SIP

Jan Růžička

janru@cesnet.cz

Seminář Sitola

17.12.2009

IP telefonie

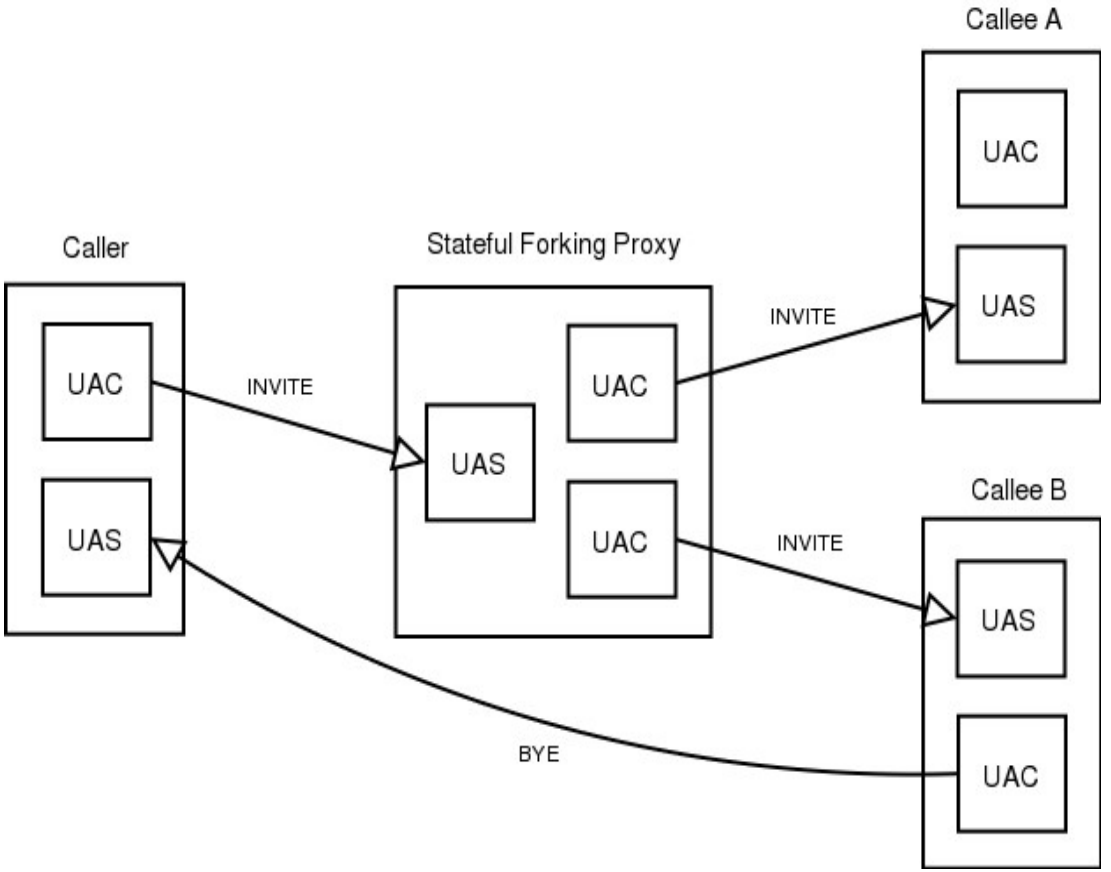
- **Simulujeme telefonní síť pomocí mnohem složitějšího souboru zařízení vyvinutého ke komplexnímu přenosu dat.**
  - Přináší nové služby
  - Konvergence prostředků, sítí,....
  - Jsou nutná čísla?
- **SIP - momentálně nejpoužívanější otevřený protokol**
  - způsobil masivní rozvoj IP telefonie
  - Stav v ČR – Vše budováno s ohledem na minimální náklady i u zákazníka – to může nést technologická omezení
  - Očekává se technologický posun s nárůstem počtu uživatelů
  - Podpora u velkých operátorů (IMS?)

SIP

- RFC3261, textový protokol podobný HTTP
- Protokol pro sestavení, řízení a ukončení spojení
- Nezávislost na přenášených mediích (hlas, video, text ...)
- Identifikátor – URI (sip:janru@cesnet.cz)
- Vícenásobný kontakt, IM, Prezence, 3rd PCC
- Využití DNS SRV, NAPTR
- Už dávno ale není jednoduchý

Architektura

- UAC je logická část posílající požadavky přijímající odpovědi
- UAS je logická část agenta přijímající požadavky a odesílající odpovědi



Prvky architektury

- **Registrar**
- **Server**
  - redirect
  - proxy
    - stateless
    - Statefull
      - Transaction
      - Dialog (Call)
- **B2BUA**
- **Gateway**
- **MCU**
- **Outbound proxy**
- **SBC SBE+DBE**
- **ALG**
- **Klient**

Metody

- INVITE – začíná a mění spojení
- BYE – ukončuje spojení
- OPTIONS – dotaz na schopnosti a ping
- ACK – potvrzení konečné odpovědi na INVITE
- REGISTER - provazuje přidělenou sip adresu a aktuální pozici
- CANCEL – přerušuje nedokončený INVITE
- MESSAGE - RFC3428
- SUBSCRIBE a NOTIFY - RFC3265
- REFER - RFC3515

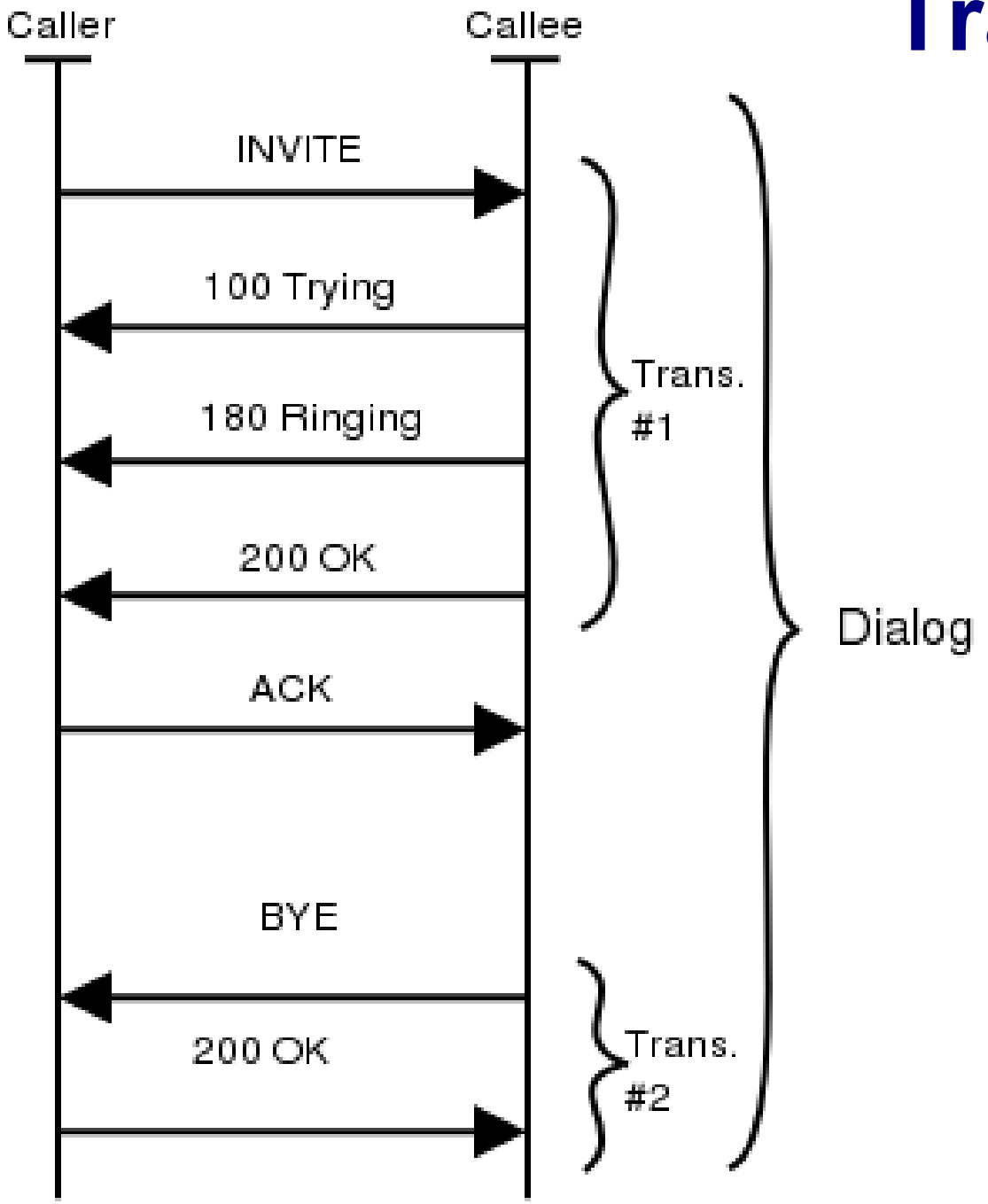
Odpovědi

- 1xx: Dočasné – potvrzení přijetí požadavku
  - 100 Trying
  - 180 Ringing
  - 183 Session Progress
- 200 - 699 finální odpovědi
- 2xx: Úspěch – požadavek byl akceptován
  - 200 OK
- 3xx: Přesměrování
  - 301 Moved Permanently
  - 302 Moved Temporarily
  - 305 Use Proxy

Odpovědi

- 4xx: Chyba Client – Požadavek je špatný nebo nemůže být takto nebo na tomto serveru zpracován
  - 401 Unauthorized
  - 404 Not Found
  - 407 Proxy Authentication Required
  - 408 Request Timeout
  - 481 Call/Transaction Does Not Exist
- 5xx: Chyba Serveru – serveru se nezdařilo zpracovat požadavek i když je v pořádku
  - 503 Service Unavailable
- 6xx: Globální chyba – požadavek nemůže být zpracován nikde.
  - 603 Decline

