TEKELEC

SIP: More Than You Ever Wanted To Know About

Jiri Kuthan, Tekelec

Dorgham Sisalem, Tekelec

March 2007

All statements are authors' and may or may not be shared by his company.

TEKELEC

Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

Outline

- About This Tutorial
- Introduction: Why SIP and SIP History.
- Where SIP Was Born: IETF Standardization
- Introduction to SIP Protocol
  - SIP Architecture
  - SIP Servers, ENUM
  - SIP Message Elements
- BCPs:
  - QoS
  - NATs and Firewalls
  - PSTN
- RTP – Multimedia Protocol
- SIP Security
- SIP Services
- Black-belt SIP
- Self-education
  - Get your hands on SER
  - Self-test
  - References
- IMS

About This Tutorial

Intended Audience

- Whoever wishes to gain basic technical knowledge of SIP protocol: administrators, developers, integrators, CS students.
- Basic knowledge of TCP/IP networks desirable.
- Out-of-scope: detailed developer-level, business aspects.

About Authors

Jiri Kuthan

- 1998: Graduated in CS from U. of Salzburg, Austria
- 1995-1998: Internship and thesis in Berlin, Germany, FhG Fokus
- 1999-2004: Affiliated as researcher in Fokus; publishing VoIP publications; involved in the IETF standardization; released world's leading SIP proxy, SIP Express Router, with his FhG team in 2002
- 2004: co-founded iptelorg which was acquired in 2005 by Tekelec
- 2005: assumed AVP/engineering position in Tekelec

Dorgham Sisalem

- 1995: Graduated in EE from Technical University of Berlin, Germany
- 1995-2005: Researcher and later department leader whose work resulted in scientific publications related to QoS, VoIP and security and being widely quoted by scientific community
- 2000: Obtained PhD from TU Berlin
- 2002: co-founded iptel.org project which later incorporated into iptelorg
- 2005: assumed position of Director Strategic Architecture in Tekelec

Acknowledgments

- The following persons provided additional material and/or feedback:
  - Raphael Coeffic, Tekelec (QoS)
  - Cristian Constantin, Tekelec (sigcomp)
  - Nils Ohlmeier, Tekelec
  - Henning Schulzrinne, Columbia University

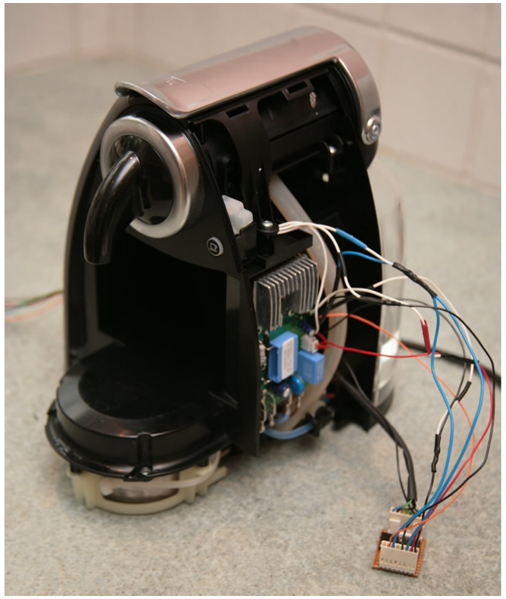
Copyright Notice

- Authors: Jiri Kuthan, Dorgham Sisalem; Tekelec
-

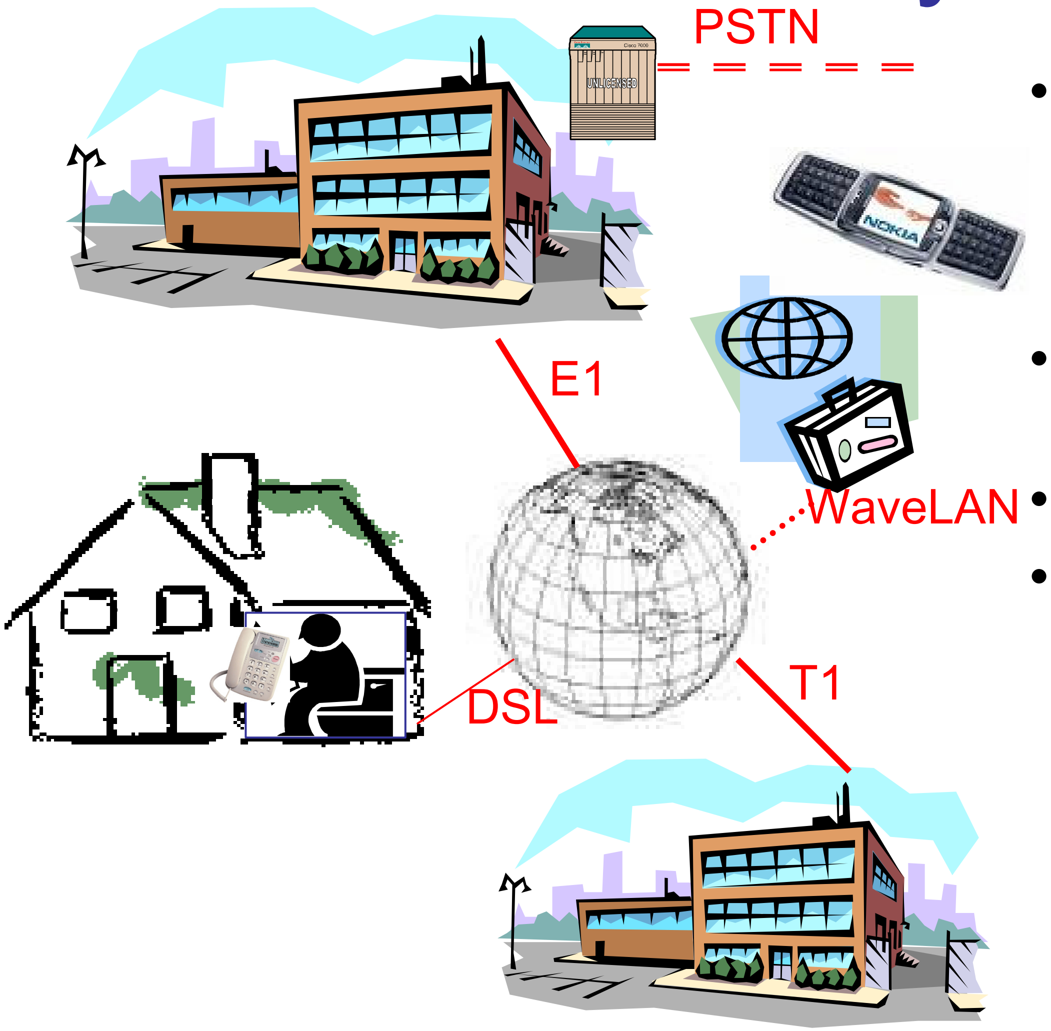
Introduction: Why SIP?

What Is SIP? Depends on Who You Are…

- **Visionary**: missing piece for running **all over IP**, including your browser, telephone and coffee machine. Richer user interface than PSTN. (Quake via DTMF just doesn't work.) Productivity/collaboration applications. Work from anywhere.
- **VP for Business Development**: technology for **all-IP**-based telephony that allows integration with Internet services and surpassing investment barriers
- **CFO:** reduction of costs by running homogenous **all-IP** technology.
- **Techie**: HTTP-like protocol specified in RFC3261 and associated standards and running similarly like Email runs over **all-IP**.



… but it is always about **ALL-IP.**



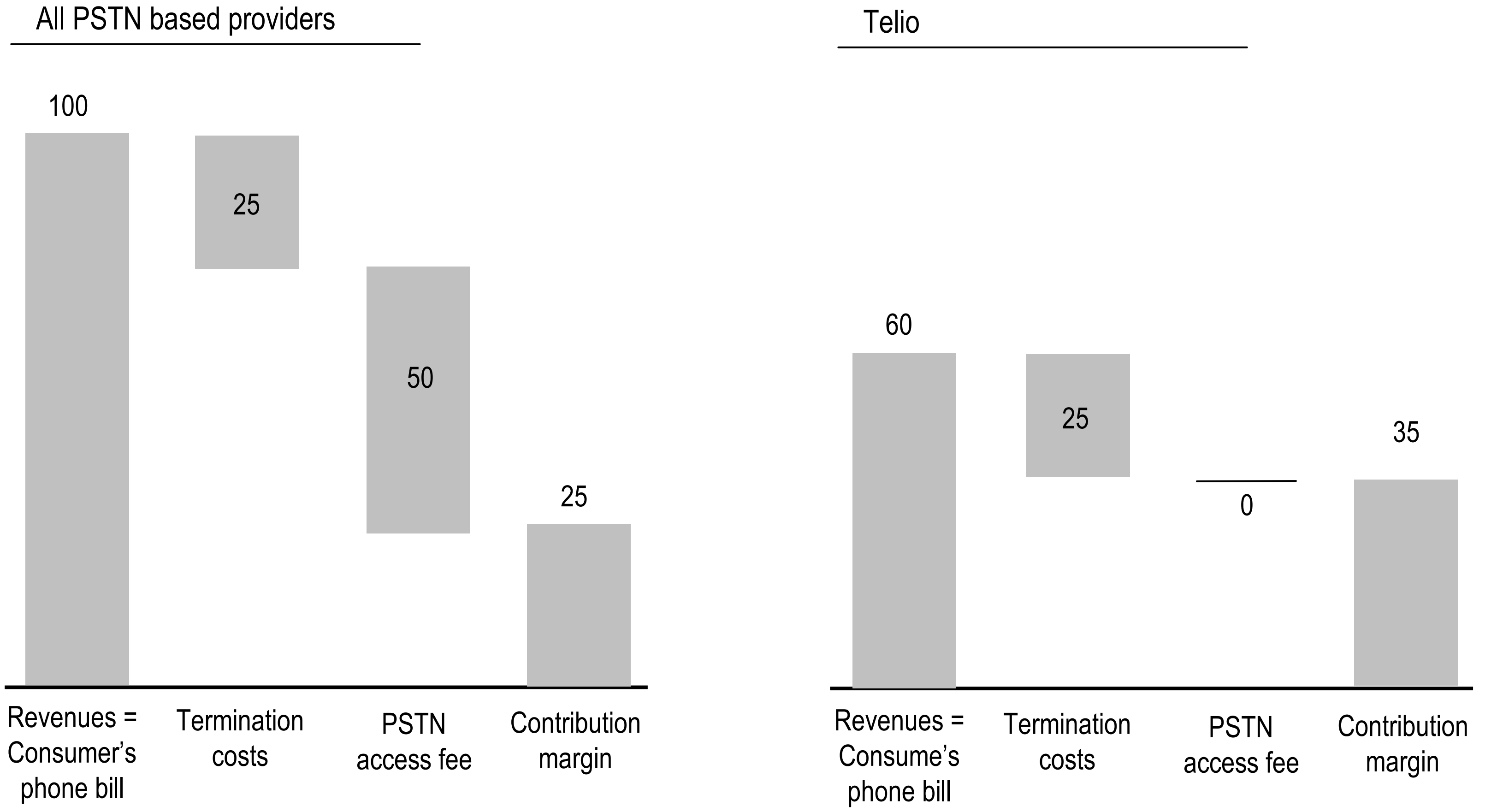
- Services available to all users, on-site, off-site, multi-site, underway, home-working, office-working.
- Single infrastructure for data and voice.
- Effectiveness tools.
- Service operation can be outsourced in a Centrex-like manner. Like with web/email, single server may host multiple domains for better efficiency.

Why to SIP?

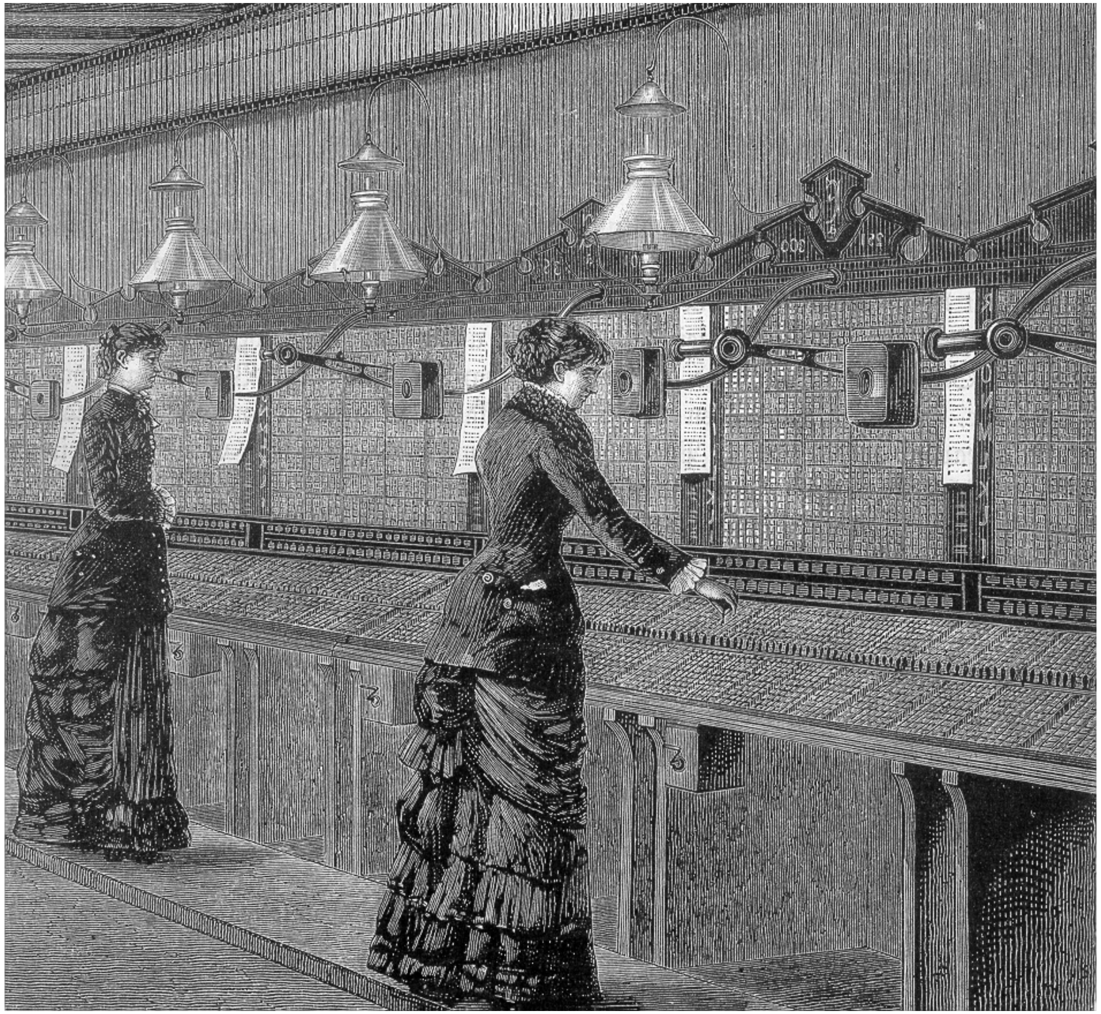
- Challengers:
  - All-IP nature opens up competition space and removes investment barriers.
- Incumbents: isn’t VoIP a cannibalization threat?
  - No – it is a Darwinist test in that well-adapting species profit of clime changes whereas the others disappear.
  - What’s the adaptation chance: running homogenous all-IP networks greatly **reduces cost and increases competitiveness**. If I was an incumbent, I would pay most attention to key assets: access, identity, retail capability.
  - Attacking other market segments like challengers do.
- Why not skype^{TM}?
  - That’s a single party game: too few devices because of proprietary technology and reportedly the only party to make $ with skype is skype.

Background Info: Cost-Saving

Advantage in Cost Structure – material provided courtesy of telio.no (2003)

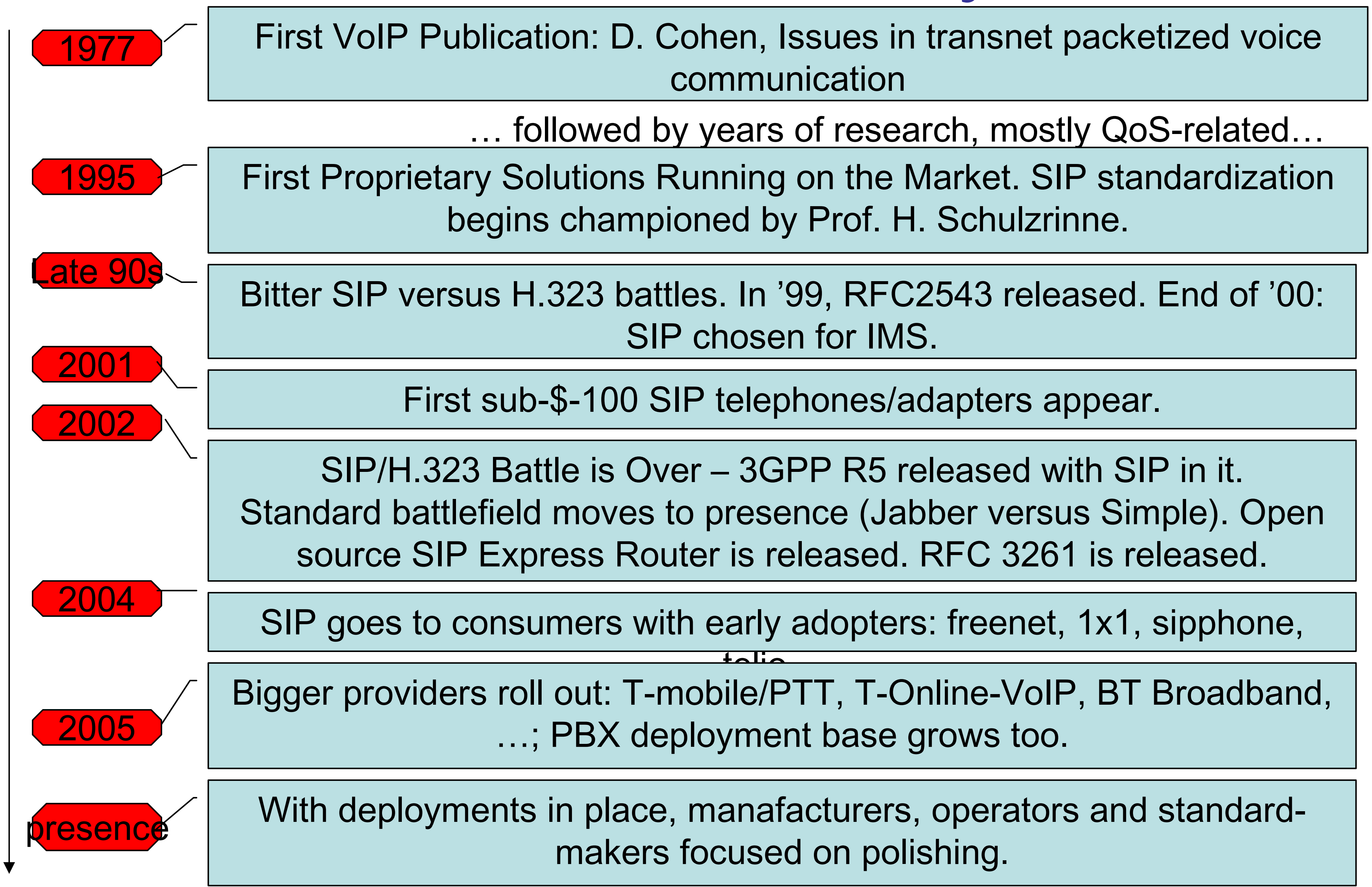


Pre-IP Telephone Systems



- Telephony began to be known in 70s of the 19’s century. Invention authorship subject to controversies.
- Picture: telephone operators in 1881 in Milan.

