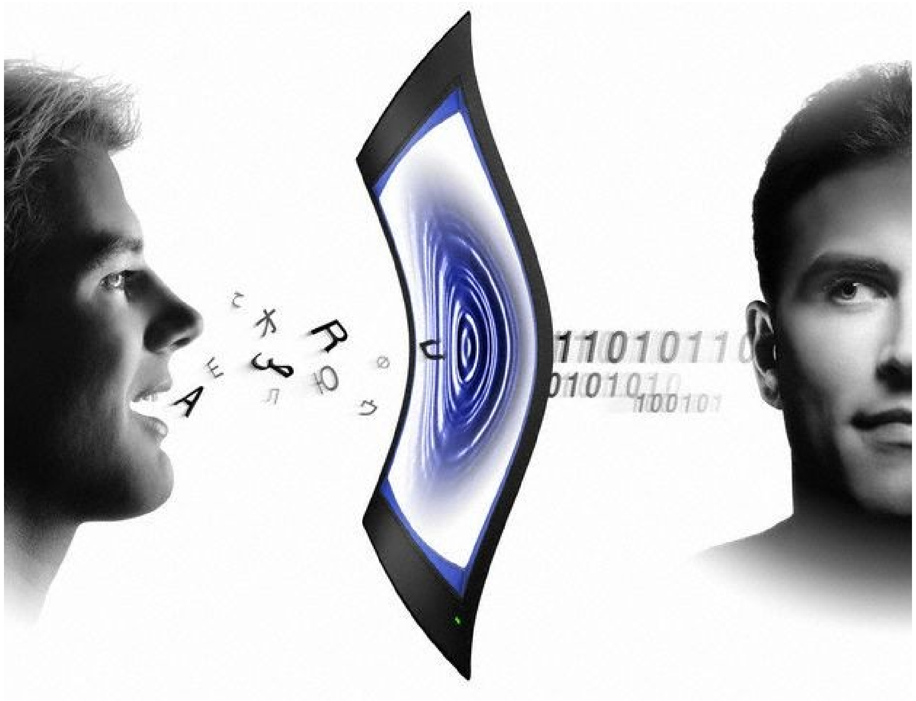
SIP Peering

Lars Strand
PhD student

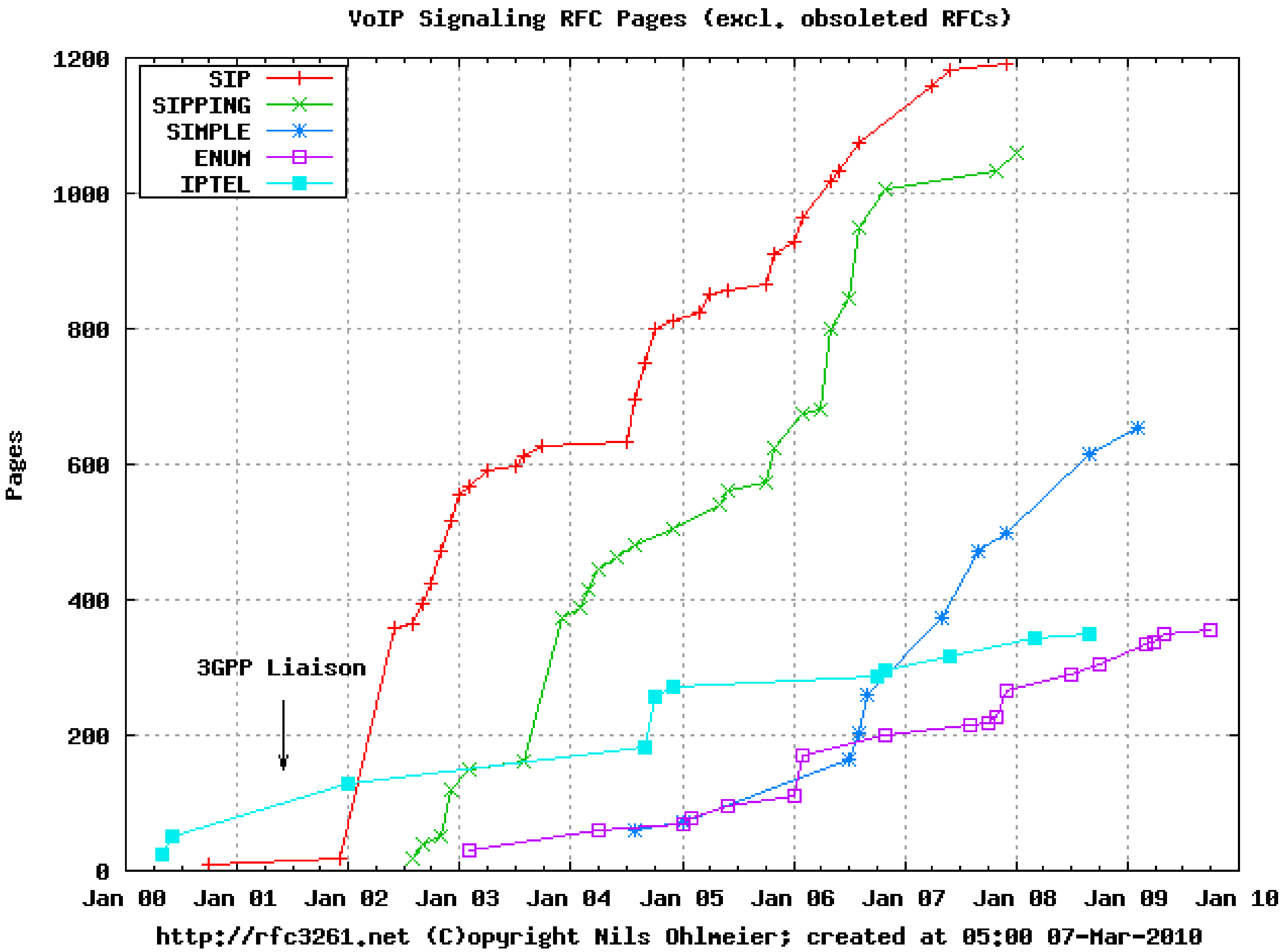
Workshop @ HPI
March 2010



NR Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

SIP

- Session Initiation Protocol (SIP) is the *de facto* standard signaling protocol for VoIP
  - Application layer (TCP, UDP, SCTP)
  - Setting up, modifying and tearing down multimedia sessions
  - Not media transfer (voice/video)
  - Establishing and negotiating the *context* of a call
- RTP transfer the actual multimedia
- SIP specified in RFC 3261 published by IETF 2002
  - First iteration in 1999 (RFC2543) – over ten years old
  - Additional functionality specified in over 120 different RFCs(!)
  - Even more pending drafts...
  - Known to be complex and sometimes vague – difficult for software engineers to implement
