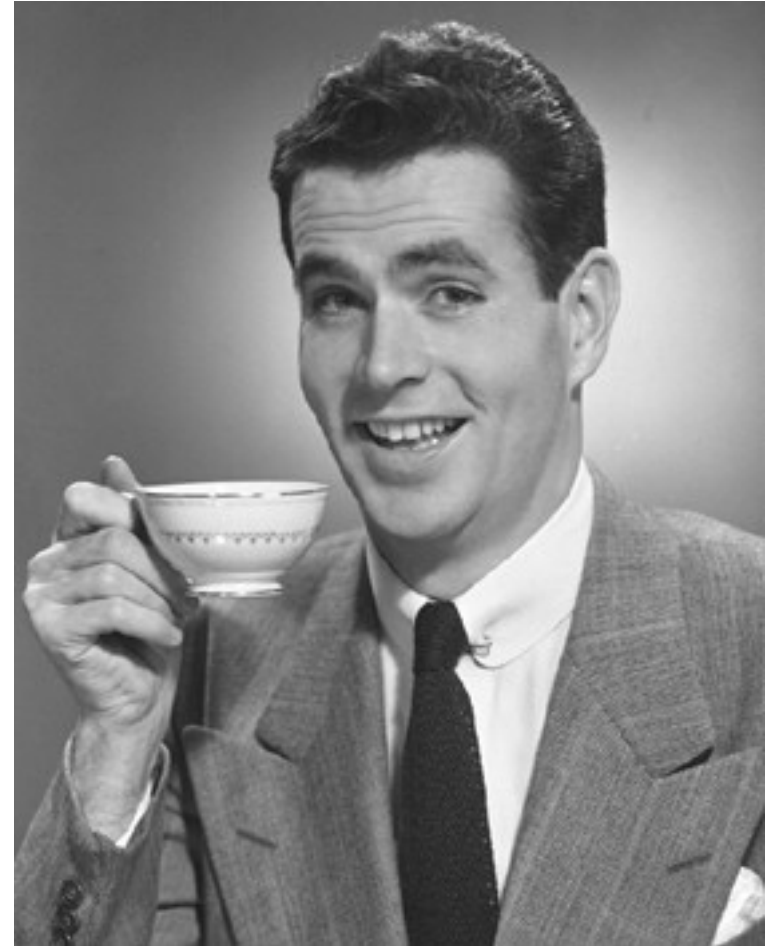


# SIP

RFC 3261



Simon P. Ditner / TAUG.CA  
simon@uc.org

# Today...

- Define SIP
- Structure of a call
- Sniffing Tools
- Common SIP dialogs

# Another Day...

- NAT/Firewall Problems
- Solutions to those problems

# SIP...

- Session Initiation Protocol
- RFC 3261

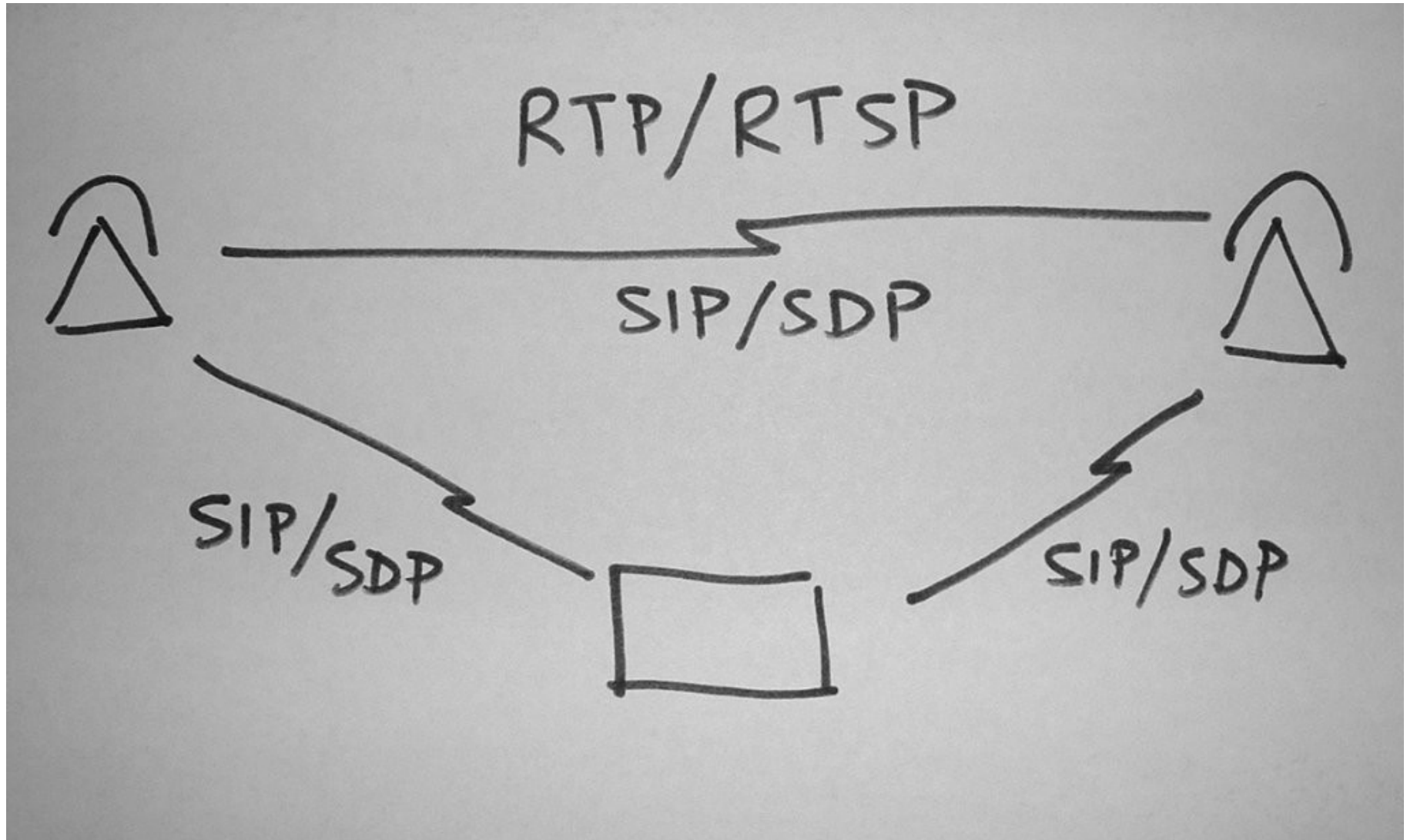
# SIP is flexible

- General-purpose tool
- Create / modify / destroy sessions
- Indep. of transport
- Indep. of type of session