Transakce a dialog



Transakce

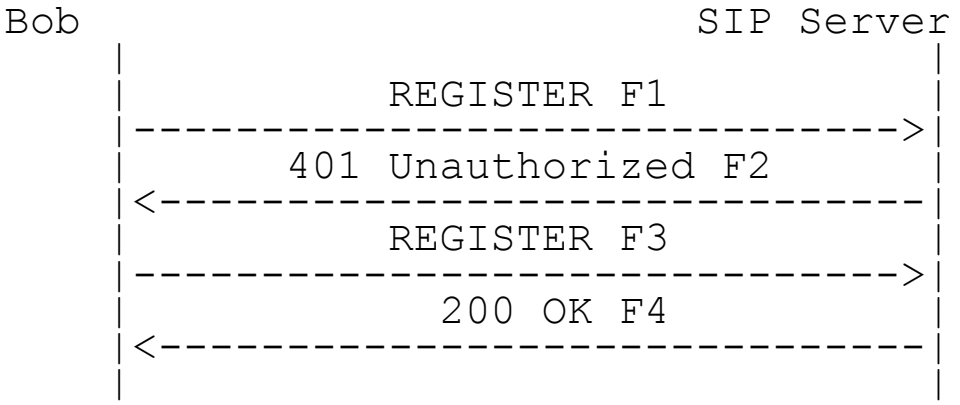
- Jeden požadavek a všechny příslušné odpoědi
- Unikatní branch parametr Via (část za z9hG4bK)

Dialog

- Identifikován sadou Call-ID, From tag, To tag
- CSeg pořadí požadavků (z každé strany nezávislý čitač)

Registrace

- Vytvoření vazby mezi konkrétní polohou (IP) klienta a je identifikátorem v SIP doméně (To)
- Poloha = Contact
  - prázdný Contact v žádosti = zjištění stavu registrací
  - V odpovědi může být i více záznamů v jedné hlavičce
- Expires
  - v požadavku navrhovaná doba
  - v odpovědi serverem potvrzená
  - 0 je zrušení registrace



Registrace

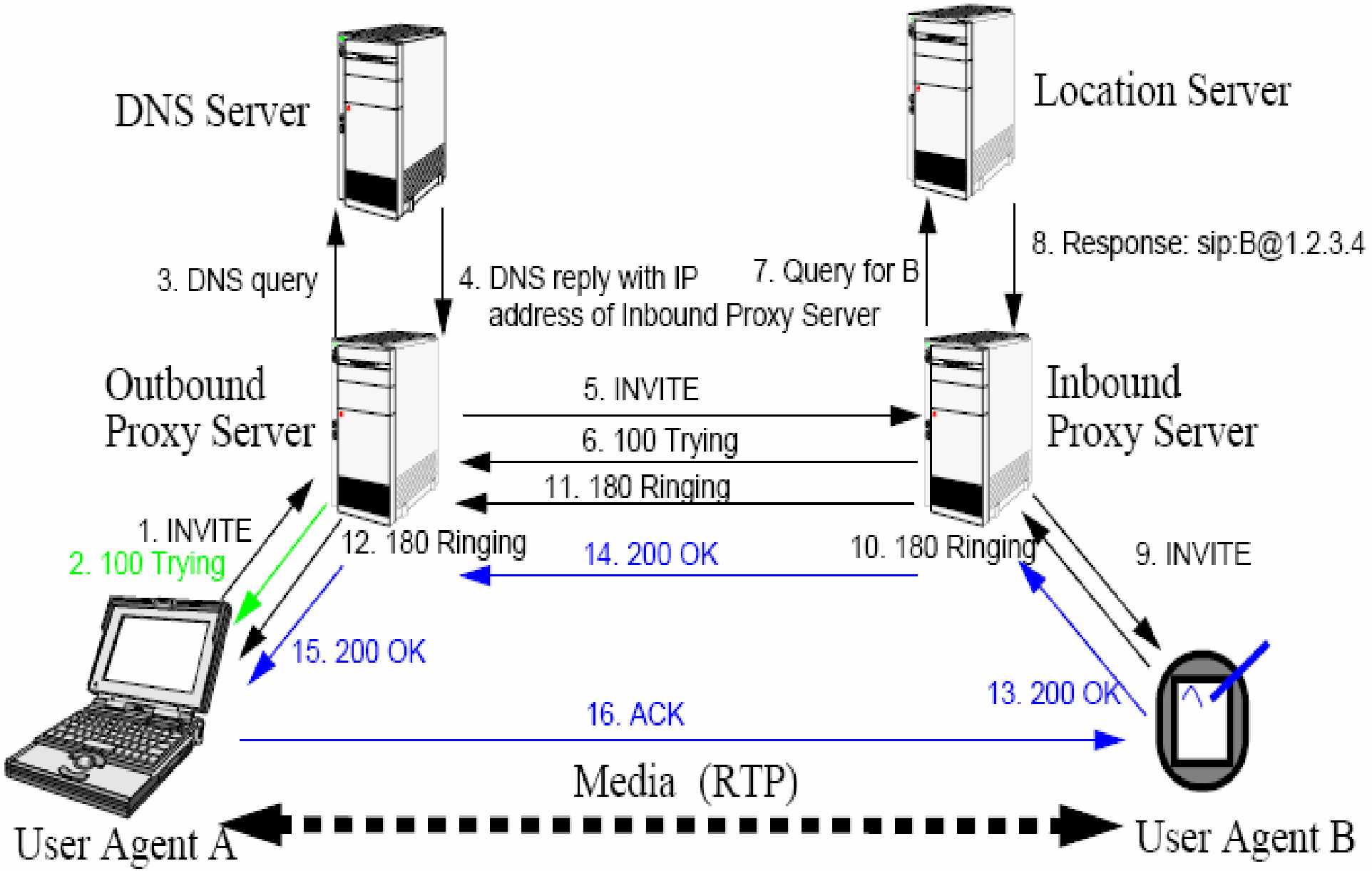
SIP/2.0 401 Unauthorized.
Via: SIP/2.0/UDP
195.178.64.172:49252;branch=z9hG4bK.6afb7404;rport=49253.
From: sip:user@cesnet.cz;tag=6c2c90b8.
To: sip:user@cesnet.cz;tag=c10ed4fff3e6fb17efd0bfbdcce87ce2.c76e.
Call-ID: 1814859960@195.178.64.172.
CSeq: 1 REGISTER.
WWW-Authenticate: Digest realm="cesnet.cz",
nonce="43eeaeb76e6eeaeffbc37d4f4018dc659c5d282a".
Server: Sip EXpress router (0.9.5-pre1 (i386/linux)).
Content-Length: 0.

REGISTER sip:cesnet.cz SIP/2.0.
Authorization: Digest username="user", uri="sip:cesnet.cz",
algorithm=MD5, realm="cesnet.cz",
nonce="43eeaeb76e6eeaeffbc37d4f4018dc659c5d282a",
response="9e83c39e8a7262901
Via: SIP/2.0/UDP 195.178.64.172:49252;branch=z9hG4bK.32f02bf2;rport.
From: sip:user@cesnet.cz;tag=6c2c90b8.
To: sip:user@cesnet.cz.
Call-ID: 1814859960@195.178.64.172.
CSeq: 2 REGISTER.
Content-Length: 0.
Max-Forwards: 70.
Expires: 15.
Contact: sip:user@a.b.c.d:1234.

INVITE

```
INVITE sip:mamut@iptel.org SIP/2.0.
Max-Forwards: 10.
Record-Route: <sip:195.113.222.3;ftag=5DAA94E7;lr=on>.
Via: SIP/2.0/UDP 195.113.222.3;branch=z9hG4bK0a5d.90580ee2.0.
Via: SIP/2.0/UDP 195.113.134.233:5062;branch=z9hG4bK2E1FD348.
CSeq: 262 INVITE.
To: <sip:mamut@iptel.org>.
Proxy-Authorization: Digest username="bbb", realm="ces.net",
    nonce="43788e90381ccbec64fced4dc7097828391e81", uri="sip:mamut@iptel.org",
    cnonce="abcdefghi", nc=00000001, response="ed4adec8
Content-Type: application/sdp.
From: "Franta Vomacka" <sip:bbb@ces.net>;tag=5DAA94E7.
Call-ID: 379332994@195.113.134.233.
Subject: sip:bbb@ces.net.
Content-Length: 234.
User-Agent: kphone/4.2.
Contact: "Franta Vomacka" <sip:bbb@195.113.134.233:5062;transport=udp>.
Remote-Party-ID: "Franta Vomacka" <sip:950070101@ces.net>;party=calling;id-
    type=subscriber;privacy=off; screen=yes.
.
v=0.
o=username 0 0 IN IP4 195.113.134.233.
s=The Funky Flow.
c=IN IP4 195.113.134.233.
t=0 0.
m=audio 33728 RTP/AVP 0 97.
a=rtpmap:0 PCMU/8000.
a=rtpmap:97 iLBC/8000.
```

