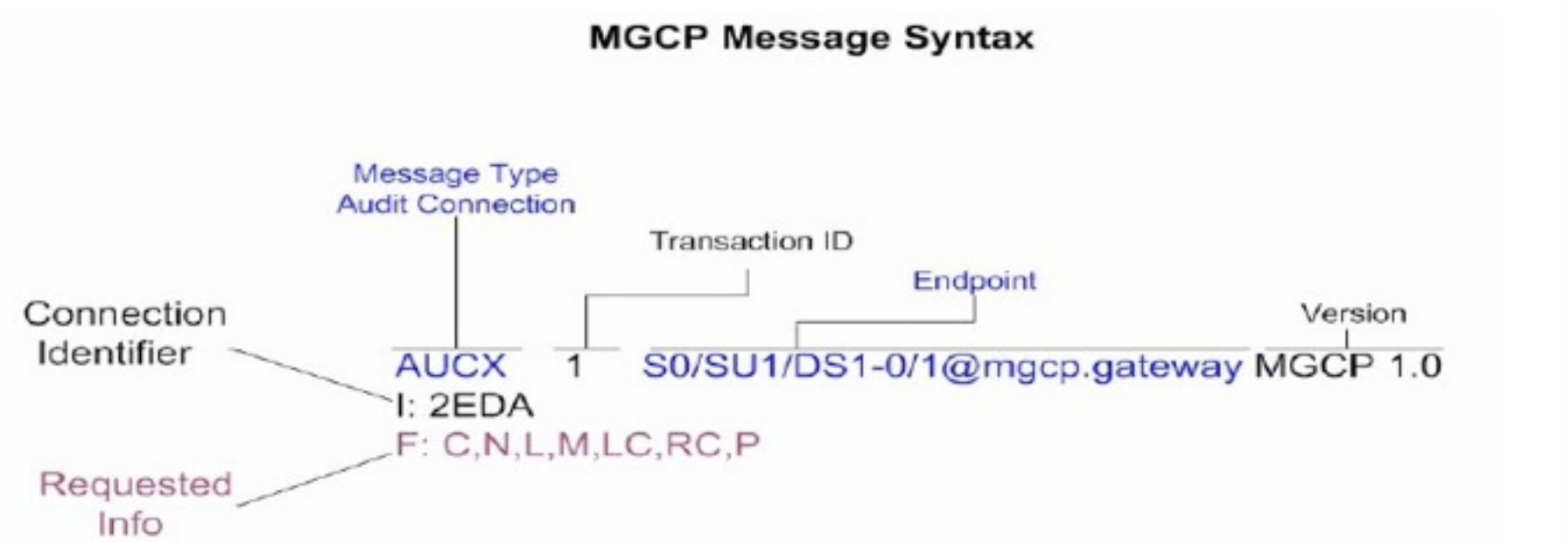
MGCP: un protocole VoIP oublié

Joffrey CZARNY

Greetings: Sandro GAUCI

MGCP

- MGCP (Media Gateway Control Protocol)
  - IETF, Softswitch (CallAgent)<->MGW
  - CallAgents->MGW (2427/UDP)
  - MGW->CallAgents (2727/UDP)
  - Used to control MGWs
  - AoC (Advise Of Charge) towards CPE



MGCP

- Quelques requêtes pouvant être utilisées :
  - AUCX-> AuditConnection.
  - AUEP-> AuditEndpoint.
  - CRCX-> CreateConnection.
  - DLCX-> DeleteConnection.
  - EPCF-> EndpointConfiguration.
  - MDCX-> ModifyConnection.
  - RQNT-> NotificationRequest.
  - NTFY-> Notify.
  - RSIP-> RestartInProgress.

http://www.networksorcery.com/enp/protocol/mgcp.htm

MGCP: Audit Endpoint

- Indentification via AUEP "AUdit End Point":
  - AUEP 1500 *@mgcp.gateway MGCP 0.1

    Response:
    - 200 1500
    - Z: So/SUo/DS1-o/1
    - Z: So/SUo/DS1-o/2
    - Z: So/SUo/DS1-o/3
    - Z: So/SUo/DS1-o/4
    - ...