  - Interoperability conference - “SIPit”


VoIP Signaling RFC Pages (excl. obsoleted RFCs)
SIP
SIPPING
SIMPLE
ENUM
IPTEL
3GPP Liaison
Pages
0
200
400
600
800
1000
1200
Jan 00
Jan 01
Jan 02
Jan 03
Jan 04
Jan 05
Jan 06
Jan 07
Jan 08
Jan 09
Jan 10
http://rfc3261.net (C)opyright Nils Ohlmeier; created at 05:00 07-Mar-2010

SIP message syntax - INVITE

Start line (method)

```
INVITE sip:bob@NR SIP/2.0
```

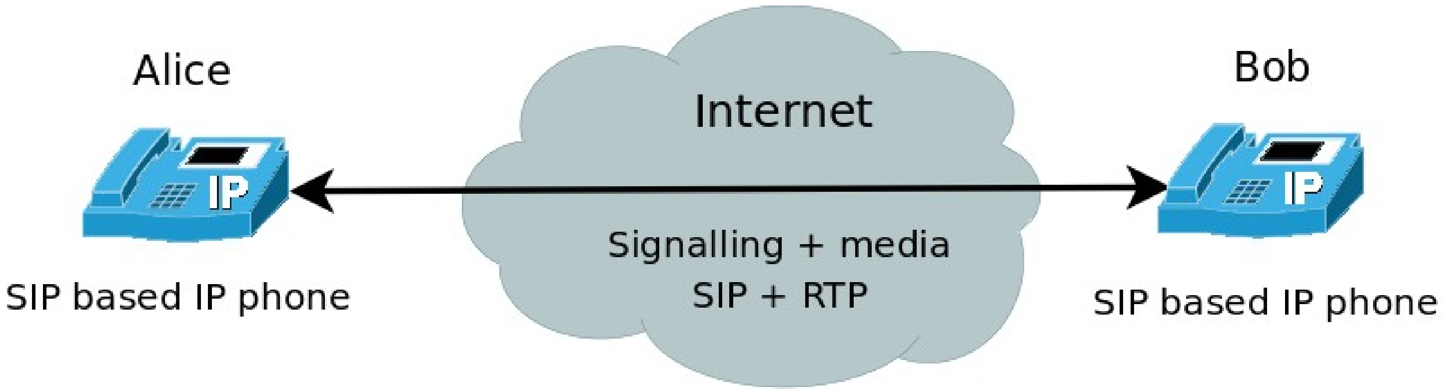
Message headers

```
Via: SIP/2.0/UDP 156.116.8.106:5060;rport;branch=z9hG4b
From: Alice <sip:alice@NR>;tag=2093912507
To: <sip:bob@NR>
Contact: <sip:alice@156.116.8.106:5060>
Call-ID: 361D2F83-14D0-ABC6-0844-57A23F90C67E@156.116.8
CSeq: 41961 INVITE
Max-Forwards: 70
Content-Type: application/sdp
User-Agent: X-Lite release 1105d
Content-Length: 312
```

Message body (SDP content)