30 Years of VoIP History



1977 — First VoIP Publication: D. Cohen, Issues in transnet packetized voice communication

… followed by years of research, mostly QoS-related…

1995 — First Proprietary Solutions Running on the Market. SIP standardization begins championed by Prof. H. Schulzrinne.

Late 90s — Bitter SIP versus H.323 battles. In ’99, RFC2543 released. End of ’00: SIP chosen for IMS.

2001 — First sub-$-100 SIP telephones/adapters appear.

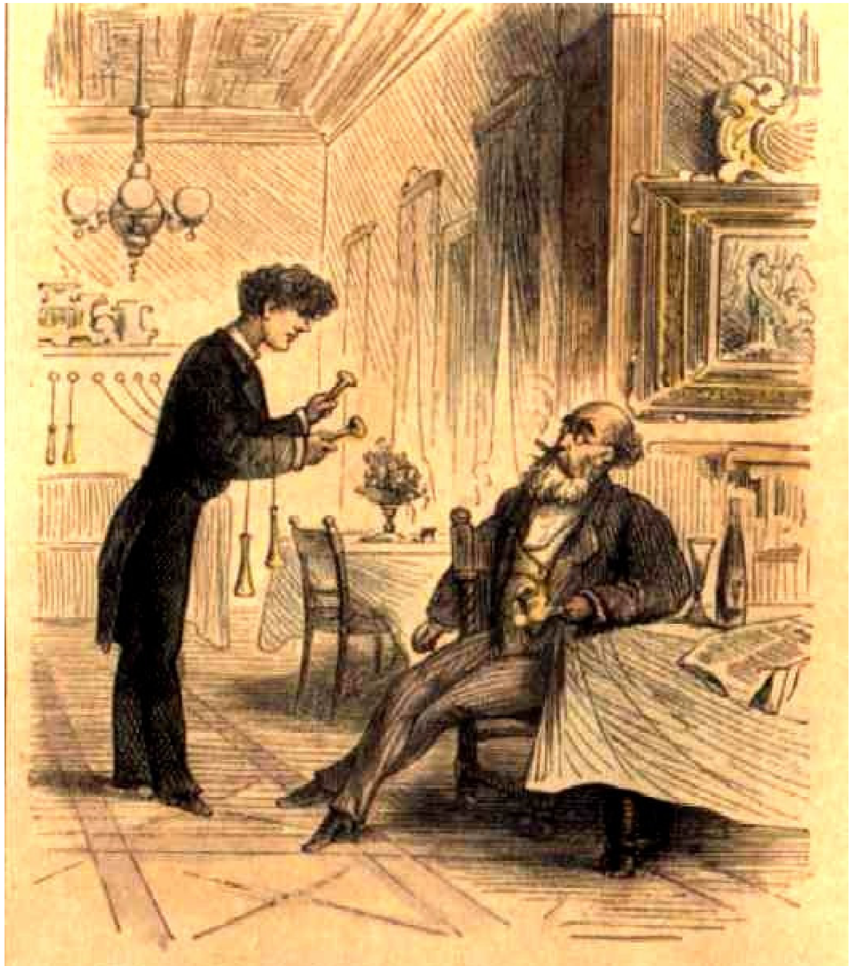
2002 — SIP/H.323 Battle is Over – 3GPP R5 released with SIP in it. Standard battlefield moves to presence (Jabber versus Simple). Open source SIP Express Router is released. RFC 3261 is released.

2004 — SIP goes to consumers with early adopters: freenet, 1x1, sipphone, telio

2005 — Bigger providers roll out: T-mobile/PTT, T-Online-VoIP, BT Broadband, …; PBX deployment base grows too.

presence — With deployments in place, manafacturers, operators and standard-makers focused on polishing.

Future of The Phone (1870)



Kellner: In unſer Hotel münden Telephons aus allen Theatern der Stadt! Soeben beginnt die Oper „Budha“, von Rich. Wagner, im Hoftheater. Wünſchen Sie ein Telephon, es koſtet nur 60 Pfennig.

- Carl Stauber.
- Waiter: “Our hotel is connected to all theaters in town. The opera "Budda" by Richard Wagner is just starting in the Hoftheater.”

(picture found courtesy of Henry Sinnreich in a Prague historical book-shop)

2007 – Where Are Thou Really?

- **Construction is Over – Operation Began, Perfection on Agenda**

Pre 2006

2006 and later…

Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

SIP Works Fine in 2007

- Working standardized technology for running Telephony over the Internet (and in the future more real-time applications, such as messaging, gaming, etc.)
- We have today a variety of interoperable equipment:
  - clients: hardphone (snom, cisco, mitel, nortel, avaya, ….), softphones (microsoft, counterpath, …), dual phones (Nokia), IADs (linksys, AVM), terminal adapters (Sipura)
  - Gateways: Tekelec, Cisco, Sonus, …
  - Servers: Tekelec/iptelorg, Oracle/hotsip, Ubiquity/Avaya, ...
- Server providers: ISPs (T-Online, Earthlink), ASPs (sipphone, vonage), fixed-mobile-c ence providers (telio

SIP Gaps in 2007

- Operator’s Concerns:
  - Setting up a network still takes integration effort.
  - Operation is not yet effort-less either – next product generating featuring automation of common processes, automated security audits, and troubleshooting aids yet to come.
  - Regulatory aspects still moving target.
  - Reliability sub-nine-fives. (IP availability, NATs, immature practices)
- Visionary Concerns:
  - New applications still rare.
  - Security: we shall really not allow being flooded with spam like with E-mail. Or would you like a 3 AM call from a tele-marketeer from other continent?
- Learner’s Concern: The standards have grown too fat.

Summary of Introduction

- SIP as of today (2007) is mature all-IP technology in polishing stage which is in wide use with an array of equipment from various vendors.
- Today’s ISP/ASP market is moving to mobile markets.
- The cost-saving promise holds, applications are coming slowly.
- Key challenges of adopters: integration effort.

IETF Standardization

Where SIP Was Born

- IETF (www.ietf.org) is a standardization body which has created a large variety of Internet protocols: TCP/IP for interconnection, SMTP for E-email, FTP for data transfer, RTP for voice, etc.
- Participation is open: typically folks from both data and telecom industry participate, so do folks from academia. Contribution coming from individuals (as opposed to companies).
- In the past years, the IETF is reinventing itself and dealing with its increased size and entrance to maintenance mode.
- SIP-related work grouped in RAI area.

Related IETF Working Groups

Core Specs

SIPPING
New work filter to SIP

SIP
Core signaling protocol spec.

AVT
Voice and RT transport

Supporting Specs

mmusic
Conferencing utilities

iptel
Supporting protocols

ENUM
Convergence of IP/PSTN Numbering

ECRIT
+
IEPREP
Emergency Calls

Apps

simple
Presence

xcon
Supporting protocols

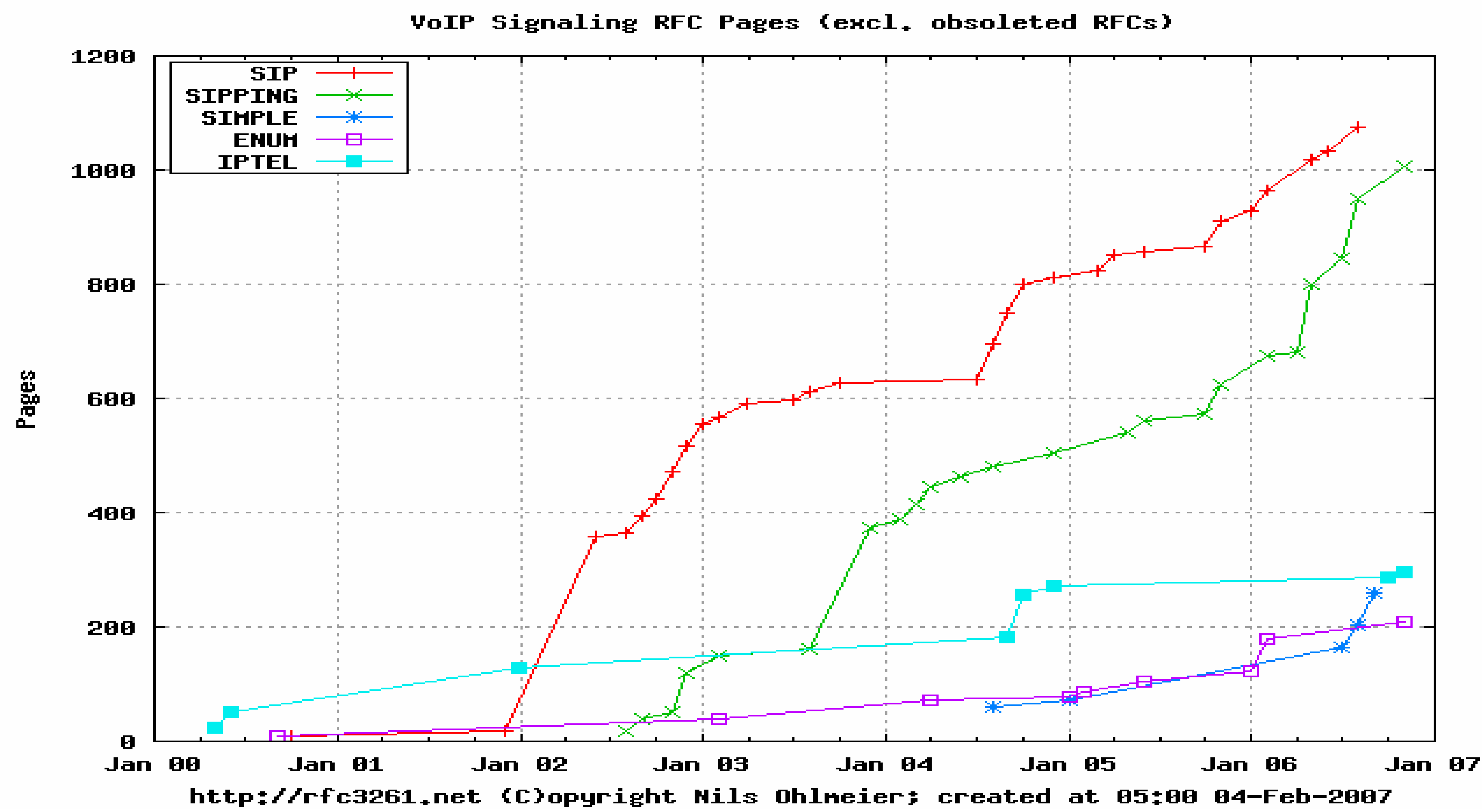
Newcomers and Identity-seekers

spearmint
Peering
(what is it really?)

SIP P2P
To be defined

Retired:
Mostly related to PSTN interop (sigtran, Megaco, pint, spirits) and QoS (diffserv, rsvp)

‘S’ in SIP Doesn’t Stand for Simple



Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

draft-ietf-sip-hitchhikers-guide

First Aid: “Hitchhiker’s Guide to Galaxy”

- SIP WG’s document that aligns all pieces of the SIP puzzle in a single picture
- Internet-draft tag: draft-ietf-sip-hitchhikers-guide
- Refers to the following group of documents: *Core SIP Specifications, PSTN Interworking, General Purpose Infrastructure Extensions, Minor Extensions, Conferencing, , Call Control Primitives, Event Framework and Packages, Quality of Service, Operations and Management, SIP Compression, SIP Service URIs, Security Mechanisms , Instant Messaging and Presence, Emergency Services*.
- Read it to get comprehensive view of the “whole picture”
- Refers to 100+ documents! (If you really need to get a list of those that matter, hire me as consultant ☺)

Introduction to SIP Architecture

-Basic Call Flow

-Architectural Fundaments

-Protocol Puzzle

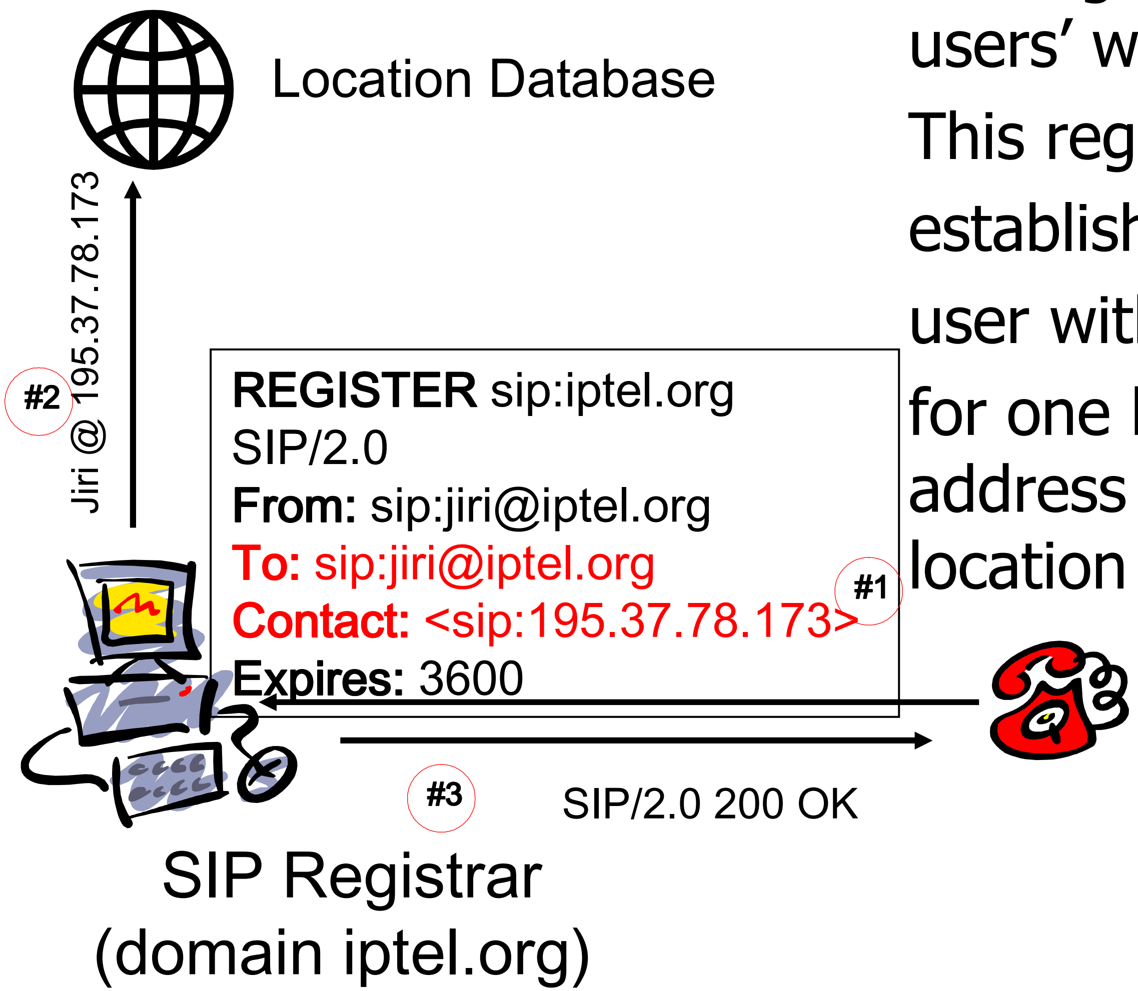
Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

User Viewpoint: SIP End-devices

- User Agent (user application)
  - UA Client (originates calls)
  - UA Server (listens for incoming calls)
- Types of UAs:
  - Softphone, hardphones, webphones
  - Messaging clients
  - Automat: PSTN gateways, media ser ail)
  - Etc.

Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

First Step When Your Phone Boots Up



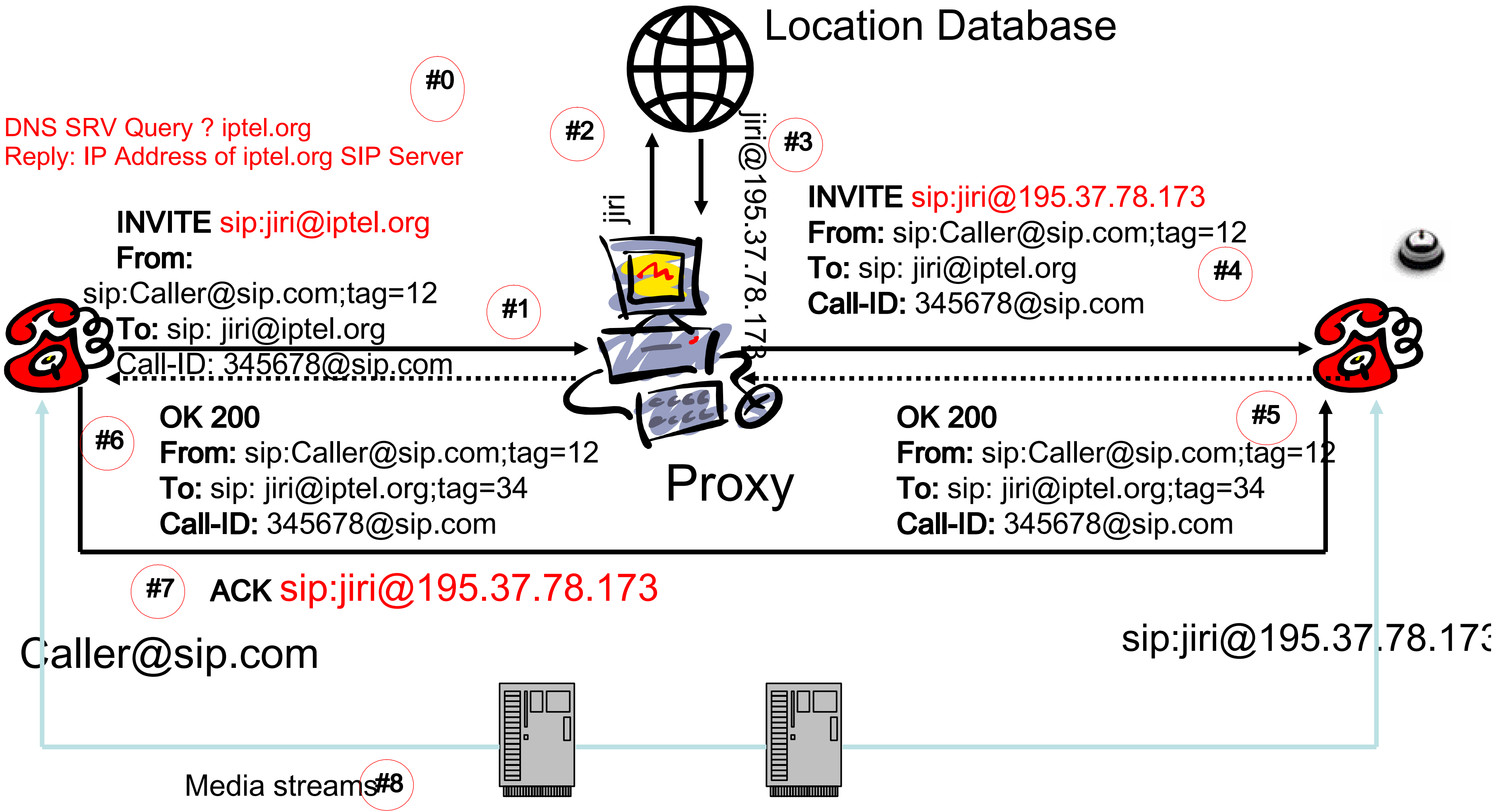
REGISTER sip:iptel.org SIP/2.0
From: sip:jiri@iptel.org
To: sip:jiri@iptel.org
Contact: <sip:195.37.78.173>
Expires: 3600

SIP registrar keeps track of users’ whereabouts.

