
Content-Length: 37

Isn't this a great presentation, Bob?
```

MESSAGE - the transfer of messages between users in near real-time

- Content (the payload) in MIME body parts
- MESSAGE does not initiate dialogs
- There is no explicit association between messages
- The body size MUST NOT exceed 1300 bytes

SIP Methods: MESSAGE


```
SIP/2.0 200 OK
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bKnashds7 ;received=10.1.3.33
To: sip: sip:bob@biloxi.com>;tag=1928301774
From: alice@atlanta.com
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 22756 MESSAGE
Content-Length: 0
```

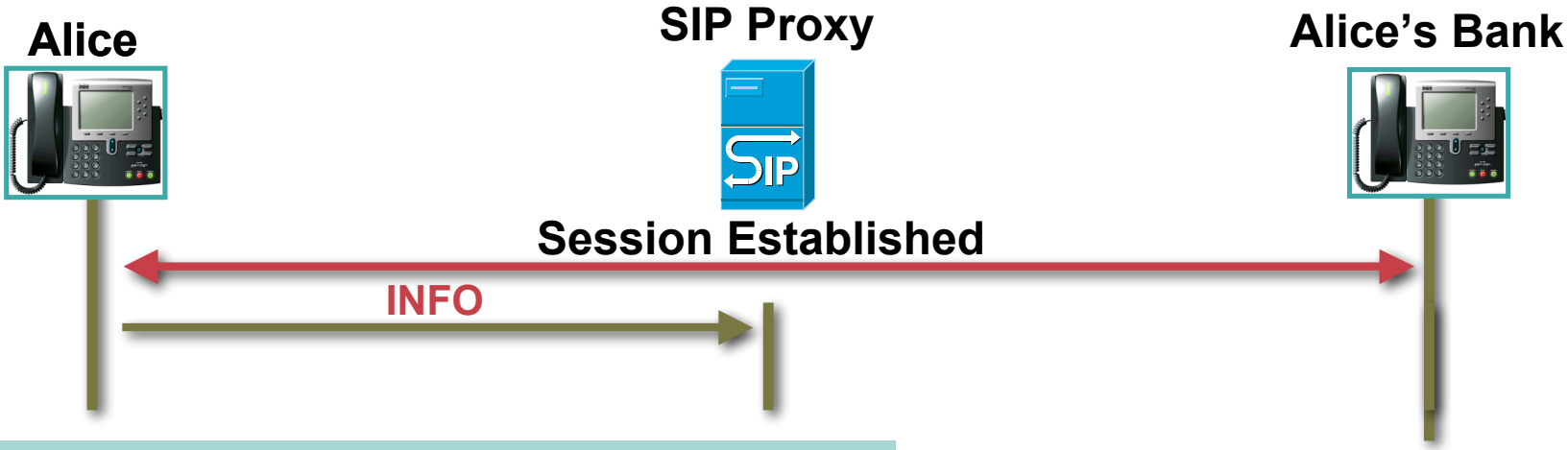
MESSAGE - the transfer of messages between users in near real-time

- **200 OK response does not necessarily mean the user has read the message**
- **A 4xx or 5xx response indicates that the message was not delivered successfully**
- **A 6xx response means it was delivered successfully, but refused**

RFC 2976

SIP Methods: INFO

Cisco.com



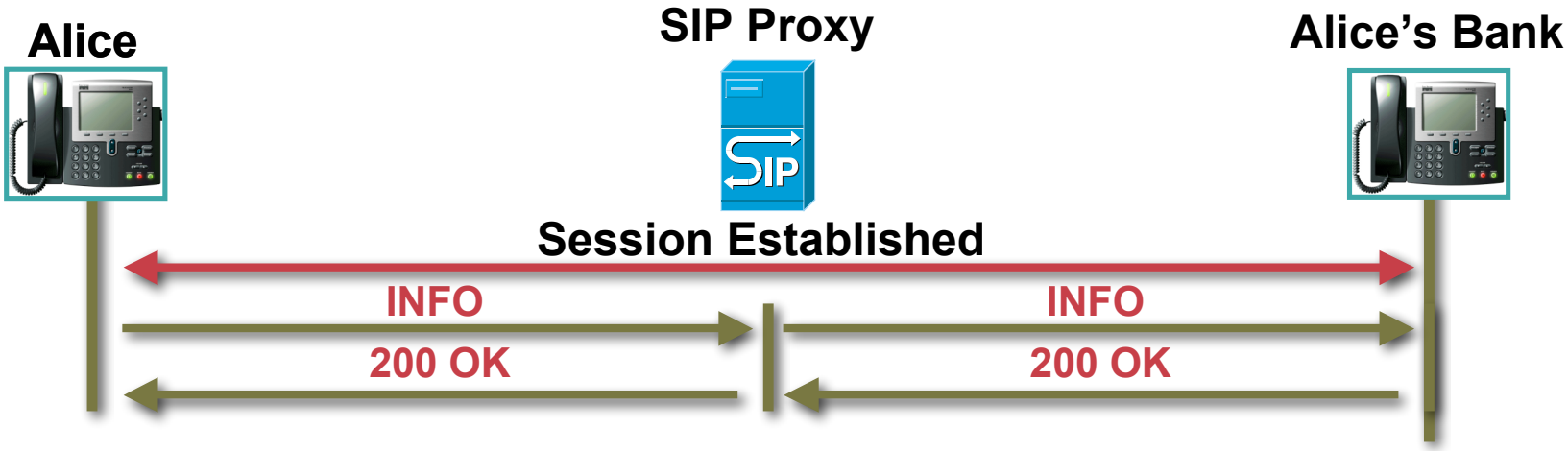

```
INFO sip:Alice's_Bank@192.168.10.20 SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
  ;branch=z9hG4bK776asegma
Max-Forwards: 70
To: Bank <sip:Bank@Bank_URI.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 22756 INFO
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: text/plain
Content-Length: 16

3 1 8 1 9 6 2
```

INFO - for the carrying of session related control information that is generated during a session

- **Content-Type is not defined by 2976, so UAs need to have agreed to one beforehand**

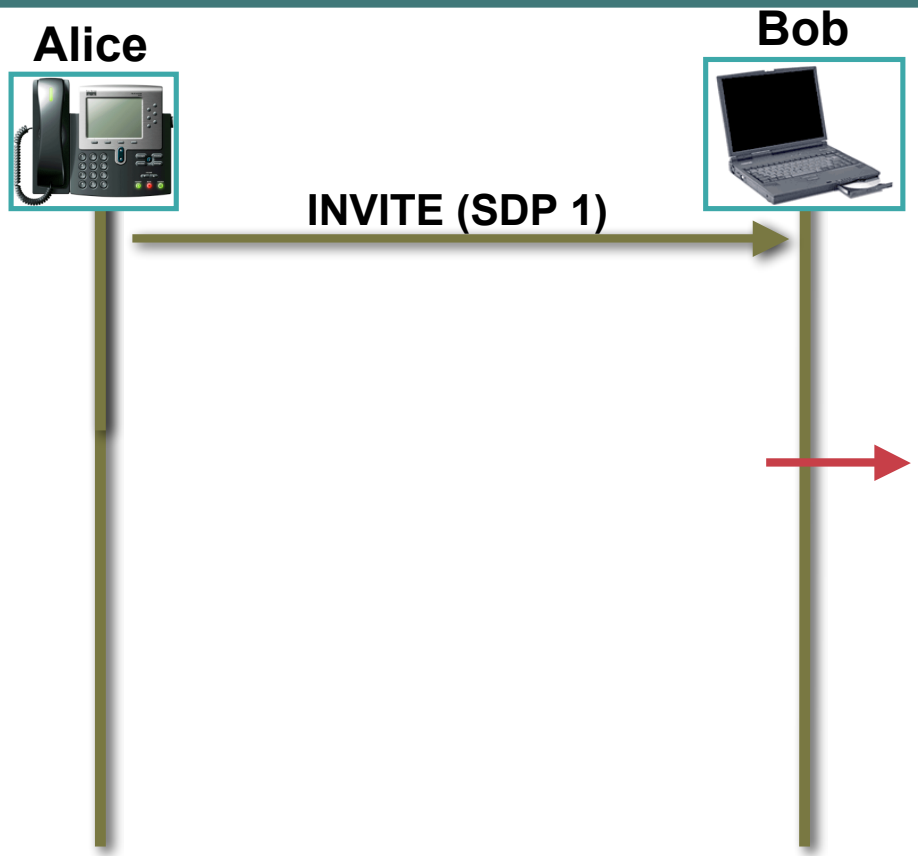
SIP Methods: INFO



INFO - for the carrying of session related control information that is generated during a session

- Examples: Carrying mid-call PSTN signaling messages between PSTN gateways
- Carrying DTMF digits generated during a SIP session
- Carrying wireless signal strength information in support of wireless mobility applications
- Carrying account balance information
- Carrying images or other non streaming information between the participants of a session
- A 487 "Request Terminated" is the proper error if this is unacceptable

SIP Methods: UPDATE



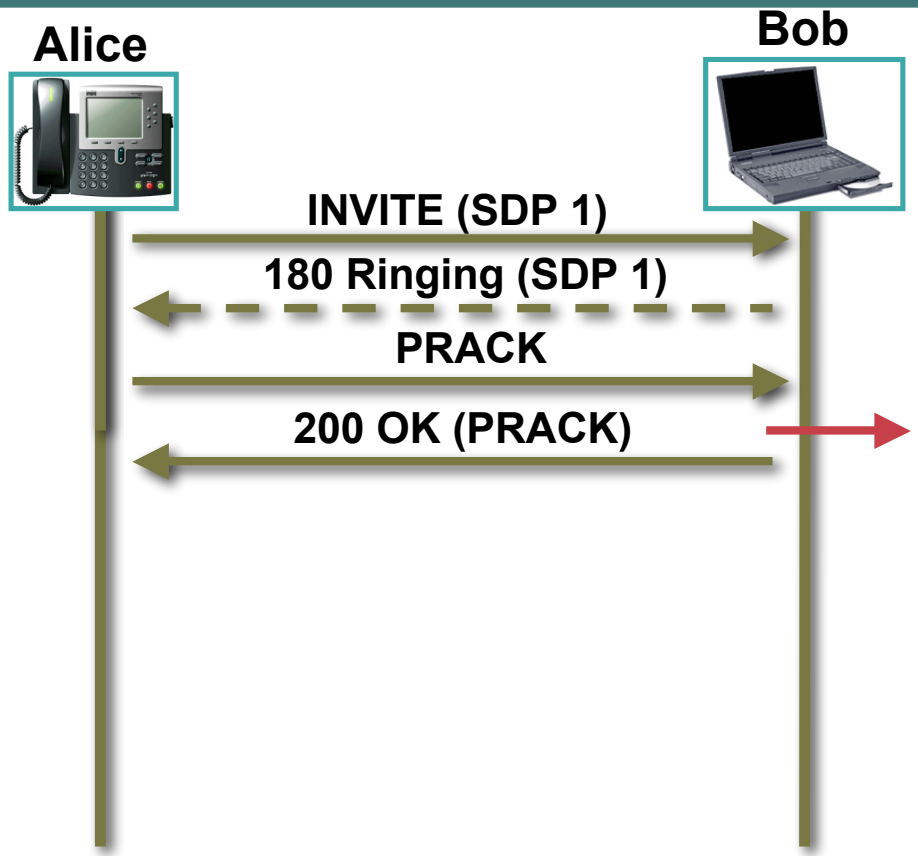

```
INVITE sip:bob@biloxi.com/TCP SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928
Call-ID: a84b4c76e66710@pc33.atlanta.com
Allow: UPDATE
CSeq: 22756 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
(but calls for the codec G.711)
```

UPDATE - allows a client to update parameters of a session

- UAC should include Allow Header indicating support for UPDATE

SIP Methods: UPDATE



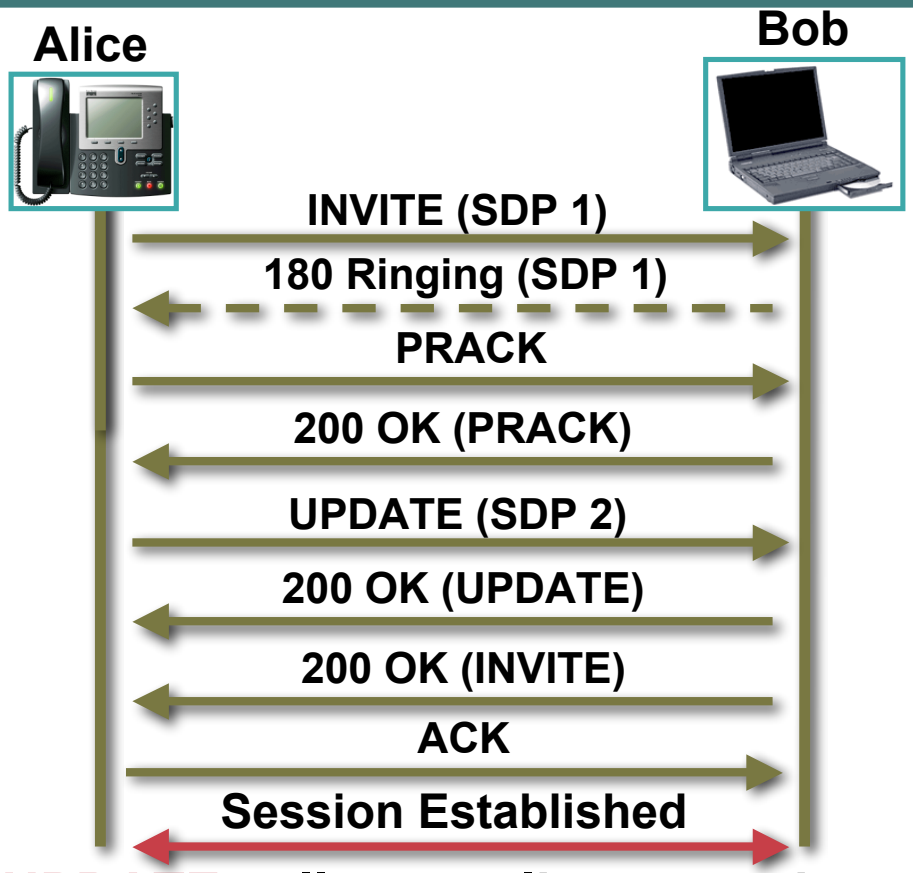
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP pc33.atlanta.com
;branch=z9hG4bK776asdhds
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928
Call-ID: a84b4c76e66710@pc33.atlanta.com
Allow: UPDATE
CSeq: 22756 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Bob's SDP not shown)
(suitable response with the codec G.711)

UPDATE - allows a client to update parameters of a session

- **UAS should include Allow Header indicating support for UPDATE**

SIP Methods: UPDATE




```
UPDATE sip:bob@biloxi.com/TCP SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
 ;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 10197 UPDATE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's new SDP not shown)
(but calls for the codec G.729)
```

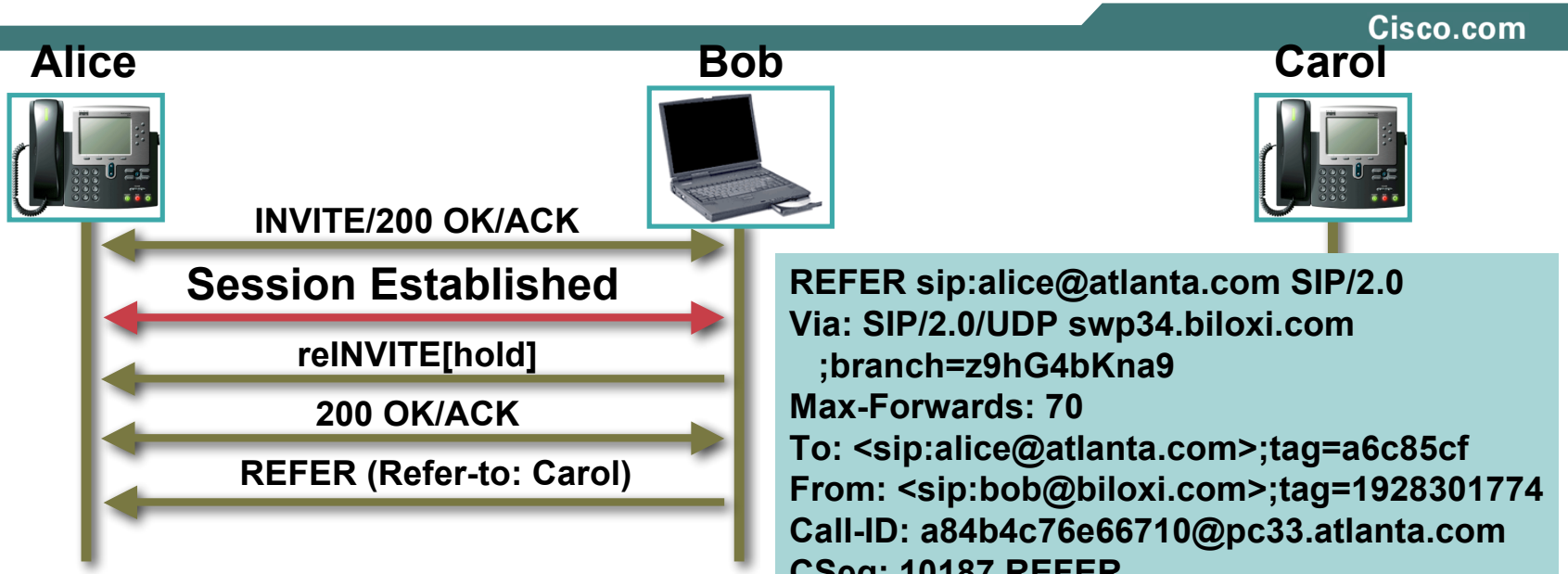
UPDATE - allows a client to update parameters of a session

- UPDATE sent here to change codec from first SDP from G.711 to G.729

- UPDATE can be used after INVITE has been accepted, but reINVITE is preferred to be used (see REFER)

RFC 3515

SIP Methods: REFER

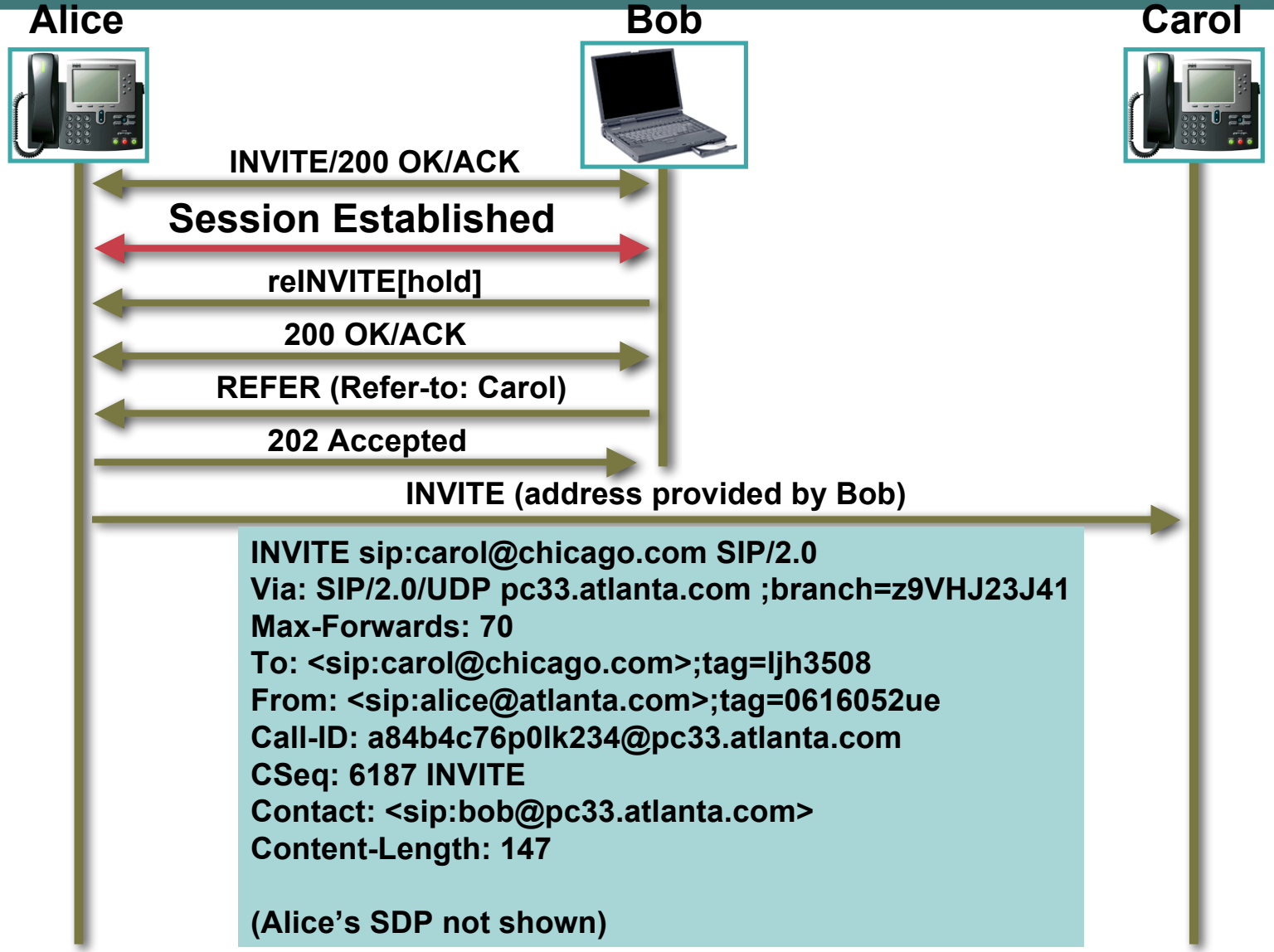


REFER sip:alice@atlanta.com SIP/2.0
Via: SIP/2.0/UDP swp34.biloxi.com
;branch=z9hG4bKna9
Max-Forwards: 70
To: <sip:alice@atlanta.com>;tag=a6c85cf
From: <sip:bob@biloxi.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 10187 REFER
Allow: INVITE, ACK, CANCEL, OPTIONS,
BYE, REFER, NOTIFY, UPDATE
Supported: replaces
Refer-To: <sip:carol@chicago.com>
Contact: <sip:bob@swp34.biloxi.com>
Content-Length: 0

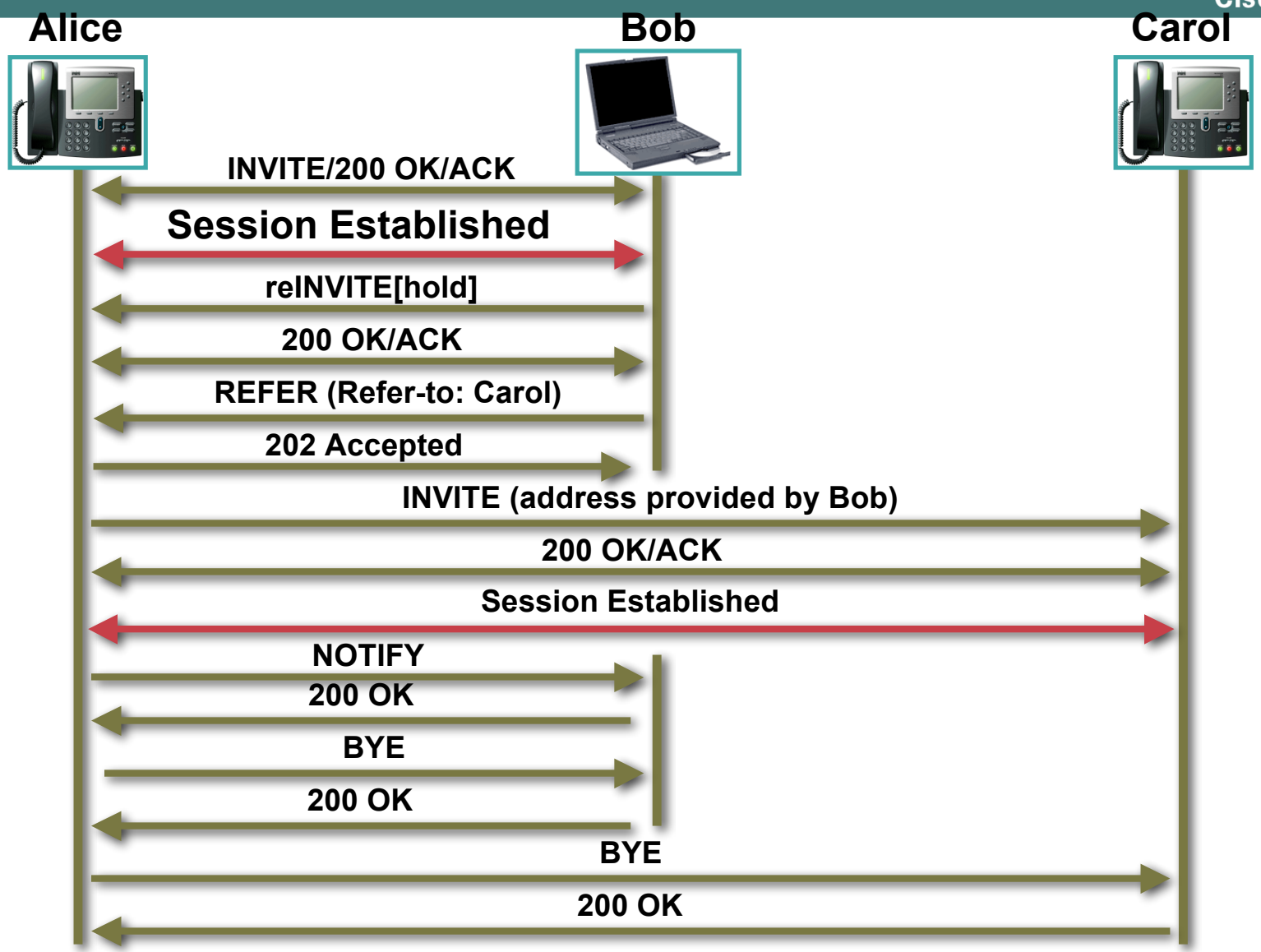
REFER – SIP Request from one UA to INVITE another to a session

- **REFER implicitly establishes a subscription with another UA**
  - **NOTIFY is required when completed**
- **The "Refer-to" SIP Header is mandatory in the REFER Request**

SIP Methods: REFER



SIP Methods: REFER



RFC 3261

Which SIP Headers can be used when?

Cisco.com

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG
Call-ID	c	r	m	m	m	m	m	m
Contact	R		o	-	-	m	o	o
Date		a	o	o	o	o	o	o
From	c	r	m	m	m	m	m	m
Max-Forwards	R	amr	m	m	m	m	m	m
Proxy-Authenticate	407	ar	-	m	-	m	m	m
Record-Route	R	ar	o	o	o	o	o	-
Via	R	amr	m	m	m	m	m	m
Via	rc	dr	m	m	m	m	m	m

SIP Headers Legend (part I)

The "where" column describes the request and response types in which the header field can be used. Values in this column are:

R: header field may only appear in requests;

r: header field may only appear in responses;

2xx, 4xx, etc.: A numerical value or range indicates response codes with which the header field can be used;

c: header field is copied from the request to the response.

An empty entry in the "where" column indicates that the header field may be present in all requests and responses.

The "proxy" column describes the operations a proxy may perform on a header field:

a: A proxy can add or concatenate the header field if not present.

m: A proxy can modify an existing header field value.

d: A proxy can delete a header field value.

r: A proxy must be able to read the header field, and thus this header field cannot be encrypted.

SIP Headers Legend (part II)

The next six columns relate to the presence of a header field in a Method:

c: Conditional; requirements on the header field depend on the context of the message.

m: The header field is mandatory.

m*: The header field SHOULD be sent, but clients/servers need to be prepared to receive messages without that header field.

o: The header field is optional.

t: The header field SHOULD be sent, but clients/servers need to be prepared to receive messages without that header field.

*: The header field is required if the message body is not empty.

-: The header field is not applicable.

Each Header is documented in this table

Cisco.com

Header field	where	proxy	INV	ACK	CAN	BYE	REG	OPT	PRA
Resource-Priority	R	amd	o	o	o	o	o	o	o
Resource-Priority	200	-	o	-	-	-	-	-	-
Accept-Resource-Priority	200	-	o	-	-	-	-	-	-
Accept-Resource-Priority	417	-	o	-	-	-	-	-	-
Accept-Resource-Priority	420	-	o	-	-	-	-	-	-

Header field	where	proxy	SUB	NOT	UPD	MSG	REF	INF	PUB
Resource-Priority	R	amd	o	o	o	o	o	o	o
Resource-Priority	200	-	o	o	-	o	-	-	-
Accept-Resource-Priority	200	-	-	-	-	-	-	-	-
Accept-Resource-Priority	417	-	m	m	-	m	-	-	-
Accept-Resource-Priority	420	-	o	o	-	o	-	-	-

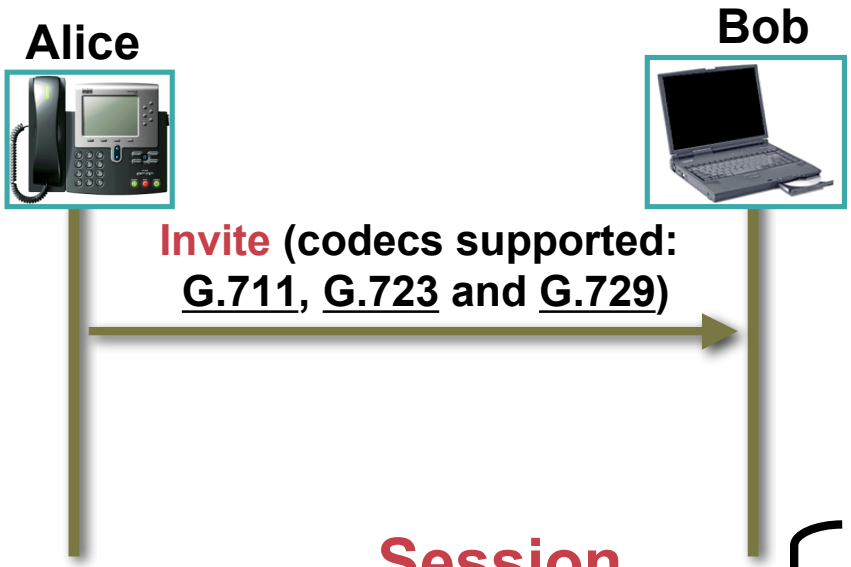
RFC 2045-49

SIP Message Body (MIME)

Cisco.com

- Multipurpose Internet Mail Extensions (MIME) – defines the message body format (US-ASCII) to allow for:
  - textual message bodies in character sets other than US-ASCII
  - an extensible set of different formats for non-textual message bodies
  - multi-part message bodies
  - textual header information in character sets other than US-ASCII
- MIME is used by SIP (as well as HTTP, MEGACO, etc) for message bodies

SIP and the Offer/Answer Model