Hovor



http://www.tech-invite.com/Ti-sip-ex3261.html

Hovor

Směrování požadavků podle RURI a Route

Směrování odpovědí podle Via

Message Request

```
INVITE sip:bob@biloxi.example.com SIP/2.0
Via: SIP/2.0/TCP client.atlanta.example.com:5060
 ;branch=z9hG4bK74bf9
Max-Forwards: 70
From: Alice <sip:alice@atlanta.example.com>
 ;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:alice@client.atlanta.example.com;transport=tcp>
Content-Type: application/sdp
Content-Length: 151

v=0
o=alice 2890844526 2890844526 IN IP4
client.atlanta.example.com
s=-
c=IN IP4 192.0.2.101
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

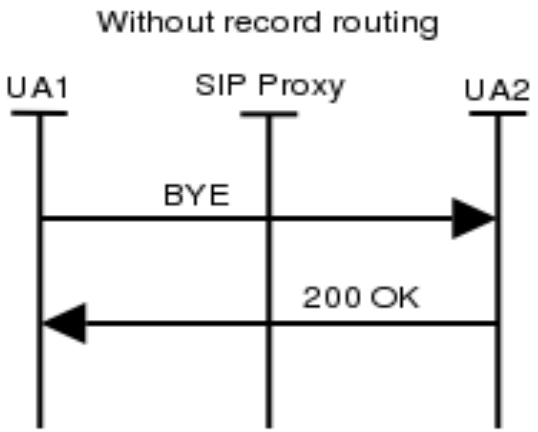
Message Response

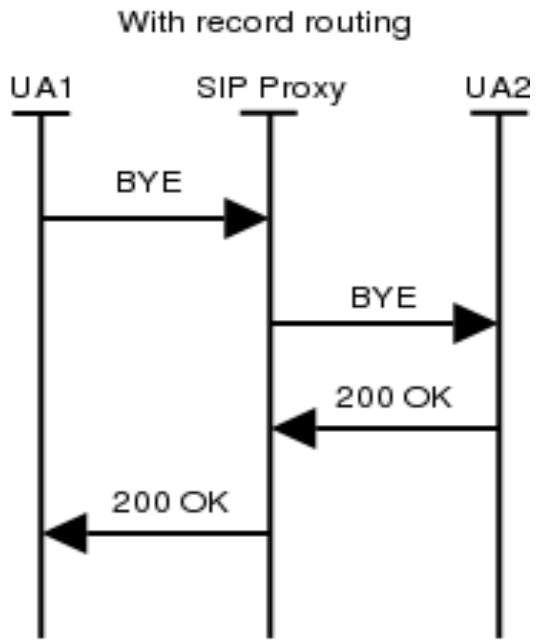
```
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP client.atlanta.example.com:5060
 ;branch=z9hG4bK74bf9
 ;received=192.0.2.101
From: Alice <sip:alice@atlanta.example.com>
 ;tag=9fxced76sl
To: Bob <sip:bob@biloxi.example.com>
 ;tag=8321234356
Call-ID: 3848276298220188511@atlanta.example.com
CSeq: 1 INVITE
Contact: <sip:bob@client.biloxi.example.com;transport=tcp>
Content-Length: 0
```

Jde to i složitěji

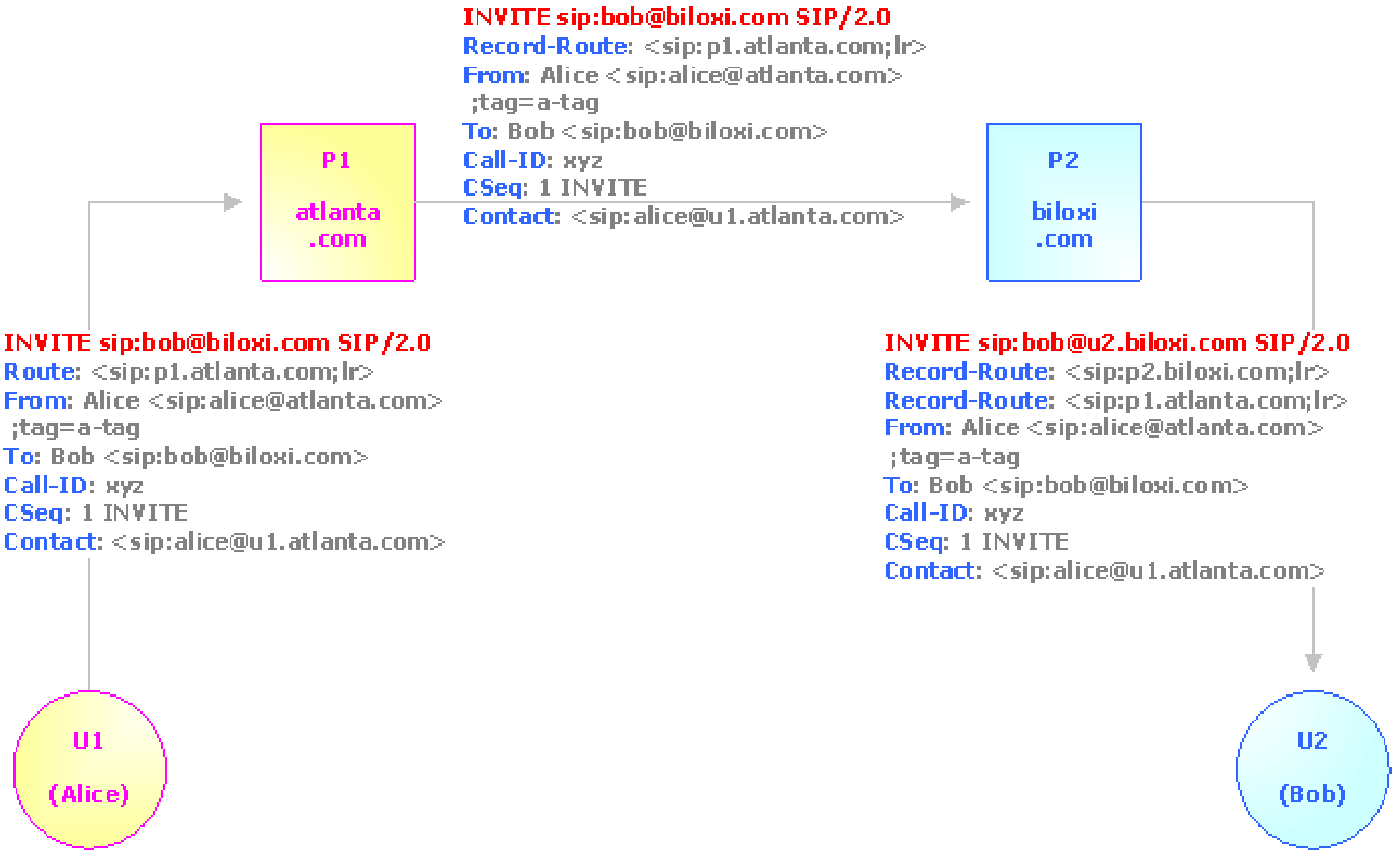
Record routing

- Jak zajistit aby prvek zůstal v cestě dalších požadavků
- Outbound proxy není dostatečná
- Do požadavků prvek přidá Record-Route: <sip:adresa;lr>
- V odpovědi dorazí Record Routa sada
- Další požadavky jsou vybaveny a směrovány podle record route sady (Route hlavičky)

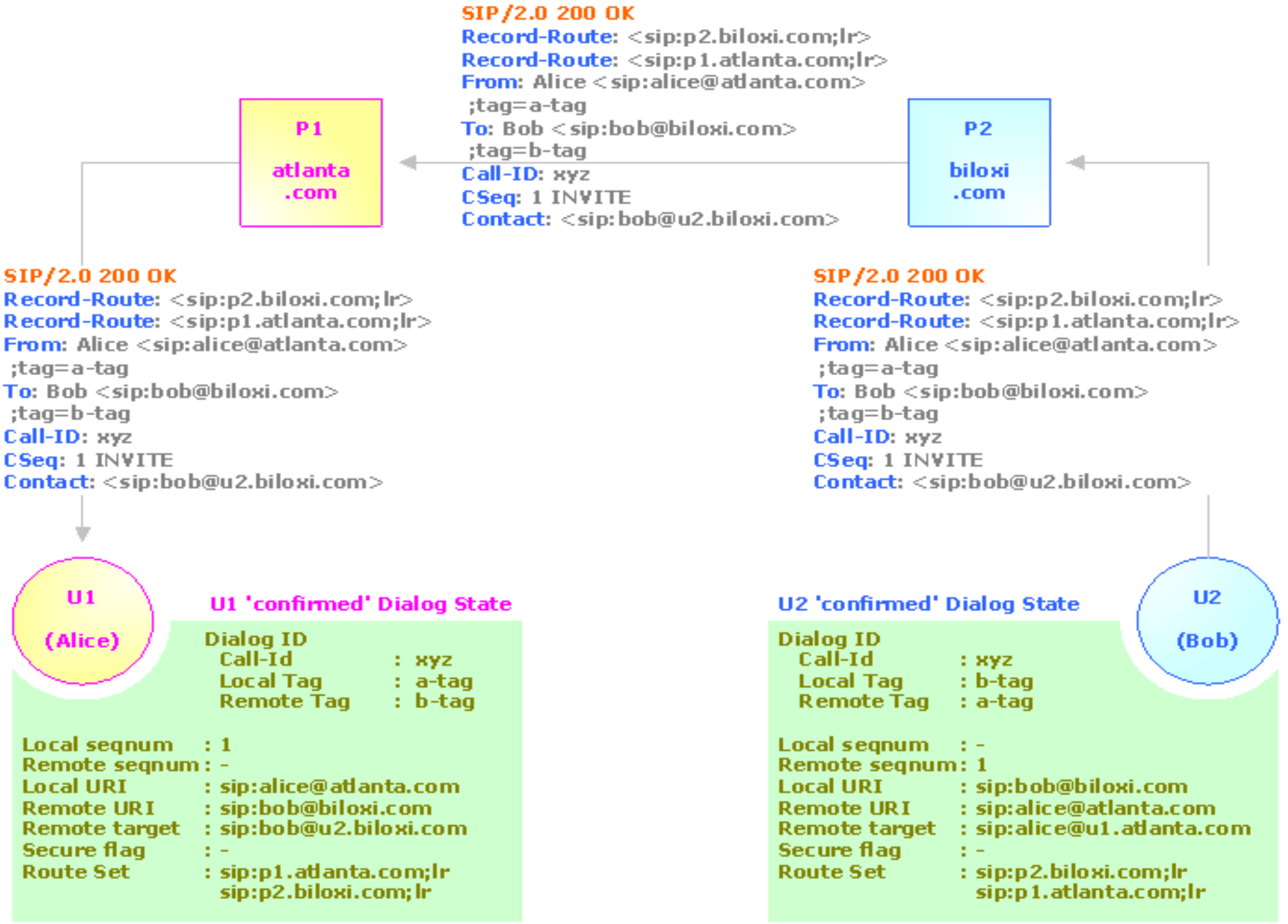


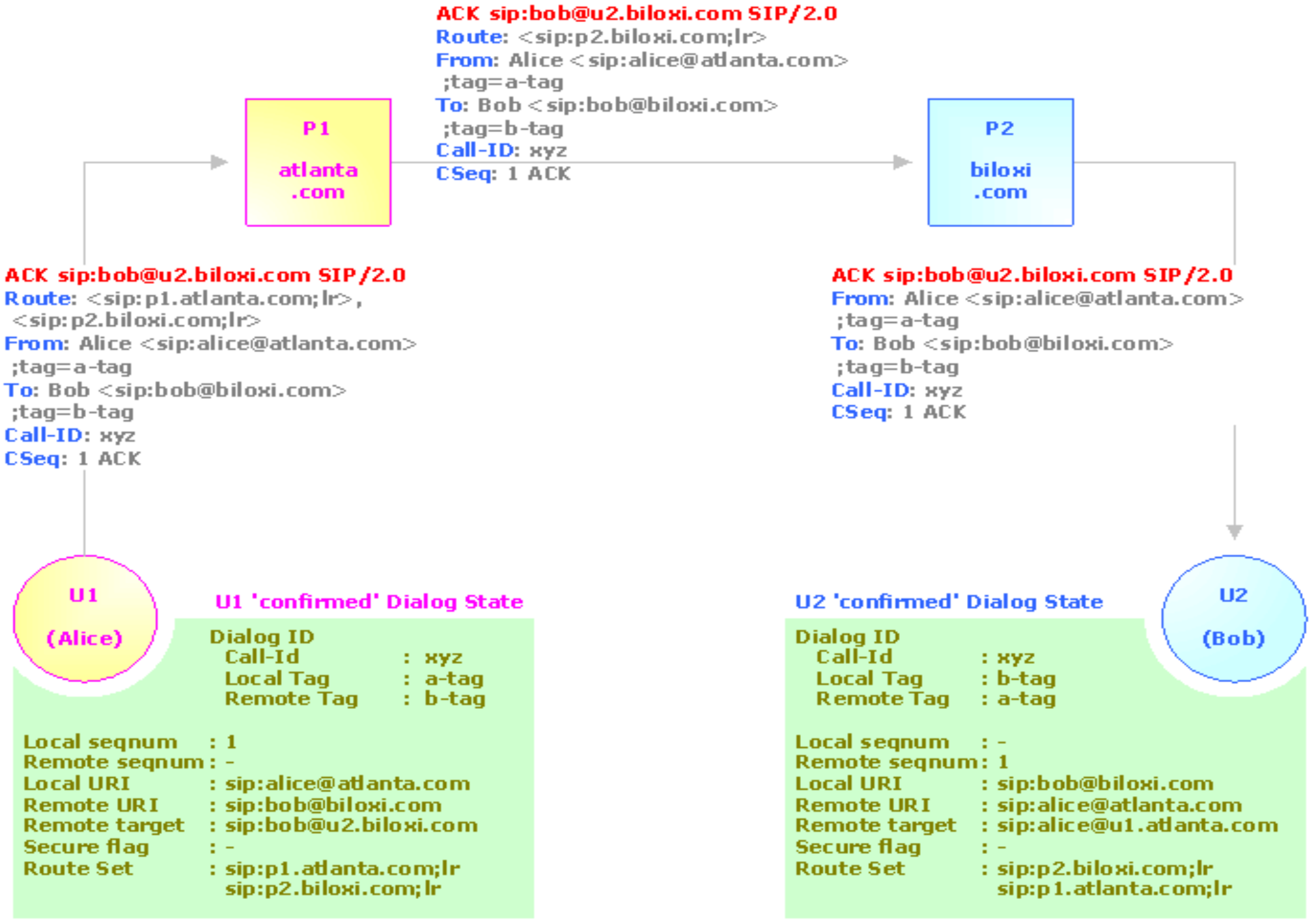


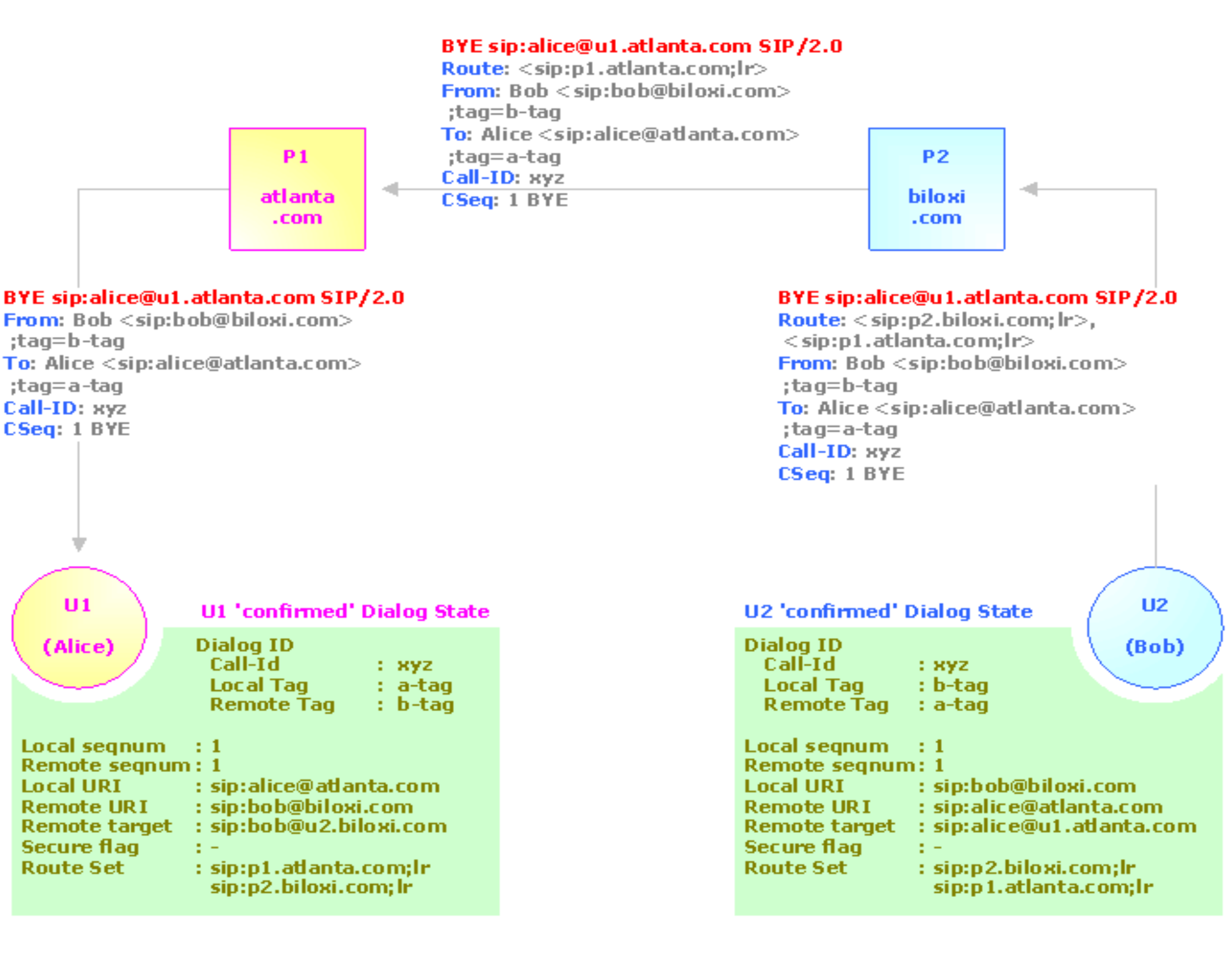
RR II



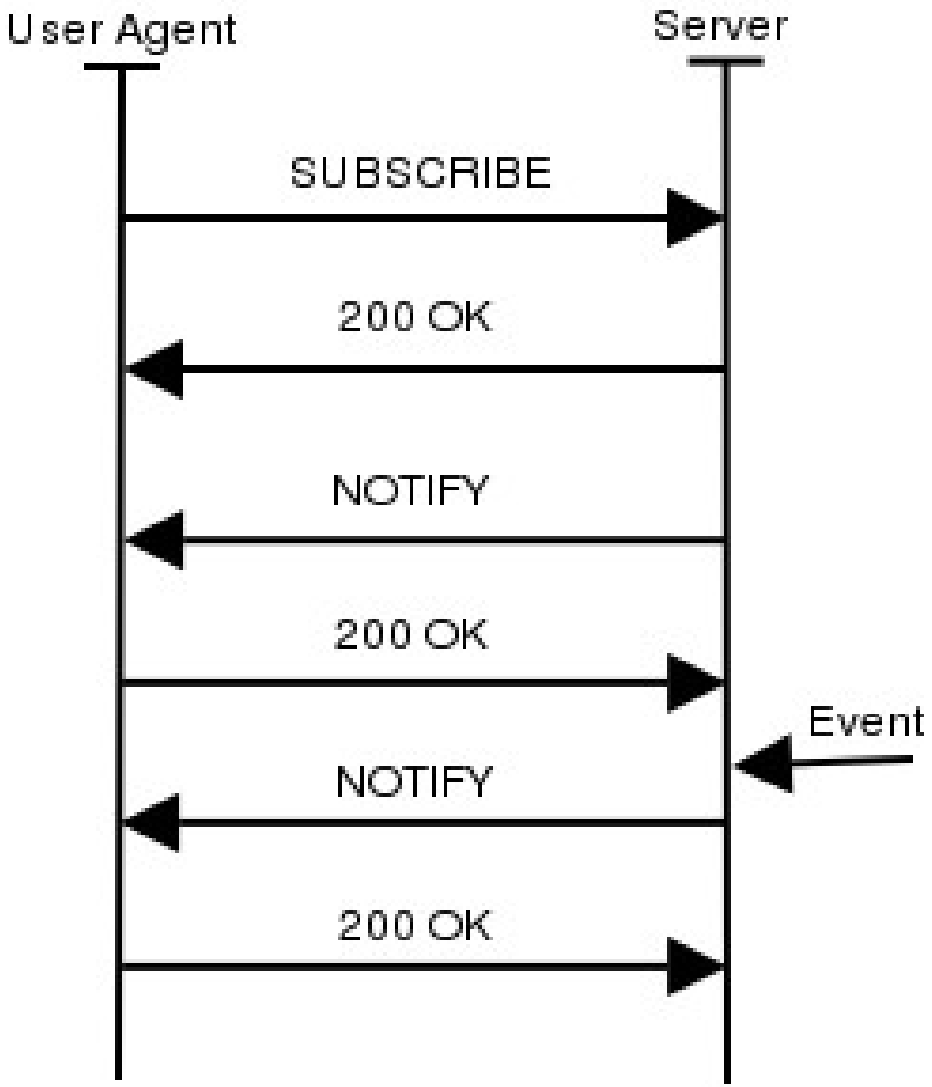
Tech Invite http://www.tech-invite.com/Ti-sip-dialog.html


SIP/2.0 200 OK
Record-Route: <sip:p2.biloxi.com;lr>
Record-Route: <sip:p1.atlanta.com;lr>
From: Alice <sip:alice@atlanta.com>
;tag=a-tag
To: Bob <sip:bob@biloxi.com>
;tag=b-tag
Call-ID: xyz
CSeq: 1 INVITE
Contact: <sip:bob@u2.biloxi.com>
P1
atlanta
.com
P2
biloxi
.com
SIP/2.0 200 OK
Record-Route: <sip:p2.biloxi.com;lr>
Record-Route: <sip:p1.atlanta.com;lr>
From: Alice <sip:alice@atlanta.com>
;tag=a-tag
To: Bob <sip:bob@biloxi.com>
;tag=b-tag
Call-ID: xyz
CSeq: 1 INVITE
Contact: <sip:bob@u2.biloxi.com>
SIP/2.0 200 OK
Record-Route: <sip:p2.biloxi.com;lr>
Record-Route: <sip:p1.atlanta.com;lr>
From: Alice <sip:alice@atlanta.com>
;tag=a-tag
To: Bob <sip:bob@biloxi.com>
;tag=b-tag
Call-ID: xyz
CSeq: 1 INVITE
Contact: <sip:bob@u2.biloxi.com>
U1
(Alice)
U1 'confirmed' Dialog State
Dialog ID
Call-Id : xyz
Local Tag : a-tag
Remote Tag : b-tag
Local seqnum : 1
Remote seqnum : -
Local URI : sip:alice@atlanta.com
Remote URI : sip:bob@biloxi.com
Remote target : sip:bob@u2.biloxi.com
Secure flag : -
Route Set : sip:p1.atlanta.com;lr
sip:p2.biloxi.com;lr
U2 'confirmed' Dialog State
U2
(Bob)
Dialog ID
Call-Id : xyz
Local Tag : b-tag
Remote Tag : a-tag