This registration example establishes presence of user with address jiri@iptel.org for one hour and binds this address to user’s current location 195.37.78.173.

Basic SIP Call-Flow (Proxy Mode)

SIP Proxy looks up next hops for requests to served users in location database and forwards the requests there.



DNS SRV Query ? iptel.org
Reply: IP Address of iptel.org SIP Server

INVITE sip:jiri@iptel.org
From: sip:Caller@sip.com;tag=12
To: sip: jiri@iptel.org
Call-ID: 345678@sip.com

INVITE sip:jiri@195.37.78.173
From: sip:Caller@sip.com;tag=12
To: sip: jiri@iptel.org
Call-ID: 345678@sip.com

OK 200
From: sip:Caller@sip.com;tag=12
To: sip: jiri@iptel.org;tag=34
Call-ID: 345678@sip.com

OK 200
From: sip:Caller@sip.com;tag=12
To: sip: jiri@iptel.org;tag=34
Call-ID: 345678@sip.com

ACK sip:jiri@195.37.78.173

RFC1958
RFC2775

Refresher: IP Design Concepts

- **Distributed end-2-end design***
- Intelligence and states resides in end-devices
- Network maintains almost zero intelligence (except routing) and state (except routing tables).
- End-devices speak to each other using whatever applications they have. There is almost no logic in the network affecting this behavior.
- Result:
  - Flexibility. Introducing new applications is easy.
  - Failure recovery. No state, no problem on failure.
  - Scalability. No state, no memory scalability issues.

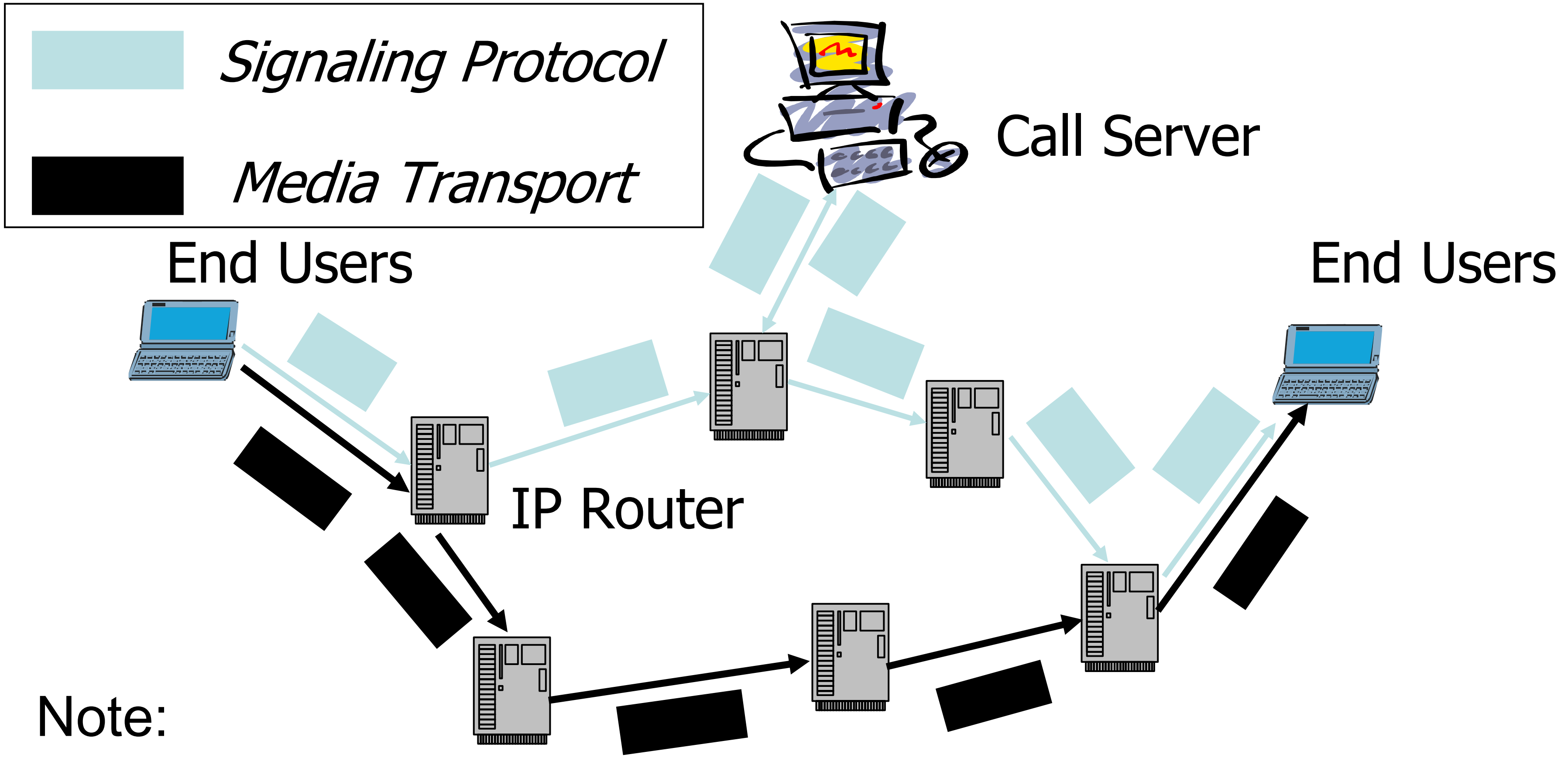
* Manifested in Saltzer-Reed-Clark: End-to-end Arguments in System Design; MIT; 1984

draft-rosenberg-sipping-sip-arch
(expired)

SIP Architecture Borrows at the Application Layer!

- To **scale well** and **easily recover** from a failure core network infrastructure is kept dumb: SIP servers keep minimum possible state. Consequently, a great deal of intelligence resides in end-devices. (existing examples: call waiting, video, encryption)
- **Low cost** of introduction of new services: SIP servers are largely unaware of the applications: they set up sessions for audio, video, gaming, what-have-you
- Make **evolution sustainable**: Individual functions are served by separate protocols: signaling by SIP, media by RTP, interdomain by DNS, etc. Consequently, signaling takes a different path than media!

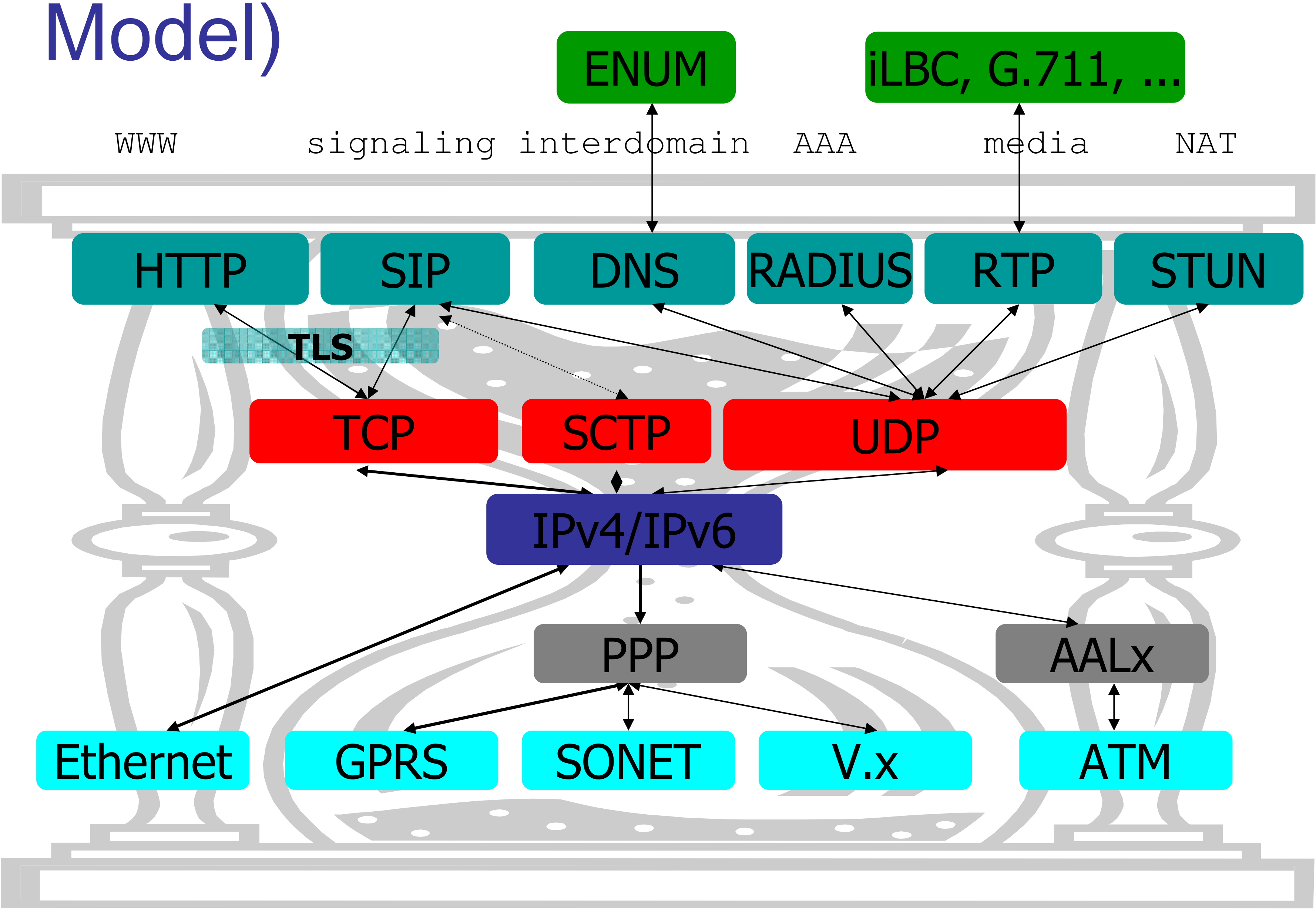
Packetized Communication



Note:

- Every packet may take a completely different path
- Signaling takes typically different path than media does
- Both signaling and media as well as other applications (FTP, web, email, …) look “alike” up to transport layer and share the same fate

All-IP Protocol Zoo (Hourglass Model)



Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

SMTP and HTTP/SMTP Legacy

- SIP is text-oriented protocol – easy to extend and debug
- The world is split in administrative domains with DNS names … foobar.com, foobar.de, etc.
- Digest authentication and TLS used for security.
- Addresses are described using URIs.
- Etc.

```
REGISTER sip:iptel.org SIP/2.0
Via: SIP/2.0/UDP 212.146.78.122
To: <sip:bogc@iptel.org>
CSeq: 671993 REGISTER
User-Agent: Asterisk PBX
Contact: <sip:s@212.146.78.122>
```

Northpole.com

Paris.com

Hawai.com

Yahoo.com

sip:jiri@iptel.org

Protocol Puzzle

- Session management
  - Users may move from terminal to terminal with different capabilities and change their willingness to communicate
  - To set-up a communication session between two or more users, a **signaling protocol** is needed: **Session Initiation Protocol** (SIP) supports locating users, session negotiation (audio/video/instant messaging, etc.) and changing session state
- Media Transport
  - Getting packetized voice over lossy and congested network in real-time
  - **RTP** – protocol for transmitting real-time data such as audio, video and games
- End-to-end delivery: underlying IP connects the whole world

Supporting Protocols: How Do I …

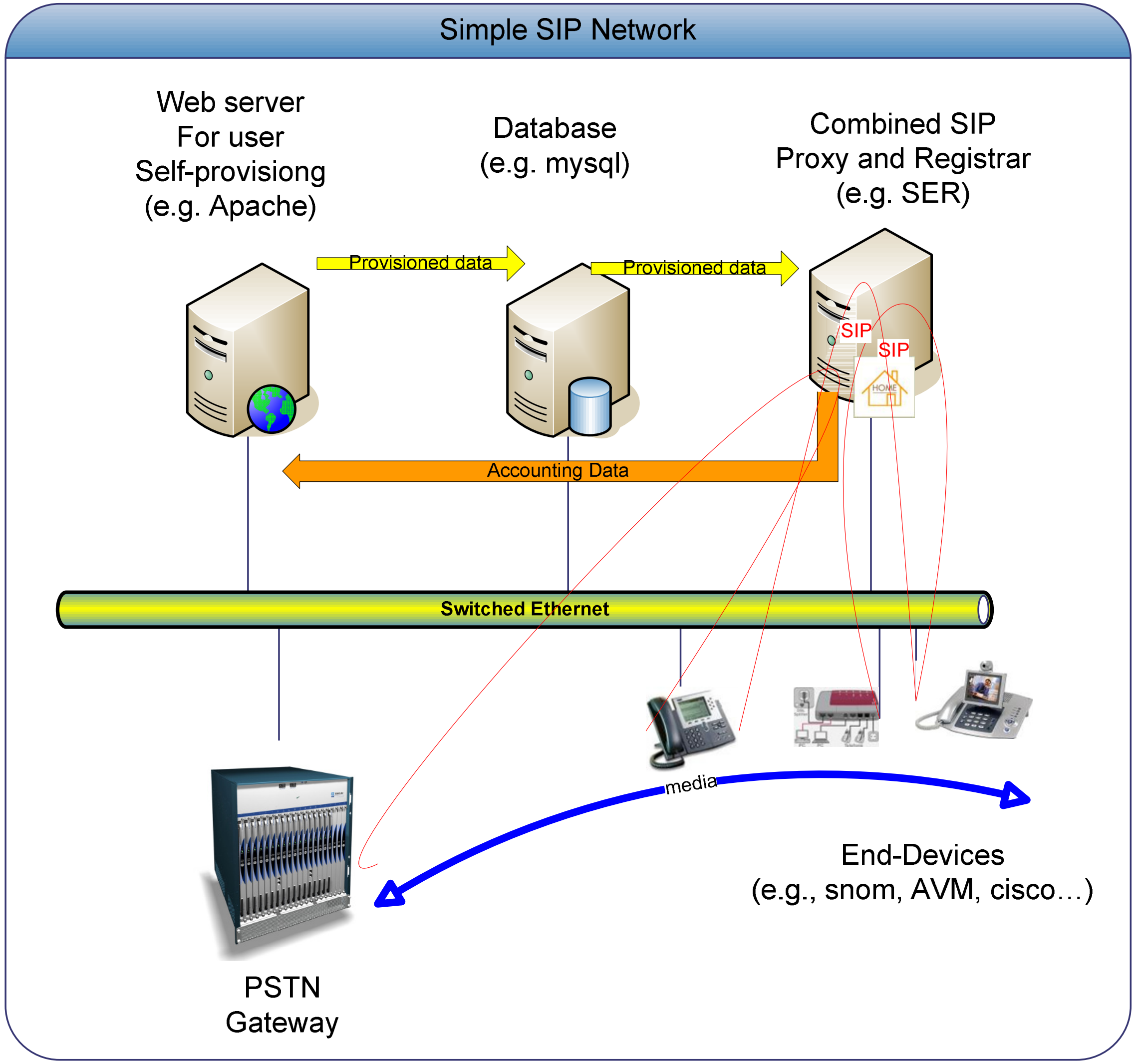
- … find domain of called party? Like with email, use DNS to resolve address of server responsible for jiri@iptel.org!
- … authenticate users and generate Call Detail Records? De-facto RADIUS standard.
- … get over NATs? STUN.
- More:
  - … set phone clock: NTP
  - … download configuration and firmware: TFTP/FTP/HTTP (no good standard for usage of these protocols)
  - … resolve phone numbers to SIP addresses? ENUM
- IETF Practice: Decomposition Principle; Separate protocols are used for separate purposes. All of them on top of IP.

Given All Supporting Protocols are In Place, What Do I need on SIP Part?

- SIP Registrar
  - accept registration requests from users
  - maintains user’s whereabouts at a Location Server (like GSM HLR)
- SIP Proxy Server
  - relays call signaling, i.e. acts as both client and server
  - operates in a transactional manner, i.e., it keeps no session state
  - transparent to end-devices
  - does not generate messages on its own (except ACK and CANCEL)
  - Allows for additional services (call forwarding, AAA, forking, etc.)
- SIP Redirect Server
  - redirects callers to other servers
  - Used rather rarely as operators appreciate staying in communication path. May be used to achieve very scalable load distribution.

All of these elements are logical and are typically part of a single server!