```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com:5060
  ;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.com>
Content-Type: application/sdp
Content-Length: 151
```

Session Description Protocol

```
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.com
c=IN IP4 10.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0 4 8
a=rtpmap:0 PCMU/8000
```

- **Session Description Protocol – is a MIME body part within the SIP Architecture**
  - **– codecs are specified in RFC 3551**

Session Description Protocol (SDP)

- A session description protocol (RFC 2327) for multimedia connections
- Presents a set of parameters for a multimedia session
- Developed by IETF MMUSIC WG
- Simple/Flexible
  - Text-based
  - Extensible
- SIP Offer/Answer Model is RFC 3264

"Lines" below are in order

- v = protocol version
- o = owner/creator and session identifier
- s = session name
- c = connection information – not required if included in all media
- k = encryption keys
- t = time the session is active
- m = media descriptions and transport address
- a = (zero or more) media attributes lines

RFC 3264

SIP and the Offer/Answer Model

Cisco.com

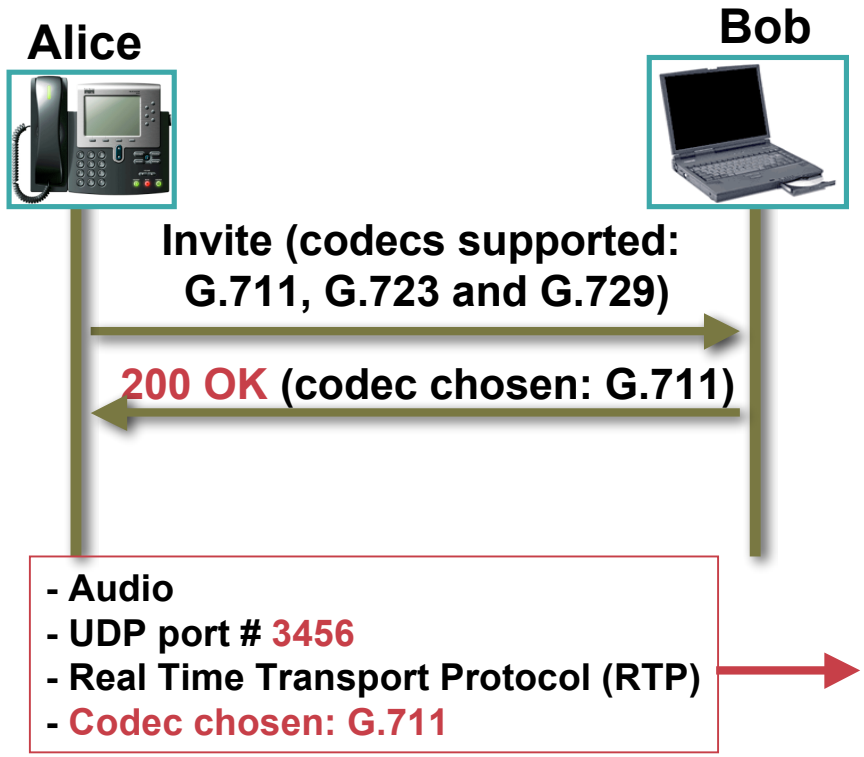

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com:5060
  ;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.com>
Content-Type: application/sdp
Content-Length: 151
```

- Audio
- UDP port # 49172
- Real Time Transport Protocol (RTP)
- Codecs supported: G.711, G.723, G.729

```
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.com
c=IN IP4 10.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0 4 8
a=rtpmap:0 PCMU/8000
```

- **Session Description Protocol**
  - What is learned from this message body?

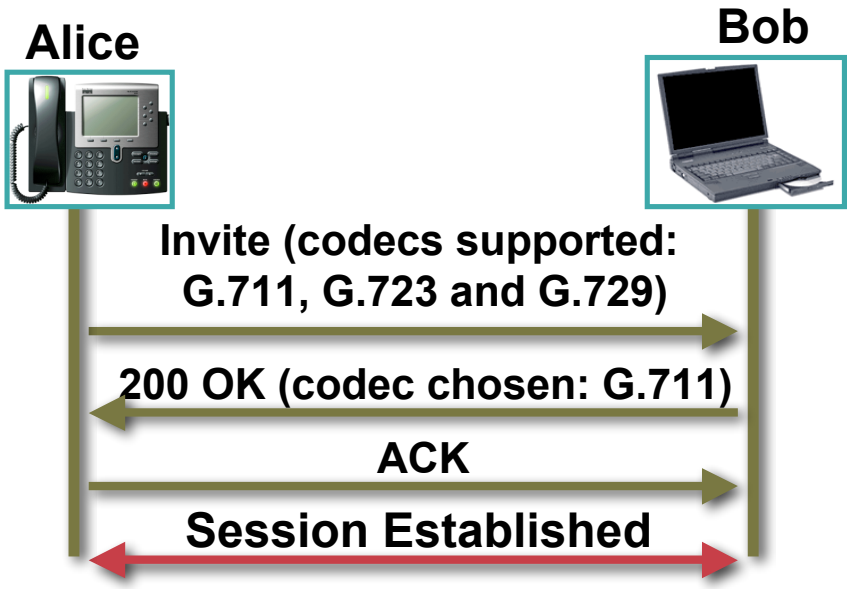
SIP and the Offer/Answer Model




```
SIP/2.0 200 OK
Via: SIP/2.0/TCP swc50.atlanta.com:5060
  ;branch=z9hG4bK74bf9 ;received=10.1.3.33
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:bob@biloxi.com>
Content-Type: application/sdp
Content-Length: 147
v=0
o=bob 2890844527 2890844527 IN IP4 biloxi.com
c=IN IP4 192.0.2.201
t=0 0
m=audio 3456 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

- **Session Description Protocol**
  - What is learned from this message body?

SIP and the Offer/Answer Model




```
ACK sip:bob@192.0.2.201 SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com:5060
  ;branch=z9hG4bK74bd5
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.com
CSeq: 6187 ACK
Content-Length: 0
```

- **Session Description Protocol**

  SDP choice from Bob *MUST* be Acknowledged

SIP and the Offer/Answer Model (w/video)


```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com:5060
  ;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.com>
Content-Type: application/sdp
Content-Length: 151
```

- Audio
- UDP port # 49172
- Codecs supported: G.711

- Video
- UDP port # 51172
- Codecs supported: H.261, H.263

```
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.com
c=IN IP4 10.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
m=video 51172 RTP/AVP 31 34
a=rtpmap:31 H.261/90000
a=rtpmap:34 H.263/90000
```

- **Session Description Protocol**
  - **Example INVITE with Voice and Video Requested**

SIP and Multipart MIME bodies


```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
  ;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.com>
Content-Type: multipart/mixed; boundary=0a0
Content-Length: 311
```

- **Multipart MIME bodies**
  - Each Body part has a different purpose
  - Need an indication of more than one body part
  - need a boundary that is a unique string
  - can be individually encrypted or group encrypted (S/MIME)

```
--0a0
Content-Type: application/sdp
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.com
c=IN IP4 10.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0 4 8
a=rtpmap:0 PCMU/8000
```

```
--0a0
Content-Type: application/cpim-pidf+xml (short form*)
<A1>Texas</A1>
<A2>Richardson</A2>
<A6>Pres Bush</A6>
<STS>Turnpike</STS>
<HNO>2200</HNO>
<FLR>3rd floor</FLR>
--0a0--
```

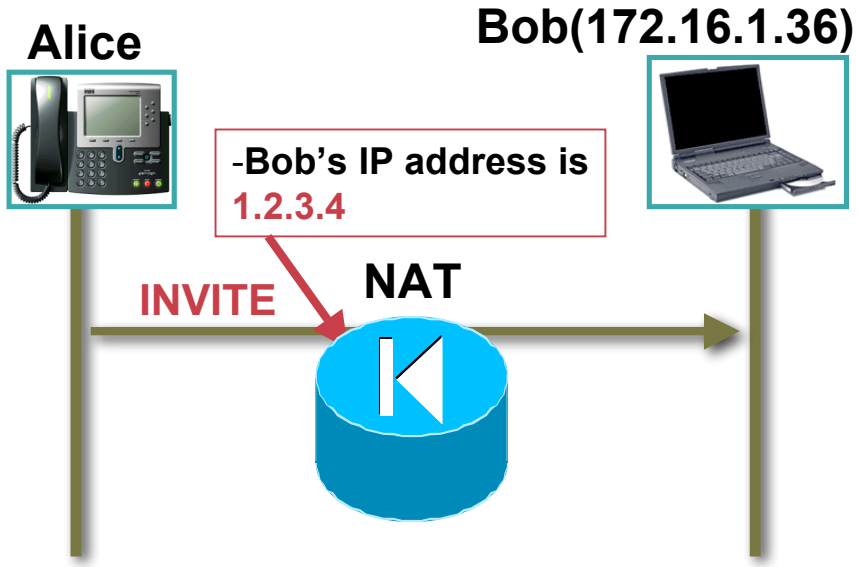
* "Short form" means not enough room here

NAT/Firewall traversal

- **Is there a NAT problem with SIP?**
  - **–Yes, if UDP is used (likely doesn't have port open)**
    - **UDP Keepalive packets don't traverse NATs**
  - **– If TCP is used, it is indirect...**
    - **It's in the mismatch of IP addresses given between the IP header and the SDP "c" line**
    - **Which leads to an RTP problem**

Alice doesn't know Bob's IP address, but is told 2 different ones in the same Response packet. Which does she believe?

NAT/Firewall traversal



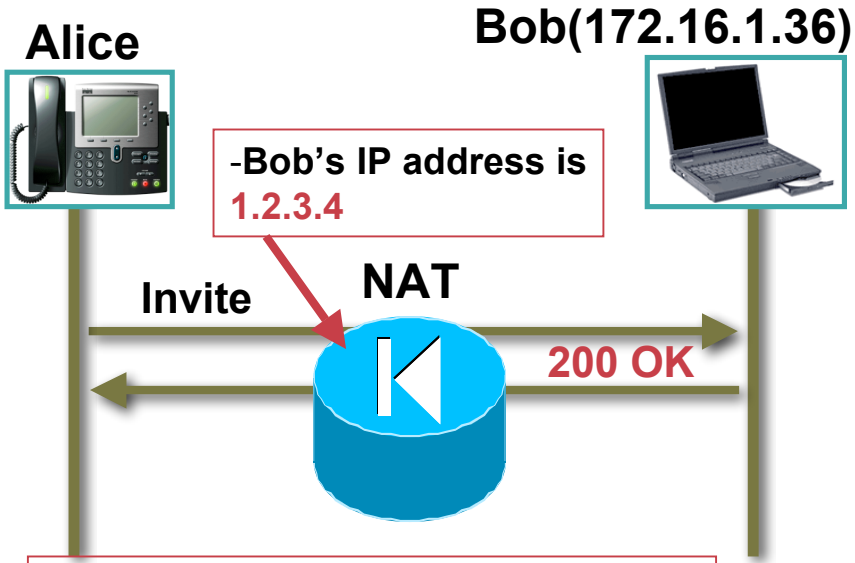

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com:5060
  ;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.com>
Content-Type: application/sdp
Content-Length: 151
```

```
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.com
c=IN IP4 10.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0 4 8
a=rtpmap:0 PCMU/8000
```

- From 10.1.3.33
- Audio
- UDP port # 49172
- Real Time Transport Protocol (RTP)
- Codecs supported: G.711, G.723, G.729

- **Is there a NAT issue here?**
  - No, Alice's IP address is in the IP Header as well as SDP body

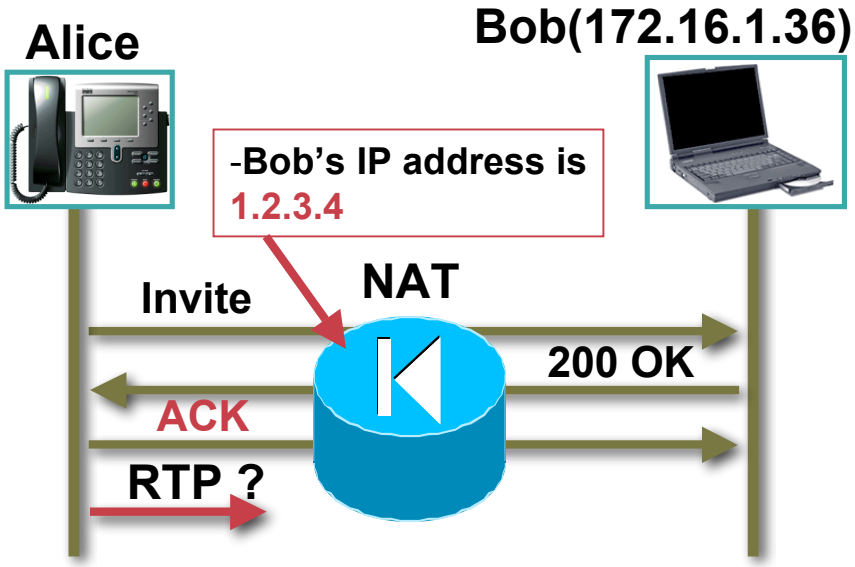
NAT/Firewall traversal




```
SIP/2.0 200 OK
Via: SIP/2.0/TCP swc50.atlanta.com:5060
  ;branch=z9hG4bK74bf9 ;received=10.1.3.33
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:bob@biloxi.com>
Content-Type: application/sdp
Content-Length: 147
v=0
o=bob 2890844527 2890844527 IN IP4 biloxi.com
c=IN IP4 172.16.1.36
t=0 0
m=audio 3456 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

- **Is there a NAT issue here?**
  - **No, Bob's IP address is 172.16.1.36, yet his NAT's untrusted side is 1.2.3.4**

NAT/Firewall traversal