# SIP has friends!

- Like Linux solutions build on Apache / MySQL / PHP
- SIP is one component in multimedia architecture

# SIP has friends!



# SIP has friends!

- Session Description Protocol
- Real-time Transport Protocol
- Real-Time Streaming Protocol

# SIP has friends!

- SDP, RFC 2327
- RTP, RFC 1889
- RTSP, RFC 2326

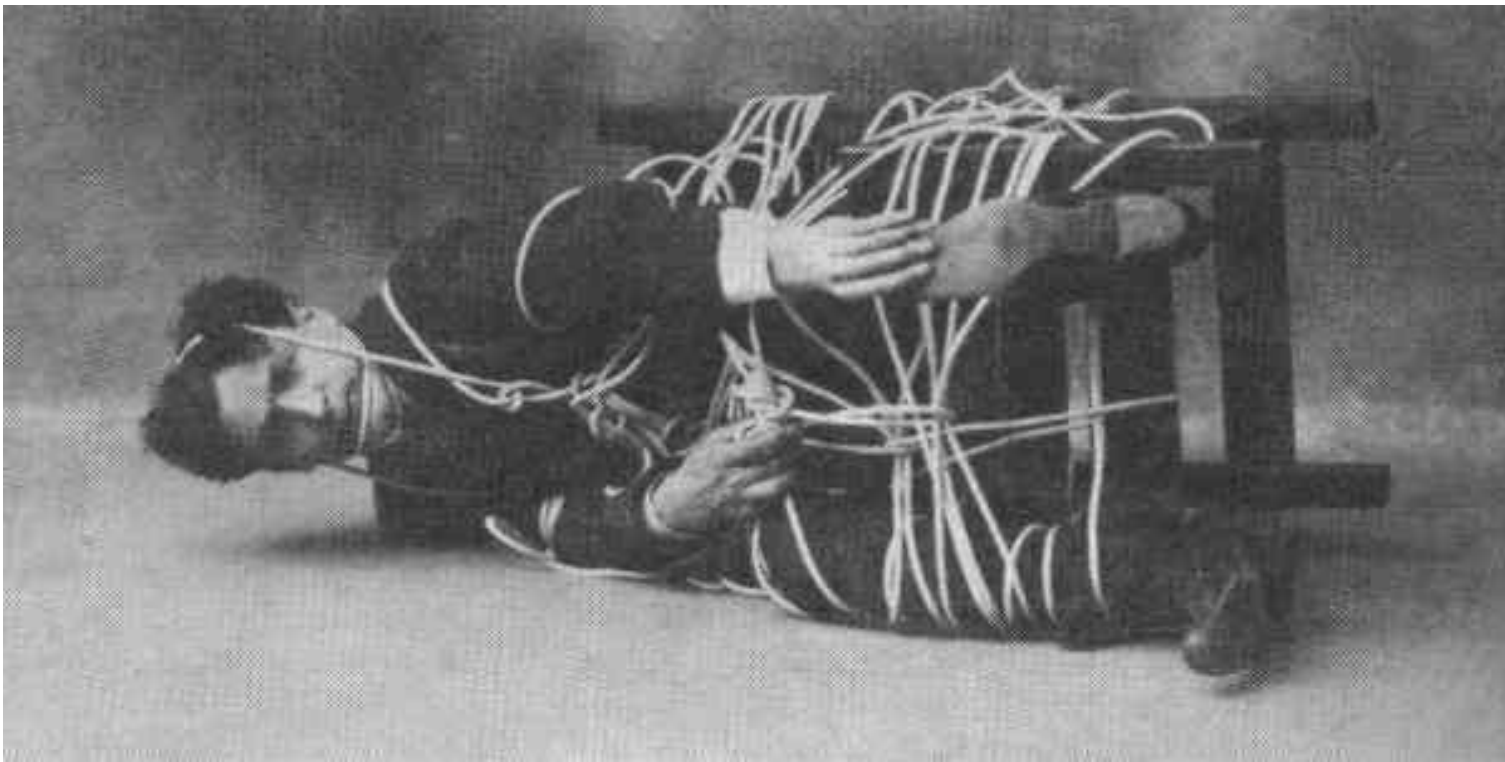
# SIP is NOT

Vertically  
Integrated  
Communications  
System



# SIP is NOT

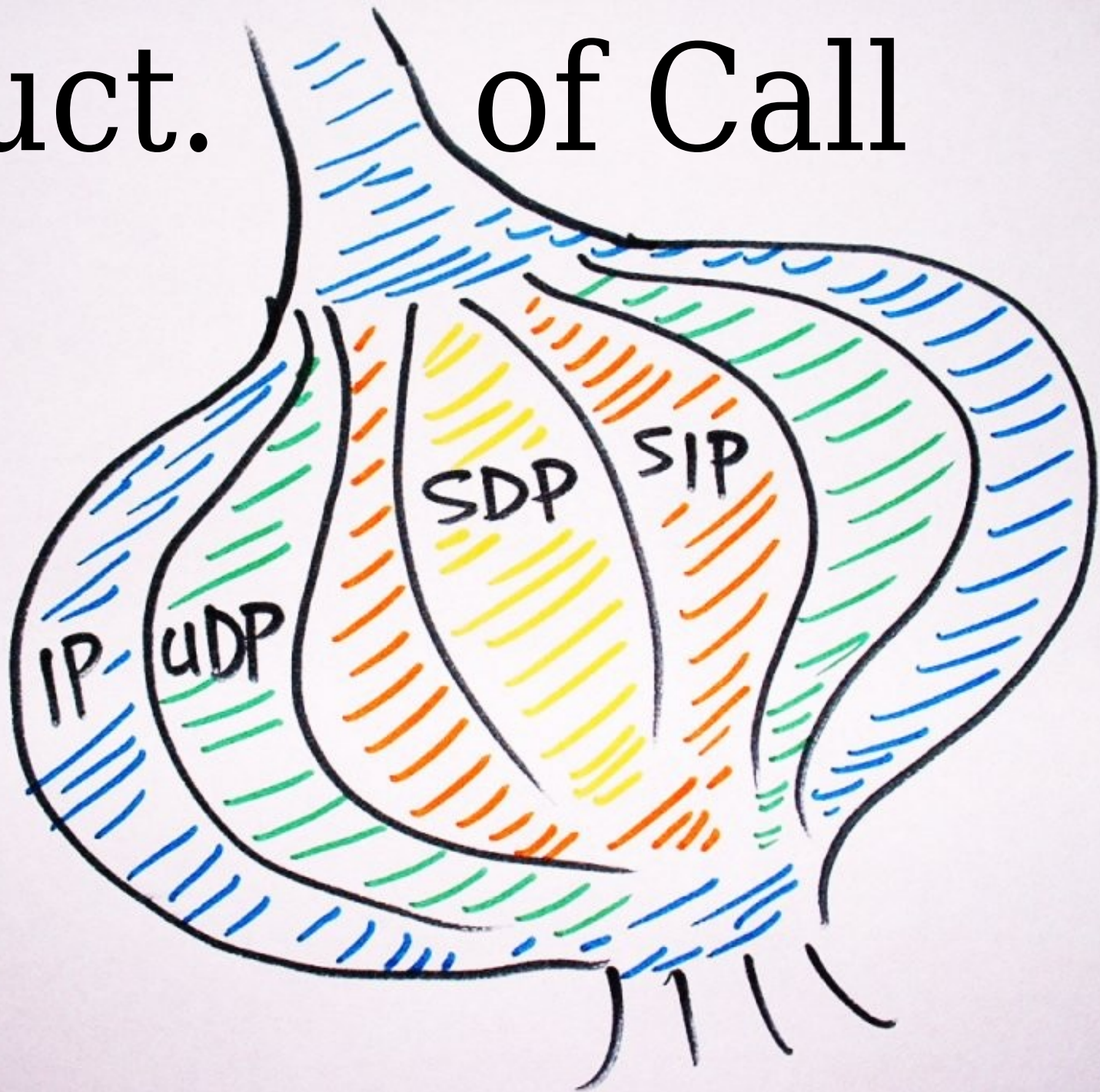
Tied to any other protocol



# SIP should be...

- Used in conjunction with appropriate protocols
- Create for specific application

# Struct. of Call



# SIP contains

- Command/Response
- ID for transaction
- Source
- Destination
- Route details
- Data (i.e. SDP packet)

# SDP contains

- Type of media (video, audio)
- Transport (RTP, H.320, ...)
- Format (H.261, MPEG, ...)
- Remote IP address
- Remote Port

# SIP Request

REGISTER

INVITE

ACK

CANCEL

BYE

OPTIONS

# SIP Request

**Alice sends Bob an invite...**

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP 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
<DATA BLOB>
```

# SIP Request

**Alice sends Bob an invite...**

```
INVITE sip:bob@biloxi.com SIP/2.0  
Via: SIP/2.0/UDP pc33.atlanta.com;  
    branch=z9hG4bK776asdhds  
Max-Forwards: 70  
To: Bob <sip:bob@biloxi.com>  
From: Alice <sip:alice@atlanta.com>:
```

```
Method Name:  
    INVITE  
SIP URI:  
    sip:bob@biloxi.com
```

```
Content-Length: 142  
<DATA BLOB>
```

# SIP Request

**Alice sends Bob an invite...**

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;
branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>:
```

Via:

Where Alice expects a response to this request

branch=

First hop's ID for this SIP transaction (not the entire call)

```
Content-Length: 142
```

```
<DATA BLOB>
```

# SIP Request

**Alice sends Bob an invite...**

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;
    branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>:
```

To:

A possible display name, and SIP URI that we were originally trying to reach

```
Content-Type: application/sdp
Content-Length: 142
<DATA BLOB>
```

# SIP Request

**Alice sends Bob an invite...**

From:

Also contains a display name, and the original SIP URI

tag=

Alice's tracking ID for this call