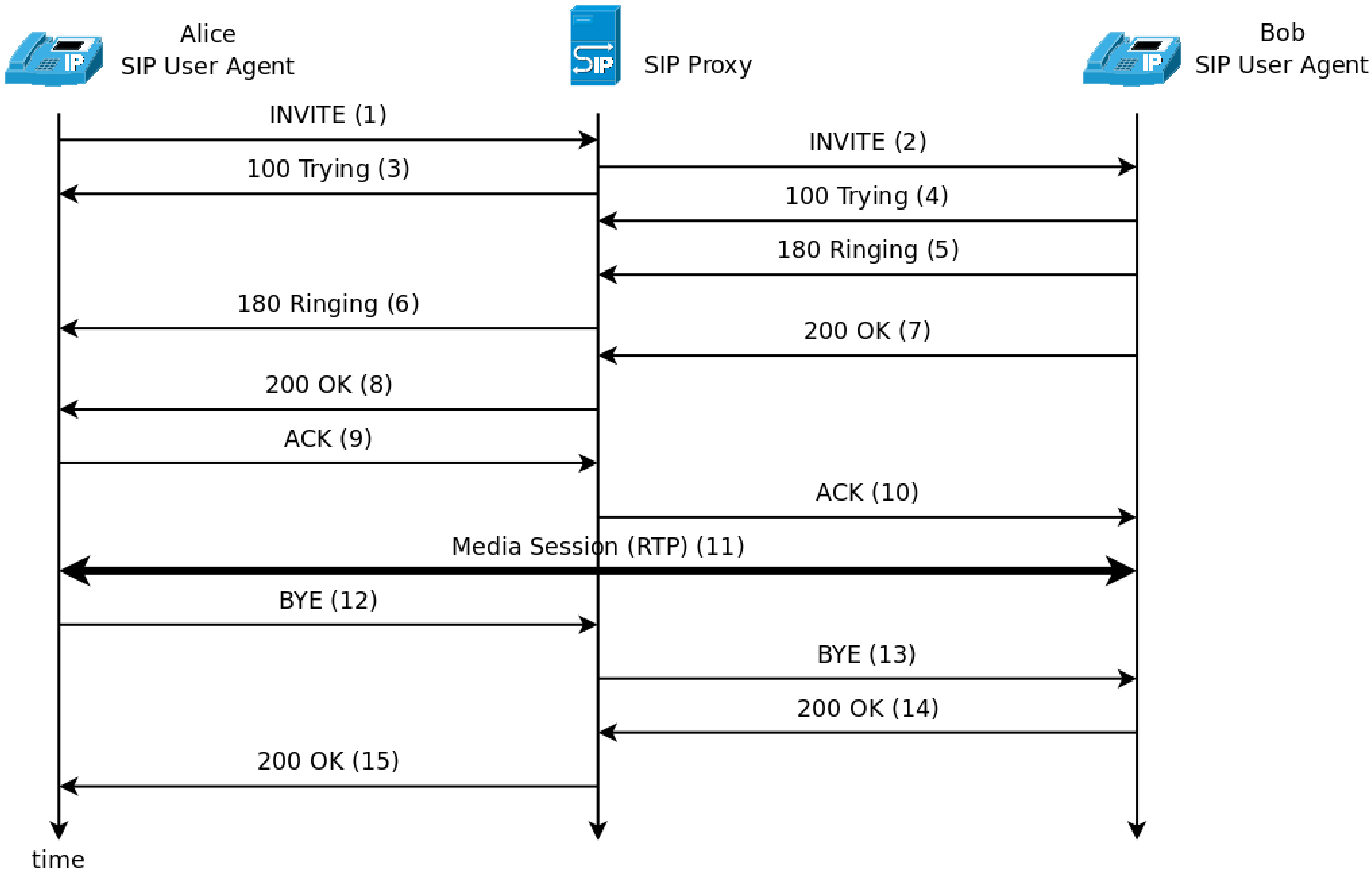
```
v=0
o=alice 2060633878 2060633920 IN IP4 156.116.8.106
s=SIP call
c=IN IP4 156.116.8.106
t=0 0
m=audio 8000 RTP/AVP 0 8 3 98 97 101
..............
```

SIP example
Direct call UA to UA



- Caller must know callee's IP or hostname
- No need for intermediate SIP nodes
- **Problems:**
  - Traversing firewalls / NAT
  - Must know IP/hostname of user
  - Mobility – change IP/hostname

SIP example



Alice
SIP User Agent
SIP Proxy
Bob
SIP User Agent
INVITE (1)
INVITE (2)
100 Trying (3)
100 Trying (4)
180 Ringing (5)
180 Ringing (6)
200 OK (7)
200 OK (8)
ACK (9)
ACK (10)
Media Session (RTP) (11)
BYE (12)
BYE (13)
200 OK (14)
200 OK (15)
time

Global reachability?