```
ACK sip:bob@1.2.3.4 SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com:5060
  ;branch=z9hG4bK74bf9 ;received=1.2.3.4
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.com
CSeq: 6187 ACK
Content-Length: 0
```

- **Is there a NAT issue here?**
  - **Alice's ACK goes to 1.2.3.4 (which will get to Bob)**
  - **Alice's RTP will go to 172.16.1.36:3456 – which won't get to Bob**

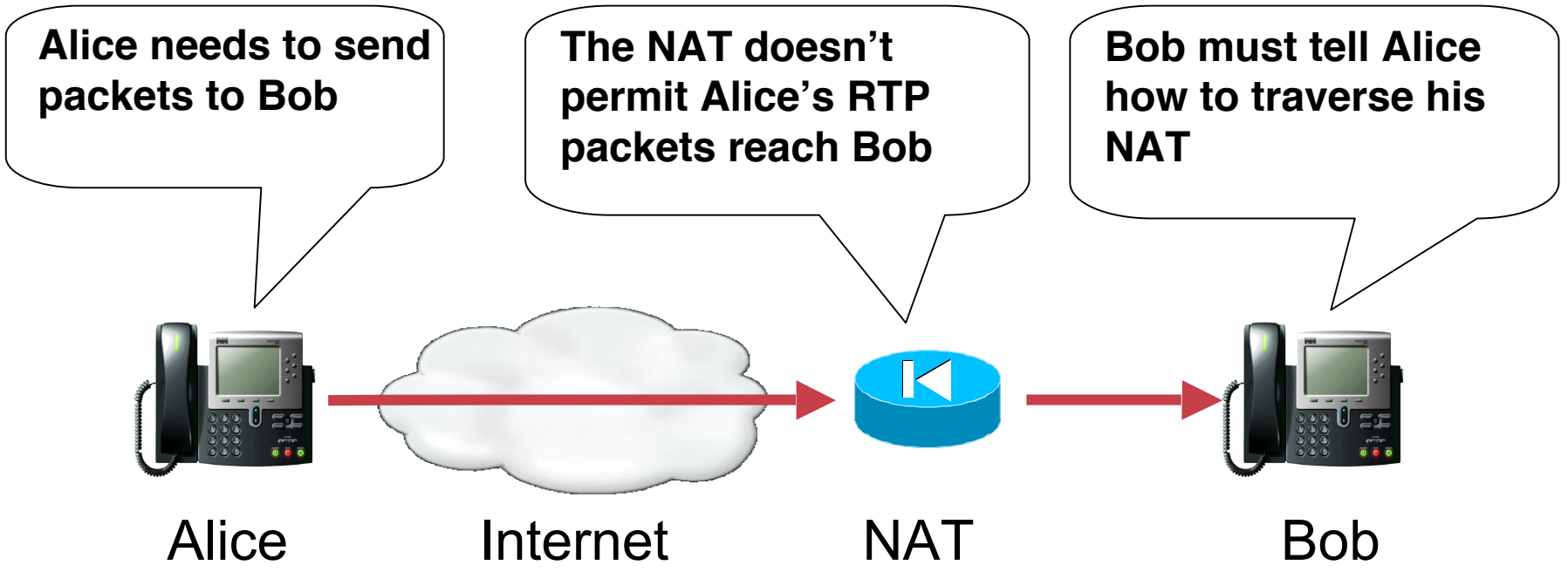
Big problem

RFC 3489

NAT traversal (Part II)

Cisco.com

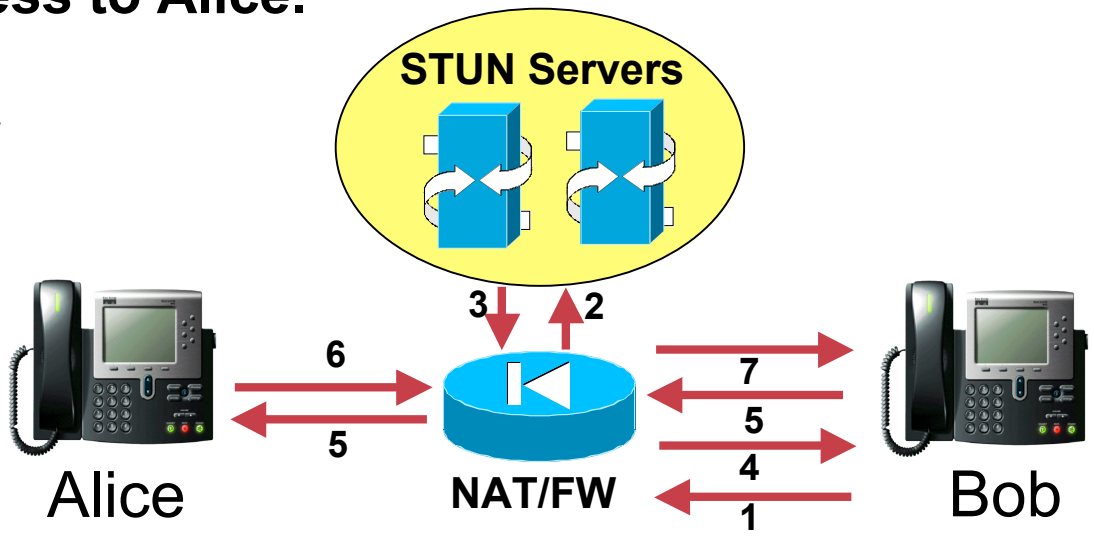
- Alice wants to call Bob, whose phone is behind a NAT
- Alice cannot find Bob because his IP address isn't Routable
- Bob needs to tell Alice where to send her IP packets to let them traverse his NAT
- STUN solves this for most NATs



How STUN works

- Bob asks the STUN server to discover the NAT's public IP address and create a forwarding in the NAT.
- Bob then tells this address to Alice.

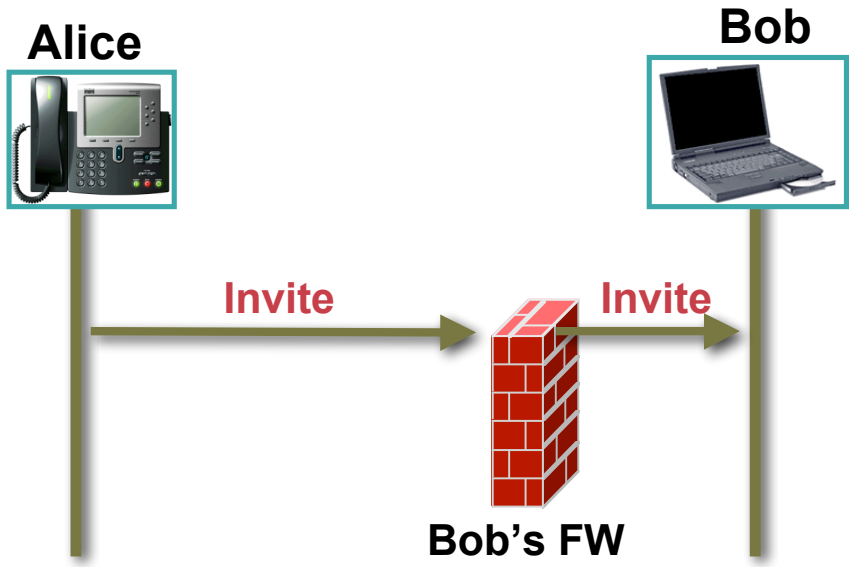
1. Bob sends packet to stun server
2. NAT maps packet to be from 1.2.3.4:5555
3. STUN replies and says address packet came from is 1.2.3.4:5555
4. NAT forwards to Bob
5. Bob tells Alice to send to 1.2.3.4:5555 and sends a packet to where Alice will send from
6. Alice sends to 1.2.3.4:5555
7. NAT forwards to Bob



NAT/Firewall traversal

- The FW problem:
  - SIP messages will traverse FWs that have port 5060 open
  - It's RTP running over UDP that's the problem
- FW solutions:
  - FWs can open all UDP ports for RTP
    - This isn't very secure (but is this really a solution?)
  - FWs can inspect SDP for the ports used (ALG)
    - Slows down FWs, some can't do this
  - MIDCOM interaction (Firewall controller) is on trusted side of each FW and some SIP entity (the UA or the Proxy, if there is one)
    - MIDCOM looks like a man-in-the-middle attack (which is a problem)

NAT/Firewall traversal



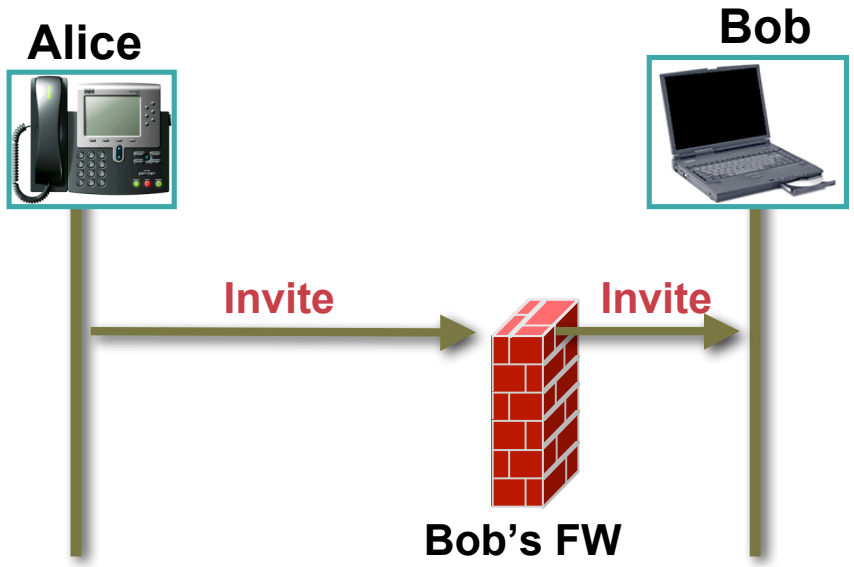

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com:5060
  ;branch=z9hG4bK74bf9 ;received=10.1.3.33
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.com>
Content-Type: application/sdp
Content-Length: 151
```

```
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.com
c=IN IP4 10.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0 4 8
a=rtpmap:0 PCMU/8000
```

- From 10.1.3.33
- Audio
- UDP port # 49172
- Real Time Transport Protocol (RTP)
- Codecs supported: G.711, G.723, G.729

- **Is there a Firewall issue here?**
  - No, SIP messages will traverse FWs that have port 5060 open

NAT/Firewall traversal




```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com:5060
  ;branch=z9hG4bK74bf9 ;received=10.1.3.33
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.com>
Content-Type: application/sdp
Content-Length: 151
```

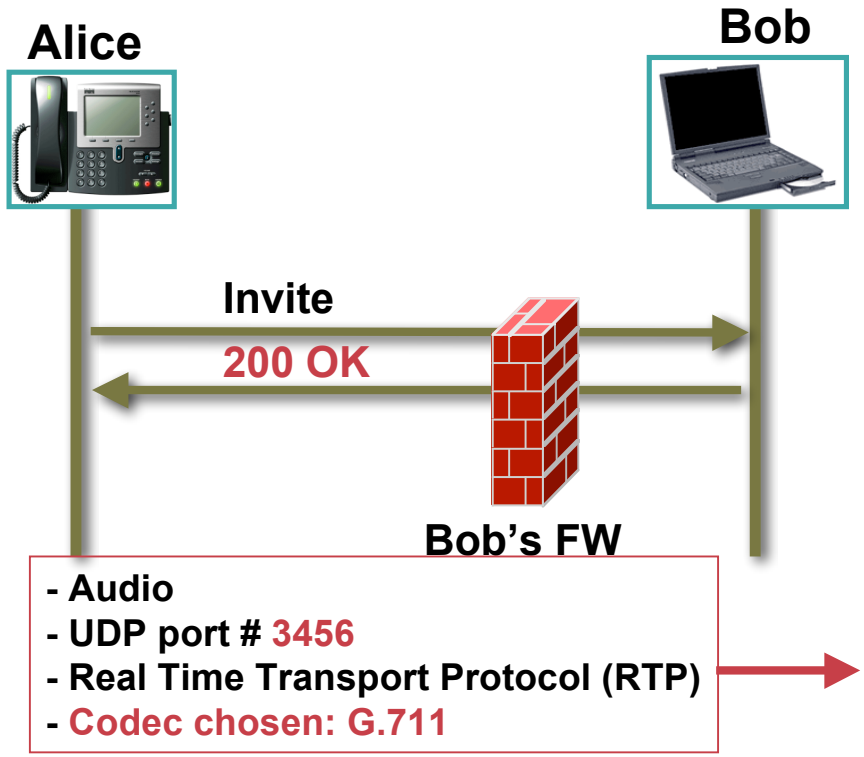
```
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.com
c=IN IP4 10.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0 4 8
a=rtpmap:0 PCMU/8000
```

This is what a FW can look for:
- From 10.1.3.33
- UDP port # 49172

But this will slow FW down greatly

- **Is there a Firewall issue here?**
  - No, FW can snoop the SDP proposed UDP port for the RTP Stream

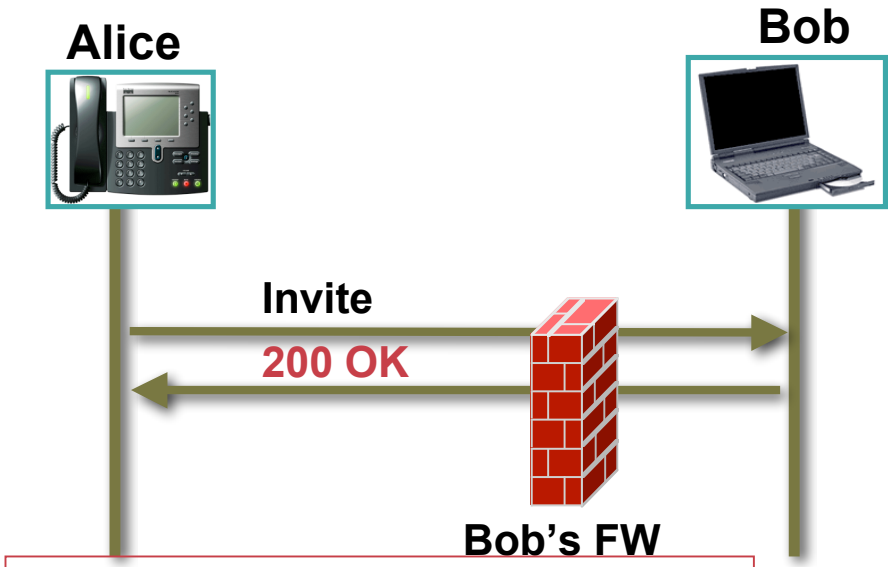
NAT/Firewall traversal




```
SIP/2.0 200 OK
Via: SIP/2.0/TCP swc50.atlanta.com:5060
  ;branch=z9hG4bK74bf9 ;received=10.1.3.33
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:bob@biloxi.com>
Content-Type: application/sdp
Content-Length: 147
v=0
o=bob 2890844527 2890844527 IN IP4 biloxi.com
c=IN IP4 172.16.1.36
t=0 0
m=audio 3456 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

- **Is there a Firewall issue here?**
  - **No, SIP messages will traverse FWs that have port 5060 open**

NAT/Firewall traversal



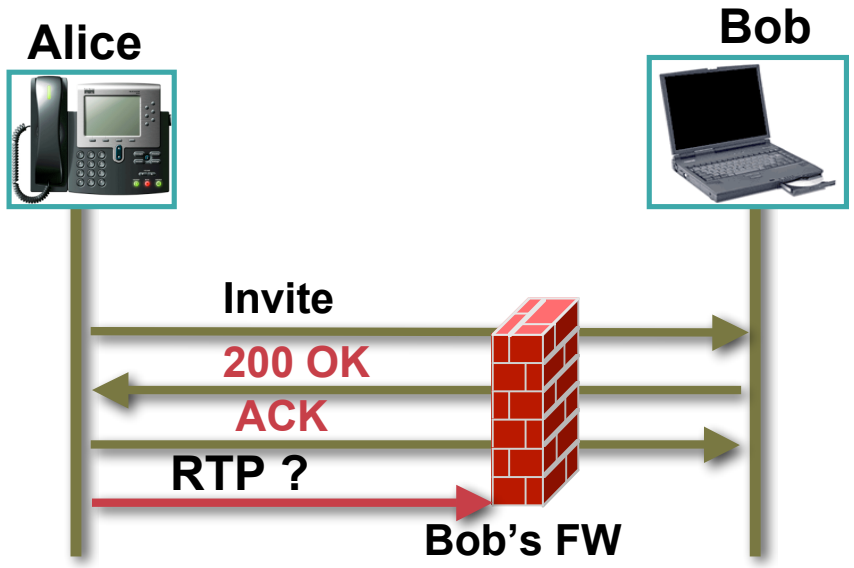
This is what a FW can look for:
- From 172.16.1.36
- UDP port # 3456

But this will slow FW down greatly

```
SIP/2.0 200 OK
Via: SIP/2.0/TCP swc50.atlanta.com:5060
  ;branch=z9hG4bK74bf9 ;received=10.1.3.33
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:bob@biloxi.com>
Content-Type: application/sdp
Content-Length: 147
v=0
o=bob 2890844527 2890844527 IN IP4 biloxi.com
c=IN IP4 172.16.1.36
t=0 0
m=audio 3456 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

- **Is there a Firewall issue here?**
  - **No, FW can snoop the SDP proposed UDP port for the RTP Stream**

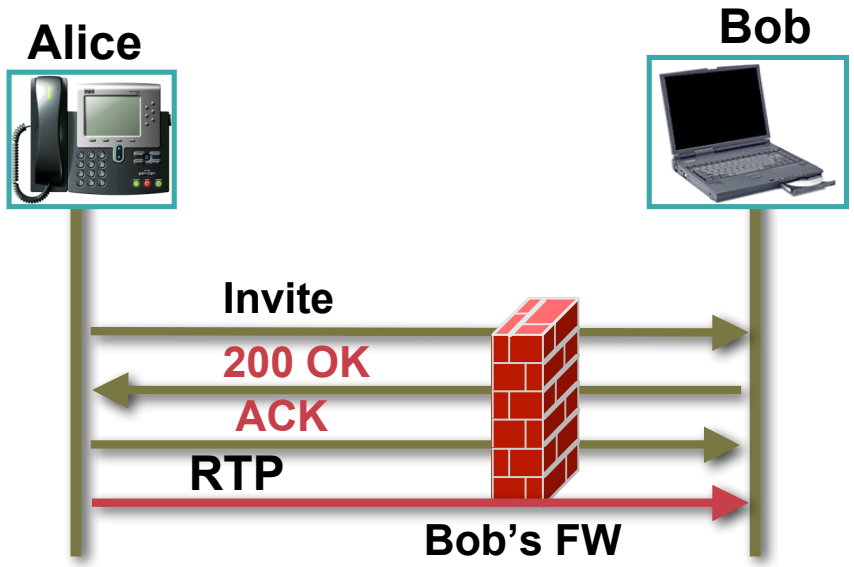
NAT/Firewall traversal




```
ACK sip:bob@172.16.1.36 SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com:5060
  ;branch=z9hG4bK74bf9 ;received=10.1.3.33
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.com
CSeq: 6187 ACK
Content-Length: 0
```

- Is there a Firewall issue here?

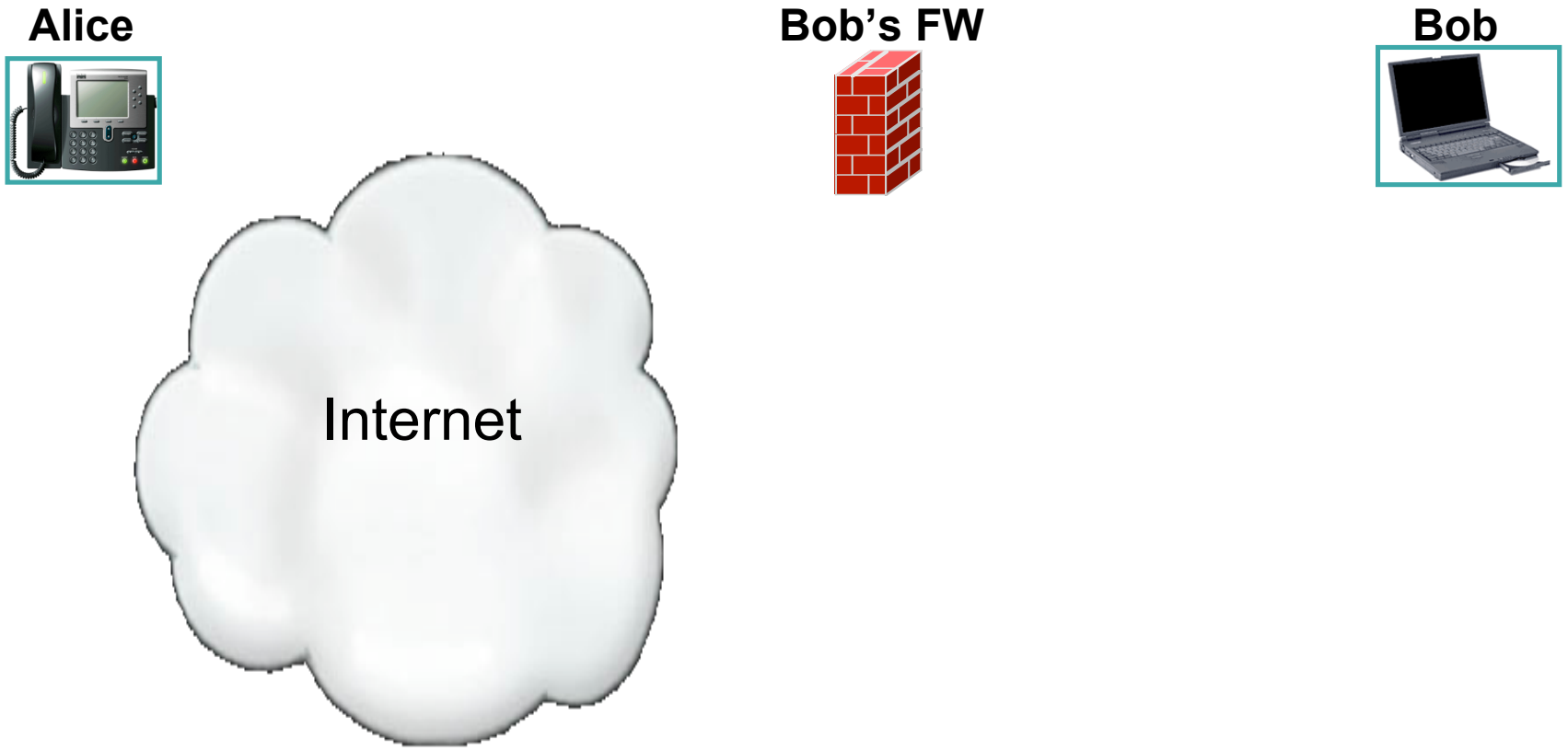
NAT/Firewall traversal




```
ACK sip:bob@172.16.1.36 SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com:5060
  ;branch=z9hG4bK74bf9 ;received=10.1.3.33
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:bob@biloxi.com>;tag=8321234356
Call-ID: 3848276298220188511@atlanta.com
CSeq: 6187 ACK
Content-Length: 0
```

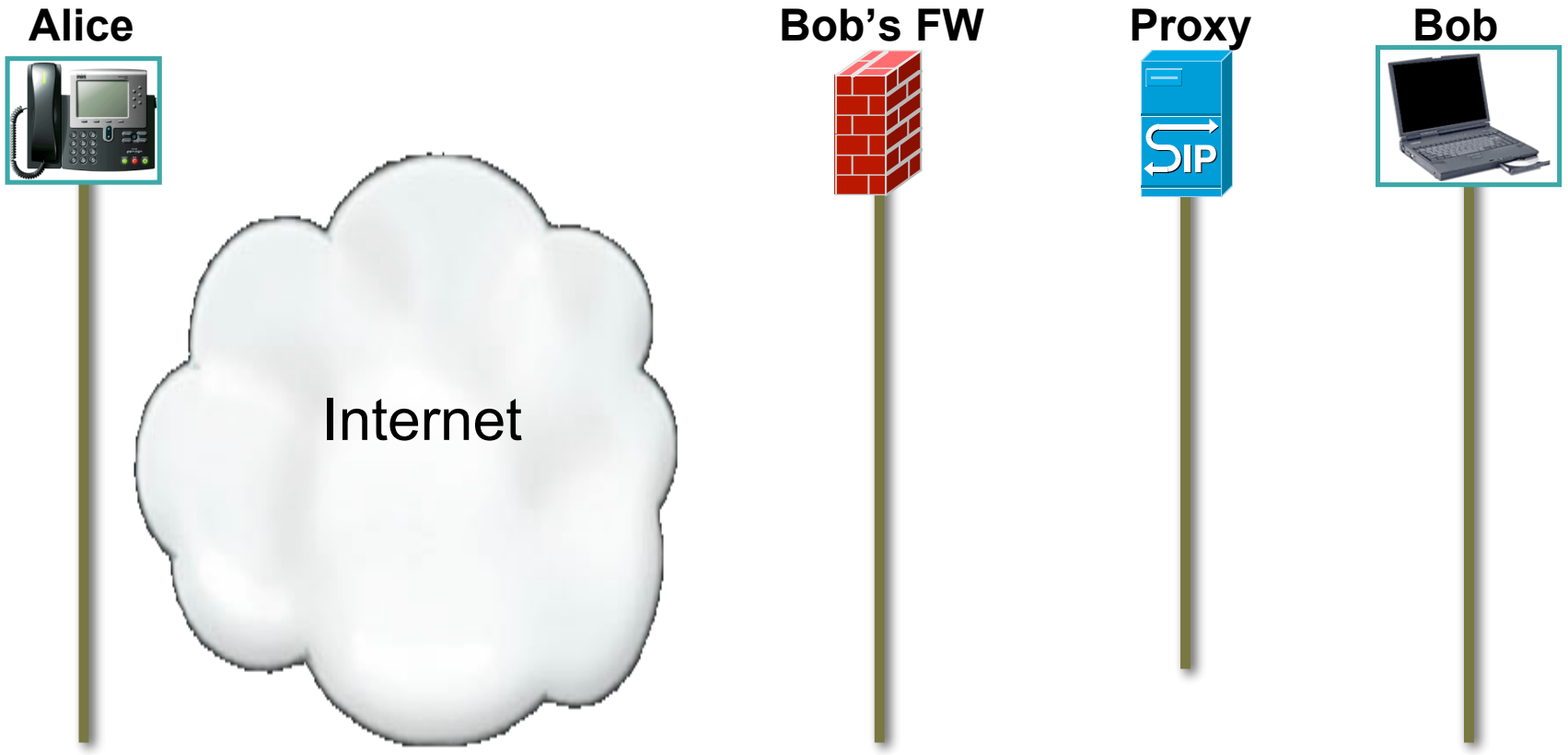
- **Is there a Firewall issue here?**
  - **nope, other than performance**