Example SIP Network



Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

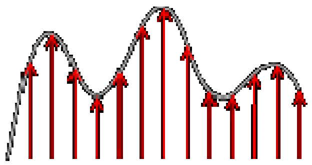
Summary of Introduction to SIP Architecture

- SIP relies un underlying end-to-end architecture
  - Most intelligence located in end-devices (similar trend like in mobile industry); networks remains fast-and-simple for better robustness
  - Every simple task in the puzzle is addressed by a single special-purpose protocol: SIP for signaling, RTP for voice, etc.
  - Adding a new SIP application does not take change to network infrastructure – SIP servers relay any application requests they receive
- Key components of SIP network:
  - SIP Phones (User-Agents)
  - SIP Servers (registrar+proxy+redirect; usually combo)
  - SIP PSTN gateways
  - Applications servers (such as media servers)

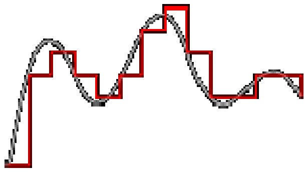
RTP: Multimedia Communication

IP Based Multimedia Communication

- Audio/Video samples are digitized, compressed and sent in UDP packets
- Compression schemes use limitations of human ears/eyes to reduce bandwidth



Discrete sample signal



Digital Signal

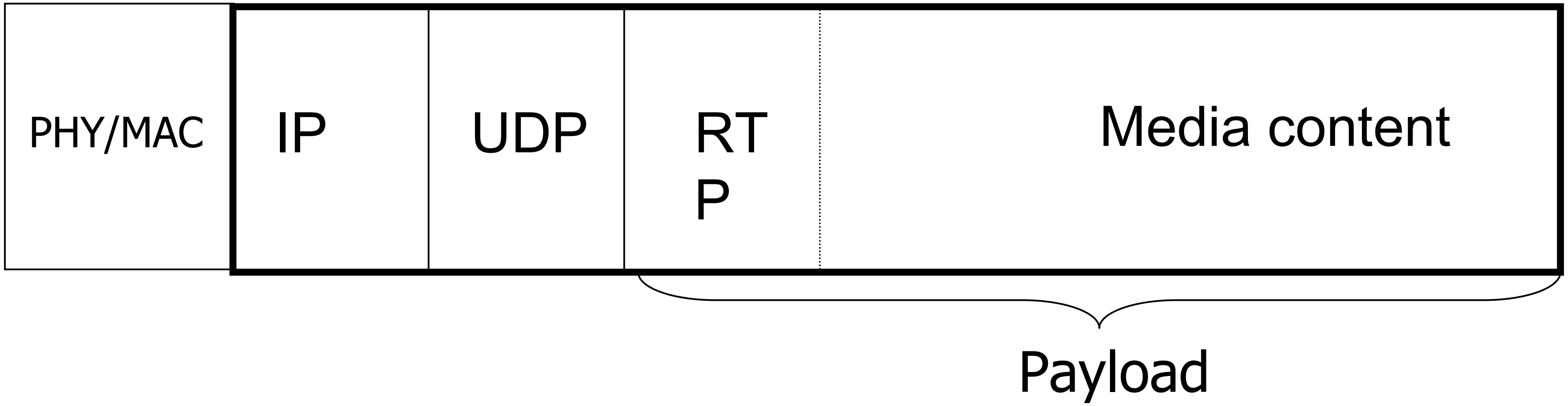
IP Based Multimedia Communication

- Sampled voice is transmitted using RTP protocol which is separate from SIP
- SIP establishes the IP addresses and port numbers at which the end systems can send and receive data
- Data packets do not follow the same path as the SIP packets

Real Time Transport Protocol (RTP)

RFC3550

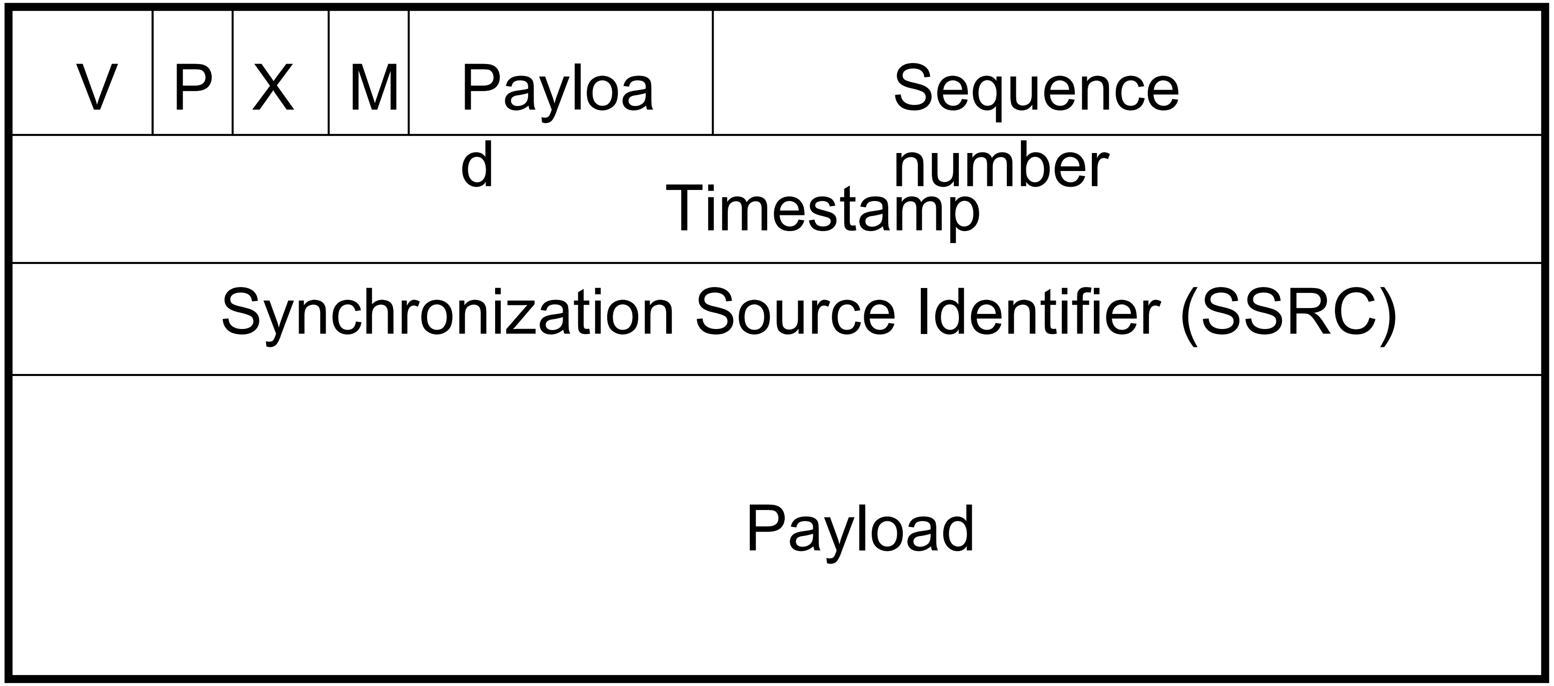
- Standardized by the IETF and used by ITU-T as well to transport real-time data such as voice and video
- Designed to be scalable, flexible and separate data and control mechansms
- RTP is UDP-based to avoid impaired voice quality which would occur if TCP's flow control hit



RTP Header Functions

- Provides information for:
  - media content type
  - talk spurts
  - sender identification
  - synchronization
  - loss detection
  - segmentation and reassembly
  - security (encryption)

RTP: Header



V P X M Payload Sequence number

Timestamp

Synchronization Source Identifier (SSRC)

Payload

RTP Body

- Can carry multimedia in arbitrary encoding
- RFC2833: DTMF
- RFC3016: MPEG-4
- RFC3385: comfort-noise
- RFC3351: basic audio (GSM, G.711, G.729, …) and video (H.261, H.263, …)
- RFC3952: iLBC
- RFC4298: Broadvoice
- See http://ietf.org/html.charters/avt-charter.html for all

Real time Transport Control Protocol (RTCP)

- Separate packets sent on a different port number
- Exchange information about losses and delays between the end systems
- Packets sent in intervals determined based on number of end systems and available bandwidth
- Many implementers don’t bother to support RTCP

Real time Transport Control Protocol (RTCP)

- **Sender Reports**: Information about sent data, synchronization timestamp
- **Receiver Reports**: Information about received data, losses, jitter and delay
- **Source Description**:Name, Email, Phone, Identification
- **Bye**: Explicit leave indication
- **Application defined parts**: Parts for experimental functions

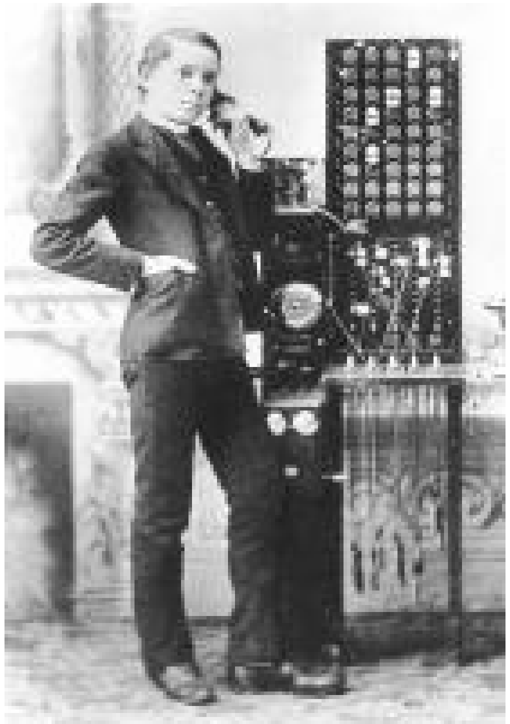
Audio Quality

- Largely depends on codec and echo cancellation in use
- Status of the art: codecs with packet loss concealment such as ILBC (used by Gizmo, skype, GoogleTalk; not used by Cisco)

SIP Servers

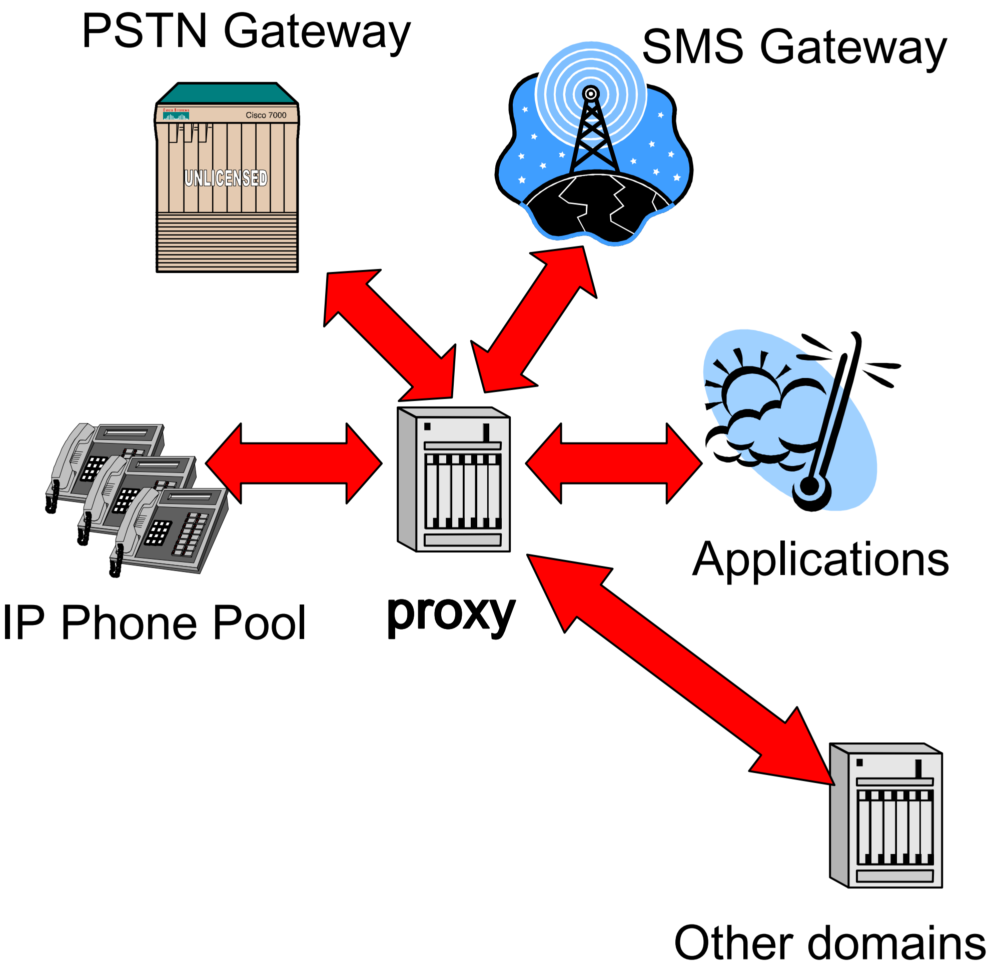
- SIP Proxy Roles
- ENUM
- SIP Proxy Features
- Redirect Servers and B2BUAs

Predecessor to SIP Servers…



- In 1879, the telephone exchange in Atlanta was opened. It consisted of a small, single switchboard which handled about 25 lines. Most of the lines were shared party lines with 2 or 3 subscribers. So there were over 60 subscribers. The first telephone operators were teenaged boys.
- Source: http://home.speedfactory.net/cardwell/part1.html

SIP Glue: Proxy Server



- Proxy servers maintain central role in SIP networks: They glue SIP components such as phones, gateways, applications and other domains by implementing some routing logic
- Example proxy server: SER (iptel.org/ser/)

Key SIP Proxy Roles

- **Security**: With admission control policy, SIP proxy enforces who may call whom, and eventually reports usage
- **Services**: proxy servers can implement a variety of services: missed calls, forwarding, screening, etc.
- **Routing**: Finding the right recipient of a call (gateway, voicemail, SIP-phone, foreign domain, etc.)

Proxy Routing Logic Examples … include but are not limited to….

- Subscribers within administrative domain are routed to based using
  - user location database (sip registrations)
  - or provisioned data (such as translation table for 800 services or PSAP lookup for 911)
- Subscribers within a foreign domain are routed to based on DNS lookup (like with Email)
- Services may be routed based on SIP method to specialized application servers (message store, voicemail, etc.)
- Subscribers with E.164 numbers are routed to based on
  - Pre-provisoned least-cost-routing tables with own or third-party PSTN termination services as targets
  - Dynamically provisioned routing-tables using TRIP (a la BGP; RFC3219; not actually deployed)
  - ENUM

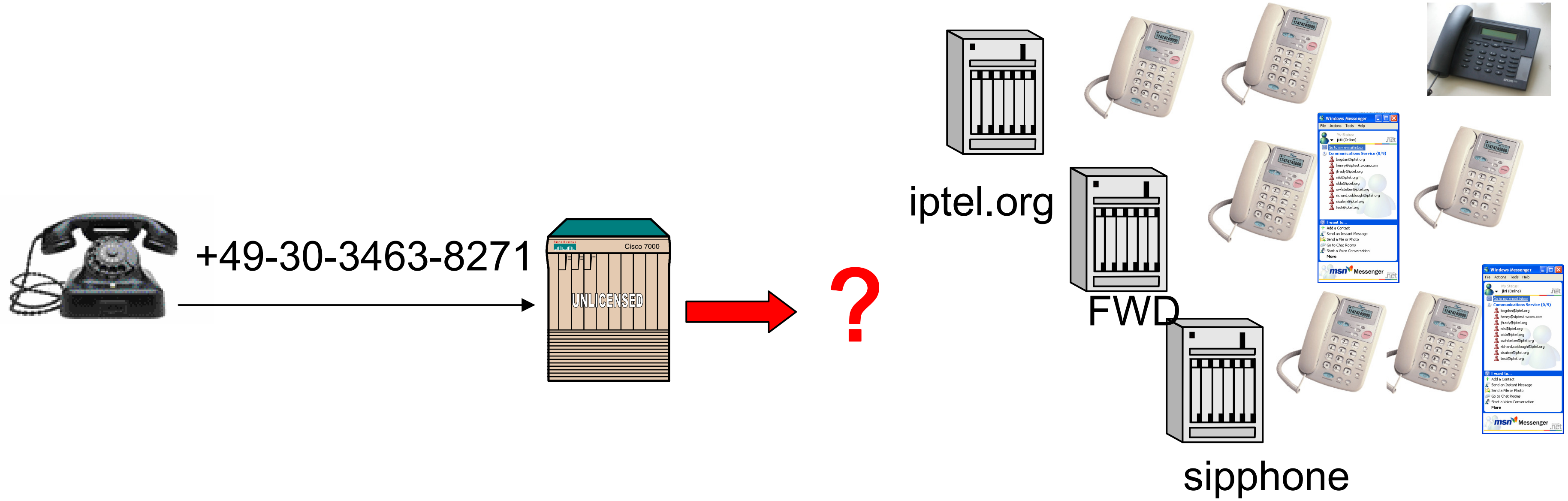
Typical Steps a Proxy Executes (simplified list)

- Sanity checks on incoming requests (syntactically valid request? Request for my domain? Sender banned?...)
- Canonization of dialled target to E.164 if applicable
- Emergency calls for 911|112
- Authenticate originator
- Execute caller's services such as anonymization
- Check request against originator's privileges
- Look up recipient
- If found, try to execute services such as call forwarding and relay the call
- If not found, try to forward to PSTN

RFC3761

ENUM

- Typical use case: caller is in PSTN (can use only digit keys) and would like to reach a SIP callee (if not for other reasons, then because PSTN routing is too costly)
- Answer: ENUM. Create a global directory with telephone numbers that map to SIP addresses (or e-mail, etc.).



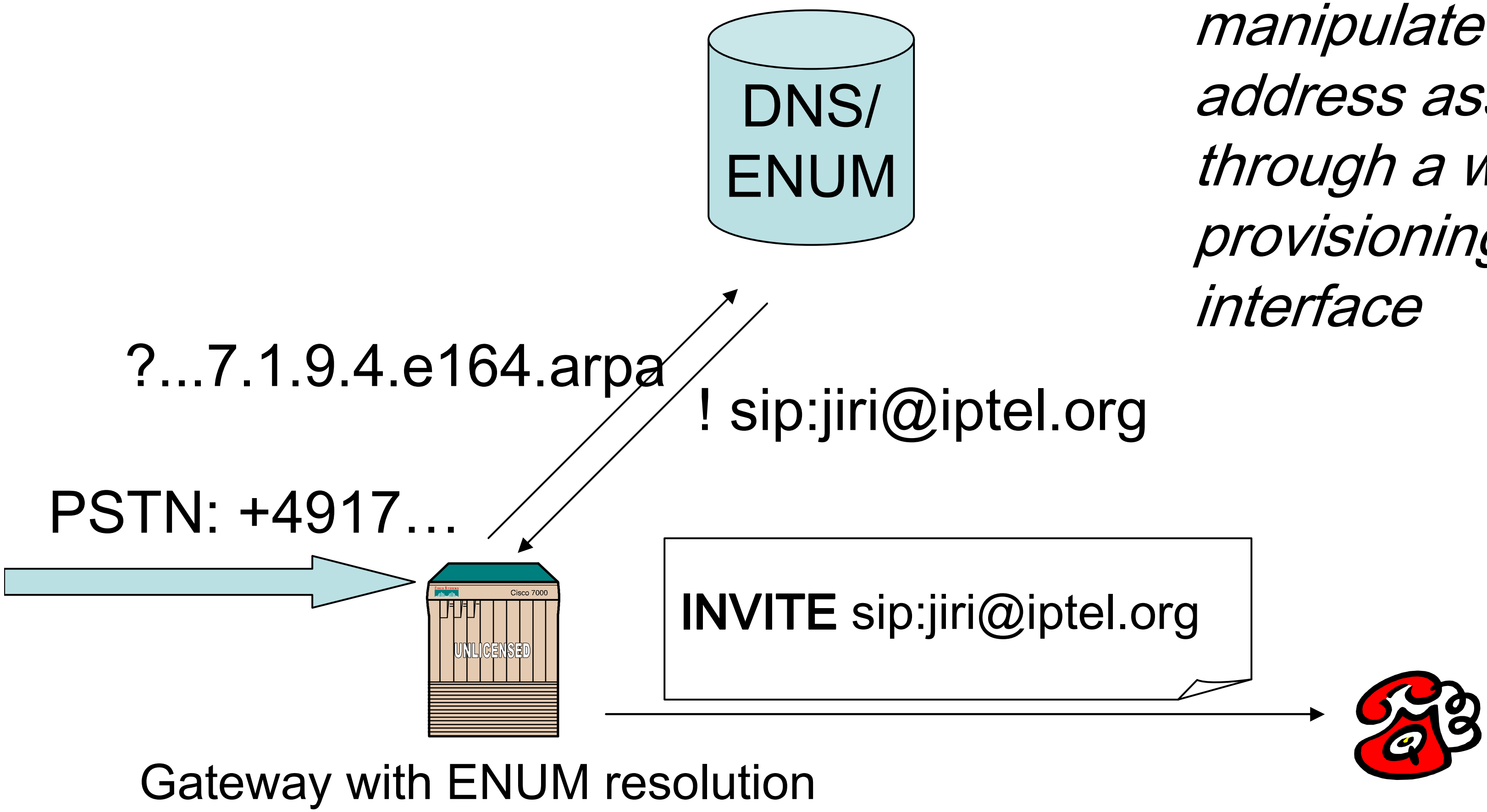
ENUM Translation and Ownership

RFC3761

- The "ENUM global directory" translates E.164 numbers into URIs, e.g.: +49-30-3463-8271=> jiri@iptel.org
- The translation mechanism utilizes DNS: The E.164 number queries are formed as a reversed dot-separated number digits, to which string ".e164.arpa" is appended, e.g.:
  - +4319793321 → 1.2.3.3.9.7.9.1.3.4.e164.arpa
- Operation of the top-level domain carried out by RIPE-NCC: http://www.ripe.net/enum/
- Responsibility for respective countries in the ENUM DNS tree is frequently claimed by local NICs (nic.at, nic.cz, …) or specialized ENUM companies (Neustar, Verisign, …). Delegation still subject to disputes in many countries; number ownership verification is matter of local policies.
- Resulting uncertainty causes some "private ENUM trees" to emerge.