TO: BOB <SIP:BOB@DILLOXI.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

<DATA BLOB>

# SIP Request

**Alice sends Bob an invite...**

Call-ID:

Globally unique ID for this call

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

<DATA BLOB>

# SIP Request

**Alice sends Bob an invite...**

CSeq:

Contains an integer and the method name

Incremented for each request in this dialog

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

<DATA BLOB>

# SIP Request

**Alice sends Bob an invite...**

Contact:

SIP URI which is a direct route back to Alice  
(NAT / Firewall complications aside)

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

<DATA BLOB>

# SIP Request

**Alice sends Bob an invite...**

Content-Type:  
Format of the <DATA BLOB>  
Content-Length:  
Length of the <DATA BLOB>

```
TO: BOB <SIP:BOB@DILLOXI.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  
<DATA BLOB>
```

# SIP Request

**Alice sends Bob an invite...**

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP 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
<DATA BLOB>
```

# SIP Response

100 Trying

180 Ringing

200 OK

401 Unauthorized

404 Not Found

500 Server Internal Error

600 Busy Everywhere

603 Decline

...

# SIP Response

**Bob accepts an invitation..**

SIP/2.0 200 OK

Via: SIP/2.0/UDP server10.biloxi.com

;branch=z9hG4bKnashds8;received=192.0.2.3

Via: SIP/2.0/UDP bigbox3.site3.atlanta.com

;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2

Via: SIP/2.0/UDP pc33.atlanta.com

;branch=z9hG4bK776asdhs ;received=192.0.2.1

To: Bob <sip:bob@biloxi.com>;tag=a6c85cf

From: Alice <sip:alice@atlanta.com>;tag=1928301774

Call-ID: a84b4c76e66710@pc33.atlanta.com

CSeq: 314159 INVITE

Contact: <sip:bob@192.0.2.4>

Content-Type: application/sdp

Content-Length: 131

<DATA BLOB>

# SIP Response

**Bob accepts an invitation..**

**SIP/2.0 200 OK**

Via: SIP/2.0/UDP server10.biloxi.com

;branch=z9hG4bKnashds8;received=192.0.2.3

Via: SIP/2.0/UDP bigbox3.site3.atlanta.com

;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2

Via: SIP/2.0/UDP pc33.atlanta.com

;branch=z9hG4bK776aedhds;received=192.0.2.1

To: Response Code:

From: 200 OK

Call

CSeq

Contact: <sip:bob@192.0.2.4>

Content-Type: application/sdp

Content-Length: 131

<DATA BLOB>

4

# SIP Response

Bob accepts an invitation..