Firewall traversal: Using MIDCOM



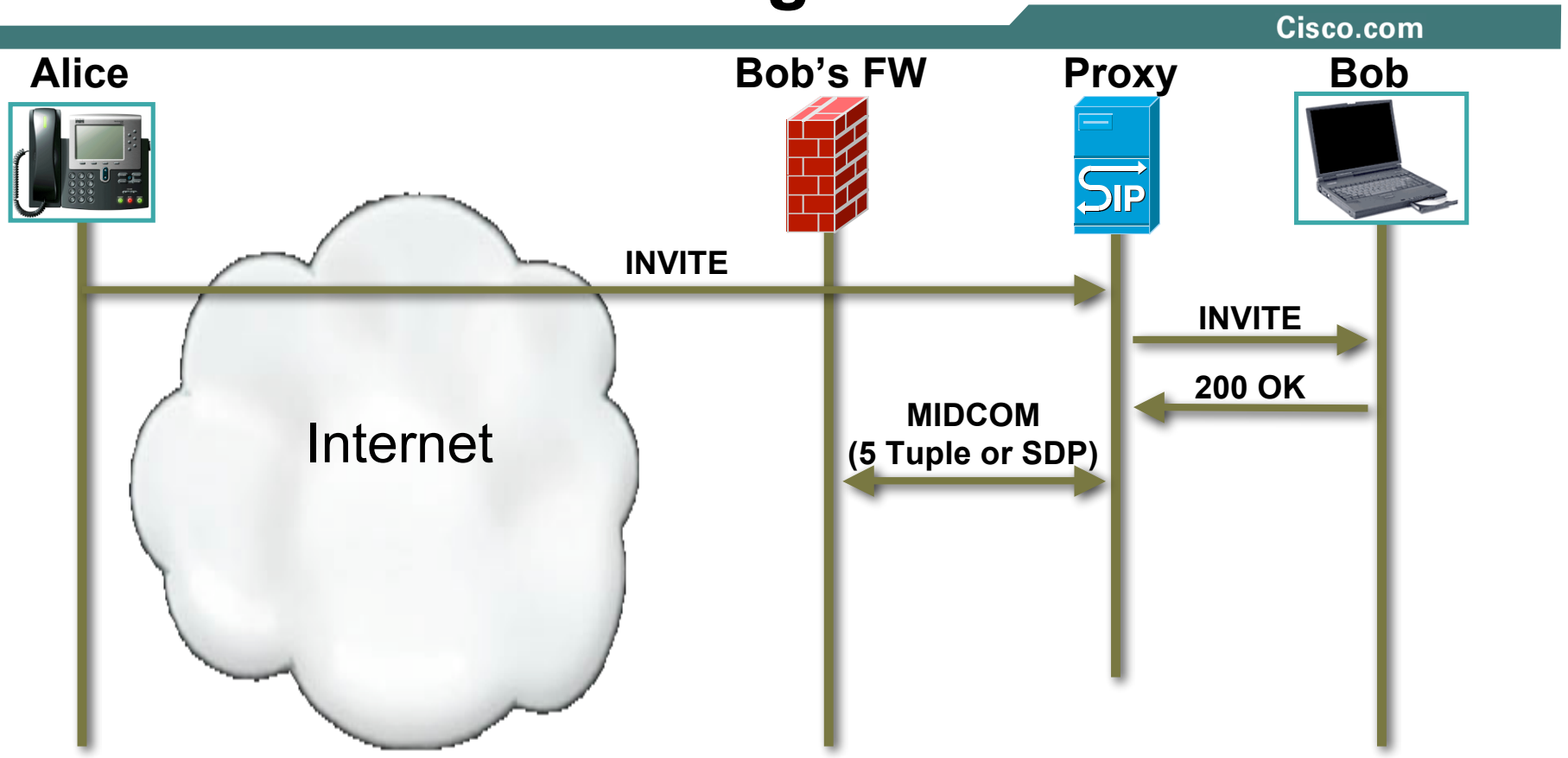
- **Alice to Bob over the Internet (or just Untrusted)**
  - **Bob needs Firewall to protect his network**

Firewall traversal: Using MIDCOM



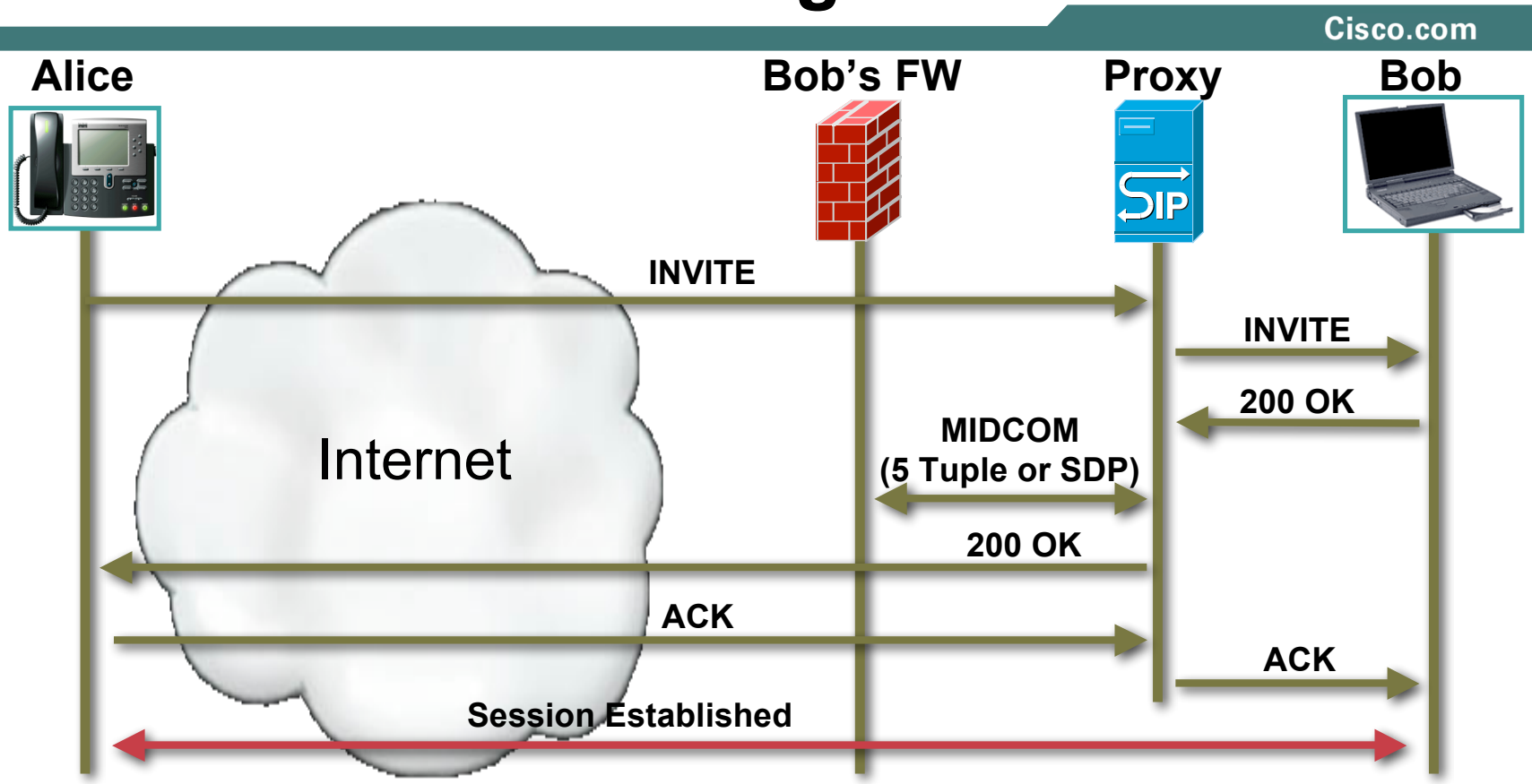
- **Alice to Bob over the Internet (or just Untrusted)**
  - **Bob needs a Proxy to interface with FW to open ports**

Firewall traversal: Using MIDCOM



- **Alice to Bob over the Internet (or just Untrusted)**
  - **Proxy tells FW via MIDCOM the 5 tuple or SDP of session**

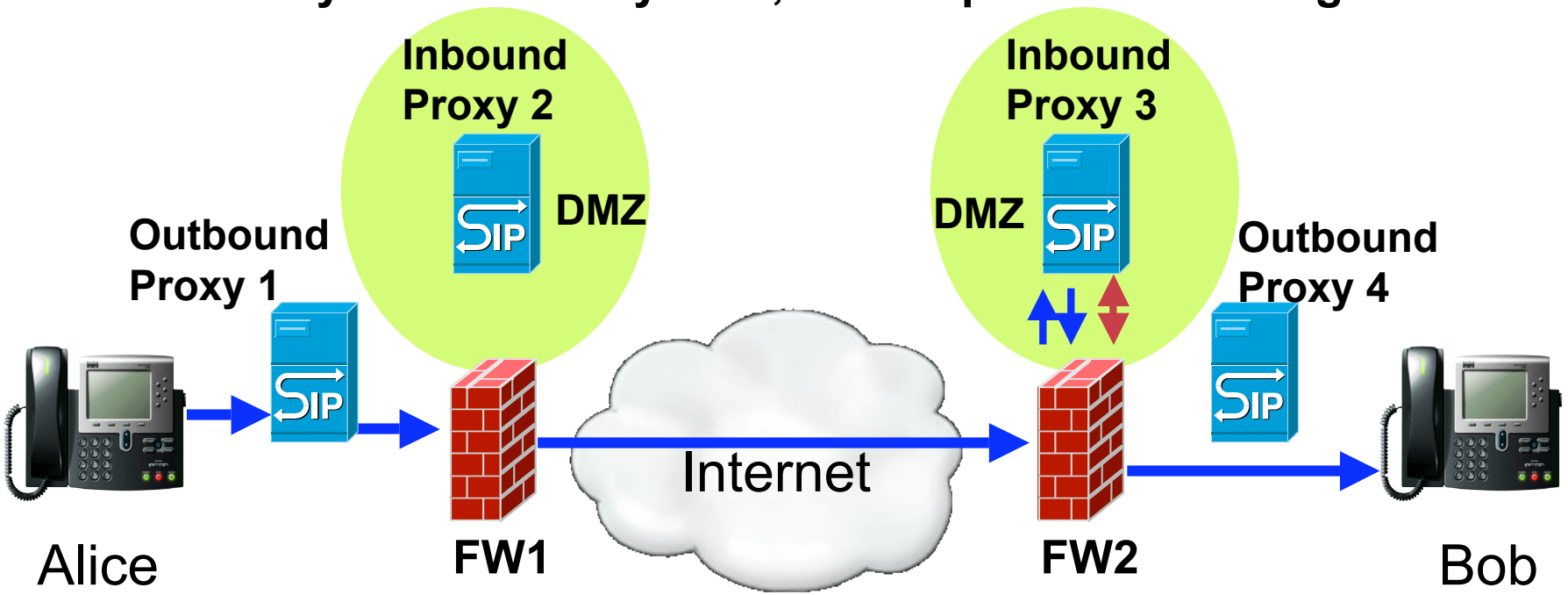
Firewall traversal: Using MIDCOM



- **Alice to Bob over the Internet (or just Untrusted)**
  - **Once FW dynamically opens ports just for Bob, 200 OK**

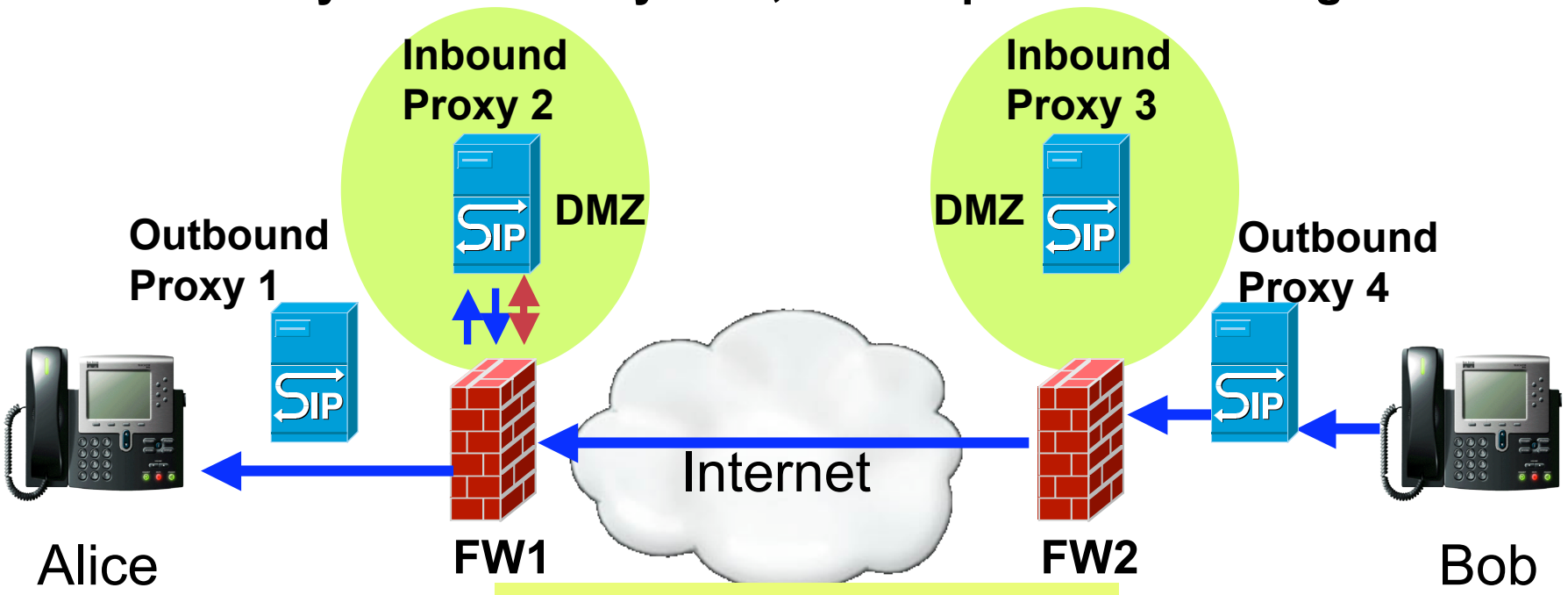
Firewall traversal: More Complicated

- **Alice wants to call Bob**
  - **Outbound interface to FW is via Proxy1**
    - **Proxy1 is trusted by FW1, tells to pass SIP message to Bob**
  - **Inbound to Bob's network is via Proxy3 (in DMZ)**
    - **Proxy3 is trusted by FW2, tells to pass SIP message to Bob**



Firewall traversal: More Complicated

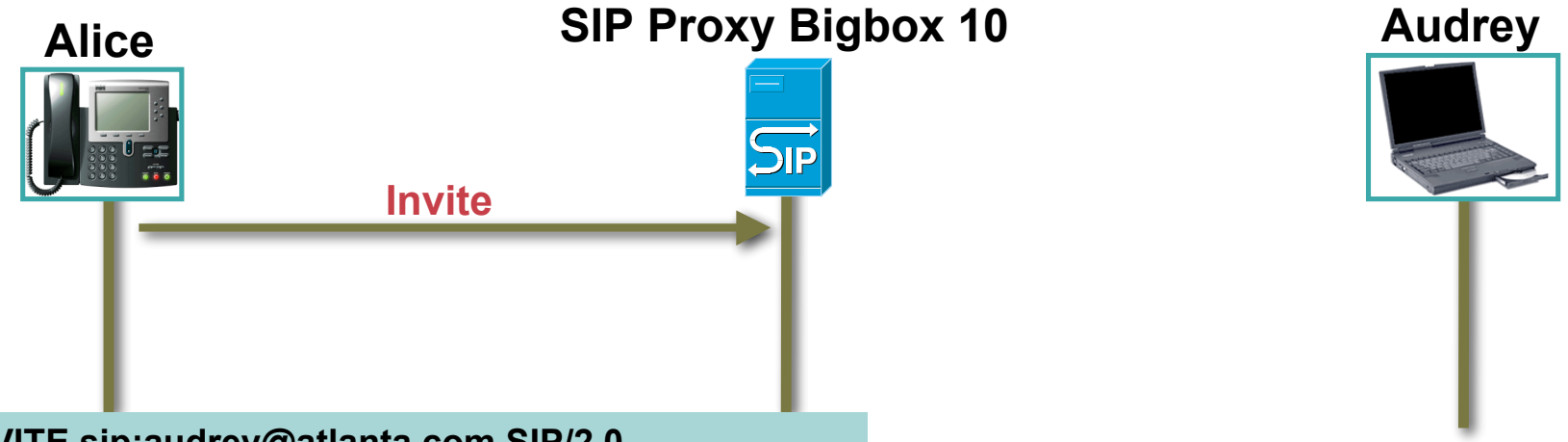
- **Bob wants to call Alice**
  - **Outbound interface to FW is via Proxy4**
    - **Proxy3 is trusted by FW2, tells to pass SIP message to Alice**
  - **Inbound to Alice's network is via Proxy2 (in DMZ)**
    - **Proxy2 is trusted by FW1, tells to pass SIP message to Alice**



SIP Security

- **Digest**
  - For Authentication of Sender
- **TLS/IPsec**
  - Confidentiality/Integrity of signaling per hop or e2e
- **S/MIME**
  - e2e message body confidentiality
- **Network Asserted Identity**
  - Network backs who the caller says they are
- **SIP Privacy**
  - Keeping certain parts of message Private to outside Domains

Digest Authentication



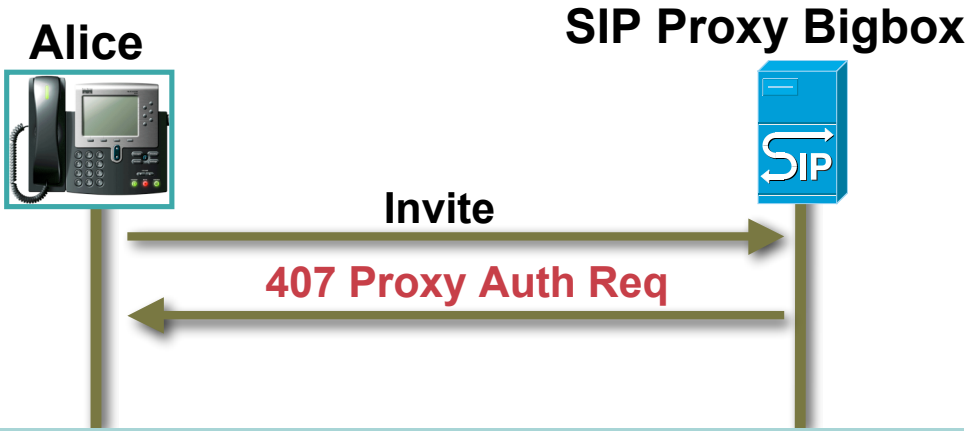

```
INVITE sip:audrey@atlanta.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
  ;branch=z9hG4bK74b43
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Audrey <sip:audrey@atlanta.com>
Call-ID: 3848276298220188511@pc33.atlanta.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.com>
Content-Type: application/sdp
Content-Length: 151

(Alice's SDP not shown)
```

Digest Authentication – Challenge Mechanism for certain Requests

- Challenge could be for an individual header or a combination of headers
- Cannot be for a message body

Digest Authentication

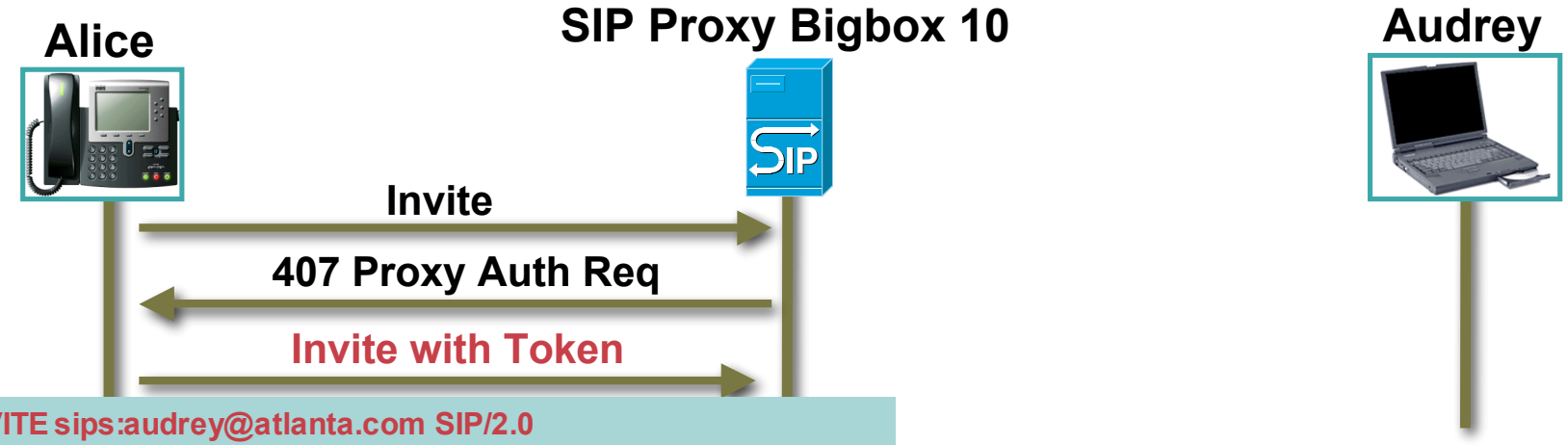



```
SIP/2.0 407 Proxy Authorization Required
Via: SIP/2.0/TLS pc33.atlanta.com
  ;branch=z9hG4bK74b43 ;received=10.1.3.33
From: Alice <sips:alice@atlanta.com>;tag=9fxced76sl
To: Audrey <sips:audrey@atlanta.com>;tag=3flal12sf
Call-ID: 3848276298220188511@pc33.atlanta.com
CSeq: 31862 INVITE
Proxy-Authenticate: Digest realm="atlanta.com",
  qop="auth", nonce="f84f1cec41e6cbe5aea9c8e88d359",
  opaque="", stale=FALSE, algorithm=MD5
Content-Length: 0
```