- SIP has won the "signaling battle" (over H.323)
  - (like SMTP won over X.400)
  - SIP incorporates many elements from HTTP and SMTP
- **Design goal: Global reachability like SMTP**
  - We call this the "email model"
- SIP has reached deployment worldwide
  - VoIP has reached high penetration both in companies and for ISP customers
  - But very few *open* SIP servers – like originally planned
  - **Why?**

SIP follows an “email alike model”

1) Email and SIP addresses are structured alike
   - username@domain
   - address-of-record (AoR): **`sip:alice@example.com`**

2) Both SIP and email rely on DNS
   - Map domain name to a set of ingress points that handle the particular connection

3) The ingress points need to accept incoming request from the Internet

4) No distinction between end-users and providers
   - Any end-user can do a DNS lookup and contact the SIP server directly

5) No need for a business relationship between providers
   - Since anyone can connect

6) Clients (usually) do not talk directly to each other – often one or more intermediate SIP/SMTP nodes

- Read more: RFC 3261 and RFC3263

Why has the email model failed?

1) **Business** – “sender keeps all” → breaks tradition
- The traditional economic model is based on termination fee
- Since anybody can connect to anybody, no business relationship is needed
- No (economical) incentives for providers to deploy open SIP servers providers

2) **Legal requirements** → written for PSTN
- Operators must comply to a wide range of regulatory requirements
- Example: Wiretapping, caller-id, hidden number, emergency calls, etc

3) **Security considerations**

A) Unwanted calls (SPIT)

B) Identity

C) Attack on availability (DoS)

A) Unwanted calls (SPIT)

- **Hard** – unknown attack vector
  - When there are enough open SIP servers, attackers will start to exploit them
  - Low amount of SPIT today (because few open SIP servers)
- **Worse than SPAM**
  - Content only available *after* the user picks up the phone = harder to filter and detect than email
  - Users tend to pick up the phone when it rings = disruptive (users can choose when to check their email)
- A number of SPIT mitigation strategies has been proposed (active research)
- The research project “SPIDER” looked at SPIT
  - Good informative deliverables
  - Project finished

“We're afraid of SPIT, so we don't have open SIP Servers”

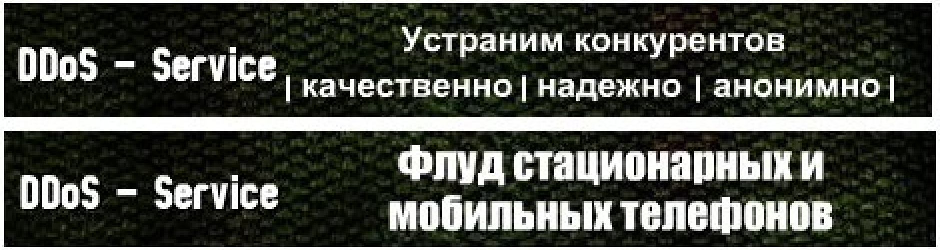
B) Identity

- PSTN
  - Provide (reasonable) good caller-id
  - Providers trust each others signaling
- SIP's email model breaks this
  - Anyone can send
  - SIP (INVITE) easily spoofed
- **The SIP authentication is terrible**
  - Modeled (copied) after HTTP Digest authentication
  - SIP also support TLS (and certificate authentication) but very limited deployment
- “SIP Identity” tries to fix this (RFC4474)
  - Rely on certificates
  - Not based on transitive trust between providers
  - No one uses this

“Since SIP has so poor identity handling, we don't want to expose our SIP servers to the Internet”

C) Attack on availability (DoS)

- **Denial of Service (DoS) attacks are HARD!**
  - Simple and effective: Send more bogus traffic than the recipient can handle
  - No simple solution to prevent DoS



- Example: DDoS for sale - The ad scrolls through several messages, including
  - "Will eliminate competition: high-quality, reliable, anonymous."
  - "Flooding of stationary and mobile phones."
  - "Pleasant prices: 24-hours start at $80. Regular clients receive significant discounts."
  - "Complete paralysis of your competitor/foe."

Reference: http://isc.sans.org/diary.html?storyid=5380

"We're terrified to become a victim of a DDoS attack"

So, what is the result?