ENUM Call Flow

- *DNS/ENUM helps ingress gateway to resolve SIP address from E.164 number*
- *Typically, owner of an ENUM entry can manipulate the address association through a web provisioning interface*



DNS/ ENUM

?...7.1.9.4.e164.arpa

! sip:jiri@iptel.org

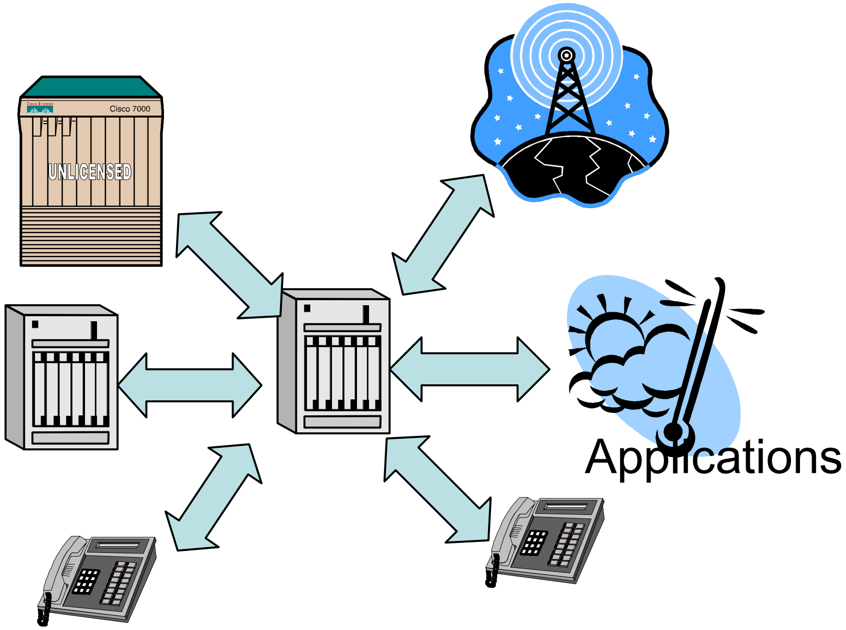
PSTN: +4917…

INVITE sip:jiri@iptel.org

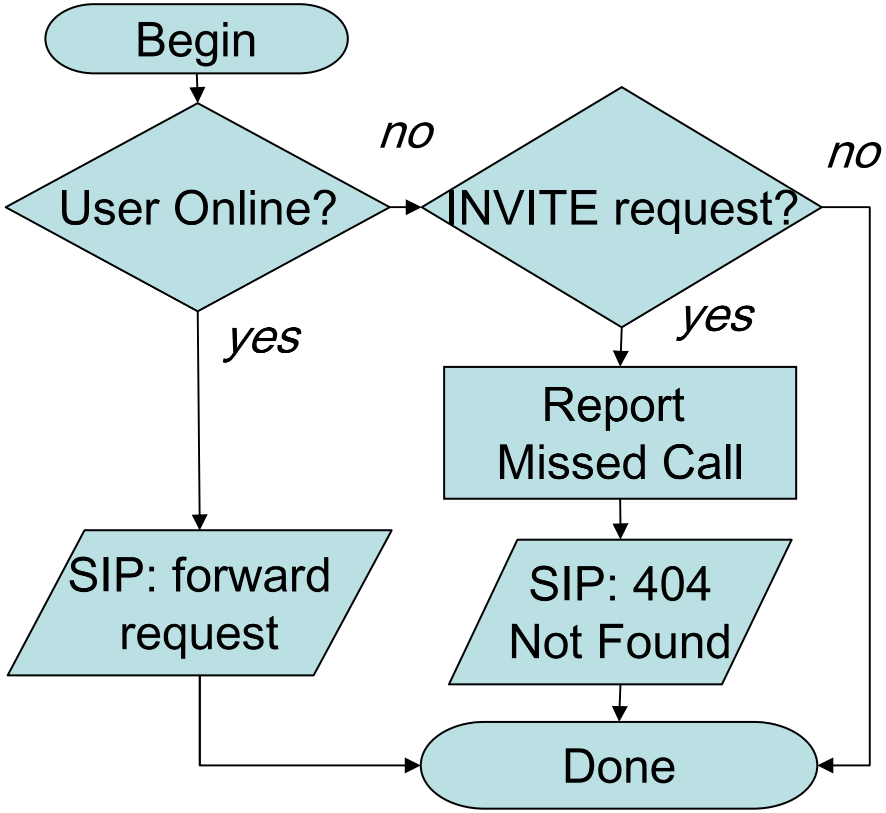
Gateway with ENUM resolution

Proxy Designer’s Dilemma

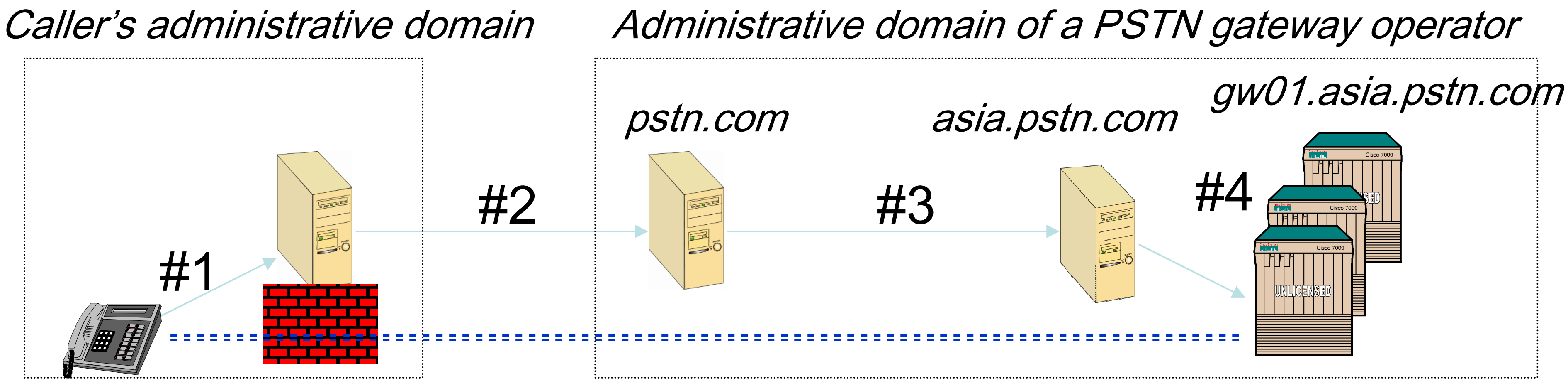
- Routing policy changes every frequently. How do you keep it up-to-date without having to touch the code?



- Iptel’s answer: routing language that allows precise definition of server behaviour.



Service composition: Added-value Server Chains


Caller's administrative domain
Administrative domain of a PSTN gateway operator
pstn.com
asia.pstn.com
gw01.asia.pstn.com
#1
#2
#3
#4
Cisco 7000
UNLICENSED

Caller's outbound proxy accomplishes firewall traversal.

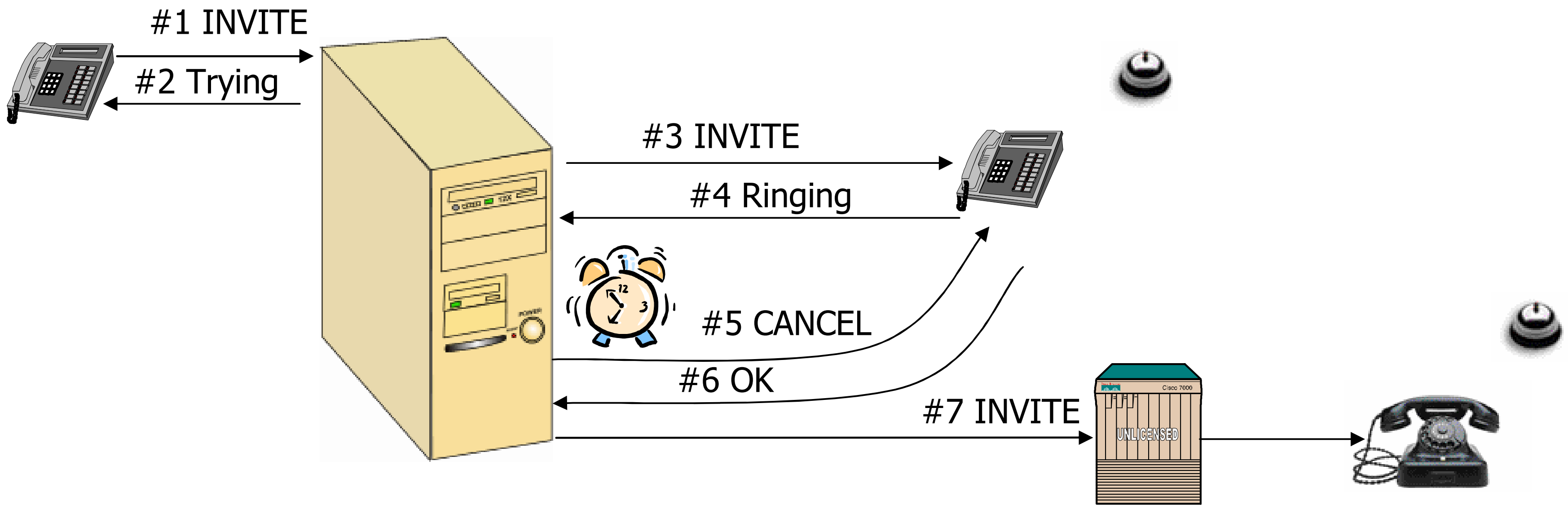
Destination's "first-hit proxy" identifies a proxy serving dialed area.

Proxy in the target area distributes load in a gateway farm.

Note: signaling (in red) may take a completely different path from media (in blue). Each proxy underway adds some value --- that's how services are composed.

Proxy feature: Ability to Try Multiple Destinations: Forking

- A proxy may fork a request to multiple destinations either in parallel (“reach me everywhere”) or serially (“forward no reply”).
- A proxy can cancel pending parallel searches after a successful response is received.
- A proxy can iterate through redirection responses (“recursive forking”).
- The first “OK” is taken.



Stateful versus Stateless Proxy Operational Mode

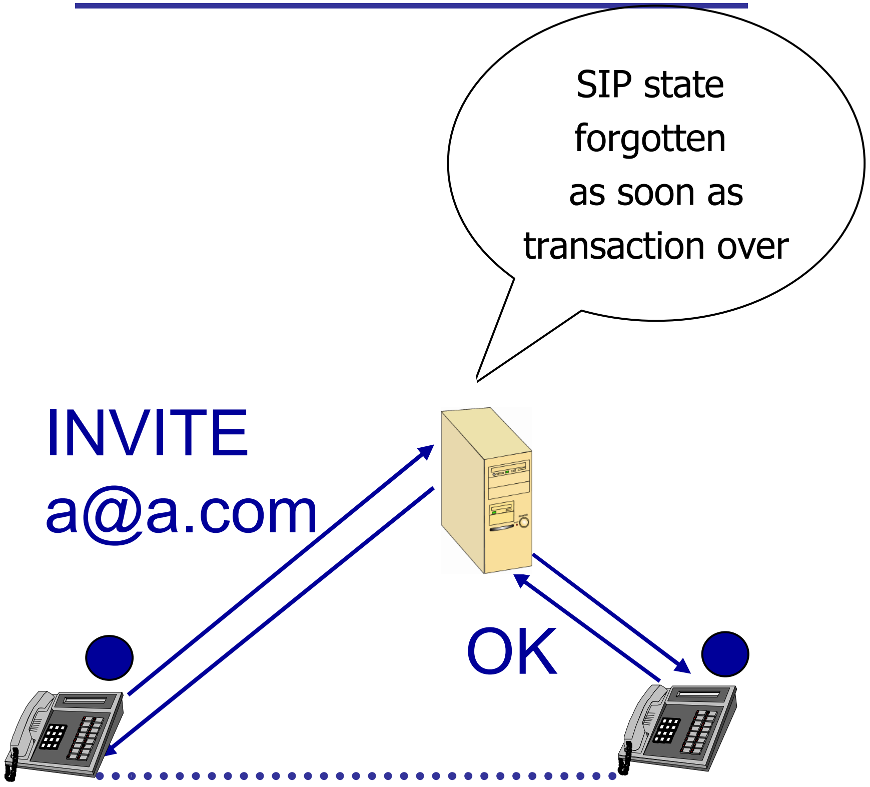
- SIP Proxies may operate either in stateful or stateless mode; which of the modes is used depends on implementation or configuration.
- stateless mode:
  - **Usage:** good for heavy-load scenarios -- works well for example if they act as application-layer load distributors.
  - **Behavior:**
    - proxies just receive messages, perform routing logic, send messages out and forget anything they knew;
    - Memory consumption is constant (which is key for some scenarios – transaction context takes up to 7k of memory!)

Stateful versus Stateless Proxy Operational Mode (cont.)

- stateful mode:
  - **Usage:** good for implementing some services (e.g., “forward on no reply”)
  - **Behavior:**
    - proxies maintain state during entire transaction; they remember outgoing requests as well as incoming requests that generated them until transaction is over; they do not keep state during the whole call
    - State is used for services such as accounting (for aggregating requests with responses and filtering retransmissions out), forking (for picking the ‘best’ answer), forwarding on some event (state helps to postpone decision making till an event such as ‘line busy’ occurs), etc.

“Stateful” Proxy Refers to Transactions

Frequently Misunderstood Issue



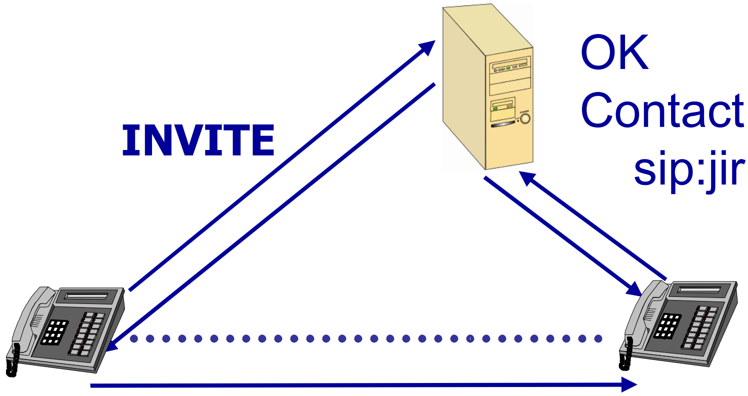
Legend

SIP signaling	←
SIP state	●
media	•••••••••••••••••

- SIP proxies deliver a “one-time rendezvous service” (as opposed to state storage service).
- Thus a stateful proxy just keeps state during a SIP “rendezvous transaction” and completely forgets it afterwards.
- A SIP proxy is not aware of existing calls. In case of failure, existing calls are <u>NOT </u>affected!
- Subsequent transactions may take a direct path!

Subsequent Transactions Bypass Proxy

Frequently
Misunderstood
Issue



INVITE

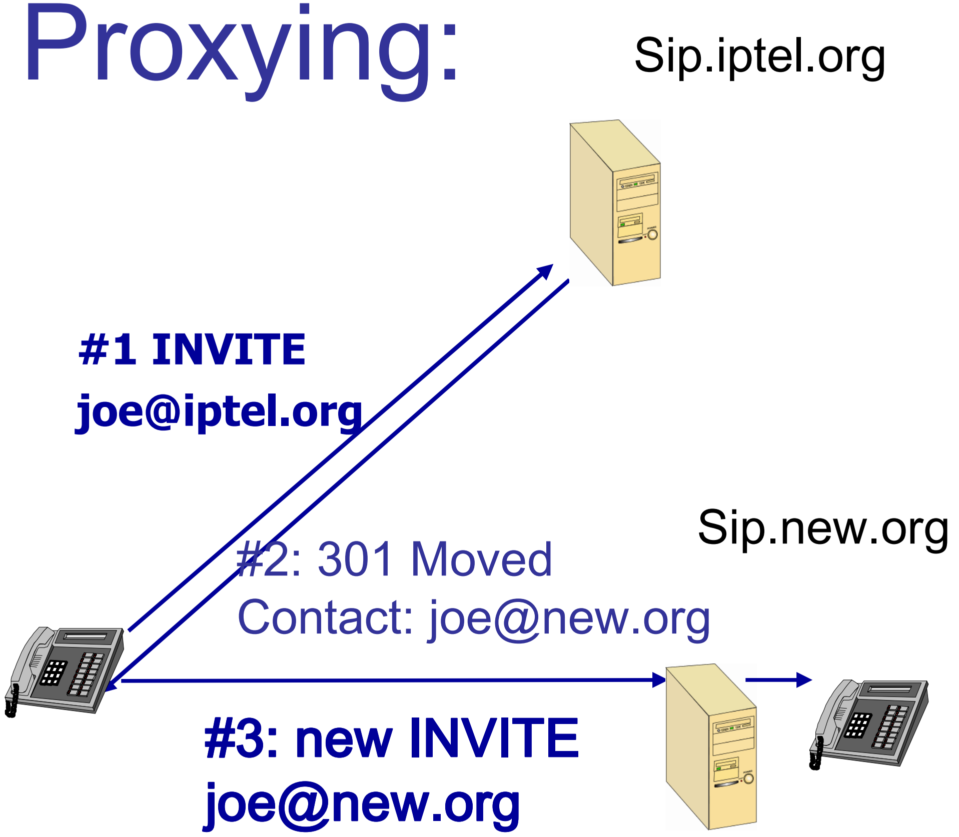
OK
Contact:
sip:jiri@195.3.4.9

BYE takes direct path

- Unless route recording is used, subsequent transactions (e.g., BYE) take a direct path to destination as indicated in **Contact**: header field.
- Today's common practice is however to turn record-routing ALWAYS on to deal with devices that speak different transport protocols and need a mediator in-between them.