Digest Authentication – Challenge Mechanism for certain Requests

- A 407 “Proxy Authentication Required” is error message

Digest Authentication

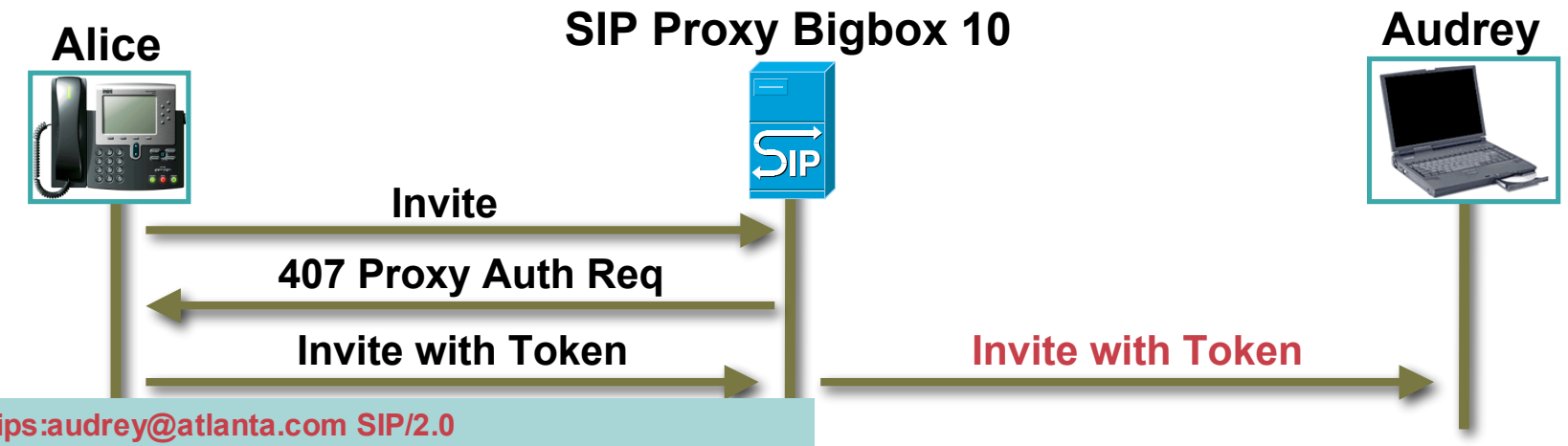



```
INVITE sips:audrey@atlanta.com SIP/2.0
Via: SIP/2.0/TLS pc33.atlanta.com
 ;branch=z9hG4bK776asdhds ;received=10.1.3.33
Max-Forwards: 70
Route: <sips:bigbox10.atlanta.com;lr>
To: Audrey <sips:audrey@atlanta.com>
From: Alice <sips:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 31863 INVITE
Contact: <sips:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 151
Authorization: Digest username="audrey", realm="atlanta.com"
  nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="",
  uri="sips:audrey@atlanta.com",
  response="dfe56131d1958046689d83306477ecc"
(Alice's SDP not shown)
```

Digest Authentication – Challenge Mechanism for certain Requests

- TLS is used due to the lack of Integrity protection in Digest

Digest Authentication

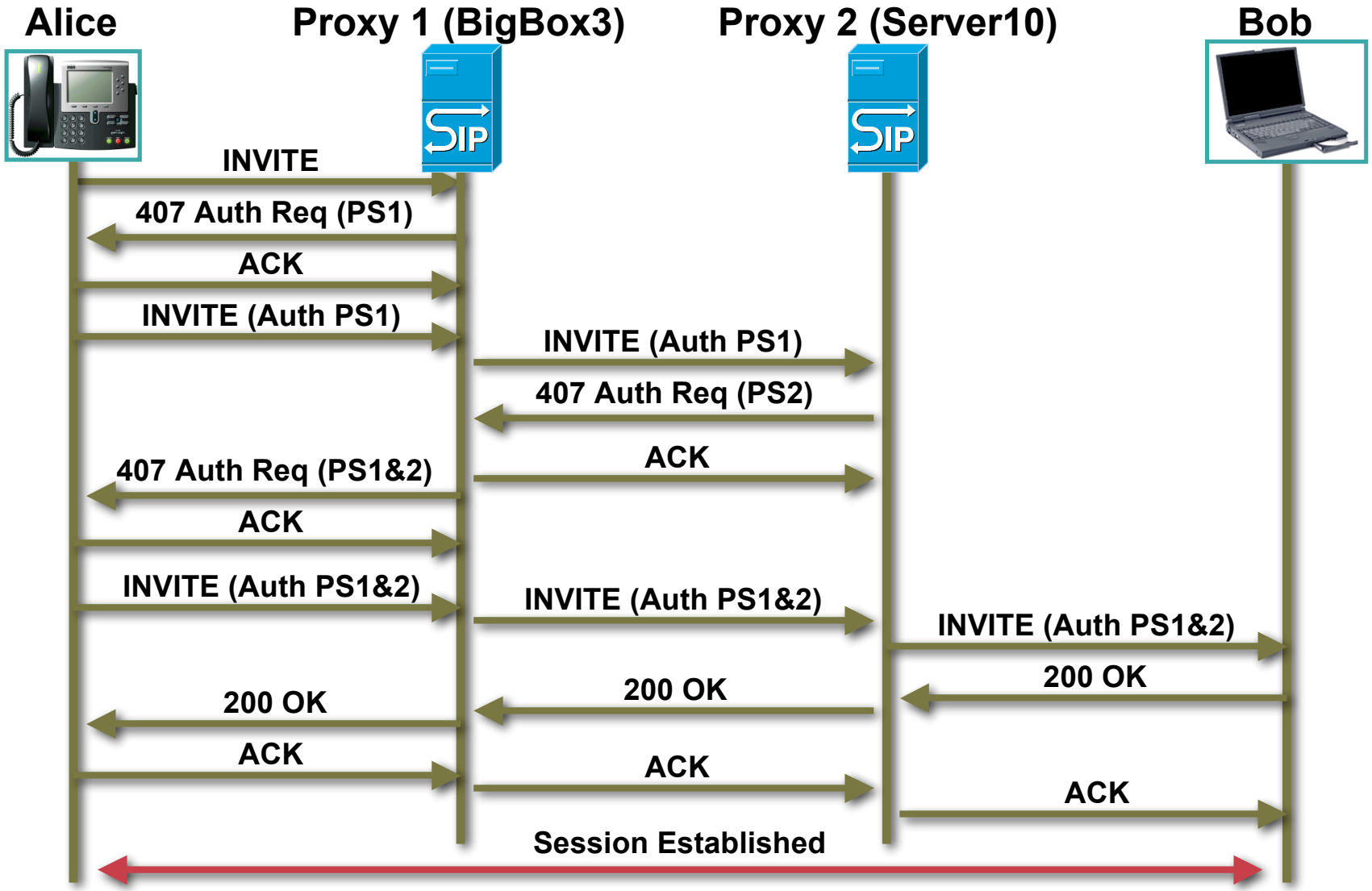



```
INVITE sips:audrey@atlanta.com SIP/2.0
Via: SIP/2.0/TLS Bigbox10.atlanta.com
 ;branch=z9hG4bKnashd92 ;received=10.1.3.1
Via: SIP/2.0/TLS pc33.atlanta.com
 ;branch=z9hG4bK776asdhds
Max-Forwards: 69
To: Audrey <sips:audrey@atlanta.com>
From: Alice <sips:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 31863 INVITE
Contact: <sips:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 151
Authorization: Digest username="audrey", realm="atlanta.com"
  nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="",
  uri="sips:audrey@atlanta.com",
  response="dfe56131d1958046689d83306477ecc"

(Alice's SDP not shown)
```

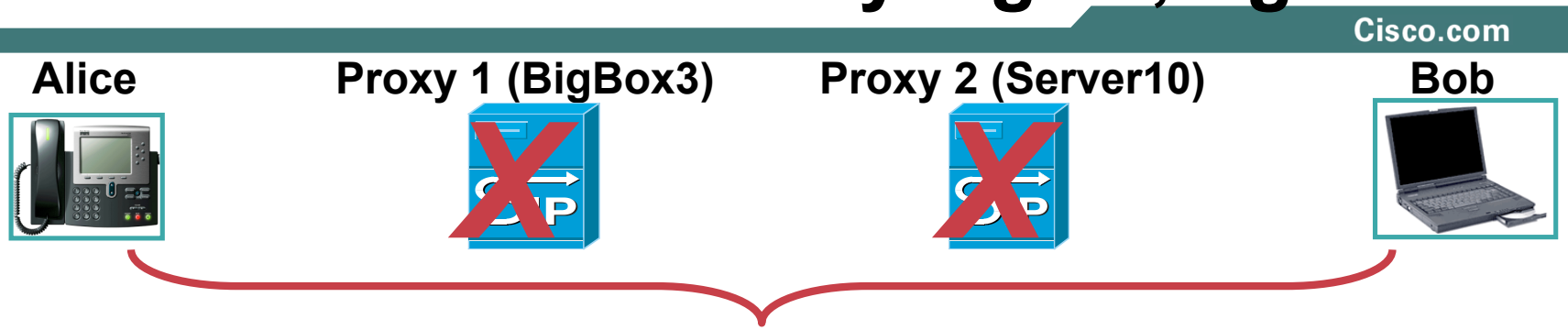
Digest Authentication – Challenge Mechanism for certain Requests

SIP Example: Digest through 2 Proxies



RFC 2401&2406&3261

SIP: End to End Security a goal, right?

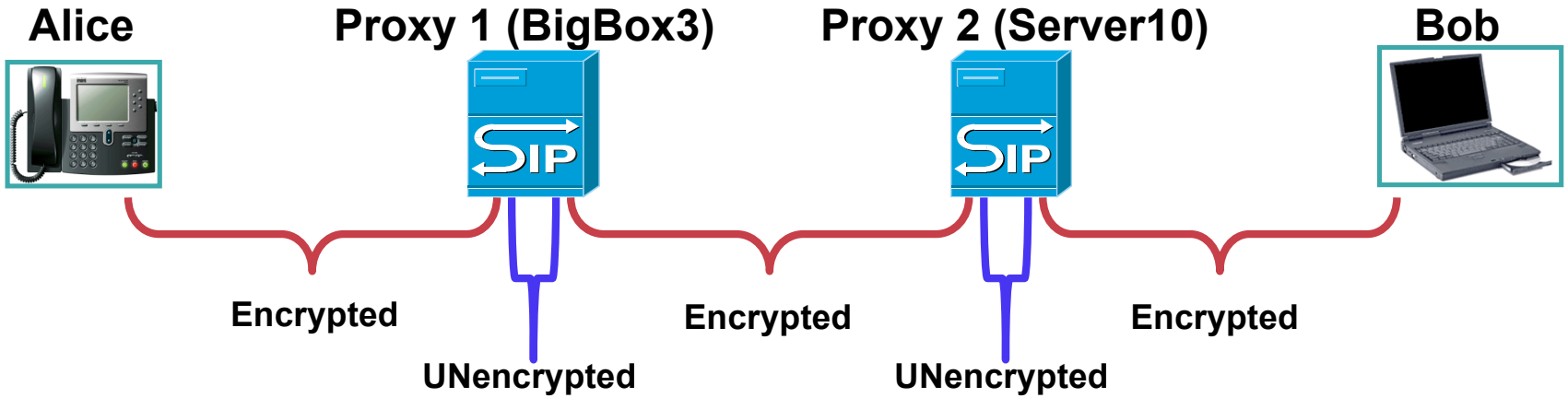


- If Alice encrypts all the way to Bob, the Proxies can't see/add/modify/delete headers they need to
  - –This is a problem for many reasons, including:
    - Alice will need to know Bob's IP address
    - Each network/domain underlying cannot help/control/log
- Therefore, a hop-by-hop Security mechanism or mechanisms will be required for SIP to function properly

RFC 2246&3546&3261

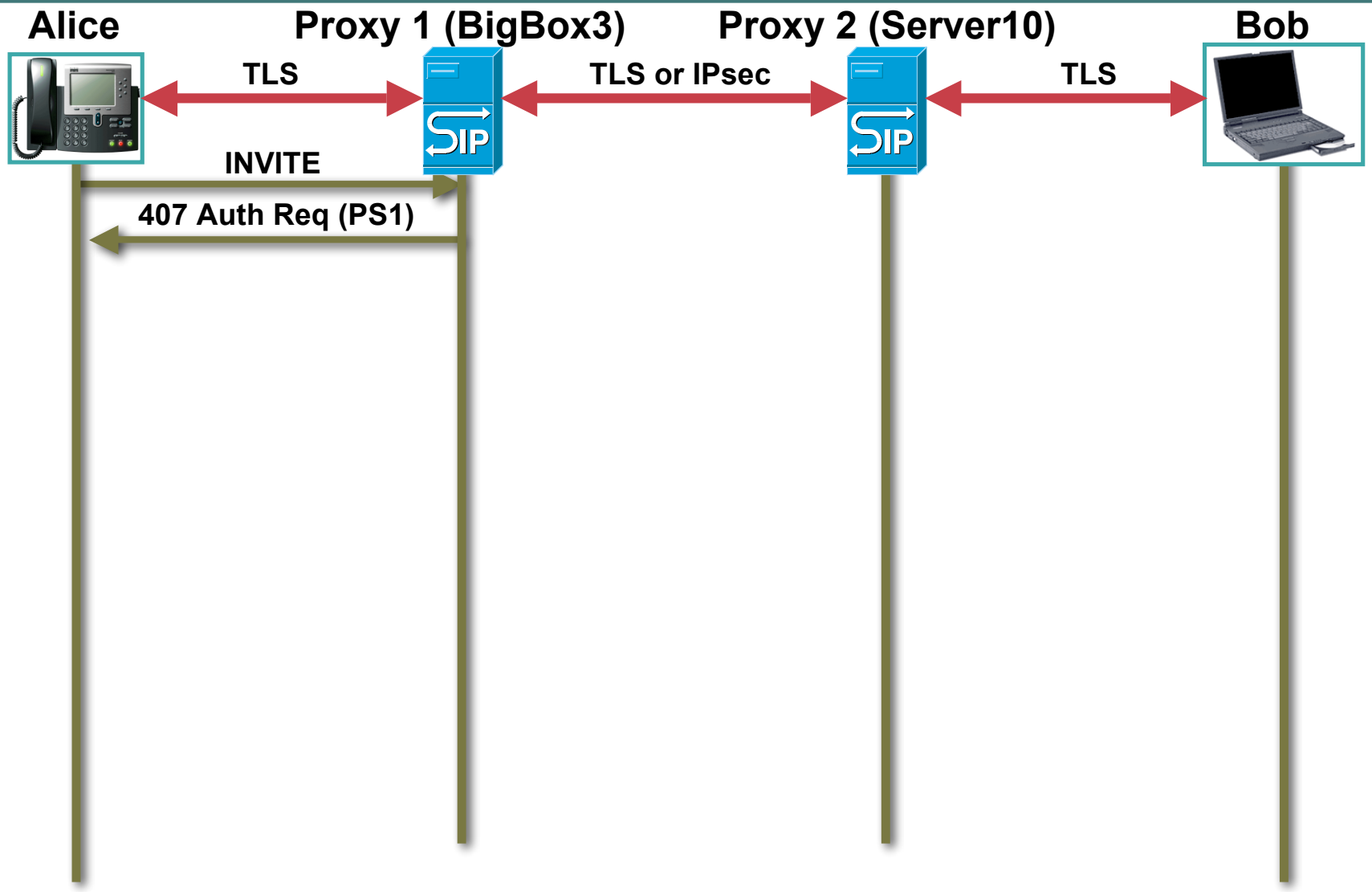
SIPS: Hop-by-Hop Security

Cisco.com



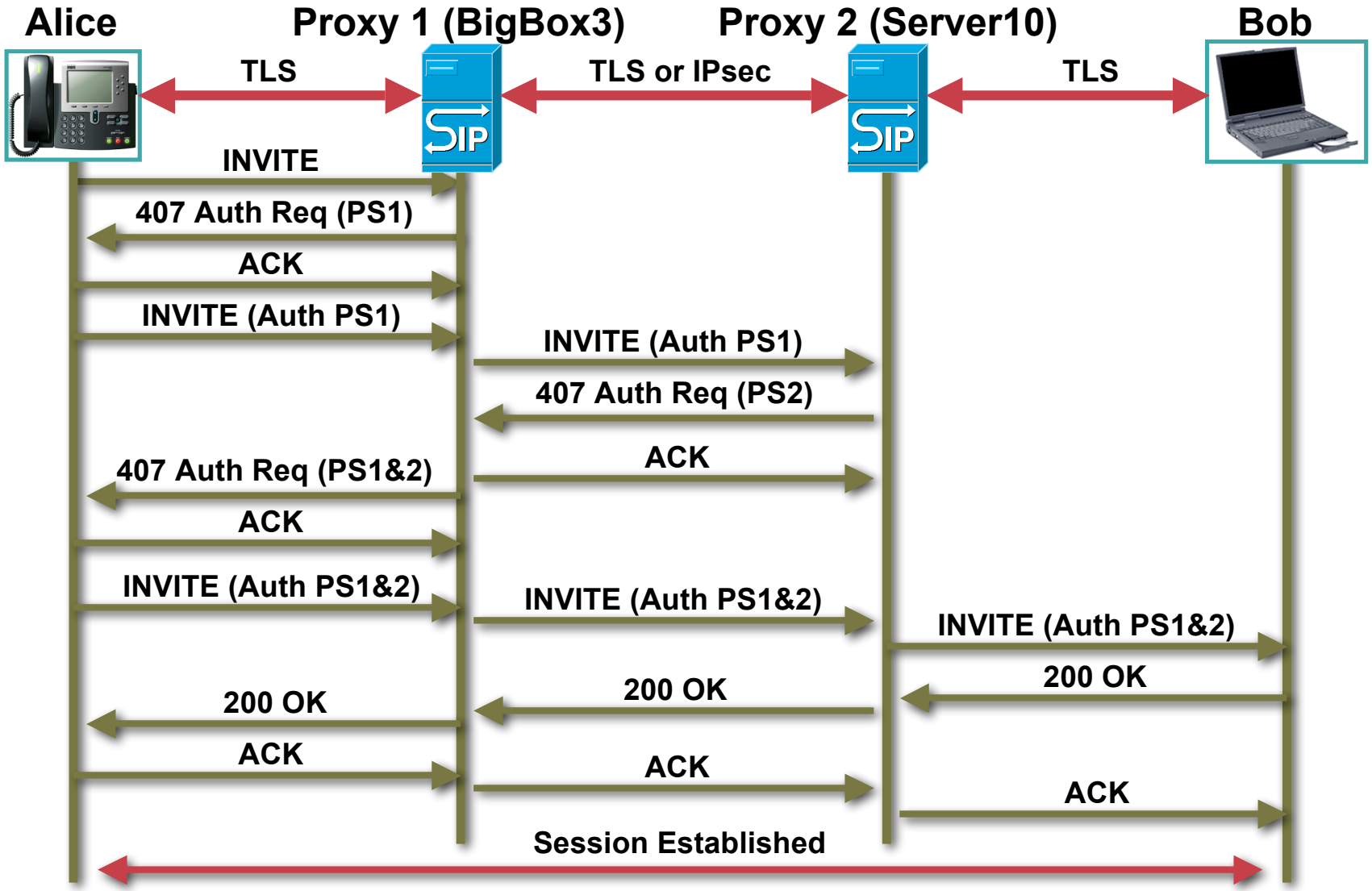
- Phone to the Server – SIP Mandates Transport Layer Security (TLS)
  - TLS works above the IP layer
  - TLS lends itself to entities that have not previously established a trust relationship
- Server to Server signaling can be either TLS or IPsec (which is considered optional – but more robust)
- One piece that's interesting is that each SIP Server decrypts each message (meaning separate keys per communication) – allowing each message Header to be viewed, which SIP needs to operate properly

SIPS (TLS): For Integrity



SIPS (TLS): For Integrity

Cisco.com



Secure/Multipart Internet Mail Extension

S/MIME

- SIP Requirement for Message body confidentiality for end-to-end communications
  - not intended for UA to Proxy
    - but there is a new effort for this type of communication as well with limited scope (e2m)
- S/MIME compliant elements MUST support SHA1 Authentication and 3DES encryption
  - separately – AES has been introduced
- Not widely deployed due to requirement of PKI
- Varying ways to self-sign certificates

RFC 3261

SIP Security: S/MIME

Cisco.com

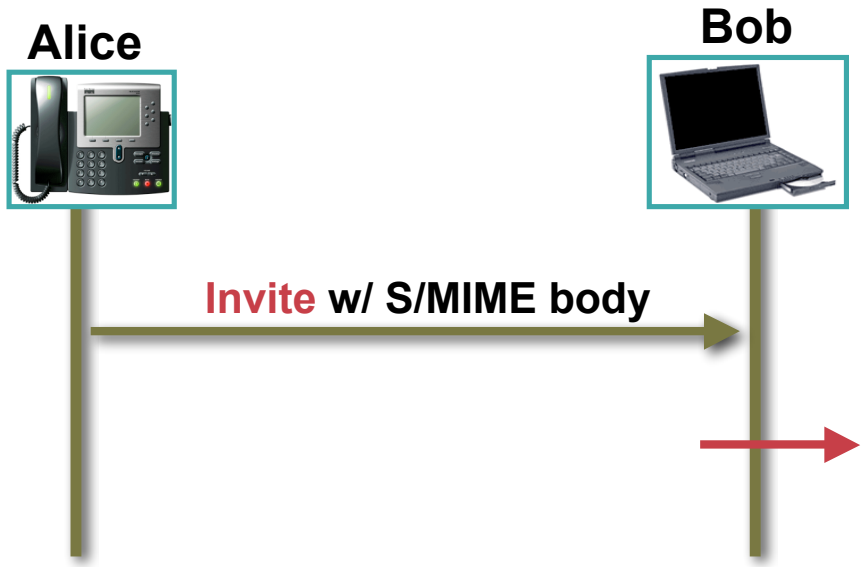
- **S/MIME body(ies)**
  - Content-Type Header indicating smime
  - SIP elements MUST support SHA1 (authentication) and 3DES encryption
    - AES is specified separately
  - Overall body should be signed once

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com
  ;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/pkcs7-mime;
   smime-type=enveloped-data; name=smime.p7m
Content-Disposition: attachment;
   filename=smime.p7m  handling=required
```

```
Content-type: application/sdp

v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.com
c=IN IP4 10.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0 4 8
a=rtpmap:0 PCMU/8000
```

SIP Security: S/MIME