MGCP: Audit Endpoint

- Interrogation d'un «end point»: Capabilities request
  - AUEP 1500 S0/SU1/DS1-0/1@mgcp.gateway MGCP 0.1

    F: A
    - 200 1500
    - L: p:10-20, a:PCMU;PCMA;G.nX64, b:64, e:on, gc:1, s:on, t:10, r:g, nt:IN;ATM;LOCAL, v:T;G;D;L;H;R;ATM;SST;PRE
    - L: p:10-220, a:G.729;G.729a;G.729b, b:8, e:on, gc:1, s:on, t:10, r:g, nt:IN;ATM;LOCAL, v:T;G;D;L;H;R;ATM;SST;PRE
    - L: p:10-110, a:G.726-16;G.728, b:16, e:on, gc:1, s:on, t:10, r:g, nt:IN;ATM;LOCAL, v:T;G;D;L;H;R;ATM;SST;PRE
    - L: p:10-70, a:G.726-24, b:24, e:on, gc:1, s:on, t:10, r:g, nt:IN;ATM;LOCAL, v:T;G;D;L;H;R;ATM;SST;PRE
    - L: p:10-50, a:G.726-32, b:32, e:on, gc:1, s:on, t:10, r:g, nt:IN;ATM;LOCAL, v:T;G;D;L;H;R;ATM;SST;PRE
    - L: p:30-270, a:G.723.1-H;G.723;G.723.1a-H, b:6, e:on, gc:1, s:on, t:10, r:g, nt:IN;ATM;LOCAL, v:T;G;D;L;H;R;ATM;SST;PRE
    - L: p:30-330, a:G.723.1-L;G.723.1a-L, b:5, e:on, gc:1, s:on, t:10, r:g, nt:IN;ATM;LOCAL, v:T;G;D;L;H;R;ATM;SST;PRE
    - M: sendonly, recvonly, sendrecv, inactive, loopback, conttest, data, netwloop, netwtest

MGCP: Audit Endpoint

- Interrogation d'un «end point»:
  - AUEP 1000 S0/SU1/DS1-0/1@mgcp.gateway MGCP 0.1

    F: R,D,S,X,N,I,T,ES
    - 200 1500
    - **I: 2BD85**
    - N: ca@mgcp.gateway:2427
    - X: 1
    - R: D/[0-9ABCD*#](N)
    - S:
    - T:
    - ES:

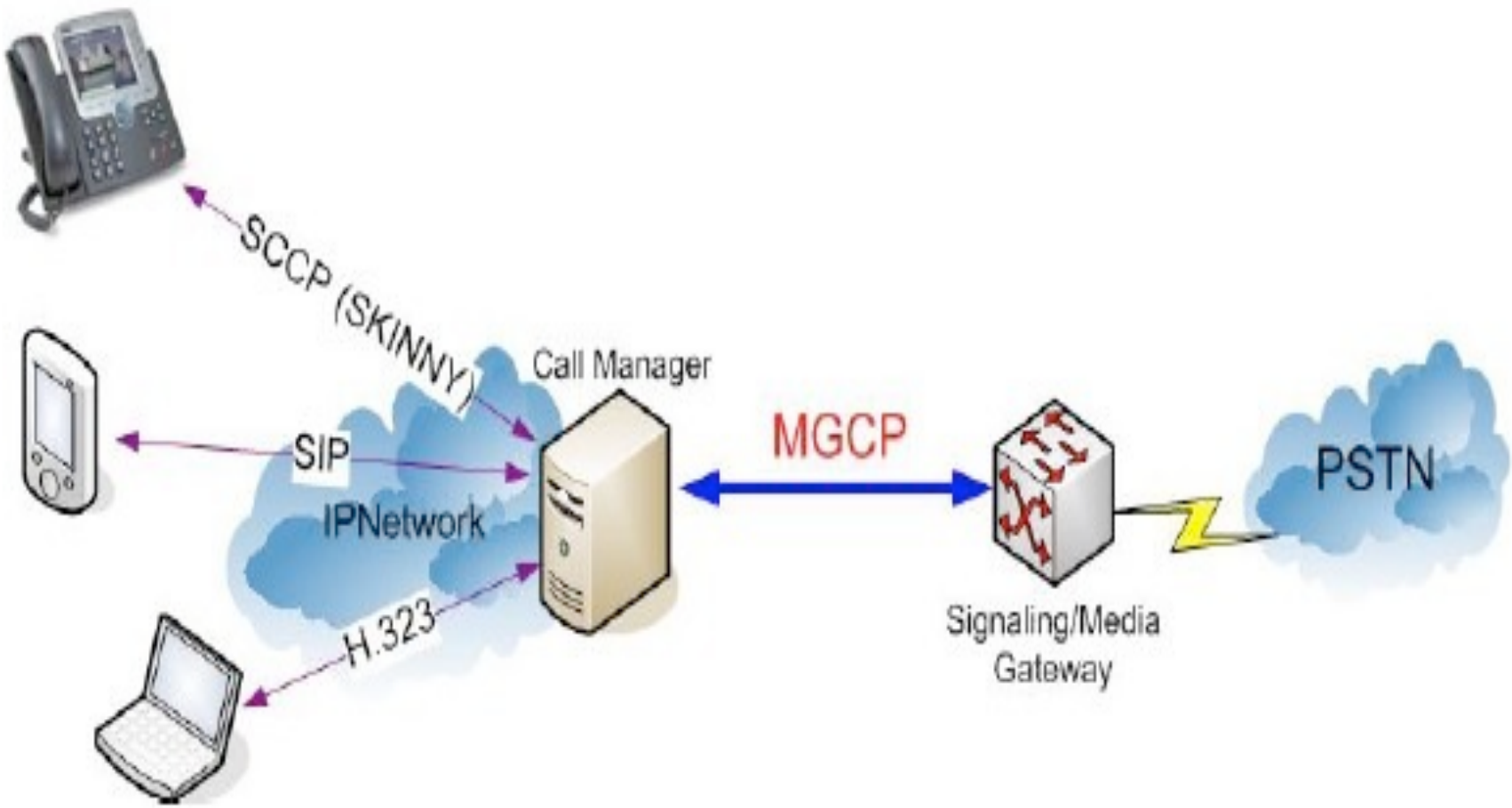
MGCP: Audit Connection

- Interrogation d'un «end point»:
  - AUCX 1500 S0/SU1/DS1-0/1@mgcp.gateway MGCP 0.1
    I: 2BD85
    F: C,N,L,M,LC,RC,P
    - 200 1500
    - C: D000000000206e6dd000000F580000aac
    - N: ca@mgcp.gateway:2427
    - L: p:20, a:PCMU, s:off, t:b8
    - M: sendrecv
    - P: PS=4148, OS=663680, PR=770, OR=122723, PL=0, JI=0, LA=0
    - v=0
    - **c=IN IP4 10.76.233.33**
    - **m=audio 18936 RTP/AVP 0 100**
    - a=rtpmap:100 X-NSE/8000
    - a=fmtp:100 192-194