SIP/2.0 200 OK

Via: SIP/2.0/UDP server10.biloxi.com

;branch=z9hG4bKnashds8;received=192.0.2.3

Via: SIP/2.0/UDP bigbox3.site3.atlanta.com

;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2

Via: SIP/2.0/UDP pc33.atlanta.com

;branch=z9hG4bK776asdhs ;received=192.0.2.1

To: Bob <sip:bob@biloxi.com>;tag=a6c85cf

From: Alice <sip:alice@atlanta.com>;tag=1928301774

Call-ID

CSeq:

Via:

Contact

All the proxies that this SIP request passed through

Content

Content-Length: 151

<DATA BLOB>

# SIP Response

**Bob accepts an invitation..**

SIP/2.0 200 OK

Via: SIP/2.0/UDP server10.biloxi.com

;branch=z9hG4bKnashds8;received=192.0.2.3

Via: SIP/2.0/UDP bigbox3.site3.atlanta.com

;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2

Via: SIP/2.0/UDP pc33.atlanta.com

;branch=z9hG4bK776asdhs ;received=192.0.2.1

To: Bob <sip:bob@biloxi.com>;tag=a6c85cf

From: Alice <sip:alice@atlanta.com>;tag=1928301774

Call-ID: a84b4c76e66710@pc33.atlanta.com

CSeq: 314159 INVITE

Contact: <sip:bob@192.0.2.4>

Content-Type: application/sdp

Content-Length: 131

<DATA BLOB>

# SDP, inside SIP

```
0: v=0
1: o=VOIPSIL_SIP 61641499 61641499 IN IP4 64.26.157.252
2: s=Sip Call
3: c=IN IP4 64.26.157.226
4: t=0 0
5: m=audio 6084 RTP/AVP 18 0 101
6: a=rtpmap:18 G729/8000
7: a=rtpmap:0 PCMU/8000
8: a=rtpmap:101 telephone-event/8000
```

# SDP, inside SIP

```
0: v=0
1: o=VOIPSIL_SIP 61641499 61641499 IN IP4 64.26.157.252
2: s=Sip Call
3: c=IN IP4 64.26.157.226
4: t=0 0
5: m=audio 6084 RTP/AVP 18 0 101
6: a=rtpmap:18 G729/8000
7: a=rtpmap:0 PCMU/8000
8: a=r
```

v=  
version

# SDP, inside SIP

```
0: v=0
1: o=VOIPSIL_SIP 61641499 61641499 IN IP4 64.26.157.252
2: s=Sip Call
3: c=IN IP4 64.26.157.226
4: t=0 0
5: m=audio 6084 RTP/AVP 18 0 101
6: a=rtpmap:18 G729/8000
7: a=rtpmap:0 PCMU/8000
8: a=r
```

o=

Owner of this call

# SDP, inside SIP

```
0: v=0
1: o=VOIPSIL_SIP 61641499 61641499 IN IP4 64.26.157.252
2: s=Sip Call
3: c=IN IP4 64.26.157.226
4: t=0 0
5: m=audio 6084 RTP/AVP 18 0 101
6: a=rtpmap:18 G729/8000
7: a=rtpmap:0 PCMU/8000
8: a=r
```

s=

Session Name

# SDP, inside SIP

```
0: v=0
1: o=VOIPSIL_SIP 61641499 61641499 IN IP4 64.26.157.252
2: s=Sip Call
3: c=IN IP4 64.26.157.226
4: t=0 0
5: m=audio 6084 RTP/AVP 18 0 101
6: a=rtpmap:18 G729/8000
7: a=rtpmap:0 PCMU/8000
8: a=r
```

c=

connection information: Internet, IPv4, IP Address

# SDP, inside SIP

```
0: v=0
1: o=VOIPSIL_SIP 61641499 61641499 IN IP4 64.26.157.252
2: s=Sip Call
3: c=IN IP4 64.26.157.226
4: t=0 0
5: m=audio 6084 RTP/AVP 18 0 101
6: a=rtpmap:18 G729/8000
7: a=rtpmap:0 PCMU/8000
8: a=r
```

t=  
time description(?)

# SDP, inside SIP

```
0: v=0
1: o=VOIPS
2: s=Sip C
3: c=IN IP
4: t=0 0
5: m=audio 6084 RTP/AVP 18 0 101
6: a=rtpmap:18 G729/8000
7: a=rtpmap:0 PCMU/8000
8: a=rtpmap:101 telephone-event/8000
```

```
m=
  media description:
    type = audio
    port = 6084
    protocol = RTP/AVP
    18 = G.729 (default)
    0 = G.711
    101 = telephony signals
```

# SDP, inside SIP

a=

attributes for supported media types

<media ID> <name>/<sample rate>[/<optional args>]