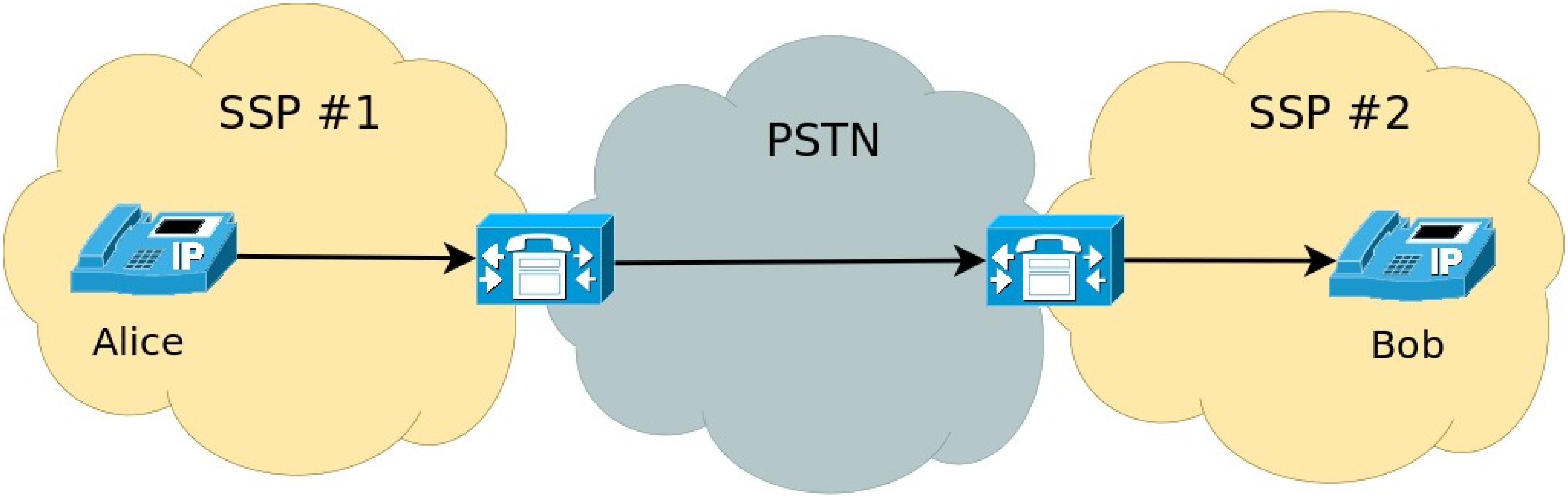
Providers do NOT have open SIP servers

All non-local calls are sent to the PSTN

Why is that a bad thing?