Alternate Mode to Proxying: Redirection

- A server can be configured to redirect an incoming request to some other destination.
- Frequent Use Cases: SIP as database lookup protocol for number translation or Migrated Subscriber.
- Redirect mode can be enabled on a request-by-request basis.



Back-to-Back UA (B2BUA)

- Some use-cases are hard to build without knowledge of call/dialog state: for example prepaid scenarios take a network component to pass the initial announcement call leg to a PSTN gateway
- If type-of-feature prevails over scalability, implementers use a server which holds dialog state, is built as two UAs “glued” together and appearing as end-device to both sides of a call
- Most prominent example: asterisk.org (www.asterisk.org)

Summary SIP Servers

- We learned key SIP proxy roles: routing, security and services
- Routing functionality can be, if destination is identified by a E.164 number, “outsourced” to DNS/ENUM
- We learned several SIP proxy characteristics and features: stateful versus stateless, forking, chaining
- Reminder: proxy servers are application agnostic – new message types (presence, messaging, gaming) can be relayed without touching the core network

SIP Message Elements

SIP Message Flows

- SIP is a client-server request-reply protocol:
  - Client sends a request to server and awaits a reply
  - Requests can take arbitrarily complex path
  - Replies take the same path in reverse direction
  - Request and replies have the same structure: first line containing key information, message headers containing supplementary information, message body containing application information (SDP for VoIP)
- Transport protocols supported now: UDP (typical as of today), TCP (emerging for “bulk” applications), SCTP (rare)
- SIP addresses have the “email format”: mrx@iptel.org

SIP Message Structure

Request

```
INVITE sip:UserB@there.com SIP/2.0
```

```
Via: SIP/2.0/UDP here.com:5060
From: BigGuy <sip:UserA@here.com>;tag=123
To: LittleGuy <sip:UserB@there.com>
Call-ID: 12345600@here.com
CSeq: 1 INVITE
Subject: Happy Christmas
Contact: BigGuy <sip:UserA@here.com>
Content-Type: application/sdp
Content-Length: 147
```

Message Header Fields

```
v=0
o=UserA 2890844526 2890844526 IN IP4 here.com
s=Session SDP
c=IN IP4 100.101.102.103
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

Payload

Response

```
SIP/2.0 200 OK
```

```
Via: SIP/2.0/UDP here.com:5060
From: BigGuy <sip:UserA@here.com>;tag=123
To: LittleGuy <sip:UserB@there.com>;tag=65a35
Call-ID: 12345600@here.com
CSeq: 1 INVITE
Subject: Happy Christmas
Contact: LittleGuy <sip:UserB@there.com>
Content-Type: application/sdp
Content-Length: 134
```

```
v=0
o=UserB 2890844527 2890844527 IN IP4 there.com
s=Session SDP
c=IN IP4 110.111.112.113
t=0 0
m=audio 3456 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

SDP (RFC2327): “receive RTP G.711-encoded audio at 100.101.102.103:49172”

SIP Addresses

- Email-like URLs used as address data format; examples:
  - sip:jiri@iptel.org
  - sip:voicemail@iptel.org?subject=callme
  - sip:sales@hotel.xy; geo.position:=48.54_-123.84_120
- SIP gives you a globally reachable address – “Address of Record”
  - Callees bind their temporary address to the global one using SIP REGISTER method.
  - Callers use this address to establish real-time communication with callees.
- may be embedded in Webpages, email signatures, printed on your business card, etc.
- non-SIP URLs can be used as well (tel:, mailto:, http:, ...)
- Address in Request-URI used to identify request recipient. It can be rewritten as the request passes proxy servers.

SIP Request Methods

- **SIP method**, specified in the first bytes of every SIP request, specifies the purpose of a message, such as INVITE == call setup and MESSAGE == instant message
- Based on method, there are two types of requests:
  - Those that **initiate** a dialog such as INVITE or SUBSCRIBE.
  - **In-dialog** requests which refer to a previously established dialog and are routed along the path taken by dialog-initiating requests (and may take a short-cut). Examples: BYE, NOTIFY

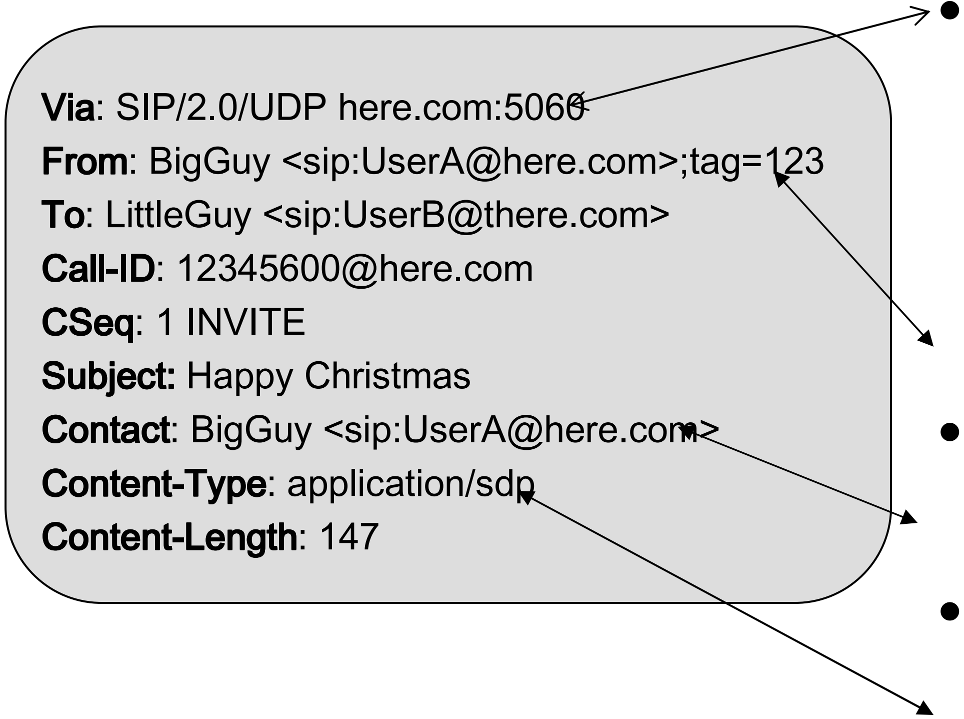
SIP Methods Specified in RFC3261

- **INVITE** initiates sessions
  - session description included in message body offers supported applications to request recepeient: audio, video, …
  - re-INVITEs used to update session state
- **ACK** confirms session establishment
  - can only be used with INVITE
- **CANCEL** cancels a pending INVITE
- **BYE** terminates sessions
- **REGISTER** binds a permanent address to current location
- **OPTIONS** capability inquiry

Some SIP Extension Methods

- SUBSCRIBE/ instant messaging and presence
  NOTIFY/ (RFC3265, RFC3428, draft-ietf-simple-*)
  MESSAGE
- REFER call transfer (RFC3515)
- PRACK provisional reliable responses acknowledgement (RFC3262)
- INFO mid-call signaling (RFC 2976)
- UPDATE change pending invitation (RFC 3311)
- Etc.

Some Important SIP Header Fields



```
Via: SIP/2.0/UDP here.com:5060
From: BigGuy <sip:UserA@here.com>;tag=123
To: LittleGuy <sip:UserB@there.com>
Call-ID: 12345600@here.com
CSeq: 1 INVITE
Subject: Happy Christmas
Contact: BigGuy <sip:UserA@here.com>
Content-Type: application/sdp
Content-Length: 147
```

- Via: “signature” of UAC and proxy servers for routing replies back along the same path
- From: SIP address of request originator
- Contact: SIP address of originator’s equipment
- Content-type: type of message payload

SIP Responses

- SIP responses inform about result of a request. SIP responses travel on the same path as requests, just reversed.
- The most important information is in beginning of the response: three-digit response code.
- First digit specifies error class so that client can roughly guess what happened even if it does not know a specific error code.
- 1yz Informational
  - 100 Trying
  - 180 Ringing (ringing tone played locally)
  - 181 Call is Being Forwarded

SIP Response Codes

- 2yz Success
  - 200 ok
- 3yz Redirection
  - 300 Multiple Choices
  - 301 Moved Permanently
  - 302 Moved Temporarily
- 4yz Client error
  - 400 Bad Request
  - 401 Unauthorized
  - 482 Loop Detected
  - 486 Busy Here
- 5yz Server failure
  - 500 Server Internal Error
- 6yz Global Failure
  - 600 Busy Everywhere

Summary of SIP “Language”

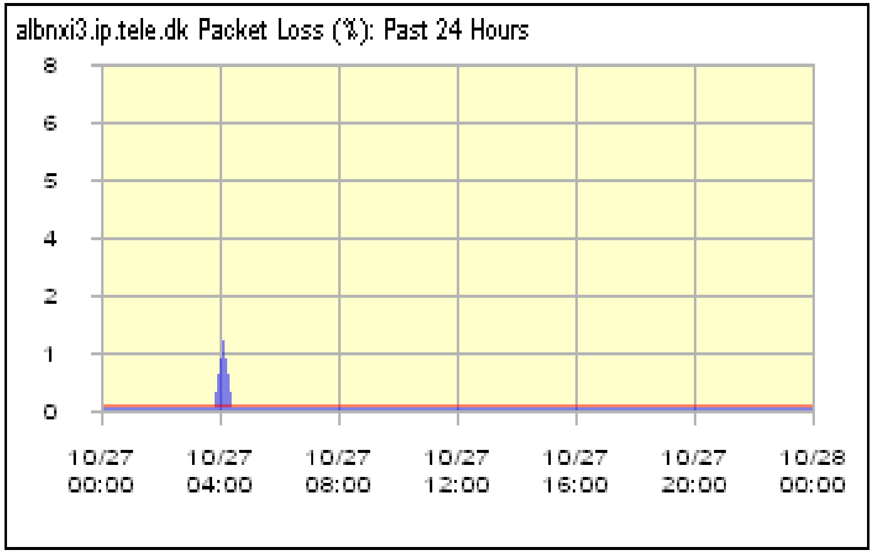
- Textual (HTTP-like) client-server request-response protocol
  - Easy to debug and process with textual operating systems
  - Easy to add new information with new header fields to facilitate new services
- Internet addressing using URIs
  - E.g., sip:jiri@iptel.org
  - Non-SIP URIs possible to for integration with other Internet services (e.g., they may be used to redirect a caller to webpage)

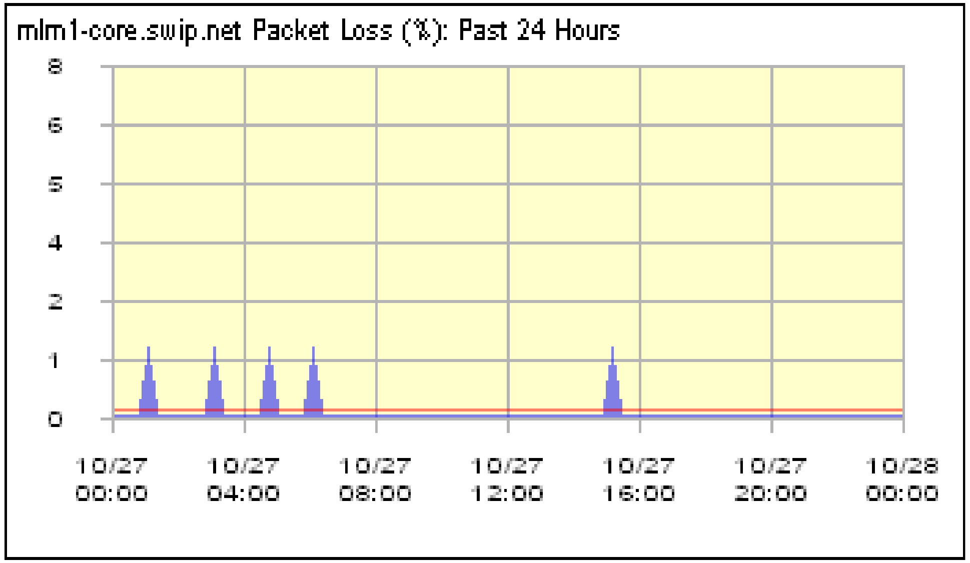
Best Current Practices

Common Operational Problems and Common Solutions to Those (Even though calling the practices "best" doesn't mean they are necessarily good….)

- QoS
- NAT and Firewall Traversal
- PSTN Interworking

Q: Is QoS Problem?





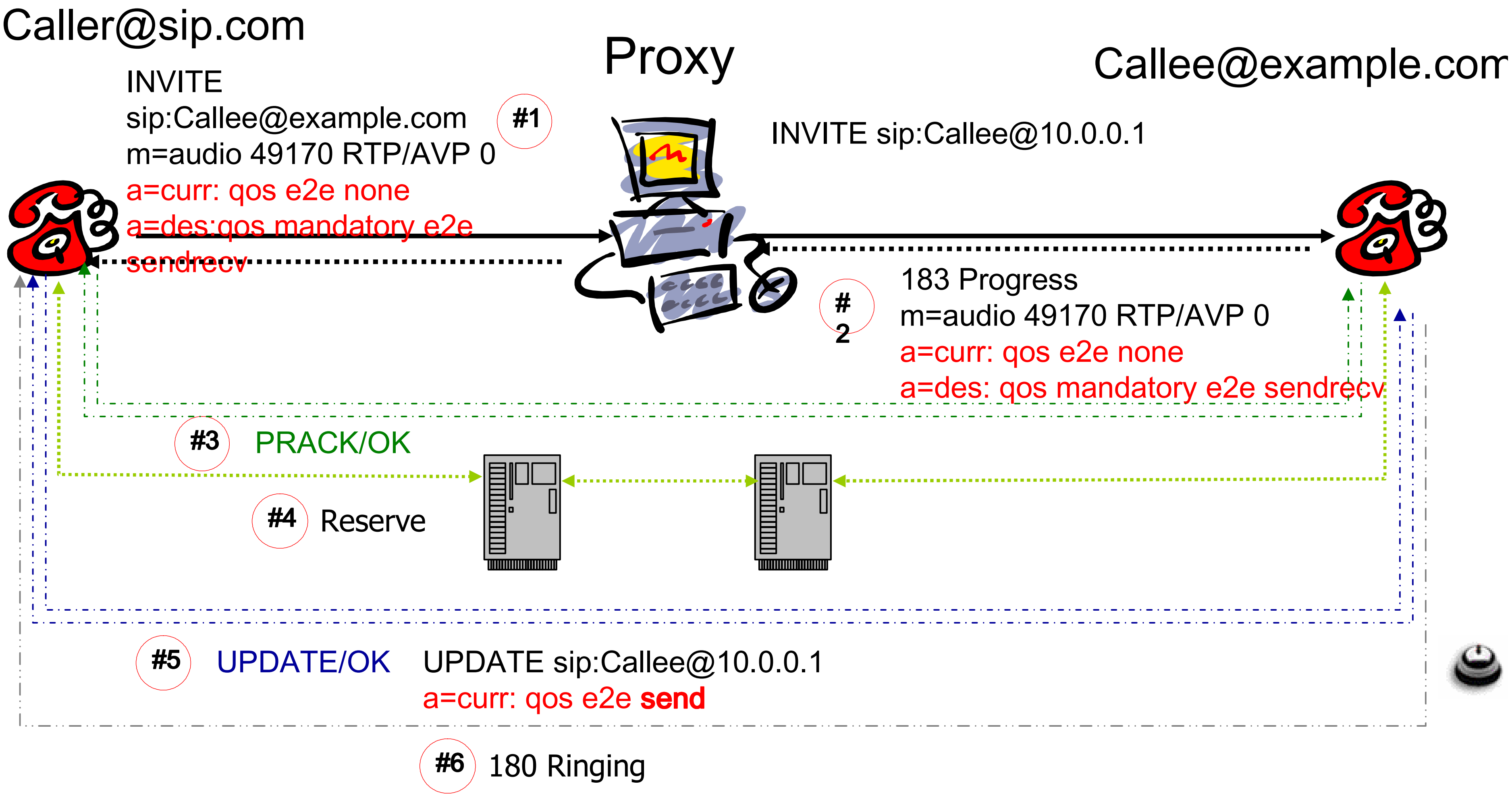
- See pictures for example of packet loss measurements in Scandinavia
- Modern end-devices can cope with QoS distortions (ILBC codec RFC 3951)
- Where is the problem?

QoS is NOT a Problem but We Still Have a Solution ☺

RFC3312
RFC4032

- SIP DOES NOT provide QoS support: QoS protocols are kept separate from signaling.
- Deadlock:
  - QoS signaling cannot begin until I learn through signaling where is the other party.
  - SIP signaling cannot complete and alert callee until QoS is established
- Proposal: “QoS Preconditions”: don’t alert until QoS established
  - find the called party (INVITE) but suppress alerting it (preconditions)
  - try to establish QoS (e.g., using RSVP)
  - if successful alert callee (UPDATE)
- Note: precondition mechanism may be applied to other services too, such as establishing a secured communication channel.