0: v=0

1: o=VOIPSIL\_SIP 61641499 61641499 IN IP4 64.26.157.252

2: s=Sip Call

3: c=IN IP4 64.26.157.226

4: t=0 0

5: m=audio 6084 RTP/AVP 18 0 101

6: **a=rtpmap:18 G729/8000**

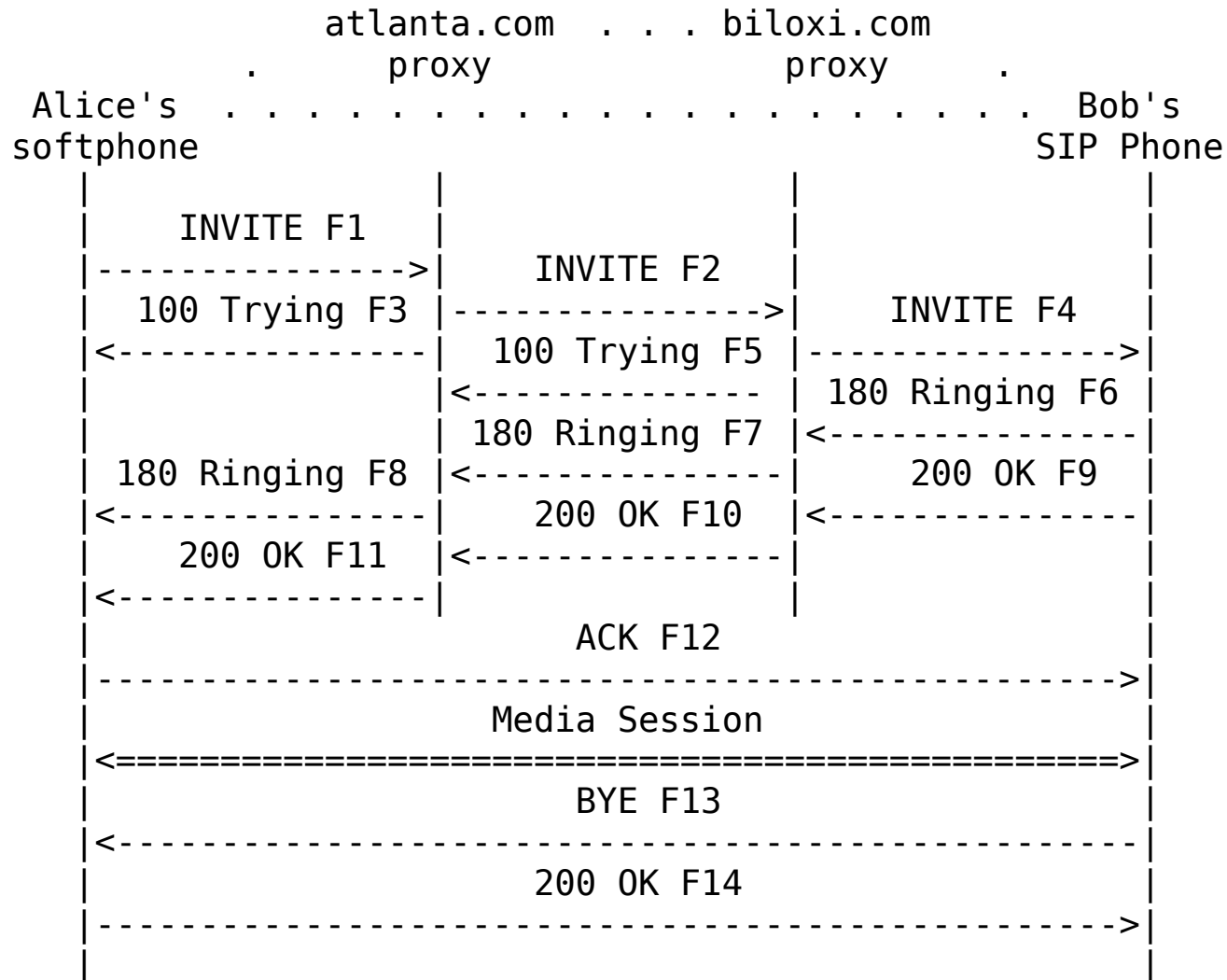
7: **a=rtpmap:0 PCMU/8000**

8: **a=rtpmap:101 telephone-event/8000**

# SDP, inside SIP

```
0: v=0
1: o=VOIPSIL_SIP 61641499 61641499 IN IP4 64.26.157.252
2: s=Sip Call
3: c=IN IP4 64.26.157.226
4: t=0 0
5: m=audio 6084 RTP/AVP 18 0 101
6: a=rtpmap:18 G729/8000
7: a=rtpmap:0 PCMU/8000
8: a=rtpmap:101 telephone-event/8000
```

# SIP can be proxied



# SIP Response

Bob accepts an invitation..

SIP/2.0 200 OK

**Via: SIP/2.0/UDP server10.biloxi.com**

**;branch=z9hG4bKnashds8;received=192.0.2.3**

**Via: SIP/2.0/UDP bigbox3.site3.atlanta.com**

**;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2**

**Via: SIP/2.0/UDP pc33.atlanta.com**

**;branch=z9hG4bK776asdhs ;received=192.0.2.1**

To: Bob <sip:bob@biloxi.com>;tag=a6c85cf

From: Alice <sip:alice@atlanta.com>;tag=1928301774

Call-ID

CSeq:

Via:

Contact

All the proxies that this SIP request passed through

Content

Content-Length: 151

<DATA BLOB>

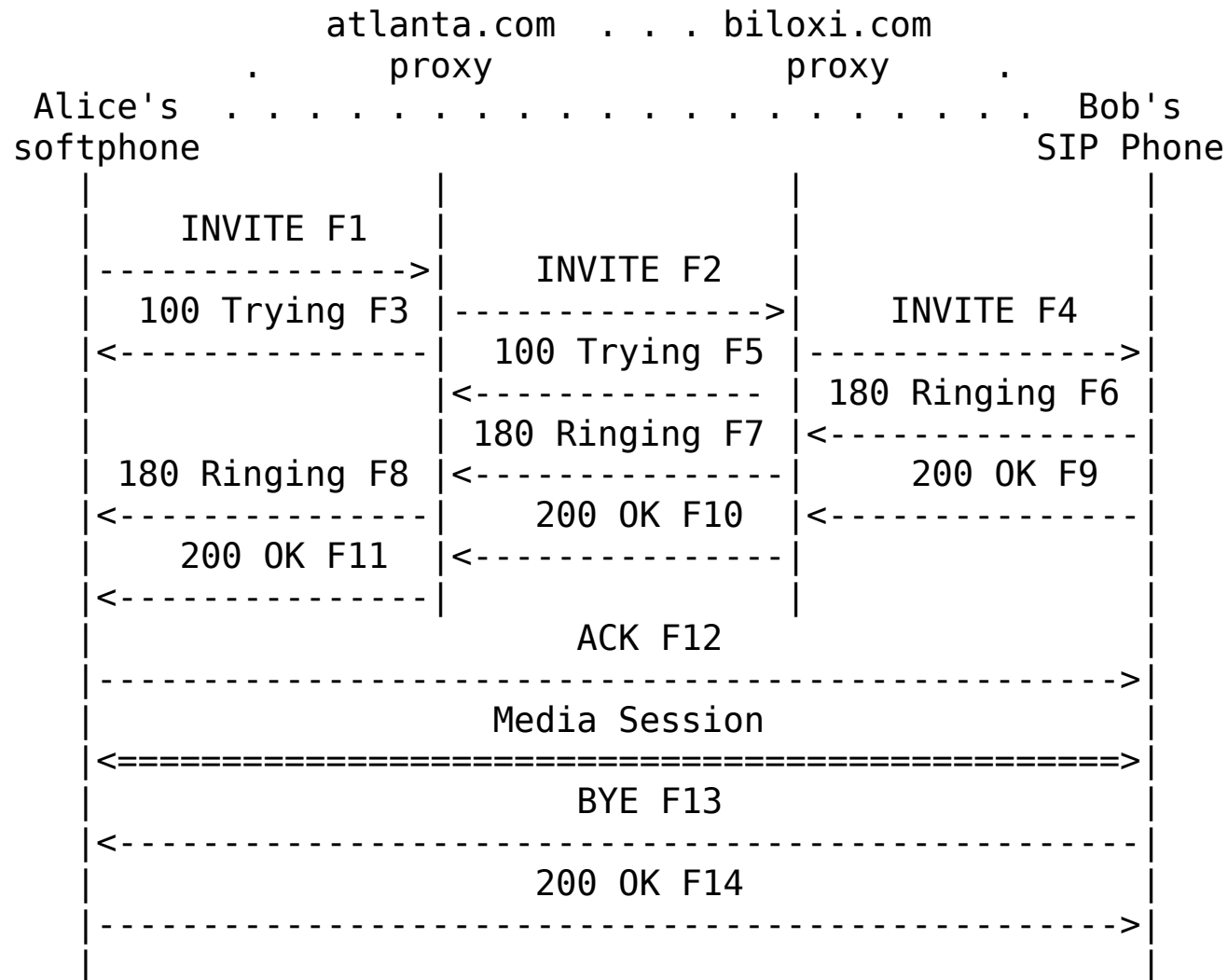
# Asterisk != SIP Proxy

- Can't proxy SIP pkts. like SER
- Different type of Proxy
- Acts as a Back-to-back User Agent (B2B-UA)

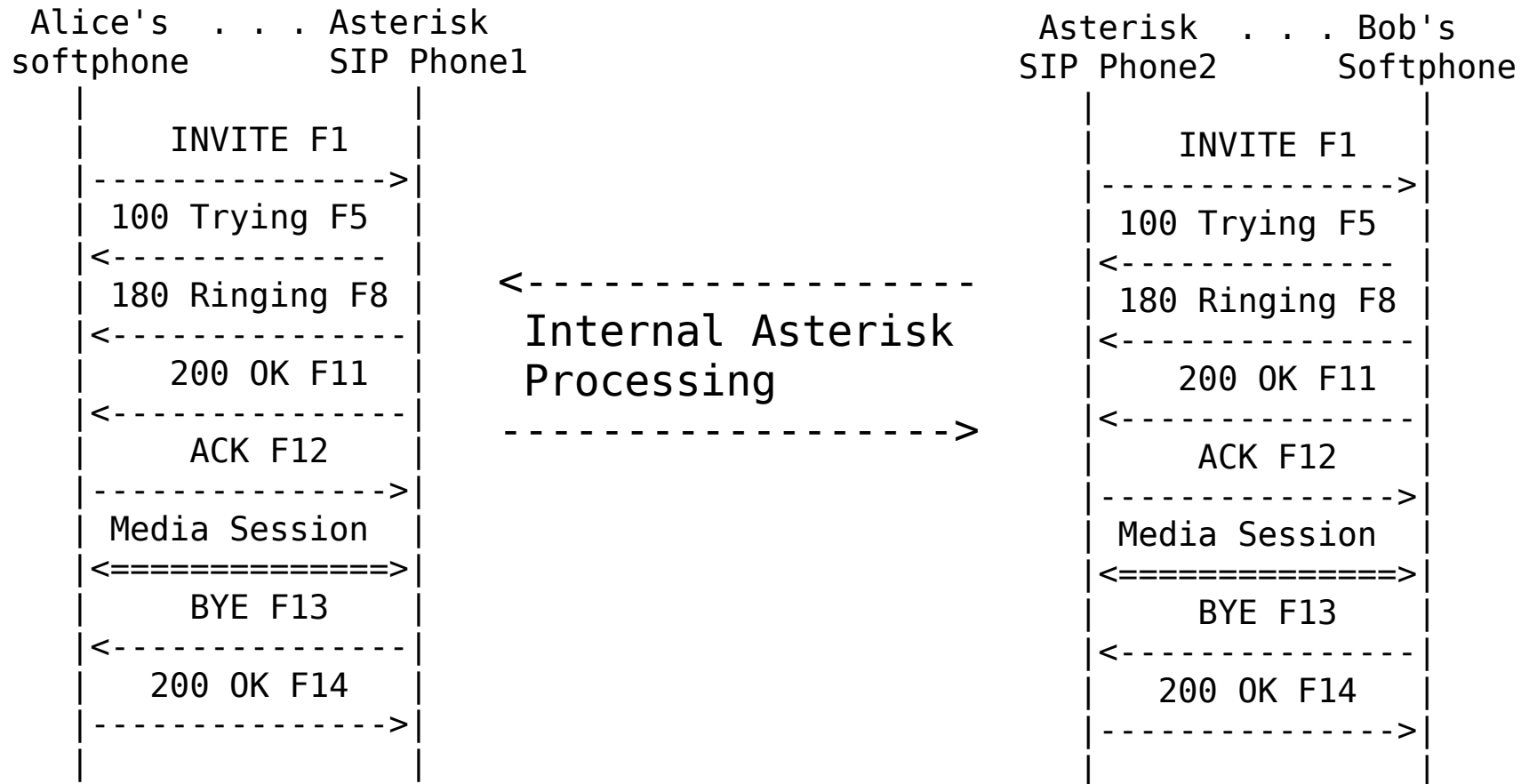
# Asterisk != SIP Proxy

- B2B-UA
- Acts as set of softphones
- Needed for PBX
- Media Gateway to IAX, MGCP, ZAP, etc.