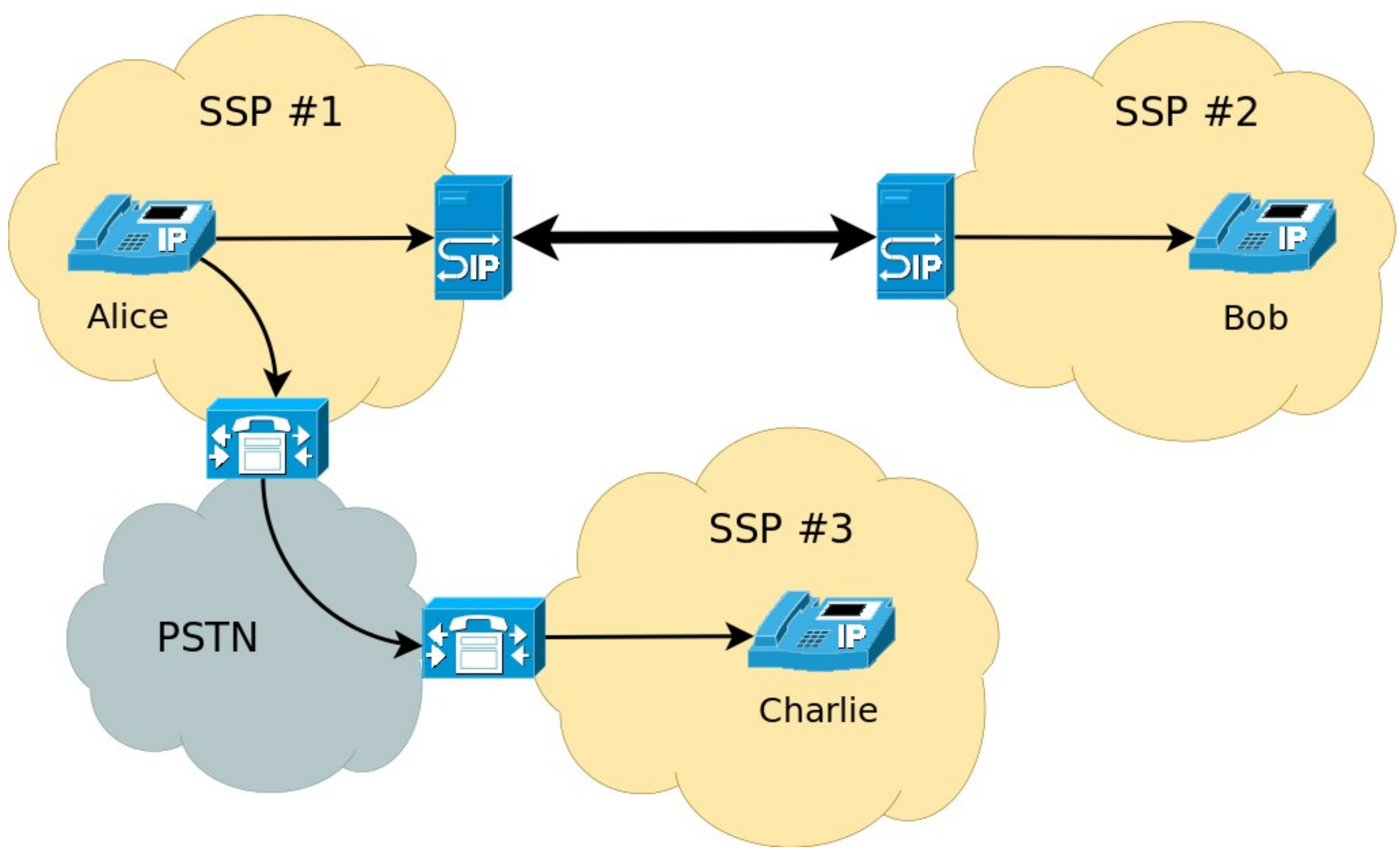
Disadvantages

1) Administrative overhead – more systems to keep track of
   - IP-to-PSTN gateway
2) More expensive than "SIP only"
   - Must pay a termination fee to the PSTN provider
   - Must maintain the IP-to-PSTN gateway
3) Poor(er) voice quality
   - Voice must be transcoded from G.711 to the PSTN (and back again)
   - Can not use wide-band codecs, like G.722 that provides superior sound quality ("HD sound")
4) Only applies to voice – miss out other functionality that SIP supports
   - IM, presence, mobility, etc.



SIP Peering

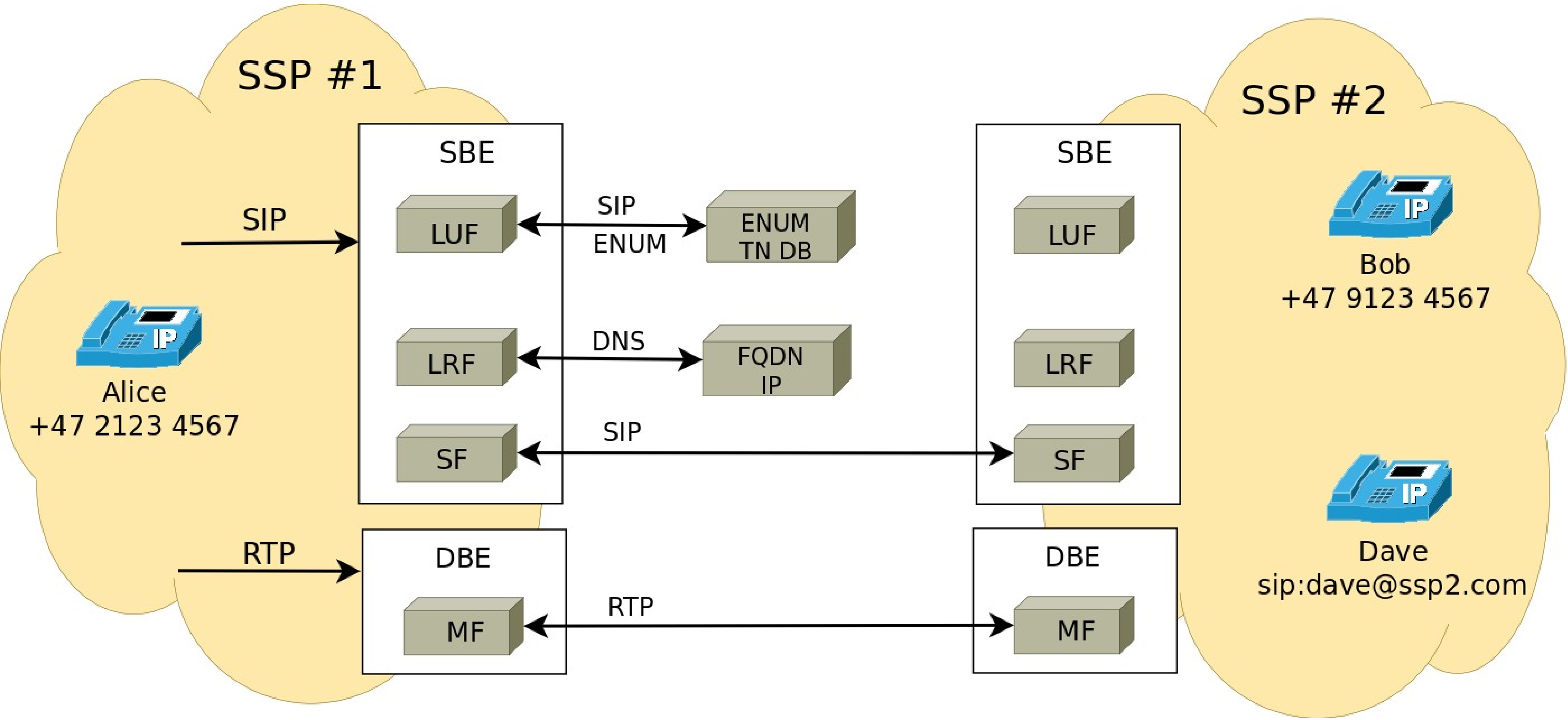
- Peering overcome these disadvantages
- Do not need an open SIP server on the Internet
- Industry has started to do this ad-hoc
  - But not standardized in any way