```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com
  ;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/pkcs7-mime;
   smime-type=enveloped-data; name=smime.p7m
Content-Disposition: attachment;
   filename=smime.p7m  handling=required
```

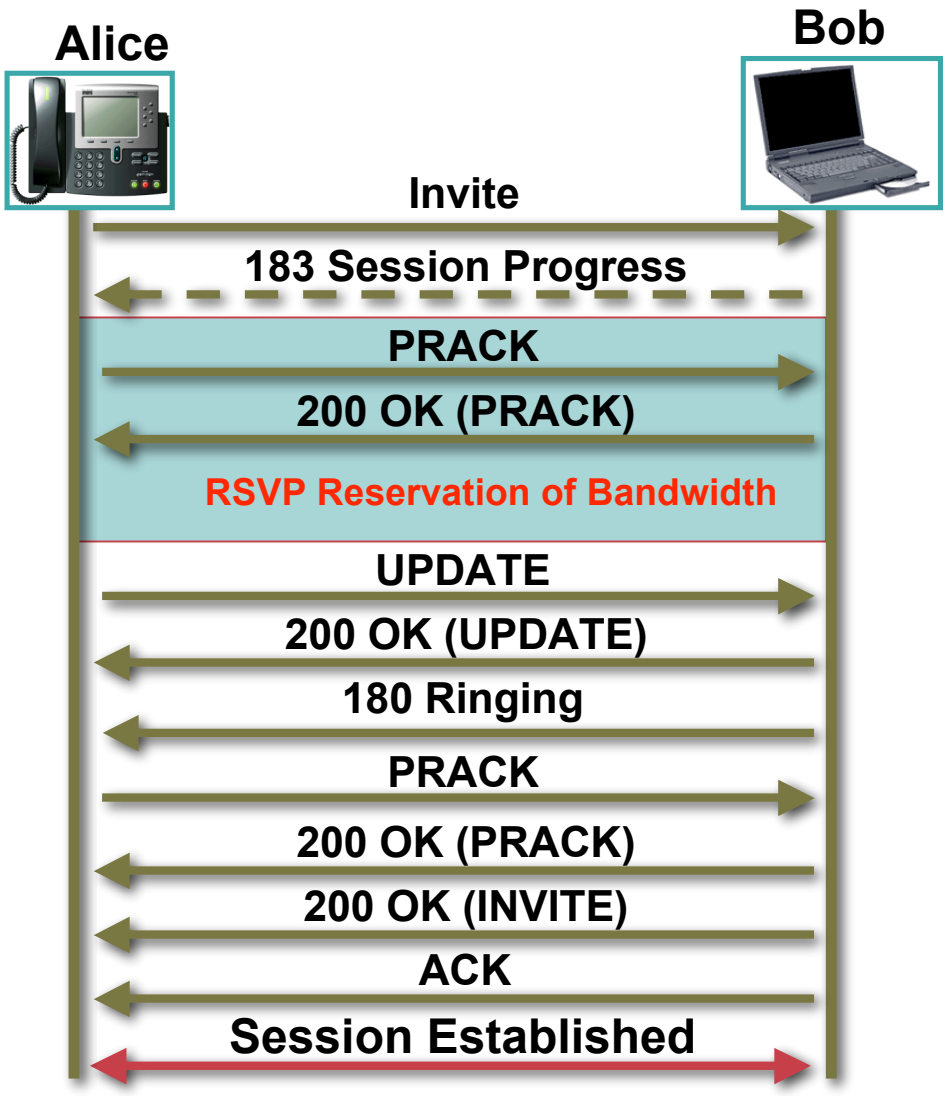
Same Message Body
S/MIME encrypted

```
JB23LB645V73V73MNB73KV7K4VLHV4T234T2T2JH
5NG5CMGX5MYM5SMN5GYCWG5CYMWYMWHNHG
5MC5YGWC5CW5WIU87W34TO8W7FLW5LWC5WC5
C4L5CLWCTYWJHC54JHCW45HCWLJ5HCWL5CLW
JH5CLJH4C5JHEWCLTJYH54CLWJ5CYWJ45CLYWJ
5HFKGFD3K7GHD4KHG7DK4T5DLTYGCK6DUK4TD
UK4GHCUK56CUY45TD6UK3TCKH45T8K3TH2DXL2
HTXLKT8K2XK82XK83K5T8D3KGHICXH4D98D4D967
763R9356T08726R85R6L2Y4F5L356D3Y5SD3754T73
967RT35PI84FY7J3FD6D3LU6D6L37Y45F639456T29
87R2RFL24YD2L6TDK3T7D3K75YU5D756RO837R3F
LY
```

RFC 3312

SIP (QoS) Preconditions

Cisco.com



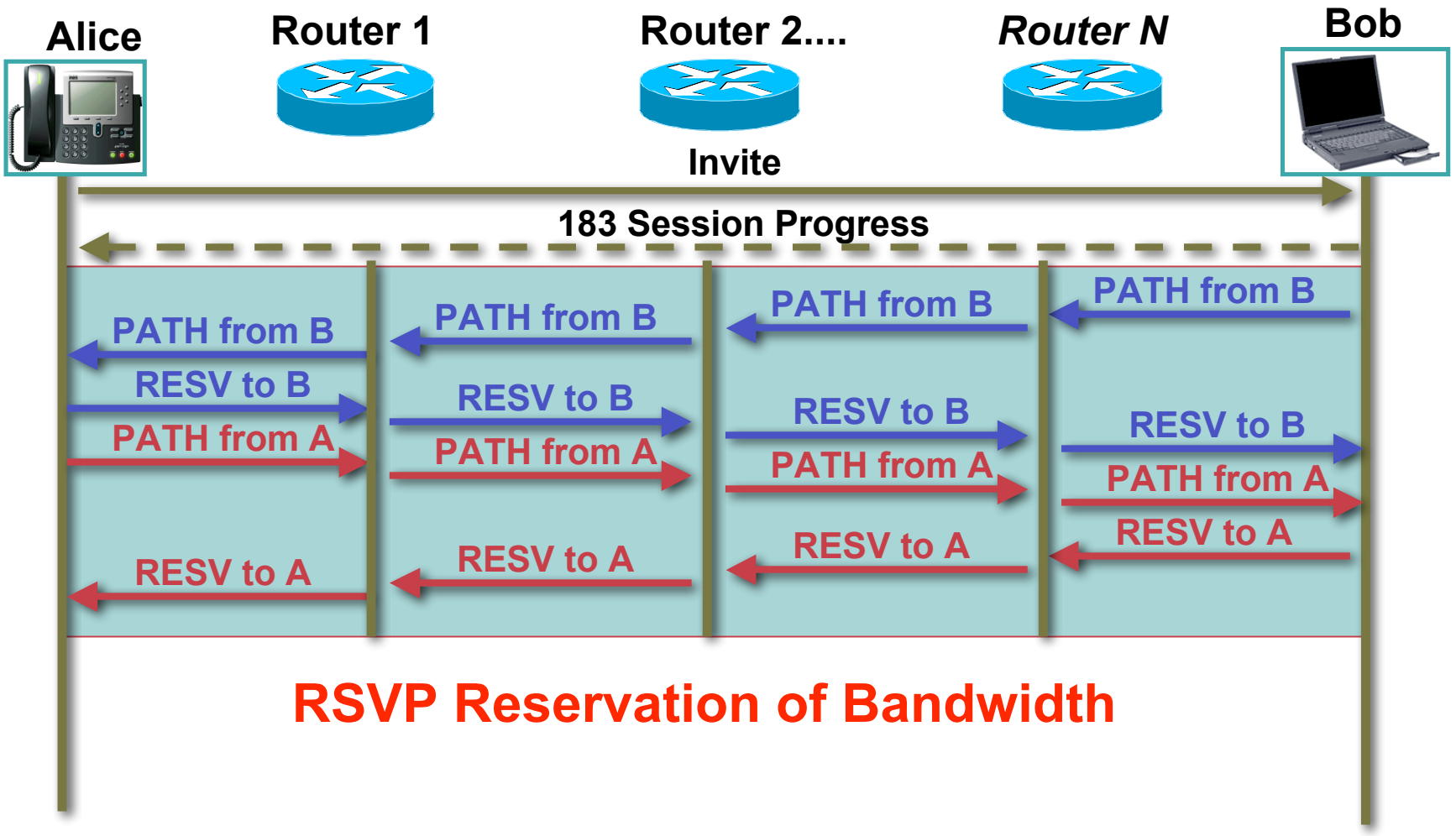
SIP Preconditions – Bandwidth guarantee mechanism for a session using RSVP

- Uses the Offer/Answer model for Session establishment
- Provides initial feedback
- Provides progress feedback
- Allows for reservation to be established BEFORE called phone rings (no ghost ringing)
- All other SIP rules and capabilities still used/available

RFC 2205

SIP (QoS) Preconditions

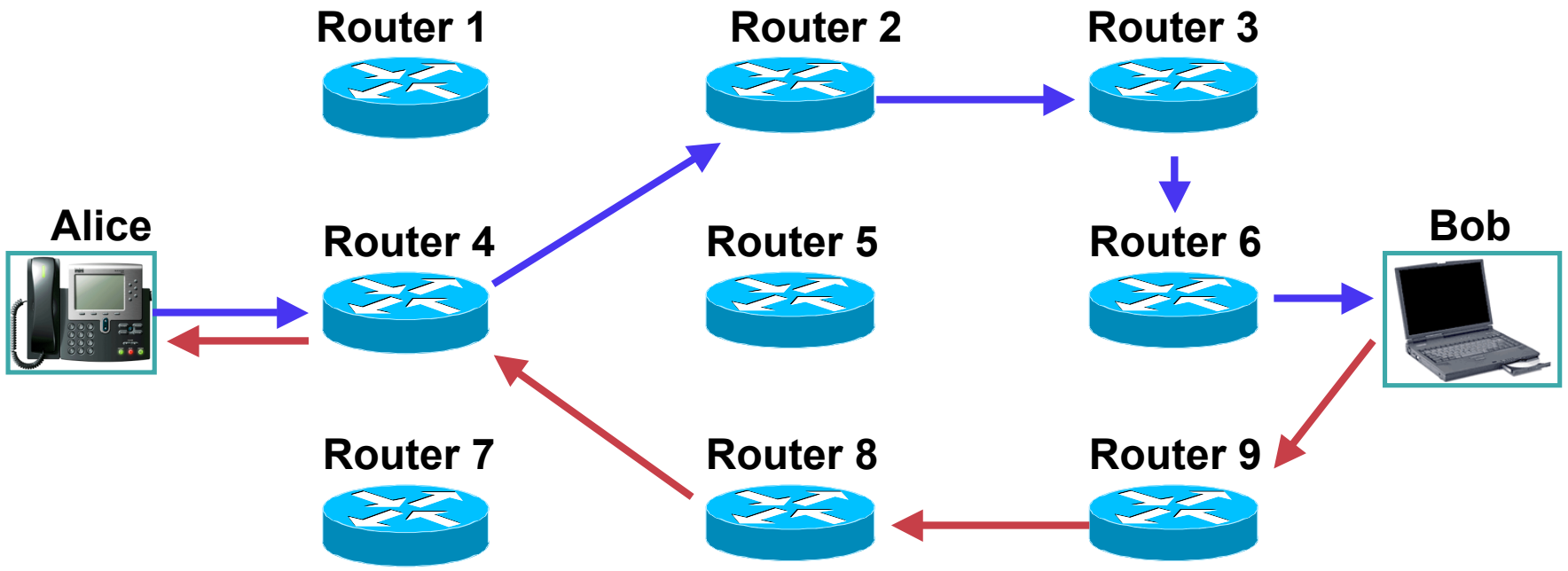
Cisco.com



RFC 2205

SIP (QoS) Preconditions

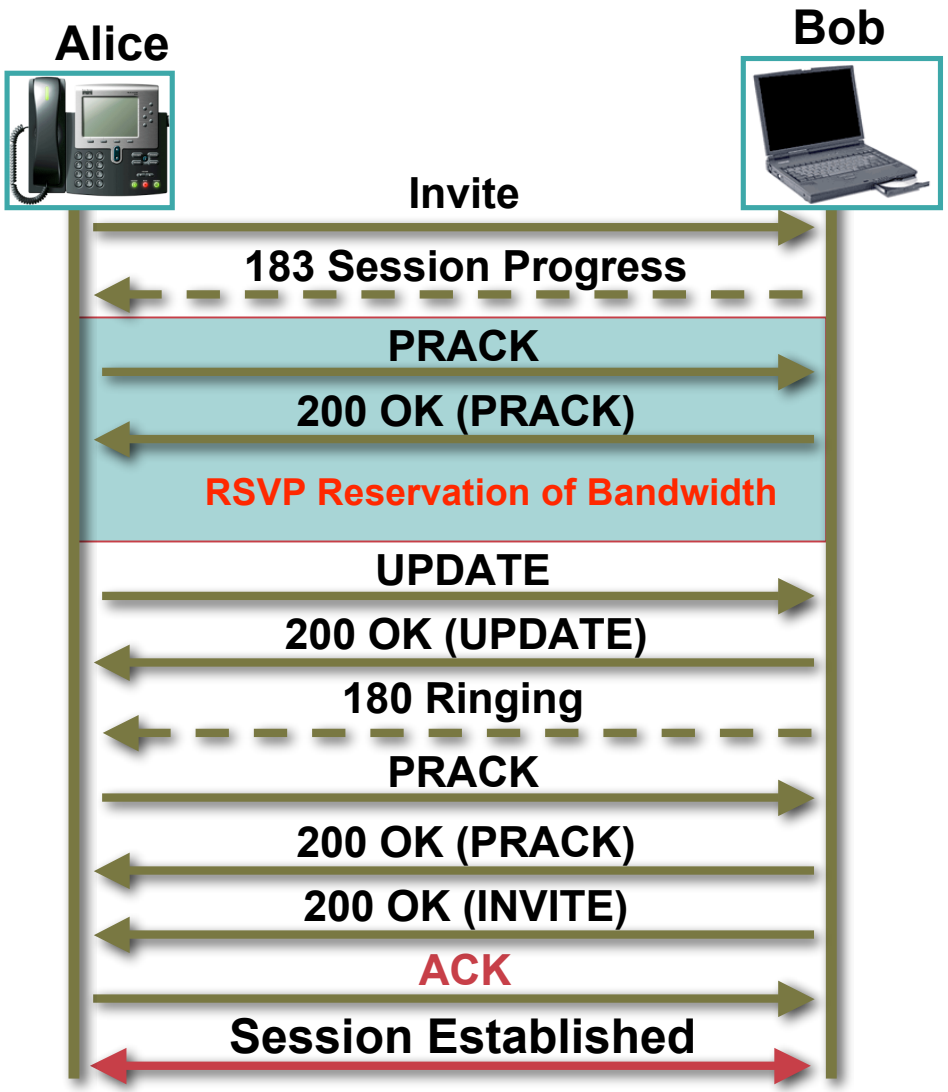
Cisco.com



RSVP Reservation of Bandwidth

- Diverse Route Paths of One-way Reservations
- Each Path is separate from the other
- SIP will synchronize that both Reservations exist
- Not all adjacent Routers have to be RSVP enabled
  - RSVP messages ignored when this is the case

SIP (QoS) Preconditions



SIP Preconditions – Bandwidth guarantee mechanism for a session using RSVP

- Once the UPDATE is 200 OKd, the rest of the session is set up normally
- If reservation set-up was a failure, a 580 “Preconditions Failure” would be the error returned
- Multiple media for between Alice and Bob could be mapped into different flows, or the same flow*

*See Single Reservation Flows (SRF) in RFC 3524

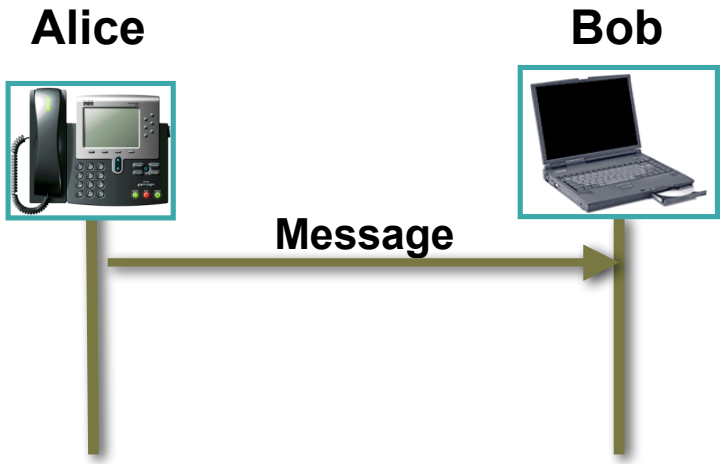
VVT-4000 Session Agenda

- SIP Refresher
- SIP Standards Efforts
- SIP Working Efforts
- SIP Summary
- Reachability

SIP Working Efforts (all Internet Drafts)

- Content Indirection
- Resource Priority (GOV/Military Emergency calling)
- Location Conveyance
- Emergency calling (911/112-style)

Content Indirection



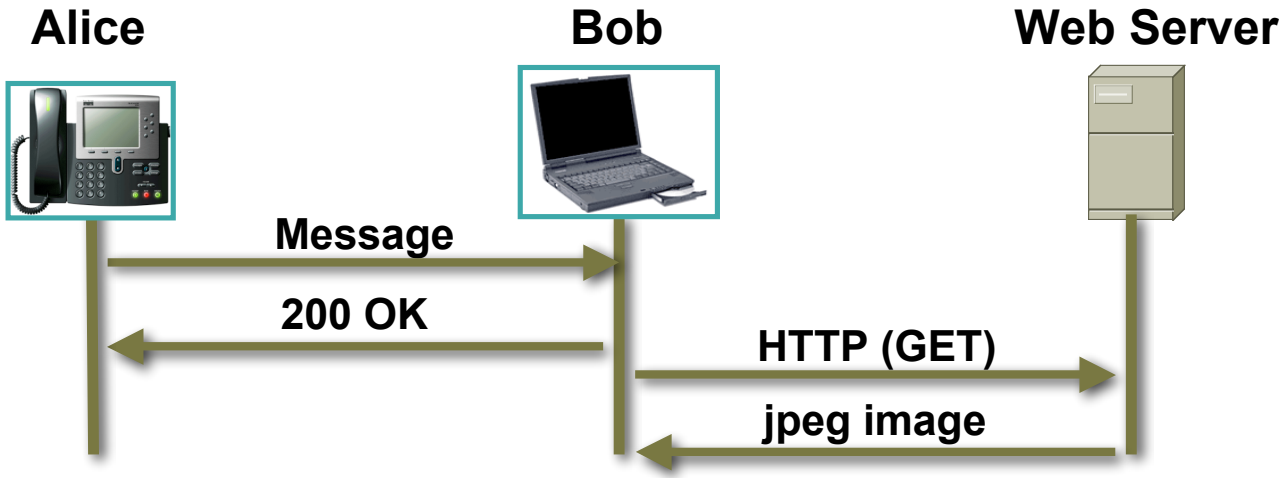
- **Content Indirection** – to indirectly specify or reference (via a URI) a SIP message body (part)
- Usage examples:
  - limited bandwidth
  - content size an issue
    - (ex. here 2.3MB)
  - does not reside in UA