Local seqnum : -
Remote seqnum : 1
Local URI : sip:bob@biloxi.com
Remote URI : sip:alice@atlanta.com
Remote target : sip:alice@u1.atlanta.com
Secure flag : -
Route Set : sip:p2.biloxi.com;lr
sip:p1.atlanta.com;lr


ACK sip:bob@u2.biloxi.com SIP/2.0
Route: <sip:p2.biloxi.com;lr>
From: Alice <sip:alice@atlanta.com>
;tag=a-tag
To: Bob <sip:bob@biloxi.com>
;tag=b-tag
Call-ID: xyz
CSeq: 1 ACK
P1
atlanta
.com
P2
biloxi
.com
ACK sip:bob@u2.biloxi.com SIP/2.0
Route: <sip:p1.atlanta.com;lr>,
<sip:p2.biloxi.com;lr>
From: Alice <sip:alice@atlanta.com>
;tag=a-tag
To: Bob <sip:bob@biloxi.com>
;tag=b-tag
Call-ID: xyz
CSeq: 1 ACK
ACK sip:bob@u2.biloxi.com SIP/2.0
From: Alice <sip:alice@atlanta.com>
;tag=a-tag
To: Bob <sip:bob@biloxi.com>
;tag=b-tag
Call-ID: xyz
CSeq: 1 ACK
U1
(Alice)
U1 'confirmed' Dialog State
Dialog ID
Call-Id : xyz
Local Tag : a-tag
Remote Tag : b-tag
Local seqnum : 1
Remote seqnum : -
Local URI : sip:alice@atlanta.com
Remote URI : sip:bob@biloxi.com
Remote target : sip:bob@u2.biloxi.com
Secure flag : -
Route Set : sip:p1.atlanta.com;lr
sip:p2.biloxi.com;lr
U2 'confirmed' Dialog State
U2
(Bob)
Dialog ID
Call-Id : xyz
Local Tag : b-tag
Remote Tag : a-tag
Local seqnum : -
Remote seqnum : 1
Local URI : sip:bob@biloxi.com
Remote URI : sip:alice@atlanta.com
Remote target : sip:alice@u1.atlanta.com
Secure flag : -
Route Set : sip:p2.biloxi.com;lr
sip:p1.atlanta.com;lr


BYE sip:alice@u1.atlanta.com SIP/2.0
Route: <sip:p1.atlanta.com;lr>
From: Bob <sip:bob@biloxi.com>
;tag=b-tag
To: Alice <sip:alice@atlanta.com>
;tag=a-tag
Call-ID: xyz
CSeq: 1 BYE
P1
atlanta
.com
P2
biloxi
.com
BYE sip:alice@u1.atlanta.com SIP/2.0
From: Bob <sip:bob@biloxi.com>
;tag=b-tag
To: Alice <sip:alice@atlanta.com>
;tag=a-tag
Call-ID: xyz
CSeq: 1 BYE
BYE sip:alice@u1.atlanta.com SIP/2.0
Route: <sip:p2.biloxi.com;lr>,
<sip:p1.atlanta.com;lr>
From: Bob <sip:bob@biloxi.com>
;tag=b-tag
To: Alice <sip:alice@atlanta.com>
;tag=a-tag
Call-ID: xyz
CSeq: 1 BYE
U1
(Alice)
U1 'confirmed' Dialog State
Dialog ID
Call-Id : xyz
Local Tag : a-tag
Remote Tag : b-tag
Local seqnum : 1
Remote seqnum : 1
Local URI : sip:alice@atlanta.com
Remote URI : sip:bob@biloxi.com
Remote target : sip:bob@u2.biloxi.com
Secure flag : -
Route Set : sip:p1.atlanta.com;lr
sip:p2.biloxi.com;lr
U2 'confirmed' Dialog State
U2
(Bob)
Dialog ID
Call-Id : xyz
Local Tag : b-tag
Remote Tag : a-tag
Local seqnum : 1
Remote seqnum : 1
Local URI : sip:bob@biloxi.com
Remote URI : sip:alice@atlanta.com
Remote target : sip:alice@u1.atlanta.com
Secure flag : -
Route Set : sip:p2.biloxi.com;lr
sip:p1.atlanta.com;lr

Události - Prezence



- Zápis k odběru oznámení o události např stavu jiného uživatele (prezence)
- Změna stavu vyvolá poslání NOTIFY např. Busy na Online
- SUBCRIBE započne dialog a NOTIFY jsou v jeho rámci

Autentizace a integrita

- **WWW Digest**