SPEERMINT

- IETF has recognized that SIP Peering must be standardized
  - (New) Working Group (WG) will fix that
  - "Session PEERing for Multimedia INTerconnect" (SPEERMINT)
- **Goal:**
  - Identify architecture requirements
  - Discuss security considerations
  - Define best practices for SIP peering
  - *"Get SIP to work reliably in a worldwide deployment"*
- Documents:
  - RFC5486: Session Peering for Multimedia Interconnect (SPEERMINT) Terminology
  - RFC5344: Presence and Instant Messaging Peering Use Cases
  - And several drafts pending

SPEERMINT architecture



Telephone number mapping (ENUM)

- Example: +47 2134 5678
  - How do we find the domain name and route the request?
- E.164 NUmber Mapping (ENUM)
  - Telephone numbers are organized in the E.164 standard
  - IP adresses on Internet uses DNS
  - E.164 + DNS = ENUM
- New DNS zone: e164.arpa
  - example: tel:+47 2123 4567 → 7.6.5.4.3.2.1.2.7.4.e164.arpa → DNS lookup
- Originally planned to be global
  - All the world (PSTN) phone numbers should be reachable via ENUM
  - (Part of the “email model” of SIP)
  - Did not happened
- Used locally within SSP and between peers

Peering scenarios

1) **Static** – peering between SSP1 and SSP2 is pre-provisioned independent of any SIP sessions between users
2) Ondemand – peering is established when a SIP session between SSP1 and SSP2 are needed

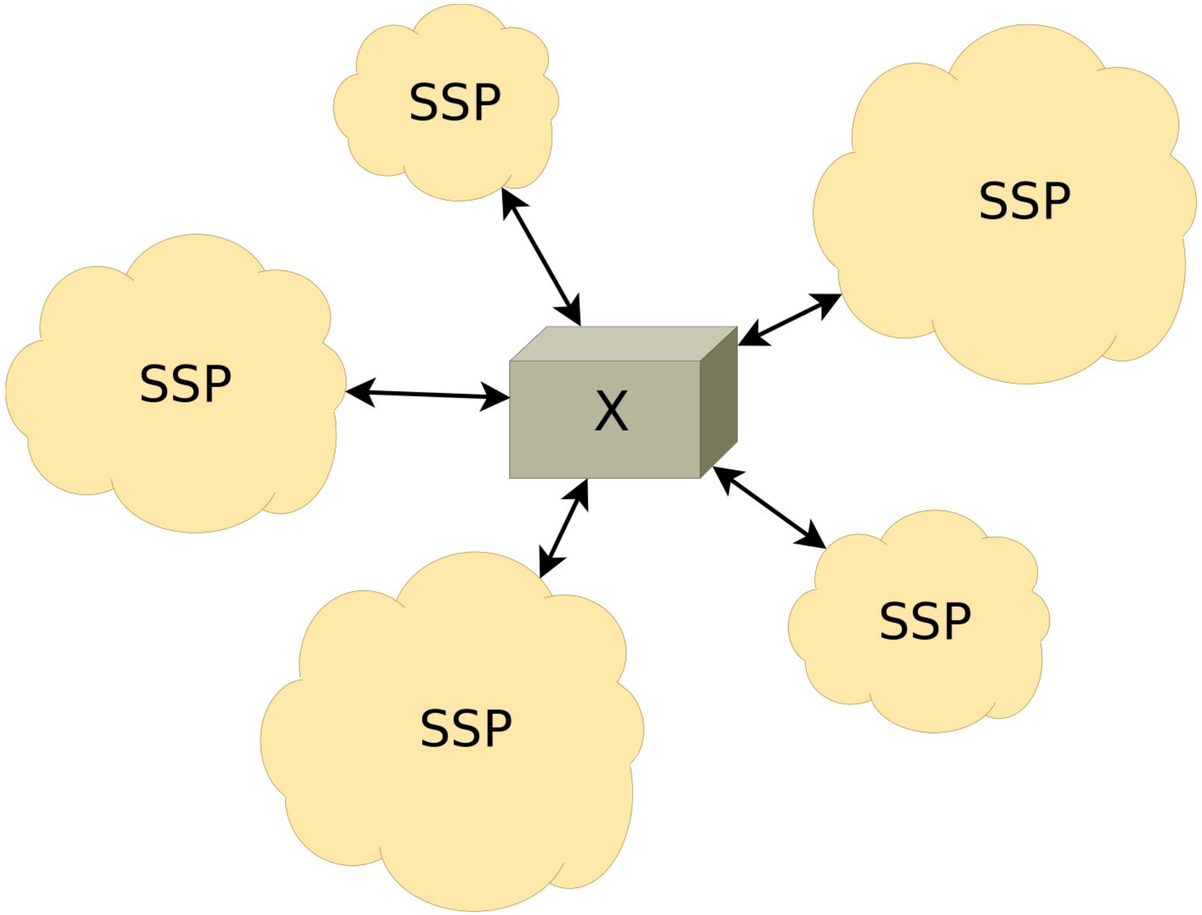
A) Direct – direct peer between SSP1 and SSP2

B) Indirect or transit – via an intermediate SSP

- In combination with assisted LUF/LRF
- XConnect

Federation

"A group of SSPs which agree to receive calls from each other via SIP, and who agree on a set of administrative rules for such calls (settlement, abuse-handling, ...) and the specific rules for the technical details."