# With SIP Proxies



# With B2B-UA



# Flip to vim...

`sip_dialog.txt`

# Sniffing tools

## SIP / RTP Specific

- `console> sip debug`
- `console> sip debug ip <address>`
- `pcapsipdump` – capture and separate
- `pjsip` – suite of SIP User Agent tools
- `rtptools` – play/send/dump RTP streams

# Sniffing tools

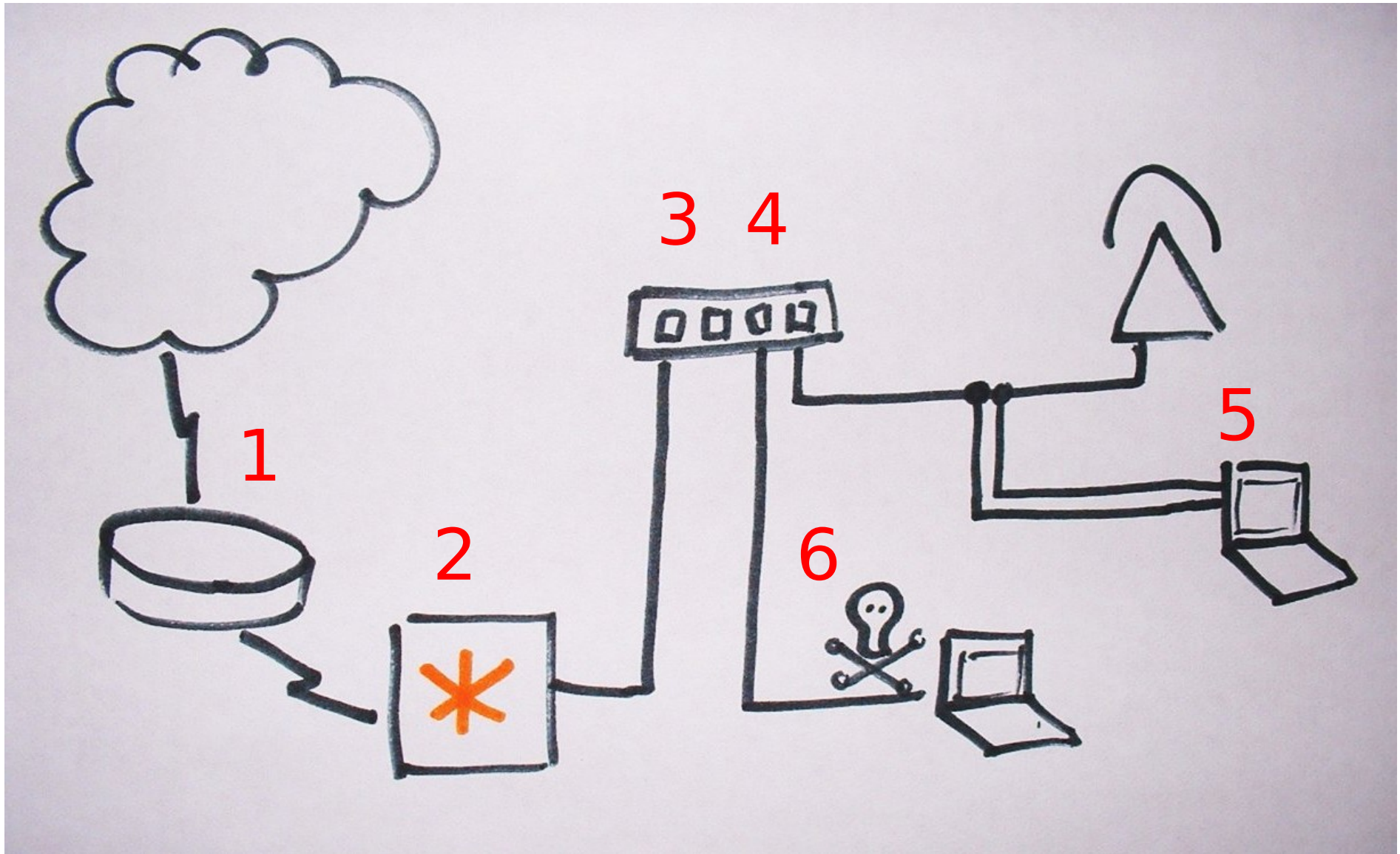
## General collection

- tcpdump – capture
- wireshark – capture + analyser
- tcpreplay – replay TCP/UDP

# Where to Acquire

1. Asterisk system
2. Routers / firewalls
3. Hubs
4. Switches w/ port mirroring
5. Passive taps
6. ARP poisoning

# Where to Acquire



# Acquiring

```
console> sip debug
```

```
console> sip debug ip <address>
```

# Acquiring

As root...

```
# tcpdump -i eth0 not port 22
```

```
# tcpdump -i eth0 -s 0 \  
-w file.pcap not port 22
```

```
# tcpdump -i eth0 -s 0 \  
-w file.pcap \  
host 192.168.0.101
```