  - User-to-user (401 Unauthorized, WWW-Authenticate,Authorization)
  - User-to proxy (407 - Proxy authentication required, Proxy-Authenticate, Proxy-Authorization)
- **S/MIME**
- **TLS – Hop by Hop**
- **identity assertions**
  - Podmínka zabezpečený “first hop” - TLS
  - Tokeny, SAML
  - Podepsané hlavičky

NAT

- Klient za NATem vkládá privátní IP adresu do zpráv – Via, Contact, SDP c-line,...
- Typy NAT – full cone, restricted cone, port restricted cone, symmetric
- Řešení
  - STUN
  - TURN
  - ICE
  - Pomoc proxy serveru (nathelper, mediaproxy in ser and openser)
  - SBC+DBE
  - ALG

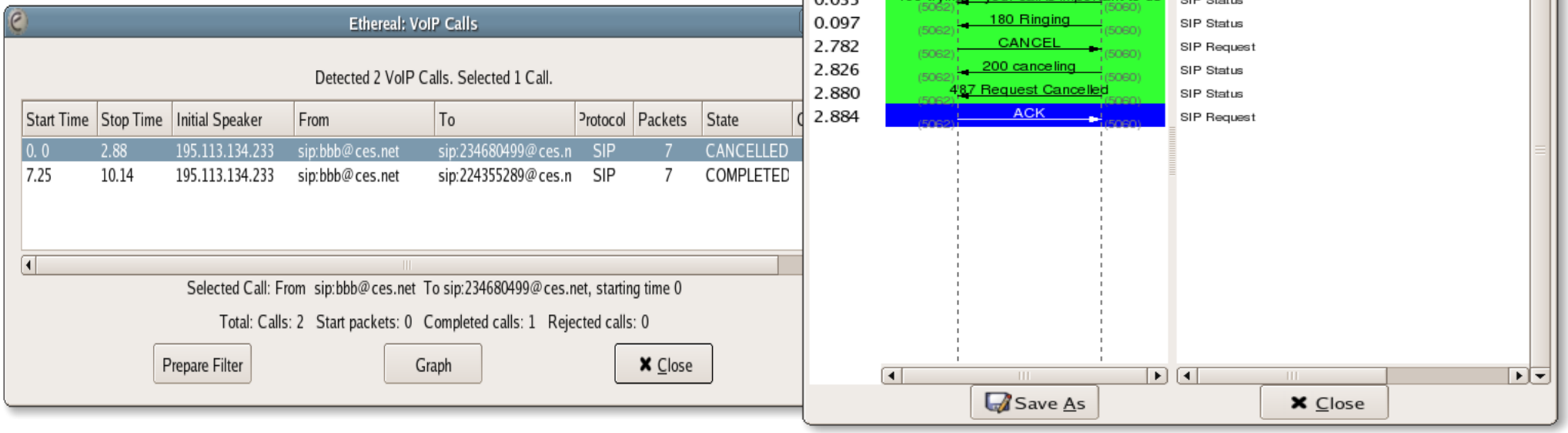
INVITE

pro NAT důležitá místa

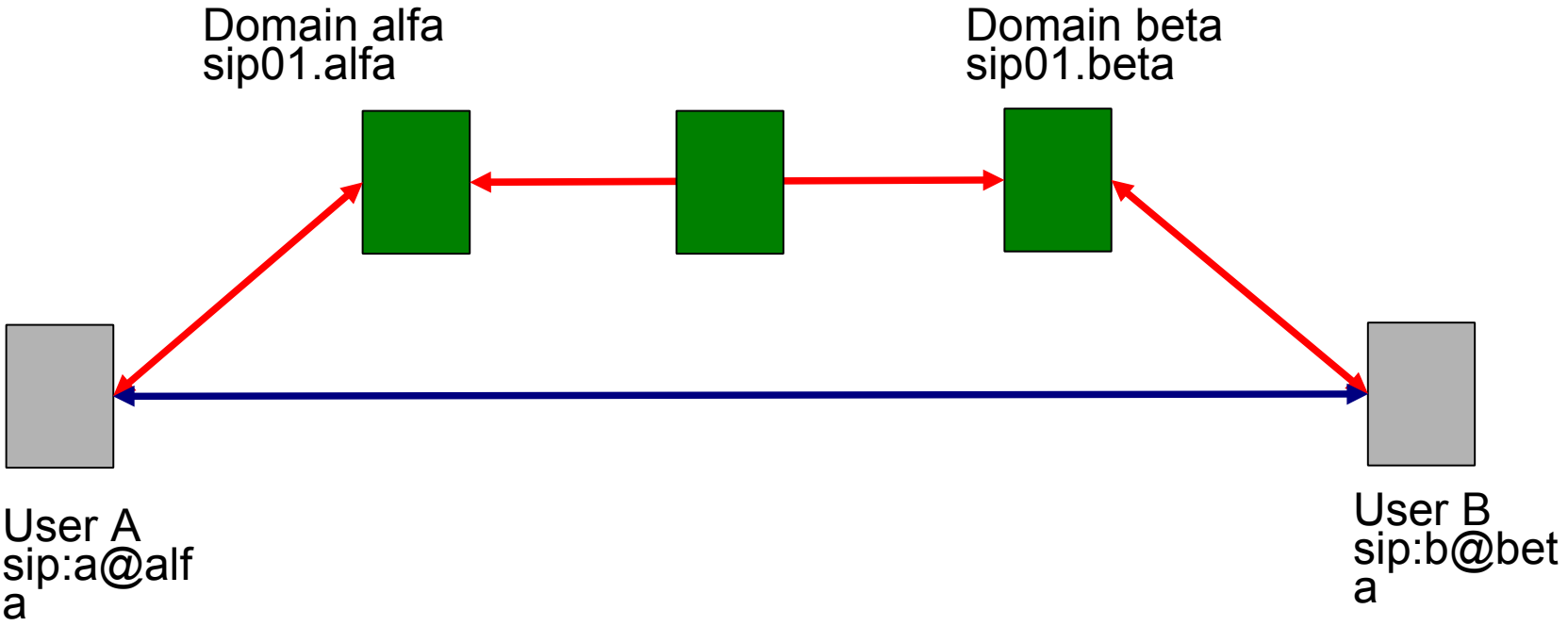
```
INVITE sip:mamut@iptel.org SIP/2.0.
Max-Forwards: 10.
Record-Route: <sip:195.113.222.3;ftag=5DAA94E7;lr=on>.
Via: SIP/2.0/UDP 195.113.222.3;branch=z9hG4bK0a5d.90580ee2.0.
Via: SIP/2.0/UDP 195.113.134.233:5062;branch=z9hG4bK2E1FD348.
CSeq: 262 INVITE.
To: <sip:mamut@iptel.org>.
From: "Franta Vomacka" <sip:bbb@ces.net>;tag=5DAA94E7.
Call-ID: 379332994@195.113.134.233.
Subject: sip:bbb@ces.net.
Content-Length: 234.
User-Agent: kphone/4.2.
Contact: "Franta Vomacka" <sip:bbb@195.113.134.233:5062;transport=udp>.
Remote-Party-ID: "Franta Vomacka" <sip:950070101@ces.net>;party=calling;id-
    type=subscriber;privacy=off; screen=yes.
.
v=0.
o=username 0 0 IN IP4 195.113.134.233.
s=The Funky Flow.
c=IN IP4 195.113.134.233.
t=0 0.
m=audio 33728 RTP/AVP 0 97.
a=rtpmap:0 PCMU/8000.
a=rtpmap:97 iLBC/8000.
```

Troubleshooting

- logy
- ngrep -W byline port 5060
- tethereal -s 1600 -w teth.eth port 5060
- Ethereal →Statistics → VoIP calls



SIP „trapezoid“



- **Enterprise vs. P2P**
- **Autentizace heslem a jiné metody vs. polohou**
- **Identita člověka vs. stroje**
- **Domácí část**
- **Mezidoménová část, i více než jeden krok**

DATA

SIP

Mezidoménová komunikace
zjištění cílové adresy

- **Číslo na Doménu**
  - Lokální pravidla – přepisy
  - ENUM – DNS
  - SIP peering servery
  - OSP,....
- **Doména na IP adresu – DNS RFC3263**
  - NAPTR
  - SRV
  - A,AAAA
- **Příma komunikace versus hierarchie (GDS)**

Co je ENUM

- **Slouží k *mapování* různých adresových a jmenných prostorů mezi sebou**
- **Výchozím prostorem je *prostor telefonních čísel***
- **Cílovým prostorem může být jakékoliv URI (Uniform Resource Indicator)**
- **Využití (v IP telefonii)**
  - Příchozí – ostatní vám mohou volat a vy říkáte „kam“
  - Odchozí - Voláte vy a nemusíte mít každého ve svém lokálním směrovacím seznamu (informaci spravuje držitel čísla)
- **ENUM není telefonování zadarmo**
- **ENUM zlatý důl spammera !?**
  - Držitel čísla zveřejňuje jen to co chce aby bylo vidět
  - Dobře prohledatelný strom (pevné kroky, NXDOMAIN)

Prostory ENUMu

	Veřejný	Privátní
Uživatelský	e164.arpa	nrenum
Operátorský		e164.info

Příklad

- V jmenném serveru pro 5.3.4.2.2.0.2.4.e164.arpa :