```
MESSAGE sip:bob@biloxi.com SIP/2.0
From: <sip:alice@atlanta.com>;tag=34589882
To: <sip:bob@biloxi.com>
Call-ID: 92428924422111117@atlanta.com
CSeq: 6187 MESSAGE
Accept: message/external-body, text/plain, image/*
MIME-Version: 1.0
Content-Type: message/external-body
      access-type="URL";
      expiration="Thurs, 22 July 2004 09:00:00 GMT";
      URL="http://www.atlanta.com/picnic/image1.jpg"
      size=2344228
Content-Type: image/jpg
Content-ID: <766534765937@atlanta.com>
Content-Disposition: render
Content-Description: Haley getting dunked in the pool
```

- Except for transport, indirected body parts are equivalent, and should have the same treatment as in-line body parts

draft-ietf-sip-content-indirect-mech

Content Indirection



- Content Indirection – to indirectly specify or reference (via a URI) a SIP message body (part)
- A 415 "Unsupported Media Type" is the error if the UAS does not support this ability
- Retrieval of the content is accomplished via a non-SIP transfer channel such as HTTP, FTP, or LDAP
  - this should be secure (HTTPS)

Preferential Treatment of SIP Messages

- “The "Resource-Priority" header field can influence the behavior of SIP UAs (including gateways) and SIP proxies to provide an indication for priority treatment of the SIP message over or under other messages”
- Divided into two pieces:

Namespace:	the domain or realm identification
Priority_value:	the priority level within a domain or realm

- Read as:

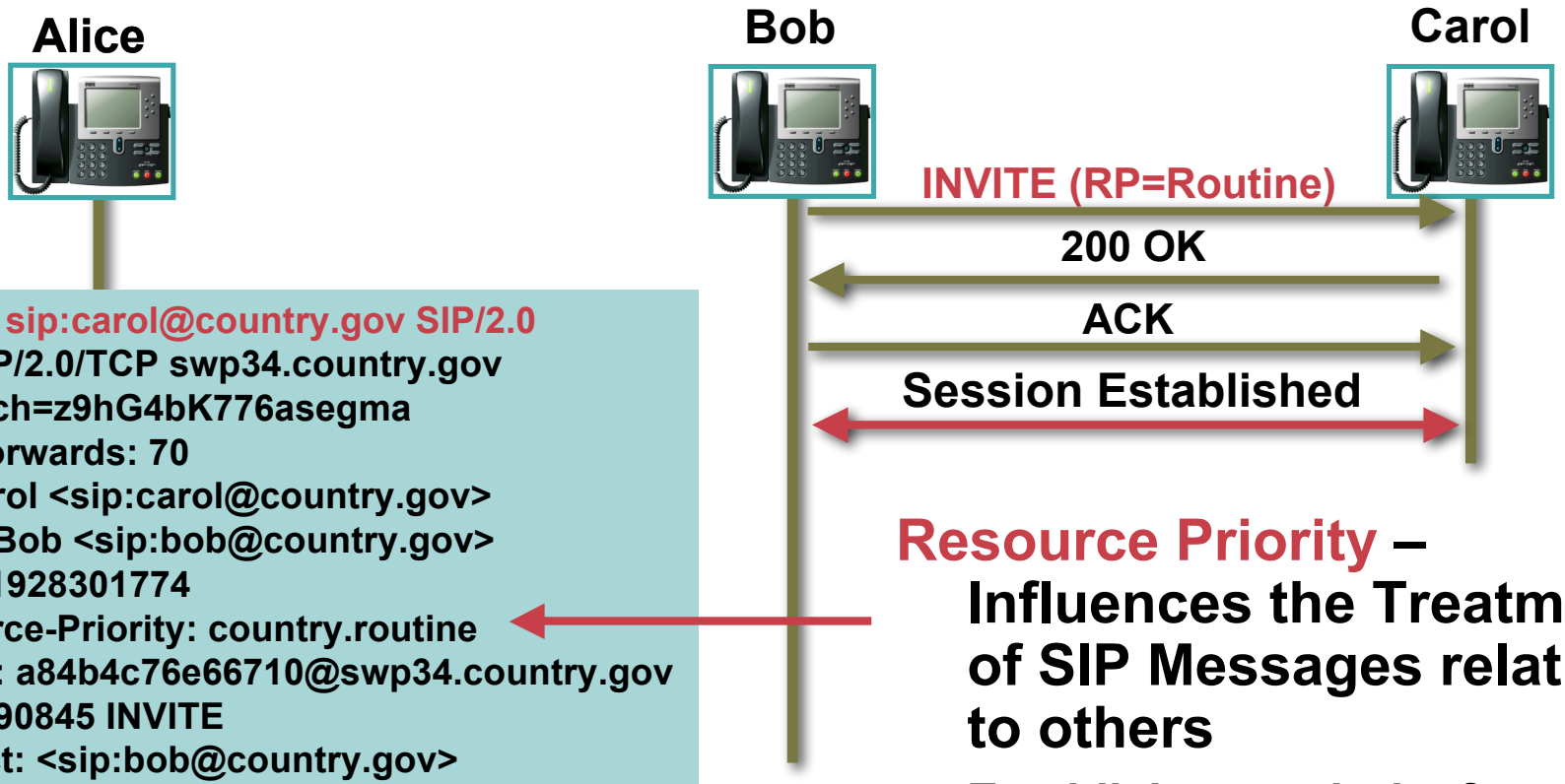
Resource-Priority : namespace.priority_value

draft-ietf-sip-resource-priority

draft-ietf-sipping-reason-header-for-preemption

Preferential Treatment of SIP Messages

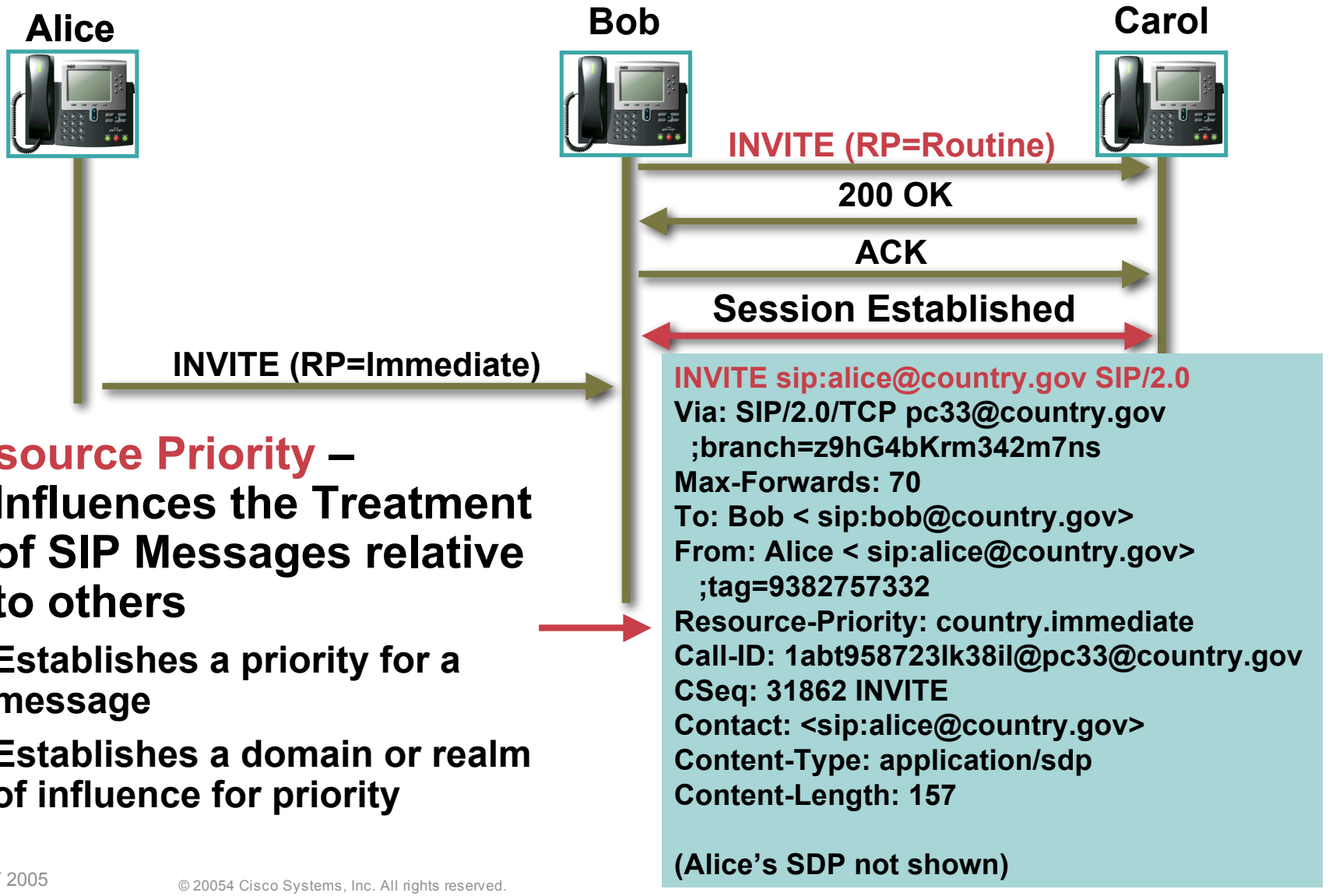
Cisco.com



Resource Priority – Influences the Treatment of SIP Messages relative to others

- Establishes a priority for a message
- Establishes a domain or realm of influence for priority

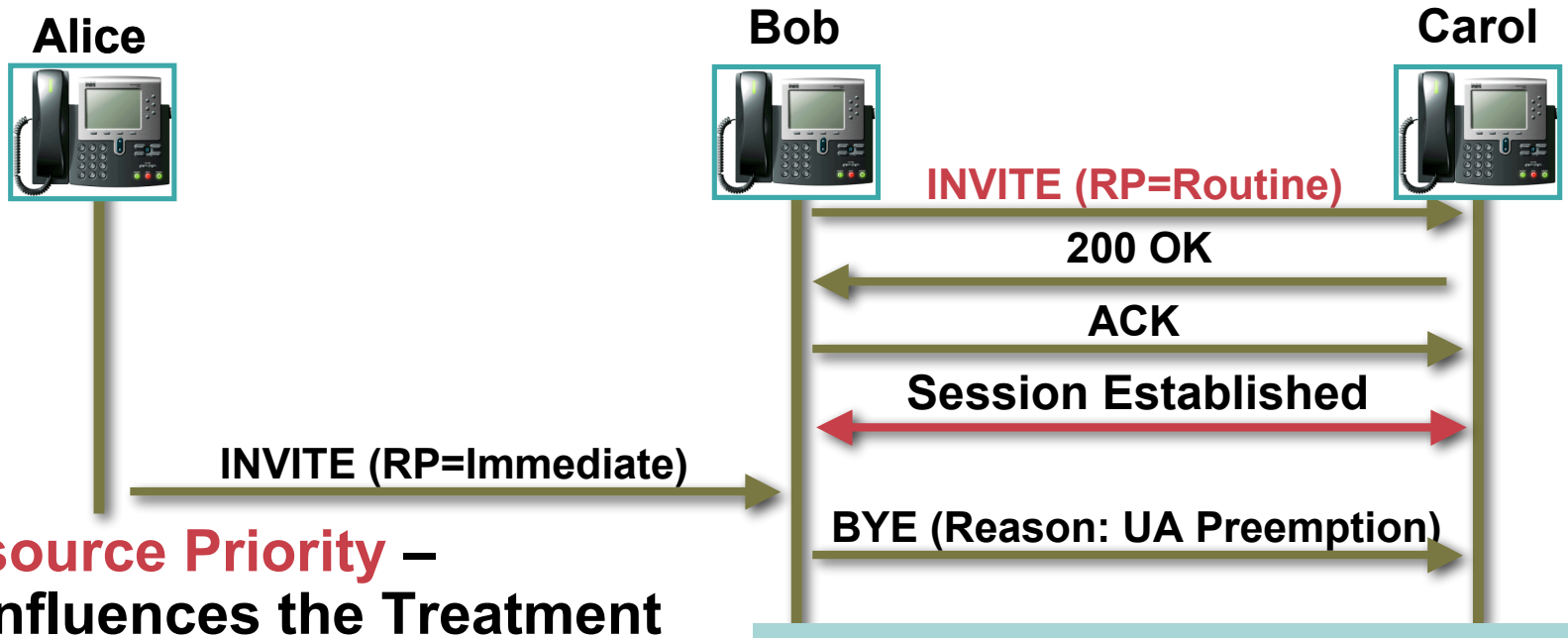
Preferential Treatment of SIP Messages



Resource Priority – Influences the Treatment of SIP Messages relative to others

- Establishes a priority for a message
- Establishes a domain or realm of influence for priority

Preferential Treatment of SIP Messages



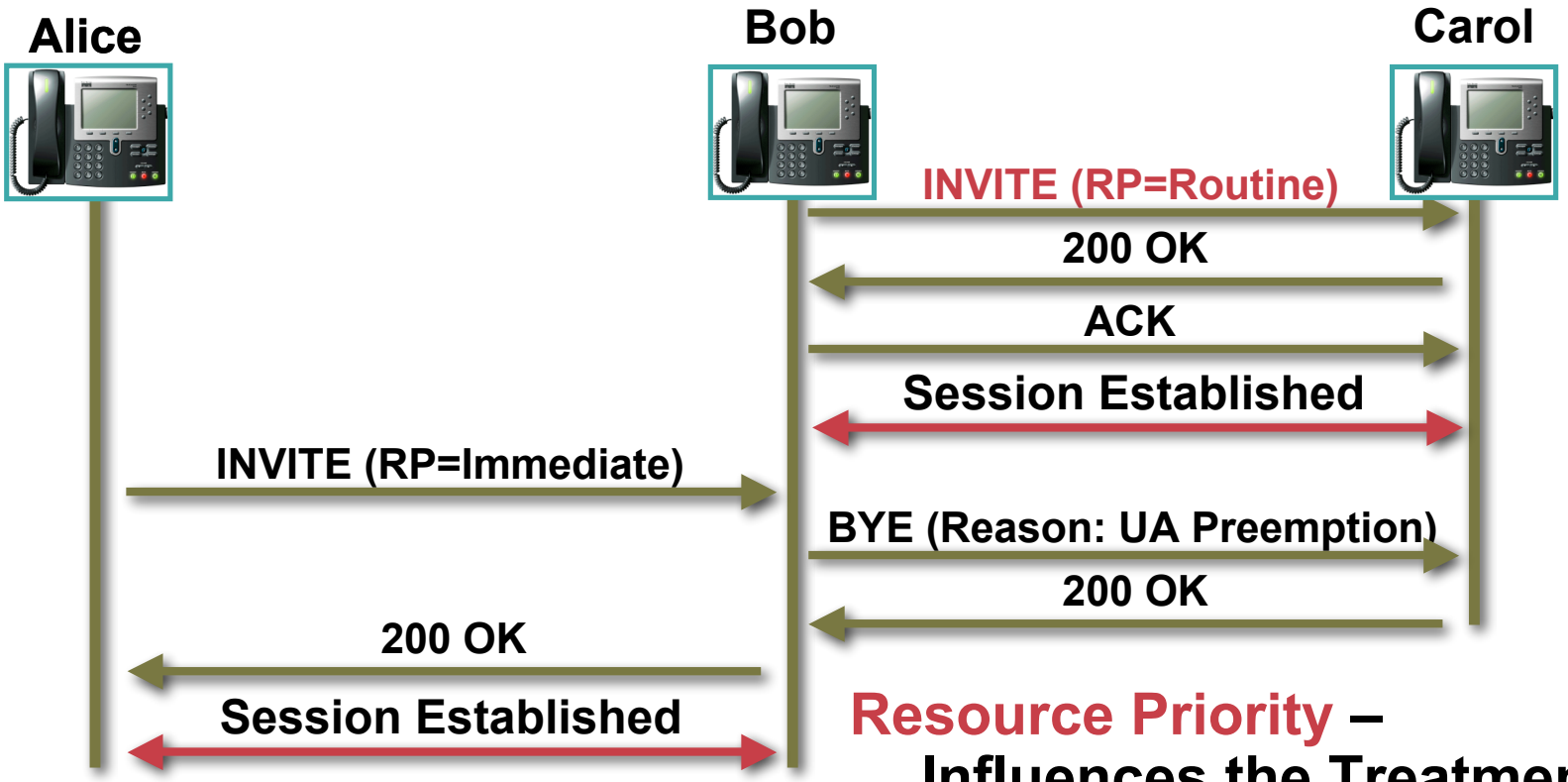
Resource Priority – Influences the Treatment of SIP Messages relative to others

- Bob's UA compares R-P values
- Bob's UA terminates call to Carol with "Reason=UA_Preemption" indication (perhaps a chime)

```
BYE sip:carol@country.gov SIP/2.0
Via: SIP/2.0/TCP swp34.country.gov
  ;branch=z9hG4bK776asegma
To: Carol <sip:carol@country.gov>
From: Bob < sip:bob@country.gov>;tag=192820774
Reason: cause=1 ;text=UA based preemption
Call-ID: a84b4c76e66710@swp34.country.gov
CSeq: 6187 BYE
Contact: <sip:bob@country.gov>
```

Preferential Treatment of SIP Messages

Cisco.com



Resource Priority – Influences the Treatment of SIP Messages relative to others

- Call between Alice and Bob established

Who wants to use this Treatment?

- Military Networks (Multilevel Precedence and Preemption)
- Government Networks tied to Military
  - Department of Homeland Security
  - 3 Letter Agencies
- Government Designed/Agreed arrangements with Service Providers for Disaster Relief
  - Federal Emergency and Medical Assistance (FEMA)
  - Local Authorities
- Large Enterprises
- Probably going to be used for parts of 911/112 Emergency calls where servers can become overwhelmed

Location Conveyance

- Based on Presence Information Data Format (PIDF) for Location Objects (LO) as defined in the Geopriv Working Group of IETF
  - simply PIDF-LO
- PIDF-LO uses GML (Geography Markup Language from OpenGIS)
- 2 Location Representations are specified:
  - Civil Addressing (basically Post Office addresses which are internationalized)
  - Coordinate or Geodetic (Lat/Long/Alt with datum)
- Two types of Location Conveyance in SIP:
  - User-to-User (I want to tell you where I am, have been or will be)
  - Routing based on UAC location (Proxies need to know my location to properly route the SIP Request (shown in Emergency example)

draft-ietf-geopriv-dhcp-lci-option

draft-ietf-geopriv-dhcp-civil

draft-ietf-sipping-location-requirements

draft-ietf-geopriv-pidf-lo

GEOPRIV Geospatial/Coordinate format

- **Based on this GML schema**
- **To a point, a line, a polygon**
- **Provides how location was derived**
- **and who is responsible for it**
  - **After the fact troubleshooting**

```
<?xml version="1.0" encoding="UTF-8"?>
  <presence xmlns="urn:ietf:params:xml:ns:pidf"
    xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
    xmlns:gml="urn:opengis:specification:gml:schema-xsd:feature:v3.0"
    entity="pres:geotarget@example.com">
   <tuple id="sg89ae">
    <timestamp>2004-07-11T08:57:29Z</timestamp>
    <status>
     <gp:geopriv>
      <gp:location-info>
       <gml:location>
        <gml:Point gml:id="point96" srsName="epsg:4326">
         <gml:coordinates>29:56:31N 90:5:49W</gml:coordinates>
        </gml:Point>
       </gml:location>
      <method>dhcp</method>
      <provided-by><nena>www.cisco.com</nena></provided-by/>
     </gp:location-info>
     <gp:usage-rules>
      <gp:retransmission-allowed>no</gp:retransmission-allowed>
      <gp:retention-expiry>2004-07-13T14:57:29Z</gp:retention-expiry>
     </gp:usage-rules>
    </gp:geopriv>
   </status>
  </tuple>
</presence>
```

draft-ietf-geopriv-pidf-lo

GEOPRIV civil format

- **Based on National Emergency Numbering Authority (NENA) XML elements**
  - **Except internationalized administrative divisions:**

```
<country>US</country>
<A1>LA</A1>
<A3>New Orleans</A3>
<A6>Convention Center</A6>
<STS>Blvd</STS>
<HNO>900</HNO>
<NAM>Morial</NAM>
<ZIP>70130</ZIP>
```

A1	**national subdivisions (state, region, province, prefecture)**
A2	**county, parish, gun (JP), district (IN)**
A3	**city, township, shi (JP)**
A4	**city division, borough, city district, ward, chou (JP)**
A5	**neighborhood, block**
A6	**street**

draft-ietf-geopriv-dhcp-civil

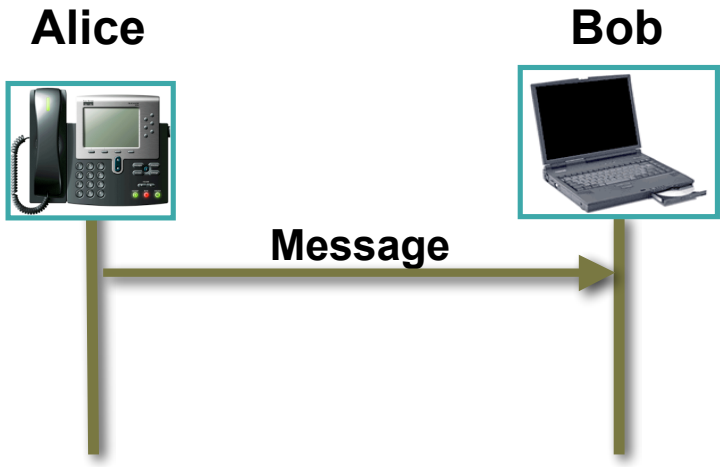
GEOPRIV civil format

- **Newly defined in the PIDF-LO ID**
  - **Specifies up to 27 fields for civil location**
  - **Provides how location was derived**
  - **and who is responsible for it**
    - **After the fact troubleshooting**

```
<?xml version="1.0" encoding="UTF-8"?>
 <presence xmlns="urn:ietf:params:xml:ns:pidf"
   xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
   xmlns:gml="urn:opengis:specification:gml:schema-xsd:feature:v3.0"
   entity="pres:geotarget@example.com">
  <tuple id="sg89ae">
   <timestamp>2004-07-11T08:57:29Z</timestamp>
   <status>
    <gp:geopriv>
     <gp:location-info>
      <cl:civilAddress>
       <cl:country>US</cl:country>
       <cl:A1>Louisianna</cl:A1>
       <cl:A3>New Orleans</cl:A3>
       <cl:A6>Convention Center</cl:A6>
       <cl:HNO>900</cl:HNO>
       <cl:NAM>Ernest N. Morial Convention Center</cl:NAM>
       <cl:PC>70130</cl:PC>
      <cl:civilAddress>
      <method>dhcp</method>
      <provided-by><nena>www.cisco.com</nena></provided-by/>
     </gp:location-info>
     <gp:usage-rules>
      <gp:retransmission-allowed>no</gp:retransmission-allowed>
      <gp:retention-expiry>2004-07-13T14:57:29Z</gp:retention-expiry>
     </gp:usage-rules>
    </gp:geopriv>
   </status>
  </tuple>
 </presence>
```

draft-ietf-geopriv-pidf-lo

Location Conveyance in SIP




```
MESSAGE sip:bob@biloxi.com SIP/2.0
From: <sip:alice@atlanta.com>;tag=34589882
To: <sip:bob@biloxi.com>
Call-ID: 92428924422111117@atlanta.com
CSeq: 6187 MESSAGE
Content-Type: application/pidf-lo+xml
Content-ID: <766534765937@atlanta.com>
Content-Disposition: render
Content-Description: my location
```

(Alice's Location on the previous slide)
(too large for this slide)

- **Location Conveyance – to provide the UAC's civil or geodetic location in a SIP message body (part)**

  Accomplished using the INVITE, MESSAGE or UPDATE Methods

Emergency Calling Requirements:

From a 10,000 ft Level

- Recognize a call is an emergency call
- Route the call to the correct PSAP based on location of the caller
- Include location in the call for dispatch
- Include a call-back address in the call

National Emergency Numbering Authority (NENA) represents North American Public Safety Answering Points (PSAPs)

NENA's i3 (e2e VoIP) assumptions:

- No carrier presumed
- Permanent, roaming and true mobile clients supported
- Multiple media types supported
- International operation supported
  - not a NENA requirement, but is an IETF requirement
- No assumption of e.164 addressing (sip:jmpolk.cisco.com)
- Big "I" Internet call path;
  - PSAP(s) may be on a private IP net
  - PSAP(s) may have specialized VSP for Emergency Services
  - Both have a firewall, etc... between PSAP and the Internet.

NENA's i3 proposal on the table includes:

- SIP-only signaling
  - SHOULD use SIPS for integrity and confidentiality, but limit the use of challenges (like with Digest)
  - protocol interwork at source/Voice SP for non-SIP systems
- sos@<anydomain> as universal address for assistance
- IETF PIDF-LO (location object), geo and/or civil
  - contained in the initial SIP INVITE message
- Call answers as (native) SIP inside the PSAP
- Callback address in Contact field of SIP message

Service identification

- In some countries, specialized numbers for police, fire, …
- We add SIP protocol header that identifies call service:

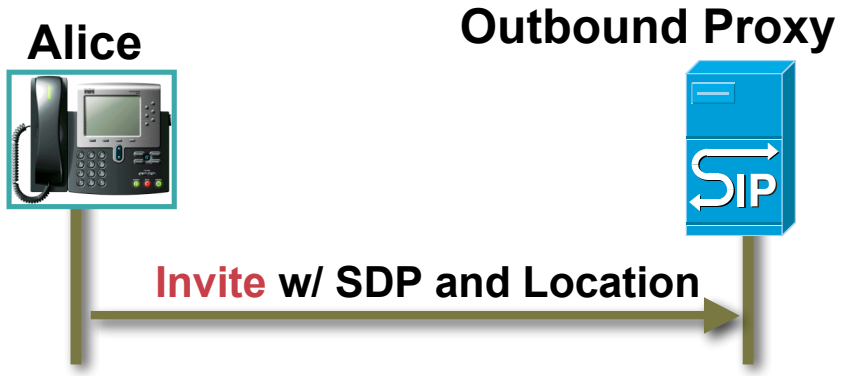
```
Accept-Contact: *
  ;service="sos.mountain"
```

- Generally, not user visible

sos.fire	fire brigade
sos.rescue	ambulance
sos.marine	marine guard
sos.police	police
sos.mountain	mountain rescue
sos.test	only testing

draft-ietf-sipping-sos

SIP Routing based on UAC's Location



- **SIP Routing based on Location**
  - "sos@" is not unique
  - Proxy MUST learn UAC's location, determine where UAC is, then Route the call to the proper Emergency Call Center

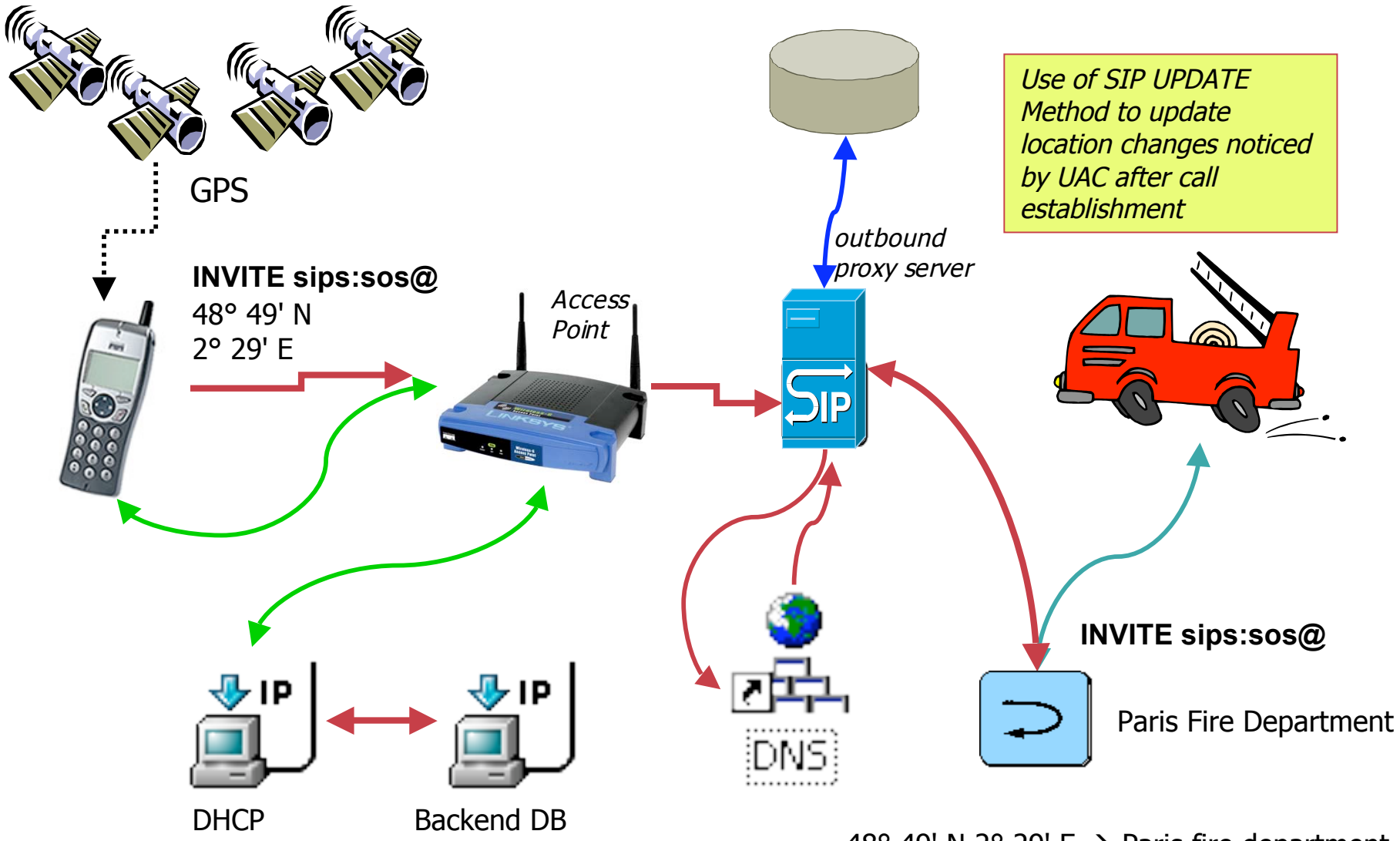
* "Short form" means not enough room here