# Acquiring

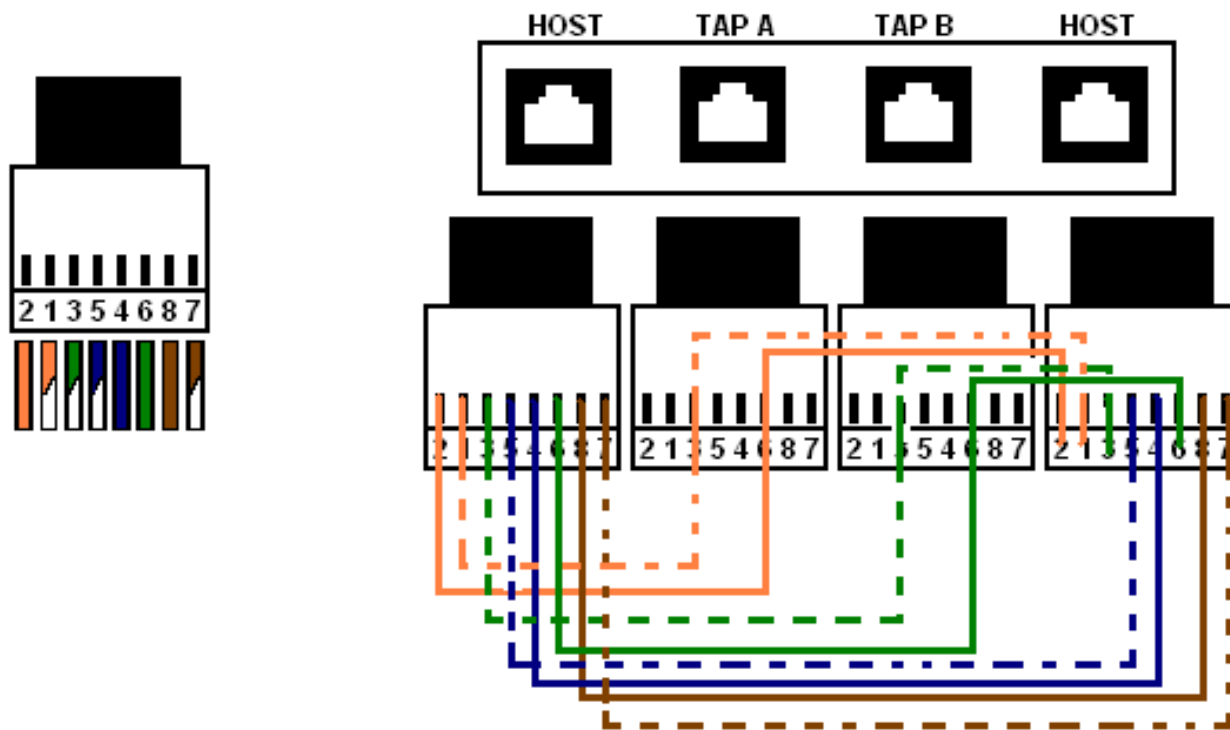
As root...

```
# tshark -i eth0 -s 0 \  
-w file.pcap \  
host 192.168.0.101
```

```
# pcapshard -f -i eth0 \  
-d ./dump
```

```
# find ./dump -type f  
./dump/20000126/10/20000126-...@192.168.2.1.pcap  
./dump/20000126/10/20000126-...@192.168.5.101.pcap
```

# Passive Taps



<http://www.snort.org/docs/tap/>

# ARP Poisoning

**Don't use on your production network  
unless you like downtime!**

```
# fragrouter -B1  
# arpspoof -i eth0 192.168.2.1
```

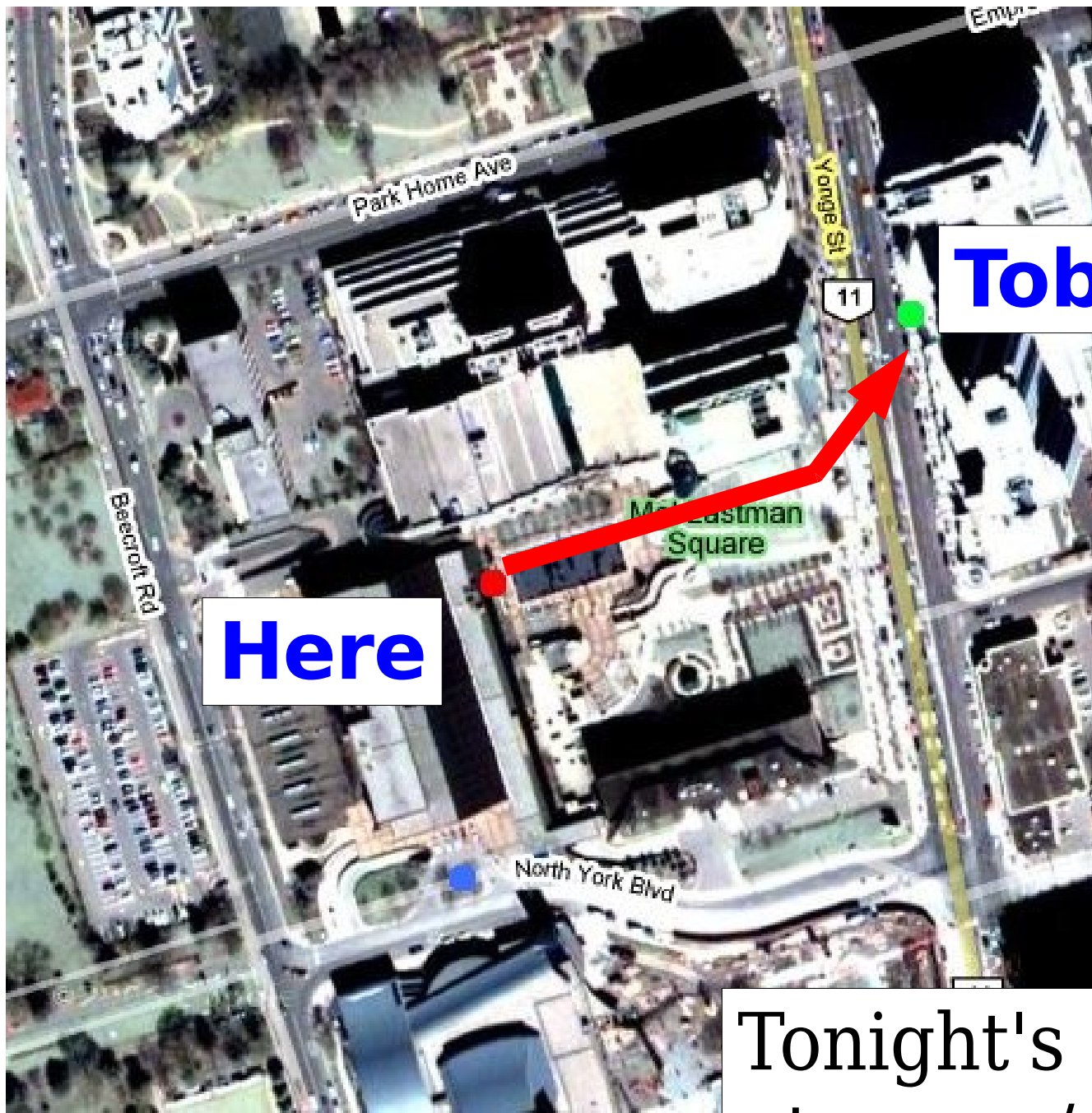
# More to come soon...

## Thanks!

Simon P. Ditner / TAUG.CA

Slides available at:

[taug.ca/node/16](http://taug.ca/node/16)



**Toby's**

**Here**

Tonight's slides at:  
[taug.ca/node/16](http://taug.ca/node/16)