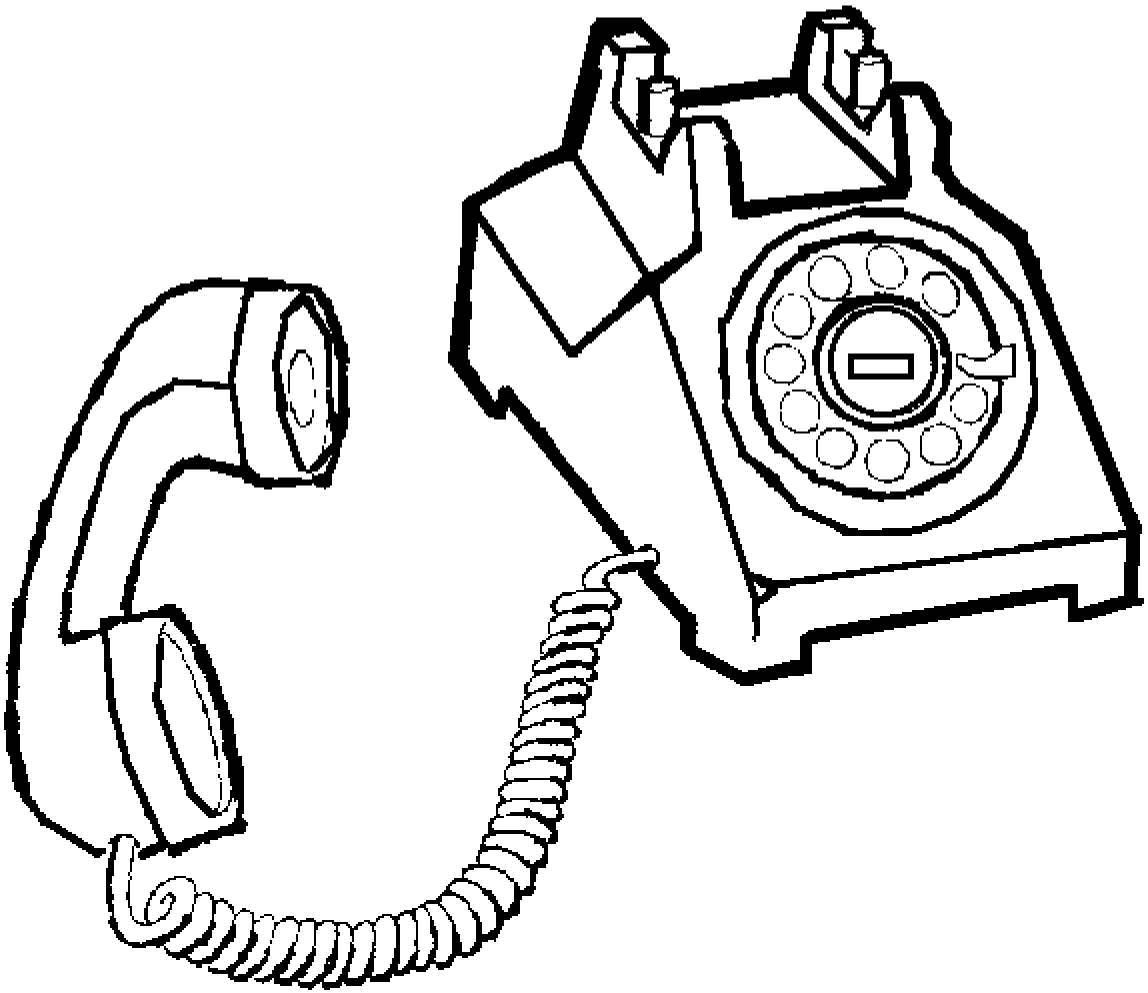


Further work

- Identity? Is it solved by peering?
  a) SIP Identity (RFC4474) → Require PKI
  b) Transitive trust between SSPs? (Combine RFC3324 and RFC3325) → Utopian?
  c) Multi-factor authentication?
  d) Web-of-trust? (aka PGP)
- SPIT? Is it solved by peering?
- DDoS? Is it solved by peering?

Some discussion in *"SPEERMINT Security Threats and Suggested Countermeasures"*, IETF draft pending.

Thank you



Project homepage: http://eux2010sec.nr.no