```
INVITE sips:sos@atlanta.com SIP/2.0
Via: SIP/2.0/TCP pc33.atlanta.com
  ;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.com>;tag=9fxced76sl
To: Bob <sip:sos@atlanta.com>
Call-ID: 3848276298220188511@atlanta.com
CSeq: 31862 INVITE
Contact: <sip:alice@atlanta.com>
Content-Type: multipart/mixed; boundary=0a0
Content-Length: 311

--0a0
Content-Type: application/sdp
v=0
o=alice 2890844526 2890844526 IN IP4 atlanta.com
c=IN IP4 1.1.3.33
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

--0a0
Content-Type: application/cpim-pidf+xml (short form*)
<A1>Texas</A1>
<A2>Richardson</A2>
<A6>Pres Bush</A6>
<STS>Turnpike</STS>
<HNO>2200</HNO>
<FLR>3rd floor</FLR>
--0a0--
```

Location-based call routing: UA learns its location



Emergency Calling in SIP (i.e. 911/112)

Cisco.com

- Routing of INVITE based on location of person in distress
- What's Required:
  - Location (civil or coordinate based) to be in the UAC (phone)
    - Local GPS, DHCP, Manual configuration, triangulation, etc
  - Location to be placed into INVITE in such as way that Proxy can read it
  - Proxy to know how that INVITE is emergency call to look for Location Information
  - Proxy to know where correct Emergency Contact Center (ECC) is for that location (of UA) to IP address properly
- Location may be updated during call (UPDATE Method)

draft-ietf-geopriv-dhcp-lci-option

draft-ietf-geopriv-dhcp-civil

draft-ietf-sipping-location-requirements

draft-schulzrinne-sipping-emergency-arch

draft-ietf-sipping-sos

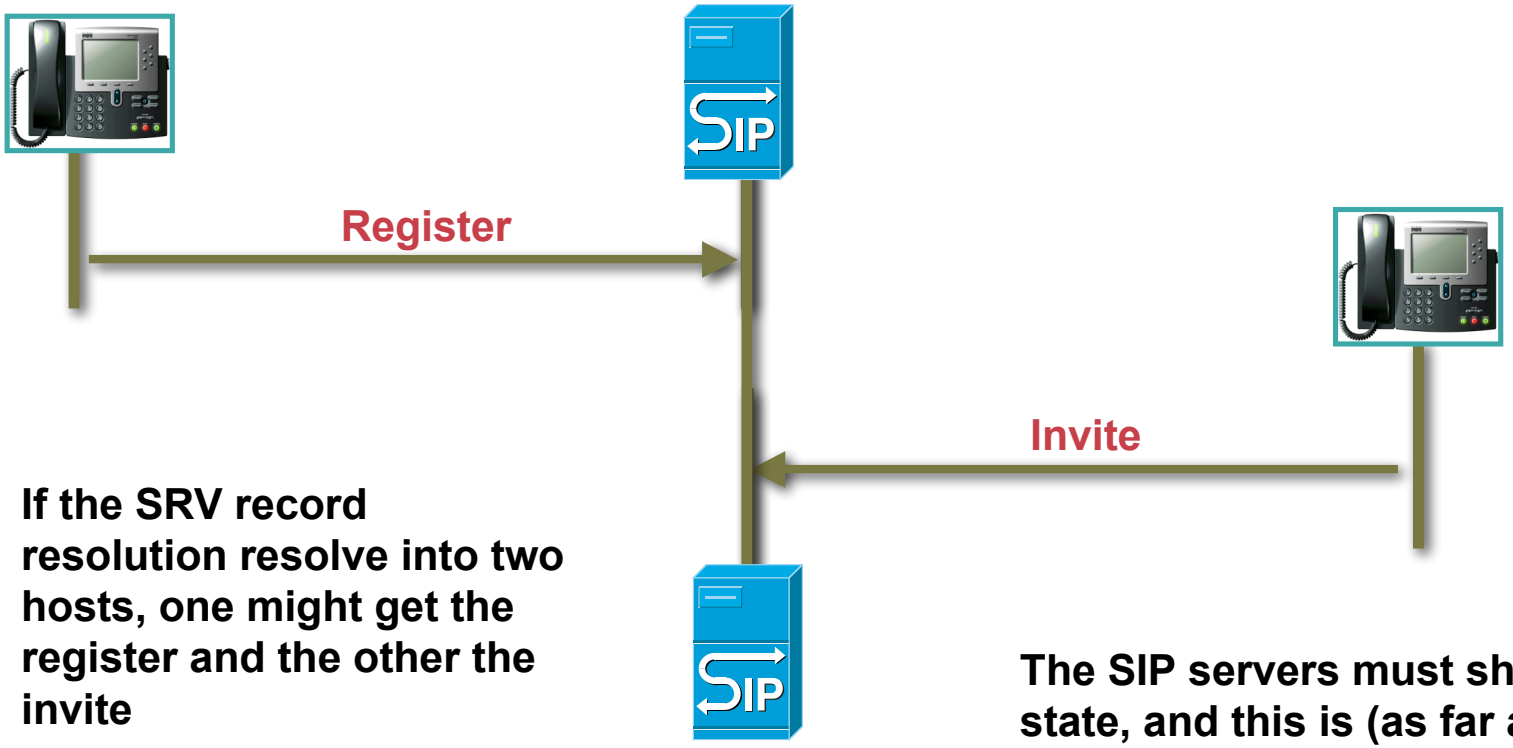
draft-rosen-dns-sos

VVT-4000 Session Agenda

- SIP Refresher
- SIP Standards Efforts
- SIP Working Efforts
- SIP Summary
- Reachability

Load balancing?

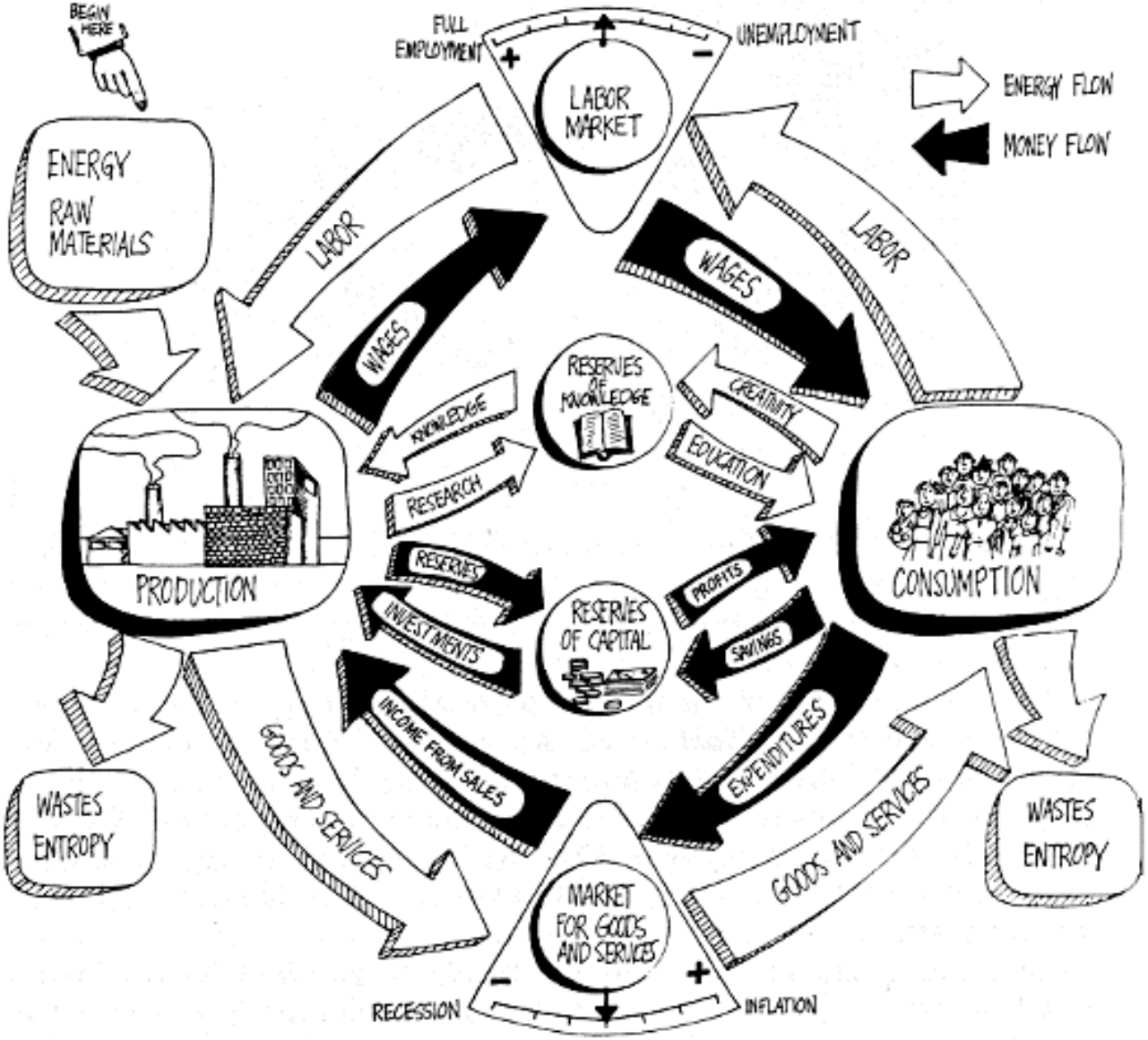
Load balancing?



If the SRV record resolution resolve into two hosts, one might get the register and the other the invite

The SIP servers must share state, and this is (as far as I know) only possible via proprietary solutions (vendor-specific) and a reliable network between them

Economical model

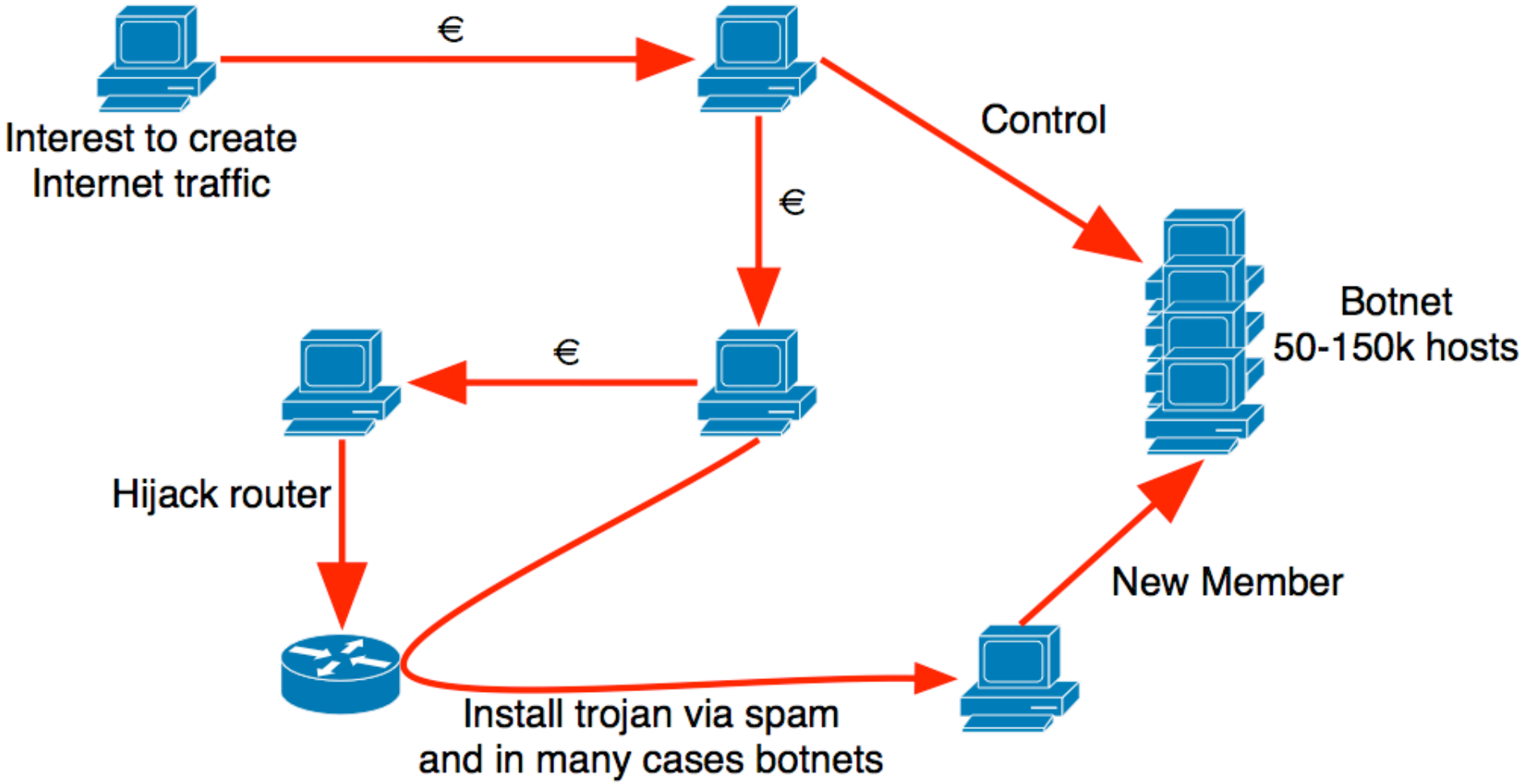


Indirect attacs are what dominate

So, what is the problem?

- SPAM is sent due to two reasons
  - Advertising
  - Install trojans (get control)
- Advertisment is part of todays life
- Trojans etc is due to bugs in software
  - I.e. generic problem we have to be better at. Higher quality software, better requirements when doing RFP's, and tools that are easier to manage.
  - Managed security is needed.

Economical model exists already!

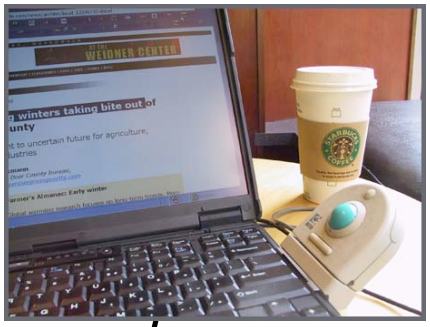


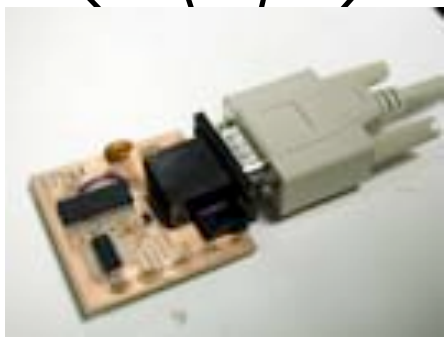
Mobility

- Mobility is a term used in too many ways
- Use of a cellphone, or radio technology
- When someone moves around (Mobile IP)

- Here, we talk about “moving around”
- What the transport is (or what kind of terminal is in use) doesn’t matter

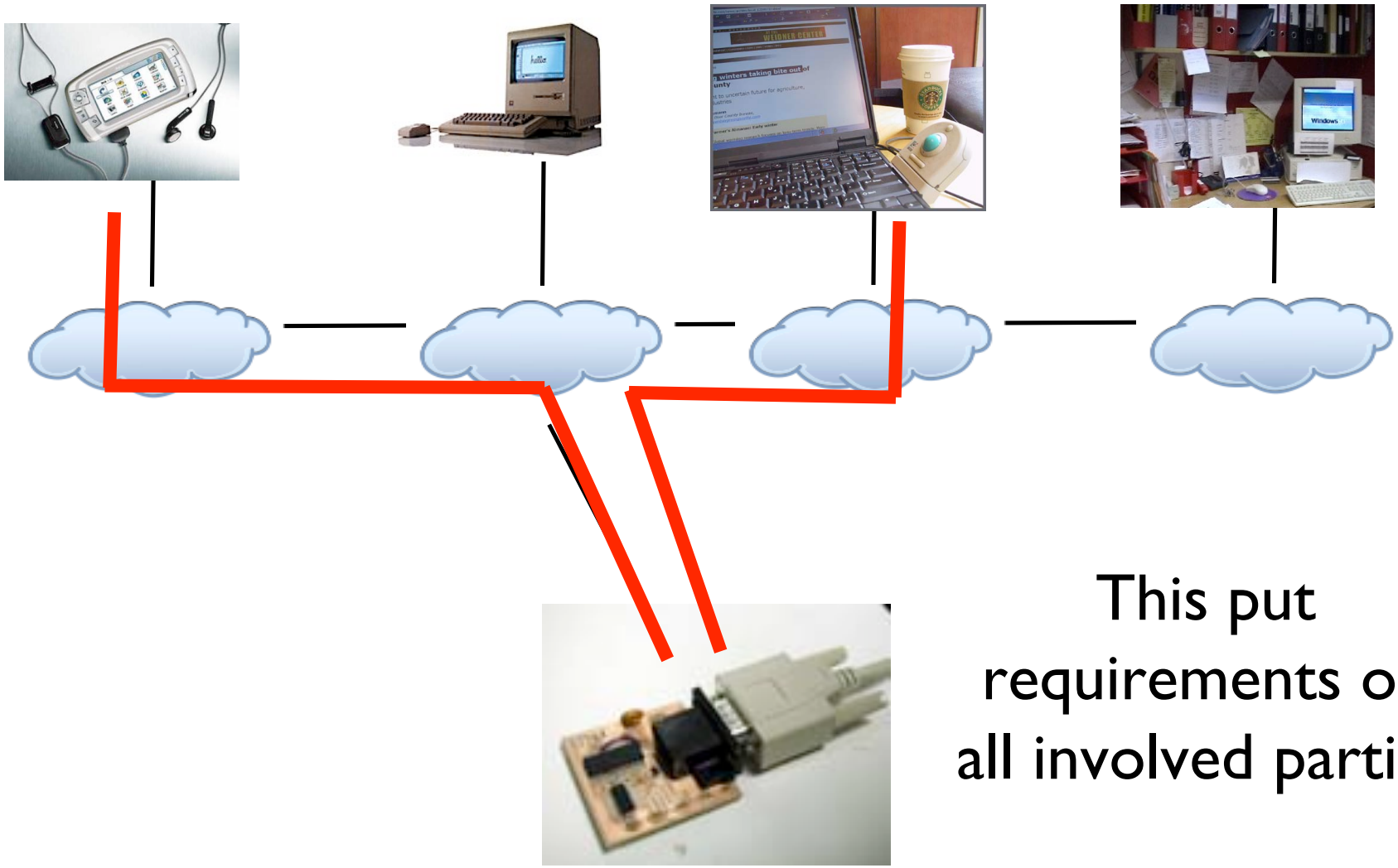
Reachability





The user want to be able to access a service from wherever he is

Reachability



This put requirements on all involved parties

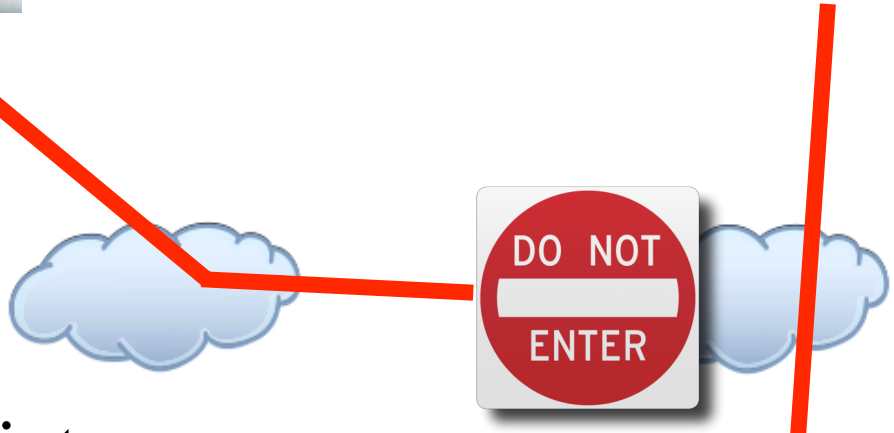
Reachability

If a service is not reachable, it can be due to many different problems

Reachability

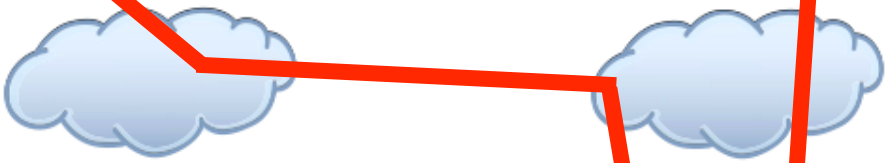
Maybe the ISP you use block outgoing traffic?

Reachability



Man kanske inte kan komma in till den operatör tjänsten använder

Reachability



The service might not accept connections

Summary

- Given access to the Internet, is it taken for granted one should be able to access all services?
- Doesn’t this imply a service that is to be reachange must have Internet access itself?
- *If a user buy a service he uses at home, doesn’t he also want to use when being on the road?*

Connection to VoIP?

- Many VoIP providers are ISP's as well
- Many VoIP services are bundled with IP
- Regulation (etc) must identify what rules apply to the VoIP service, and what applies to the IP service
- Consumer must be able to know what VoIP services are bundled and what are not (else she can not choose)

General SIP References

- http://www.cisco.com—Search for SIP, Cisco proxy server
- http://www.cs.columbia.edu/~hgs/sip/—SIP homepage
- http://www.ietf.org/html.charters/sip-charter.html/—IETF SIP WG
- http://www.ietf.org/html.charters/sipping-charter.html/—IETF SIPPING WG
- http://search.ietf.org/rfc.html—IETF RFC search page
- http://search.ietf.org/search/brokers/internet-drafts/query.html—Internet draft search page
- http://www.softarmor.com/sipwg/—SIP WG supplemental site
- http://www.softarmor.com/sipping/—SIPPING WG supplemental site
- http://www.sipcenter.com/—The SIP center