```
;;          order pref flags  service       regexp                                  replacement
IN NAPTR 100   50   "u"   "E2U+h323"  "!^\\+420(.*)$!h323:\\1@cesnet.cz!"     .
IN NAPTR 200   50   "u"   "E2U+sip"    "!^\\+420(.*)$!sip:\\1@cesnet.cz!"      .
IN NAPTR 300   50   "u"   "E2U+smtp"  "!^(.*)$!mailto:info@cesnet.cz!“        .
```

- Dotazující SIP klient nebo server provede:

+420224352942 -> 2.4.9.2.5.3.4.2.2.0.2.4.e164.arpa

Obdrží oba výše uvedené záznamy a vybere si dle služby E2U+sip

Aplikováním regulární ho výrazů získá SIP URI
sip:224352942@cesnet.cz

Pomocí SRV záznamů je přesměrován na SIP server ser.cesnet.cz

- RFC 3401-3405, RFC3761, RFC3762, RFC3764, …
- host -t naptr 9.9.4.0.8.6.4.3.2.0.2.4.e164.arpa

Veřejný uživatelský ENUM

- **e164.apra - jeden oficiální strom**
- **Potřeba kritického množství**
- **V ČR v provozu**
- **Okolní země**
  - Rakosko,Německo, Polsko – v provozu
  - Slovensko trial
- **http://crawler.enum.at**
- **http://enumdata.org**

Mezidoménová komunikace
zjištění cílové adresy

- **Číslo na Doménu**
  - Lokální pravidla – přepisy
  - ENUM – DNS
  - SIP peering servery
  - OSP,....
- **Doména na IP adresu – DNS RFC3263**
  - NAPTR
  - SRV
  - A,AAAA
- **Příma komunikace versus hierarchie (GDS)**

Nalezení SIP serveru

- Doménová část URI sip:janru@dom.cz
- RFC3263 Locating SIP servers
- “servisní” NAPTR záznamy