SIP and QoS Control



Caller@sip.com

Proxy

Callee@example.com

INVITE
sip:Callee@example.com
m=audio 49170 RTP/AVP 0
a=curr: qos e2e none
a=des:qos mandatory e2e
sendrecv

#1

INVITE sip:Callee@10.0.0.1

#2

183 Progress
m=audio 49170 RTP/AVP 0
a=curr: qos e2e none
a=des: qos mandatory e2e sendrecv

#3 PRACK/OK

#4 Reserve

#5 UPDATE/OK

UPDATE sip:Callee@10.0.0.1
a=curr: qos e2e **send**

#6 180 Ringing

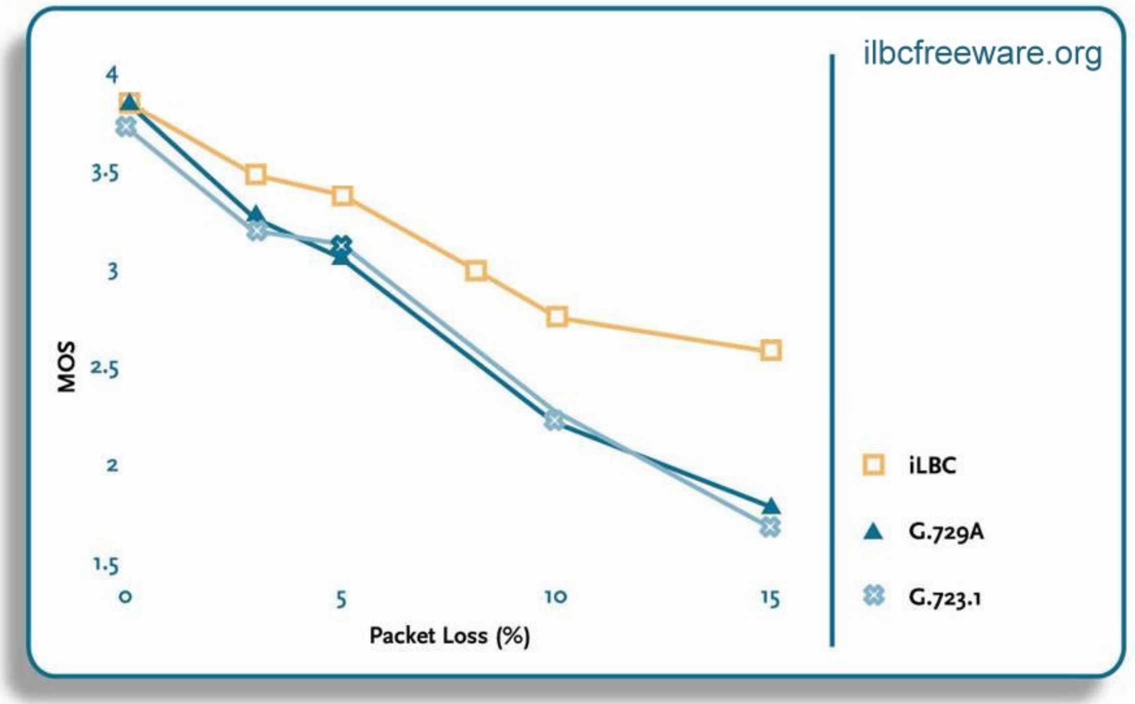
At step #6, path is reserved and callee's phone can begin ringing. Then, SIP completes as usual (180 confirmed by PRACK, 200 sent when callee answers, media exchange begins.)

RFC 3951

A: What is the Answer to QoS Really?

- Make sure your equipment speaks Internet-ready codecs: **ILBC** (RFC 3951)
  - 8 kHz sampling, 13.3/15.2 kbps bitrate,linear-predictive coding, and importantly Packet Loss Concealment
  - Consequently: occasional packet losses are “polished” (interpolated) so that subjectively QoS doesn’t degrade
  - See http://www.ilbcfreeware.org/
  - Trouble: gateways vendor have not deployed it, it is applicable only for IP-phone-2-IP-phone conversations
- **Do nothing else** – there is plentiful of bandwidth, the real problem is how to sell it and additional QoS mechanisms just add to overall complexity and cost of the network

ILBC Benchmarks



The tests were performed by Dynstat, Inc., an independent test laboratory.
Score system range: 1 = bad, 2 = poor, 3 = fair, 4 = good, 5 = excellent

Courtesy of GLOBAL IP SOUND

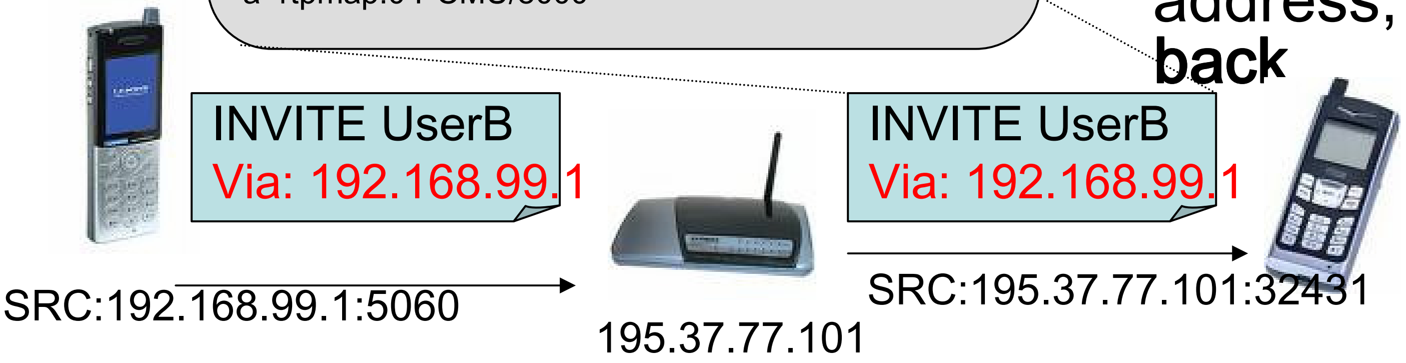
Q: How to Deal with NAT and Firewall Traversal; Part I: NATs

- NATs popular because they conserve IP address space and help residential users to save money charged for IP addresses. They do so by having multiple end-devices shared a single IP address.
- Problem: VoIP does not work over NATs without extra work.
- Problem size: HUGE. Hand-waving estimate: hundreds of millions of Internet users behind NATs.
- Straight-forward solution: replace NATs with IPv6 – unclear when deployed if ever.

Where NATs Affect SIP

```
INVITE sip:UserB@there.com SIP/2.0
Via: SIP/2.0/UDP 192.168.99.1:5060
From: BigGuy <sip:UserA@here.com>
To: LittleGuy <sip:UserB@there.com>
Call-ID: 12345600@here.com
CSeq: 1 INVITE
Subject: Happy Christmas
Contact: BigGuy <sip:UserA@192.168.99.1>
Content-Type: application/sdp
Content-Length: 147

v=0
o=UserA 2890844526 2890844526 IN IP4 here.com
s=Session SDP
c=IN IP4 100.101.102.103
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

- After passing a NAT, SIP message appears like if it came from the public Internet, BUT:
- Contact and Via header fields advertise unroutable private IP (192.168.99.1)
- So does SDP payload
- → Call recepient fails when attempting to send back to the unroutable address; **no traffic comes back**



draft-ietf-sipping-nat-scenarios

NAT Solution Space

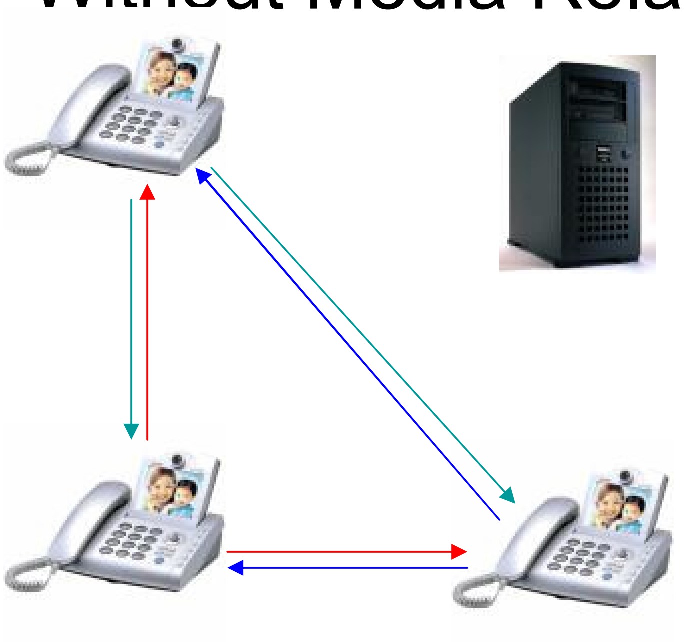
- Application Layer Gateways (**ALG**s) – built-in application awareness in NATs that fixes changed addresses.
  - Requires ownership of specialized software/hardware and takes app-expertise from router vendors (Intertex, PIX). It frequently fails.
- **UPnP**: Automated NAT control: have phones negotiated the use of NAT's public address.
  - Requires ownership of UPnP-enabled NATs and phones. NATs available today, phones rarely (Snom).

NAT Solution Space (cont.)

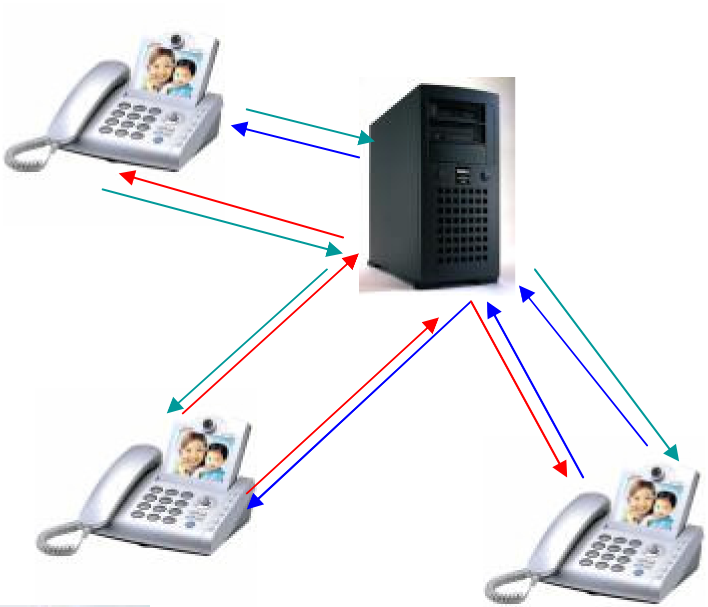
- Smart clients: they use NAT detection technique ‘**STUN**’ (RFC3489) to pretend being in front of NATs… not applicable to all kinds of NATs.
- Brute-force approach: **media relay**: break the voice peer-to-peer traffic into two client-server legs relayed via a public Internet relay, which is more friendly to NATs assuming web-like client-server traffic (note: extra latency; high bandwidth consumption)

Media Relay: Before and After

- Without Media Relay



- With Media Relay



Ethernet bandwidth consumption for three depicted G711/20ms sampling calls: 3 calls x 4 streams x 95.2 kbps
1.116 Mbps

ICE

- All of the suggestion somewhat cumbersome: none of them works any time
- IETF suggestion: have User Agents tried all of them in a preference order and use whichever works best: Interactive Connection Establishment (ICE)
- ICE tutorial: http://www.jdrosen.net/papers/ice-ietf-tutorial.pdf
- Problem: It is not available yet (and it will take some time till it is).

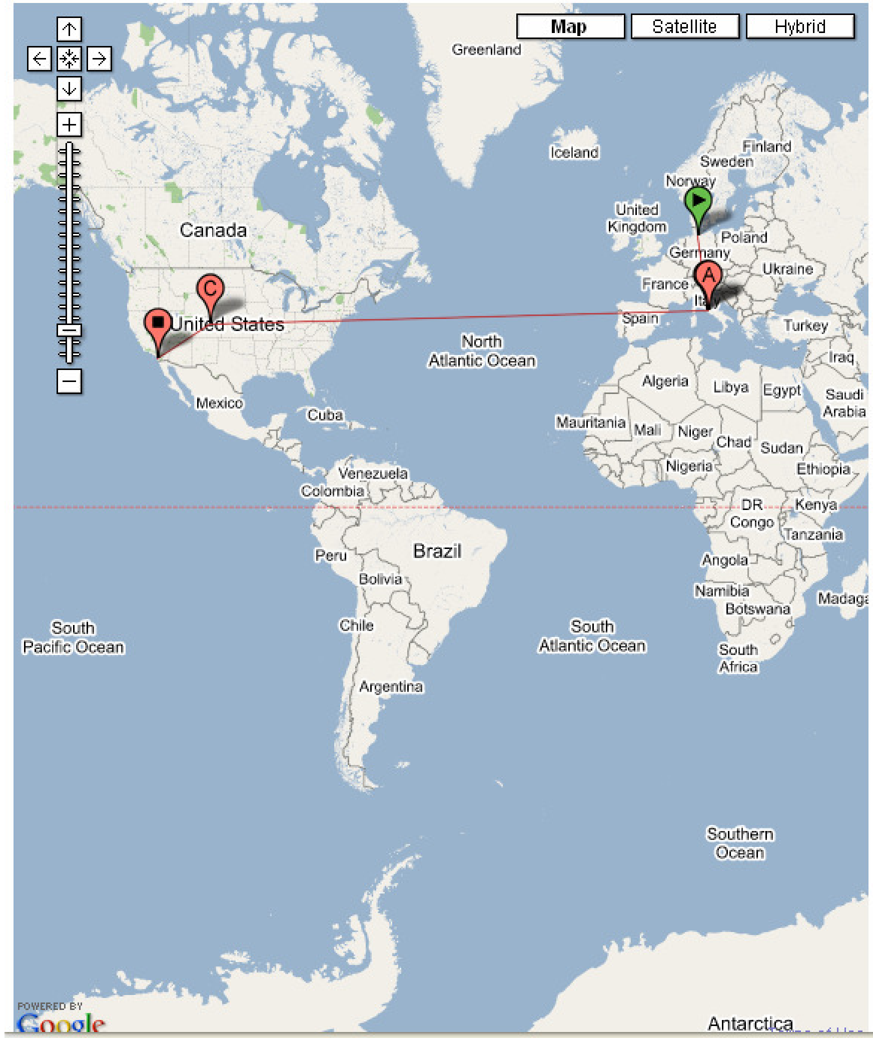
A1: NAT (?Best?) Current Practice

- The solution space as painted before is just not easily practicable, the industry is thus seeking an alternate approach till ICE establishes itself.
- The big-hammer solution is **media-relay** – it is horribly, horribly inefficient, but it works in a majority of cases. Basically, one trades the CAPEX (media relay) + OPEX (relayed media) for price of supporting other immature alternatives.
- The media relay concept is frequently marketed as Session Border Controller. Smarter SBCs can at least avoid relaying media if unnecessary, like when both call parties clearly on the public Internet.

The SBC Concerns

- The SBC doesn’t come for free and is thus better seen as a temporary measure till ICE becomes widely available.
- … (not speaking of the impact on your budget) …
- How can QoS be, if SBC forces “triangular routing” while increasing latency and network bandwidth consumption?
- If it uses application knowledge for “best judgement”, how can the judgment be facing new previously unknown applications running on the end-devices?
- Can it be that this “magic bullet” which centralizes control is actually a single point of failure?
- Where is auditable security with a device designed conceptually as a solve-your-security-problems blackbox?

QoS: How is Your Latency Today



Hops detail | Whois | Raw Traceroute | Help

Hop	Ip	Country	Region	City
1	192.168.178.1	N/A	N/A	N/A
2	213.191.89.1	🇩🇪	Hamburg	Alsterdorf
3	213.191.88.41	🇩🇪	Hamburg	Alsterdorf
4	213.191.87.210	🇩🇪	Hamburg	Hamburg
5	213.191.89.155	🇩🇪	Hamburg	Alsterdorf
6	195.22.211.113	🇮🇹	Lazio	Roma
7	195.22.216.225	🇮🇹	Lazio	Roma
8	195.22.206.30	🇮🇹	Lazio	Palo
9	129.250.2.86	🇺🇸	Colorado	Englewood
10	129.250.2.170	🇺🇸	Colorado	Englewood
11	129.250.2.10	🇺🇸	Colorado	Englewood
12	129.250.2.246	🇺🇸	Colorado	Englewood
13	129.250.2.159	🇺🇸	Colorado	Englewood
14	129.250.27.84	🇺🇸	Colorado	Englewood
15	129.250.27.85	🇺🇸	Colorado	Englewood
16	198.65.166.139	🇺🇸	California	San Diego

Two phones in .de calling over a US/CA based service may experience RTT of about 200 ms → QoS impairment.

Applet ip_investigator__Traceroute_Applet loaded

A2: Long-term Answer to NAT Problem

- If SBC/MRs perform so poorly … what next?
- Deploy ICE as a technique for Media Relay avoidance
- Build NATs that are more application-friendly (that's what the IETF chartered the BEHAVE WG for)
- ETA: 3 years min.

Q: How to Get over Firewalls?

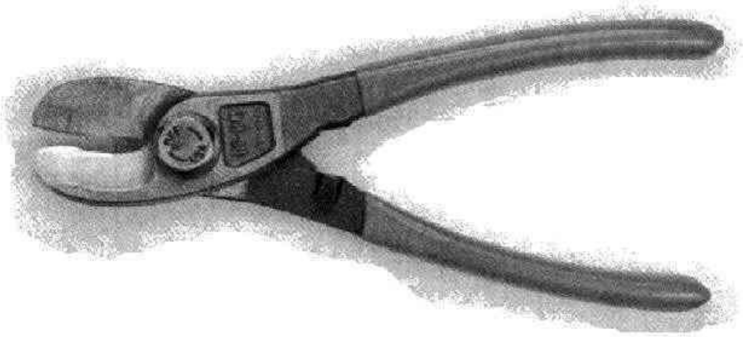
- With NATs, failure to get over the NAT was unfortunate side-effect which we can deal with some way
- With Firewalls failure to get over them is a feature: there is a conflict of interest between user’s desire to communicate and administrator’s desire to limit traffic to well-known data which is auditable and associated with minimum security risk.
- Technically speaking: SIP is dynamic: it opens wide port ranges for media dynamically which is causing conflict with static narrow packet filtering policy.

Firewall Traversal

Ultimately Secure Firewall

Installation Instructions: For best effect install the firewall between the CPU unit and the wall outlet. For Internet use install the firewall between the demarc of the T1 to the Internet. Place the jaws of the firewall across the T1 line lead, and bear down firmly. When your Internet service provider's network operations center calls to inform you that they have lost connectivity to your site, the firewall is correctly installed.

(© *Marcus Ranum*)



Firewall Solution Space

- Educate Administrators
  - If you wish to get your users over a firewall, educate your administrator to open up proper port ranges and coordinate those with ports used by phones.
  - Not practicable for ASPs who can’t educate administrators of their subscribers.
- Deploy Application-Level-Gateways, i.e., firewalls with explicit support for SIP (such as PIX)
  - ALGs punch the holes as needed. However, not all firewalls support SIP as of today and frequently application support is imperfect (which seems kind of inherent).
  - Not practicable for ASPs who can’t upgrade firewalls of their subscribers
- Circumvent firewall policy: just tunnel all the traffic in HTTP
  - This is not really nice ☺ …
  - But it works even for ASPs and it is the feature which made Skype so popular

A: How to Get over Firewalls

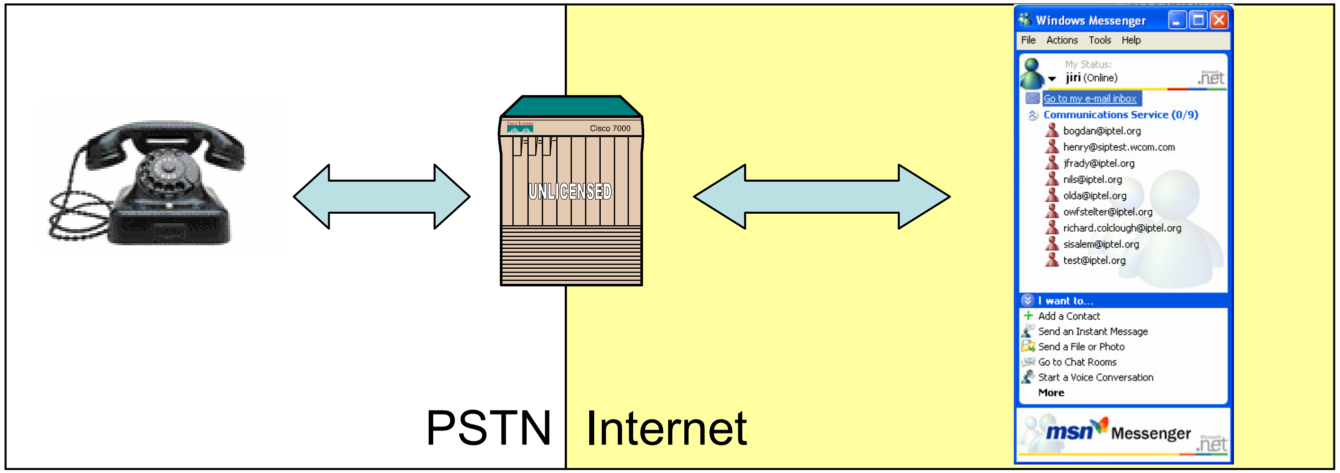
- If in control of your firewall and in possession of enlightened administrator:
  - Have a subnet with VoIP equipment attached to it
  - Configure VoIP equipment to use a predefined port range
  - Configure your firewall to permit this range
  - This way you have well-mounted security policy and applications will work
- If in control of your firewall and seeking for an ‘out-of-the-box’ solution
  - Deploy a SIP-aware firewall and configure it properly
  - Be prepared that unusual call-flows will break
- If not in control of firewalls of your users and in possession of a good lawyer
  - Build a client-server pair that tunnels the firewalls

About SIP-to-PSTN Connectivity

- SIP Telephony is really nice. There are however still 200 million PSTN users hanging around and you would like to talk at least to some of them.

PSTN Gateways

- Problem #1: your device speaks a different language than your grandmother’s.
- Solution: use a gateway, i.e., adapter which converts signaling and speech from Internet to PSTN and vice versa.

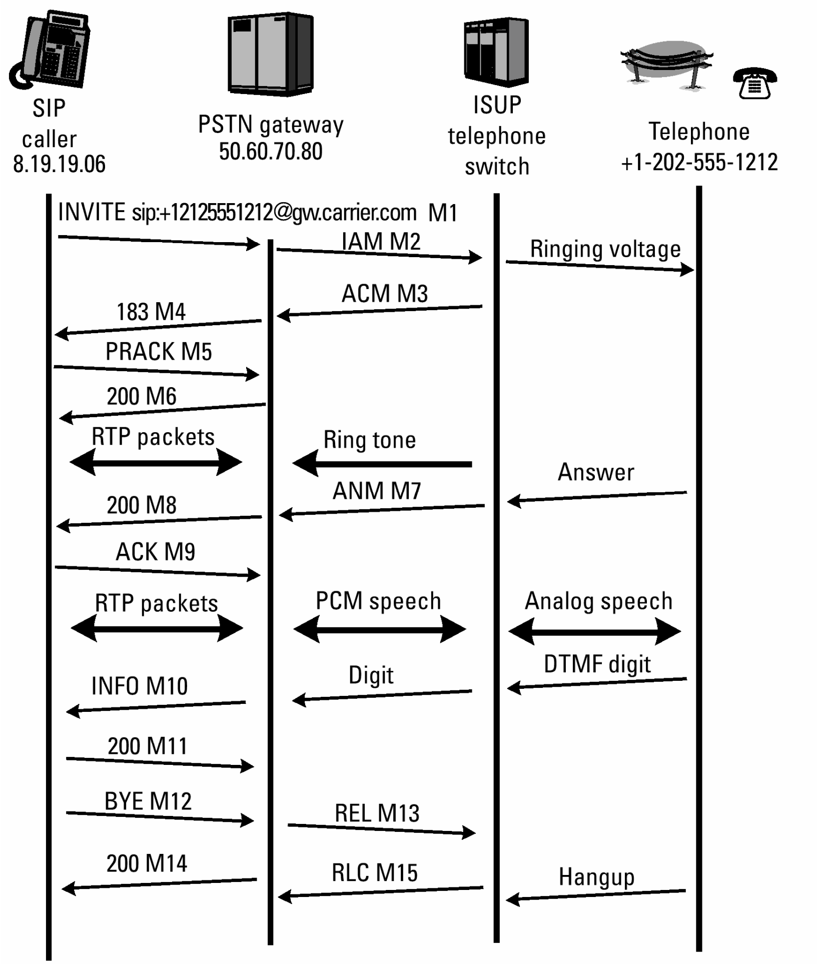


- Gateway market established: Tekelec, Cisco, Ericsson, Lucent. Sonus, Vegastream, etc. Open-source as well (Asterisk).

Call Flow SIP to PSTN

ISDN/ISUP: RFC 3398
QSIG: RFC 4497

- Request-URI in the **`INVITE`** contains a Telephone Number which is sent to PSTN Gateway.
- The Gateway maps the **`INVITE`** to a SS7 ISUP IAM (Initial Address Message)
- **`183 Session Progress`** establishes early media session so caller hears Ring Tone.
- Two way Speech path is established after ANM (Answer Message) and **`200 OK`**



SIP caller 8.19.19.06

PSTN gateway 50.60.70.80

ISUP telephone switch

Telephone +1-202-555-1212

INVITE sip:+12125551212@gw.carrier.com M1

IAM M2

Ringing voltage

ACM M3

183 M4

PRACK M5

200 M6

RTP packets

Ring tone

Answer

ANM M7

200 M8

ACK M9

RTP packets

PCM speech

Analog speech

DTMF digit

Digit

INFO M10

200 M11

BYE M12

REL M13

200 M14

RLC M15

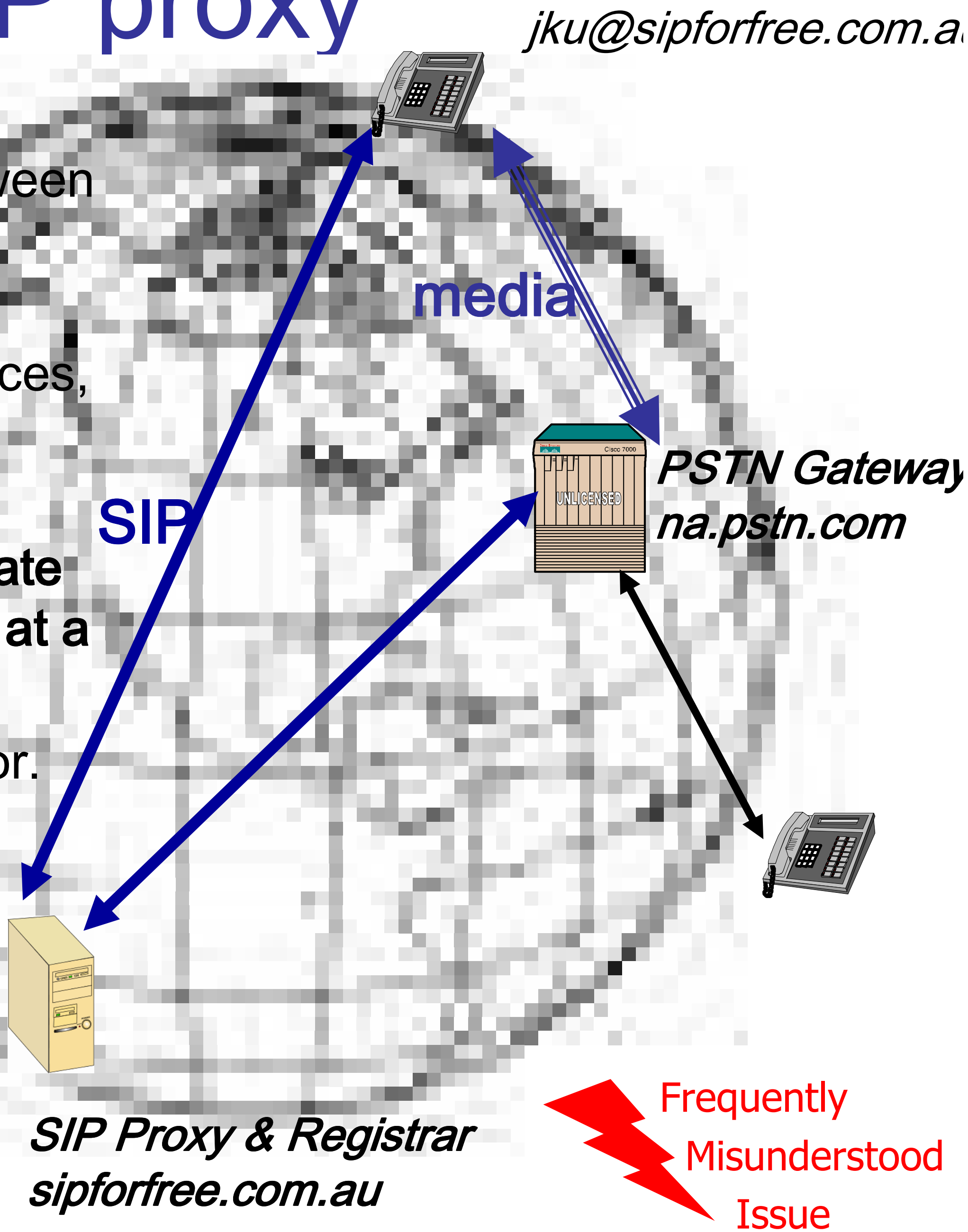
Hangup

Slide courtesy of Alan Johnston, WorldCom. (See reference to Alan's SIP book.)

PSTN GW != SIP proxy

- PSTN gateways are adapters between two different technologies.
- From SIP perspective, PSTN gateways are SIP termination devices, i.e., SIP User Agents just like IP phones.
- **PSTN gateway functionality separate from call processing logic residing at a proxy.**
- Gateway operator != proxy operator.