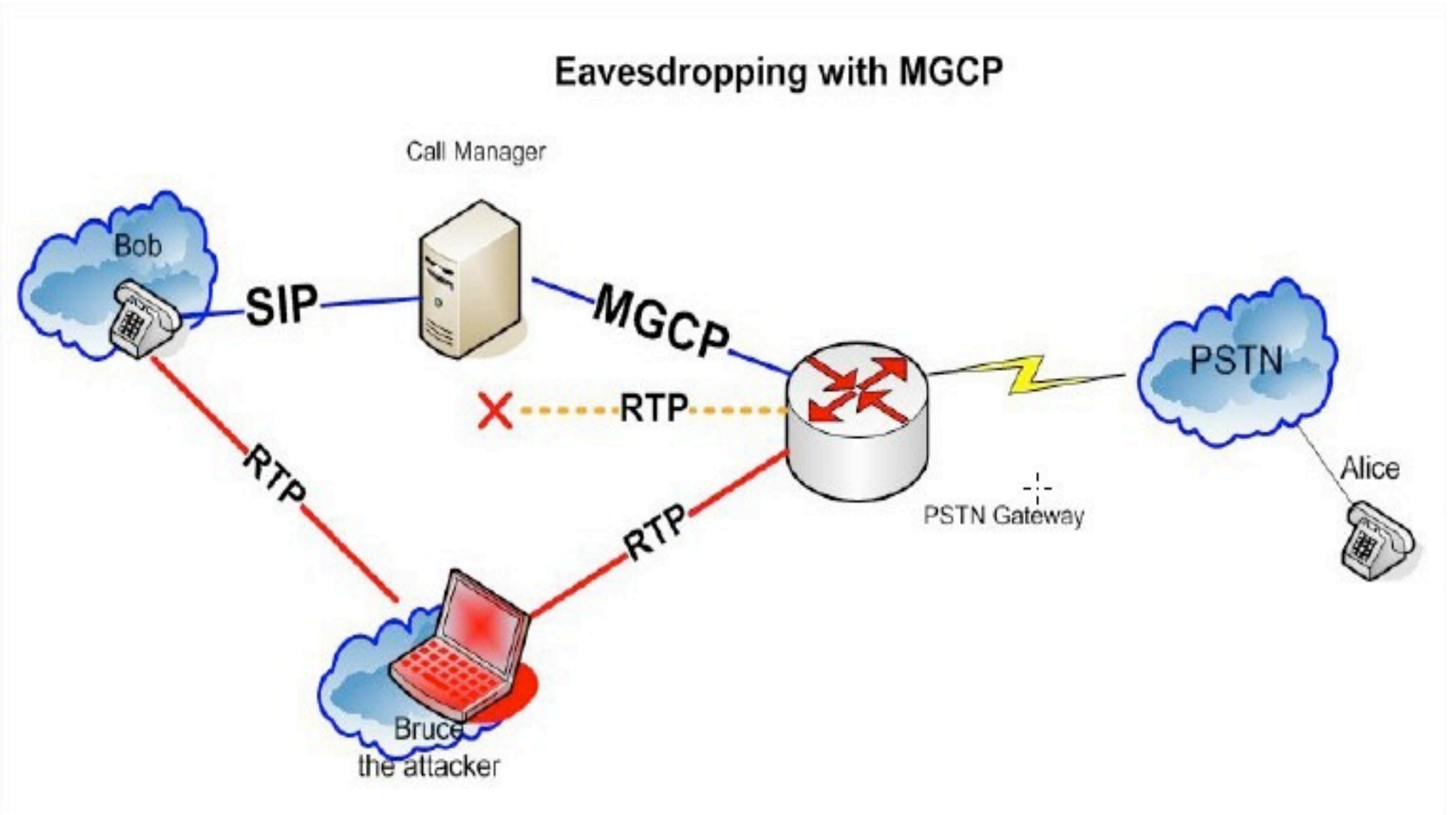
MGCP

- Modification d'un «end point»:
  - MDCX 1000 S0/SU1/DS1-0/1@mgcp.gateway MGCP 0.1
    M=audio 17994 RTP/AVP
    C=IN IP4 10.100.100.1

MGCP
redirection RTP



MGCP
redirection RTP



MGCP video demo

```
nop:mgcpscan obscure$ python mgcptest.py 10.100.100.252
```

Santé Bonheur :)

- MGCPscan & MGCPforge
- https://bitbucket.org/SnorkY
- snorky[a]insomnihack.net