```
;;          order pref flags  service        regexp     replacement

IN NAPTR 1  5  "s"  "SIPS+D2T"  ""  _sips._tcp.dom.cz.
IN NAPTR 2  5  "s"  "SIP+D2T"   ""  _sip._tcp.dom.cz.
IN NAPTR 3  5  "s"  "SIP+D2U"   ""  _sip._udp.dom.cz.
```

NAPTR

- Výchozí URI sip nebo sips – preference volajícího
- NAPTR vyjařuje nabídku a preference voláného
- TLS s nejvyšší prioritou = nejnižší hodnota
- Sip URI je možno „povýšit“ na TLS
- Při selhání je možné využít dalších protokolů – Nikoliv u sips

SRV záznamy

- **RFC 2782**
- **„záznam pro služby” - rozšířené MX**

_sip._udp, _sip._tcp, _sips._tcp, _*sip._tls*

;;			**priority**	**weight**	**port**	**server**
_sip._tcp.dom.cz	IN	SRV	10	0	5060	ser1.dom.cz.
_sip._udp.dom.cz	IN	SRV	10	0	5060	ser1.dom.cz.
_sips._tcp.dom.cz	IN	SRV	10	0	5061	ser1.dom.cz.
_sip._tls.dom.cz	*IN*	*SRV*	*10*	*0*	*5061*	*ser1.dom.cz.* ;M$

_h323ls._udp.dom.cz IN SRV 10 0 1719 gk1.dom.cz.

_h323rs._tcp.dom.cz IN SRV 10 0 1720 gk1.dom.cz.

DNSSEC

- **Nástup DNSSEC – slepice nebo vejce**
- **Informaci je nutné dostat do aplikace**
- **Politika -** Žádný nebo nevalidní DNSSEC záznam = žádná odpověď?
- **Nedostatek knihoven v aplikacích**
  - Vložení DNSSEC resolveru do cesty (BIND, unbound) těsně před službu – na tomtéž stroji
- **Další možná využití**
  - Úložistě certifikátů …
- **Stav v ČR – podepsané .cz i .0.2.4.e164.arpa**

Útoky na infrastrukturu

- **Automaticky „podděděny“ útoky v rámci IP**
  - Útoky na podpůrné systémy - **DNS**
- **Útoky na prvky infrastruktury (DoS, DDoS)**
  - sip servery, brány
  - rychlé vyčerpání některých prostředků například ISDN linky do ústředny
- **Jednoduchost provedení**
  - SIP už sice dávno není jednoduchý, ale stále je dost jednoduchý
- **Ostrovy vs. mezidoménová komunikace**
  - Email také nefunguje jen uvnitř firmy

Útoky na signalizační úrovni

- **Odposlech a skenování**
  - lokalizace komponent a číslovacího plánu
- **DoS, DDoS**
  - využití implementačních chyb nebo jen záplava
- **Odposlech medií**
  - E2E šifrování (SRTP, ZRTP, problematika výměna klíčů)
- **Krádež identity (hesla) a zneužití účtu**

- http://www.voipsa.org
- http://sipp.sourceforge.net/
- http://www.tech-invite.com

Útoky na signalizační úrovni

- **příklady**
  - Převzetí či ukončení registrace
  - Pozměnění či ukončení hovoru
  - Podvržení identity (Caller ID)
  - Upravení SDP

Registrace

REGISTER sip:cesnet.cz SIP/2.0.
Authorization: Digest username="user", uri="sip:cesnet.cz",
algorithm=MD5, realm="cesnet.cz",
nonce="43eeaeb76e6eeaeffbc7d4f4018aad59c5d282a",
response="9e83c39e8a7262901
Via: SIP/2.0/UDP
195.178.64.172:49252;branch=z9hG4bK.32f02bf2;rport.
From: sip:user@cesnet.cz;tag=6c2c90b8.
To: sip:user@cesnet.cz.
Call-ID: 1814859960@195.178.64.172.
CSeq: 2 REGISTER.
Content-Length: 0.
Max-Forwards: 70.
Expires: 15.
Contact: sip:user@a.b.c.d:1234.

INVITE

INVITE sip:mamut@iptel.org SIP/2.0.
Max-Forwards: 10.
Record-Route: <sip:195.113.222.3;ftag=5DAA94E7;lr=on>.
Via: SIP/2.0/UDP 195.113.222.3;branch=z9hG4bK0a5d.90580ee2.0.
Via: SIP/2.0/UDP 195.113.134.233:5062;branch=z9hG4bK2E1FD348.
CSeq: 262 INVITE.
To: <sip:mamut@iptel.org>.
Content-Type: application/sdp.
From: "Franta Vomacka" <sip:bbb@ces.net>;tag=5DAA94E7.
Call-ID: 379332994@195.113.134.233.
Subject: sip:bbb@ces.net.
Content-Length: 234.
User-Agent: kphone/4.2.
Contact: "Franta Vomacka" <sip:bbb@195.113.134.233:5062;transport=udp>.
Remote-Party-ID: "Franta Vomacka" <sip:950070101@ces.net>;party=calling;id-
type=subscriber;privacy=off; screen=yes.
.
v=0.
o=username 0 0 IN IP4 195.113.134.233.
s=The Funky Flow.
c=IN IP4 **195.113.134.233**.
t=0 0.
m=audio **33728** RTP/AVP 0 97.
a=rtpmap:0 PCMU/8000.
a=rtpmap:97 iLBC/8000.

ACK BYE

ACK sip:234680499@147.32.240.25:5060 SIP/2.0.
Via: SIP/2.0/UDP 195.113.150.170:5060; branch=z9hG4bK-62fa494f.
From: "janru" <sip:janru@cesnet.cz>;tag=d71ce015c904084do0.
To:<sip:234680499@cesnet.cz>;tag=fcbce42a-a00c-4e6e-9208-8d4aafa39602-25051818.
Call-ID: 21bf1b5-b267232d@195.113.150.170.
CSeq: 102 ACK.
Max-Forwards: 70.
Route: <sip:195.113.144.245;ftag=d71ce015c904084do0;lr=on>.
Contact: "janru" <sip:janru@195.113.150.170:5060>.
User-Agent: Linksys/SPA942-6.1.5(a).
Content-Length: 0.

BYE sip:234680499@147.32.240.25:5060 SIP/2.0.
Via: SIP/2.0/UDP 195.113.150.170:5060; branch=z9hG4bK-1cfe22de.
From: "janru" <sip:janru@cesnet.cz>; tag=d71ce015c904084do0.
To:<sip:234680499@cesnet.cz>; tag=fcbce42a-a00c-4e6e-9208-8d4aafa39602-25051818.
Call-ID: 21bf1b5-b267232d@195.113.150.170.
CSeq: 103 BYE.
Max-Forwards: 70.
Route: <sip:195.113.144.245; ftag=d71ce015c904084do0;lr=on>.
User-Agent: Linksys/SPA942-6.1.5(a).
Content-Length: 0.

RTP manipulace

```
v=0
o=- 0 2 IN IP4 158.196.192.32
s=CounterPath Bria
c=IN IP4 158.196.192.32
t=0 0
m=audio 58940 RTP/AVP 0 8 3 101
a=sendrecv
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:3 GSM/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

```
v=0
o=- 0 2 IN IP4 195.113.113.147
s=CounterPath Bria
c=IN IP4 195.113.113.147
t=0 0
m=audio 57890 RTP/AVP 0 8 3 101
a=sendrecv
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:3 GSM/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

Pozor na hodnotu Content-Length

SPIT

- **Hovory, IM, Prezence**
- **Hovor = zvonění telefonu, které okamžitě vyruší**
  - Mail „jen“ spadne do schránky
- **ZATÍM není moc vidět**
  - Ostrůvky
  - Cena je vyšší než u emailu, ale nižší než PSTN, některé typy ochrany lze překonat botnety.
  - Důležité je nezaspat – nesmíme se dostat do situace, jaká je u mailu, ale uzavřené ostrůvky nejsou řešení.
- **IETF EG – RUCUS**
  - Průzkum navrhovaných metod a standardizace těch efektivních
- **RFC5039 SIP s SPAM**

CESNET

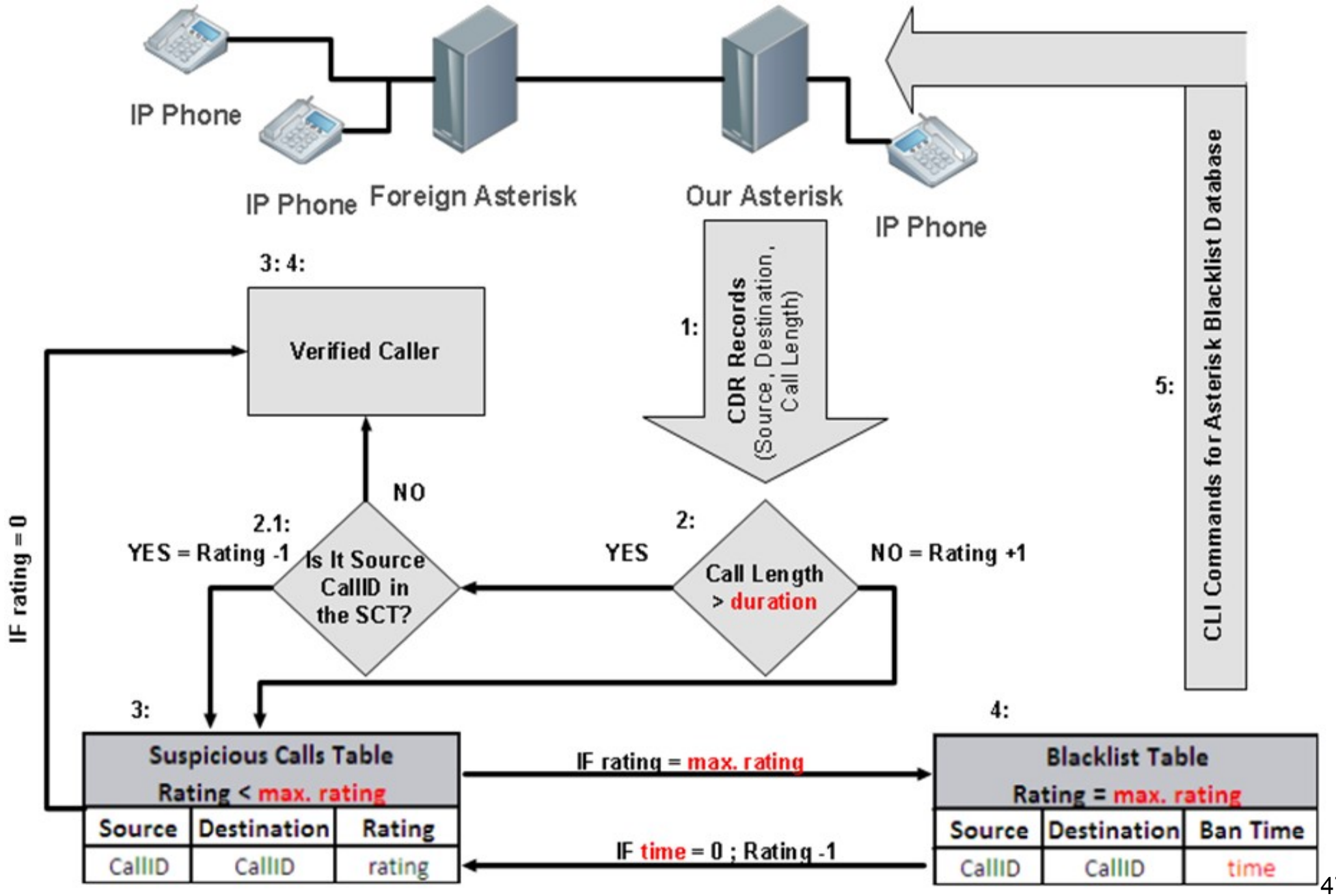
Metody obrany

- **Podstata komunikace v reálném čase**
  - Odložení do fronty je problém
  - Obrana vs. možné omezení dostupnosti služby
- **Whitelisty, Blacklisty, Greylisty ...**
- **Problém počátečního představení iniciátora**
- **Interakce s uživatelem**
  - CAPTCHA (IVR),
  - výpočetní zátěž – problém poměru výkonu zařízení
  - mikroplatby
- **Silná identita jako podmínka fungování předchozích bodů pro následnou komunikaci**
- **Centralizovaná architektura jako u PSTN**

Metody obrany II

- **Silná = důvěryhodná identita**
- **Domácí část - první krok**
  - nahrazení či zabalení HTTP Digest
  - TLS – perzistentní spojení - „obálka“, nutně nemusí být klientské certifikáty, chrání i odpovědi
- **Mezidoménová identita – obdoba DKIM**
  - TLS – Hop By Hop – omezené na 1 skok
  - P-Asserted-Identity je nedostačující
  - SIP Identity (RFC4474) a SIP SAML
  - Princip vložení doménového podpisu

AntiSPIT and its implementation into Asterisk



SIP identity

- **Persistentní SIP hlavičky podepsány hraničním SIP elementem**
- **Ověřitelná identita přes více skoků bez nutnosti důvěry mezi skoky**
- **Pro vložení je třeba**
  - Definova sadu hlaviček (RFC) – rozšiřitelnost?
  - Politiky – kdo může podposi vložit
  - Zabezpečený první skok - TLS.
- **Nejen cílová proxy může ověřit identitu**
- **Problémy**
  - Jen pro odpovědi
  - Čísla (nemají jednoznačnou vazbu na doménu)

SIP identity II

- **Zajímavé hlavičky**

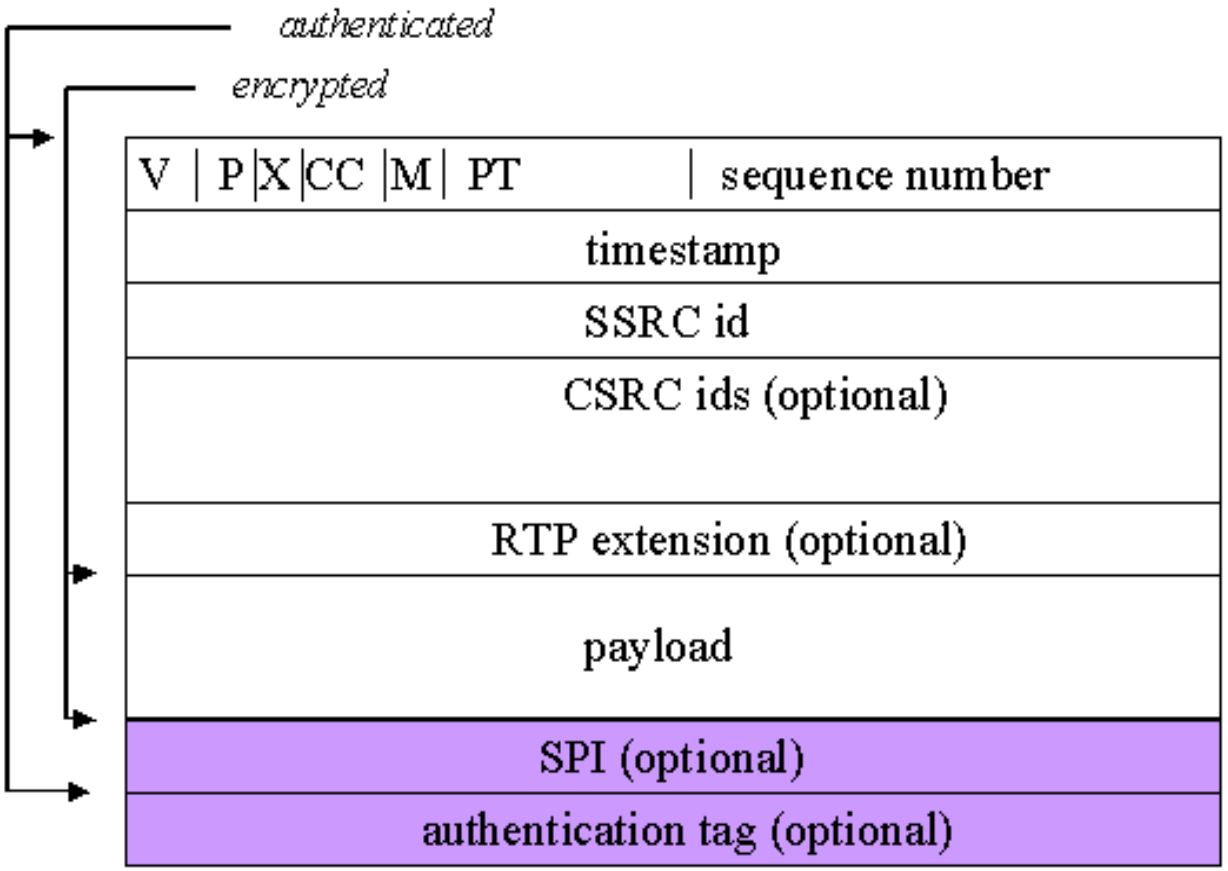
```
sip:alice@atlanta.example.com|sip:bob@biloxi.example.org|a84b4c76e66710|
314159 INVITE|Thu, 21 Feb 2002 13:02:03 GMT|alice@pc33.atlanta.example.com|
v=0
  o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com
  s=Session SDP
  c=IN IP4 pc33.atlanta.example.com
  t=0 0
  m=audio 49172 RTP/AVP 0
  a=rtpmap:0 PCMU/8000
```

- **Vložený podpis**

```
Identity:"kjOP4YVZXmF0X3/4RUfAG6ffwbVQepNGRBz58b3dJq3prEV4
      h5GnS4F6udDRCI4/rSK9cI+TFv45nu0Qu2d/0WPPOvvc3JW
          wuUmHrCwGwC+tW7fOWnC07QKgQn40uwg57WaXixQev5
          N0JfoLXnO3UDoum89JRhXPAIp2vffJbD4="
Identity-Info: <https://atlanta.example.com/atlanta.cer>;alg=rsa-sha1
```

SRTP

- **Rozšíření RTP**
  - Důvěrnost
  - Autenticita



Distribuce master klíče

- **Přímo v SDP SDES RFC4568**
  - a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:WbTBosdVUZqEb6Htqhn+m3z7wUh4RJVR8nE15GbN
  - Slabě nebo vůbec nechráněno
  - TLS? Jen Hop by hop
- **MIKEY RFC3830**
  - E2E bezpečnost
  - Jednoduše a efektivně (málo pásma, kódu, zátěže, kroků komunikace – Initiator I a Responder R Message)
  - Možnost tunelování (vnoření do sestavení spojení, SDP)
  - Nezávislost na transportním protokolu nižší vrstvy
- **ZRTP**

ZRTP

- **DH**
- **Krátký autentizační kód SAS**
- **Hash přes utajované hodnoty a krátký kód**
- **Hodnota použita jen jednou a část uložena pro forward secrecy**
- **Ochrana pro MitM**
- **Postup**
  - Detekce podpory ZRTP
  - Výměna symetrických klíčů
  - Přepnutí do SRTP

Děkuji za pozornost

Diskuze