```
call processing logic:

If ($destination in PSTN) then

route_to_least_cost_gateway();
elseif local(“sipforfree.com.au”)
then
    lookup_registry;
else proxy_to_foreign_domain();
```



Frequently Misunderstood Issue

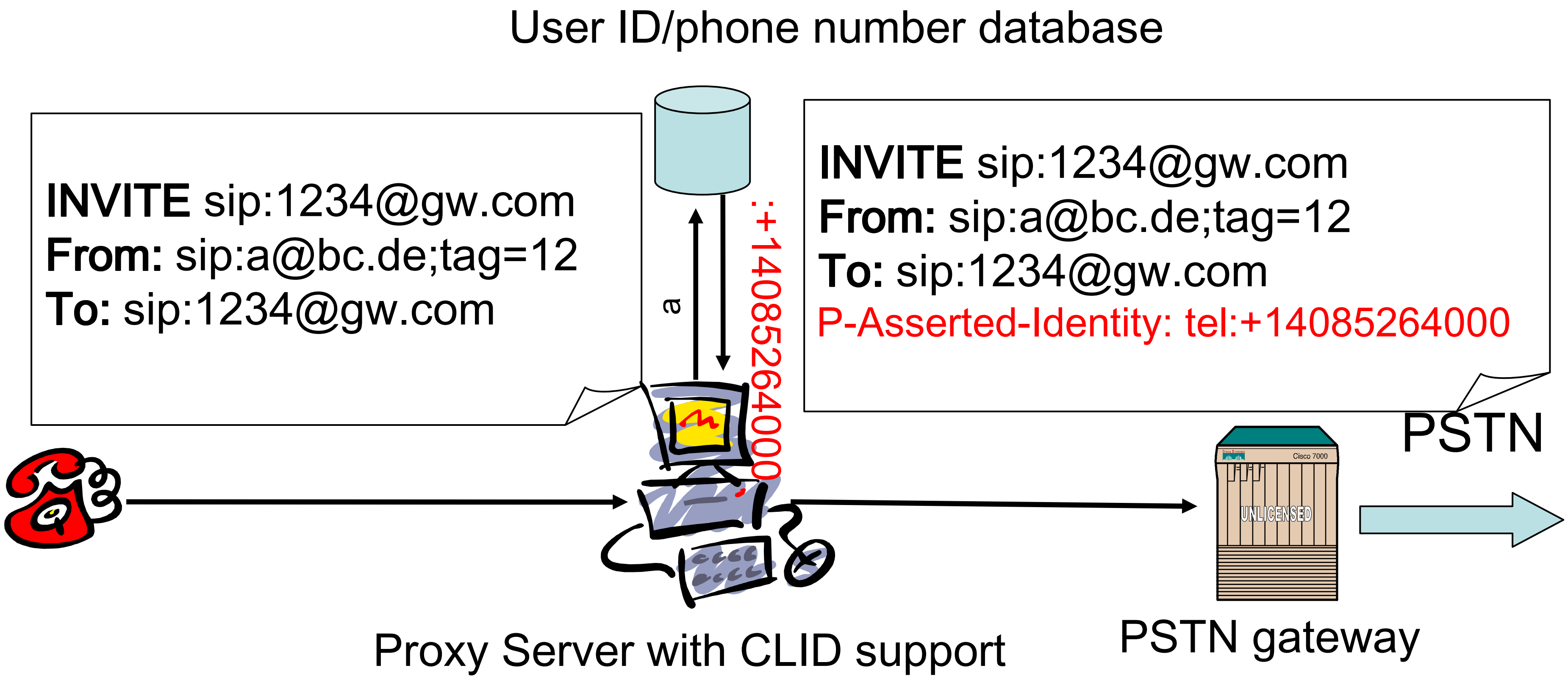
Gateways Ship Today, What Is the Problem Then? Integration!

- Identity: jiri@iptel.org calls out through PSTN gateway. What Caller-ID will display down in PSTN?
- Interdomain settlement: your SIP service operator does not have the capability to terminate anywhere in world cheaply. How can he establish a secure channel to PSTN termination operators?
- How do you locate a proper PSTN termination gateway?
- And some other ugly legacy problems like DTMF, overlap dialing.

CLID

- Typical deployment problem: jiri@iptel.org (in possession of a valid PSTN number) would like to call to PSTN through his gateway operator – how does the gateway know which telephone number to display?
- The proxy server “knows” the number (part of subscriber’s profile) and can append it to SIP requests.
- Missing piece: communicating the PSTN number a server determined to gateway in .
- The standard: “asserted identity“, RFC3325.

CLID – message example



```
INVITE sip:1234@gw.com
From: sip:a@bc.de;tag=12
To: sip:1234@gw.com
```

```
INVITE sip:1234@gw.com
From: sip:a@bc.de;tag=12
To: sip:1234@gw.com
P-Asserted-Identity: tel:+14085264000
```

RFC2833

DTMF Support

- Actually, I would wish this slide wasn’t here: IVRs are horribly inconvenient devices. I like voicemail message delivery by e-mail and flight-ticket shopping with web much better. But …
- … Large deployed base for telephony applications.
- Solution 1: include tones in audio. It works fairly well with G.711 codecs. More compressive codec may degrade quality so that tones are no longer recognized by receiver.
- Solution 2: special DTMF payload for RTP: RFC 2833. Reliability achieved through redundant encoding (RFC2198).

RFC3578

Overlapped Dialing

- Problem: ingress PSTN2IP gateway operates in overlapped dialing mode whereas SIP operates en-block;
- Solution #1: initiate en-block SIP dialing using knowledge of numbering plans or after a period of overlapped dialing inactivity; drawback: delay
- Solution #2: send a new INVITE for each new digit

Q: How to Route Emergency Calls? A: Use Pre-provisioned Data

- How can be an emergency call routed to the closest PSAP the way we know it from the PSTN?
- The BCP is trivial: pre-provision the closest PSAP in subscriber’s profile (either in SIP profile for ASP, or alternatively in access profile for ISPs)
- Some providers used outsourced emergency services too.
- Downside: subscriber who plugs in his SIP-phone out of his default destination will still get his home PSAP when dialing emergency…
- More work going on in the IETF ECRIT WG (location-to-service protocol, URN convention) and IEPREP WG (broader architectural impact)

More PSTN-Related Reads

- Mapping of of Integrated Services Digital Network (ISUP) Overlap Signalling to the Session Initiation Protocol [RFC3578]
- Session Initiation Protocol PSTN Call Flows [RFC3666]
- Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping [RFC 3398]
- Session Initiation Protocol for Telephones (SIP-T): (SIP-T): Context and Architectures [RFC3372]
- Interworking between SIP and QSIG [RFC4497]

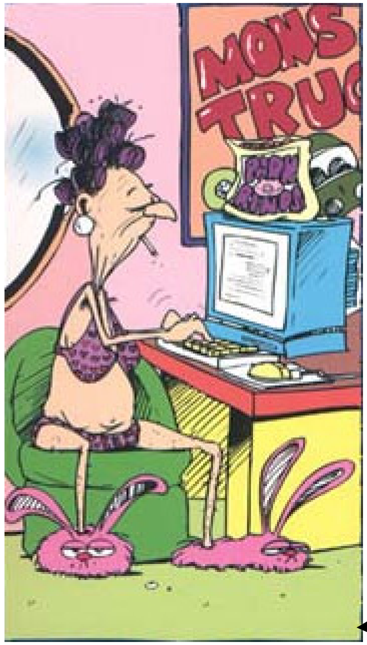
VoIP Protocol Security

- Intro: What security protocols can(not) do for you
- Security in SIP Protocol Family
- SPIT
- Security in deployments

(Most focus on servers … hacking a server powering thousands of users appears more appealing to hackers than hacking a SIP phone.)

Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

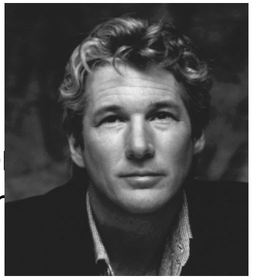
What Security Protocols Will NOT Do for You … Social Engineering



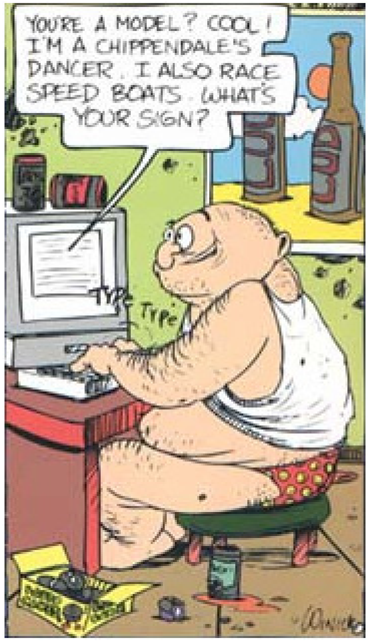
SIP INVITE w/JPEG

INVITE sip:UserB@there.com SIP/2.
Via: SIP/2.0/UDP here.com:5060
From: BigGuy <sip:UserA@here.com
To: LittleGuy <sip:UserB@there.com>
Call-ID: 12345600@here.com
...

200 OK w/JPEG



SIP/2.0 200 OK
Via: SIP/2.0/UDP here.com:5060
From: BigGuy <sip:UserA@here.co
To: LittleGuy <sip:UserB@there.co
Call-ID: 12345601@here.com...


YOU'RE A MODEL? COOL! I'M A CHIPPENDALE'S DANCER. I ALSO RACE SPEED BOATS. WHAT'S YOUR SIGN?
TYPE TYPE

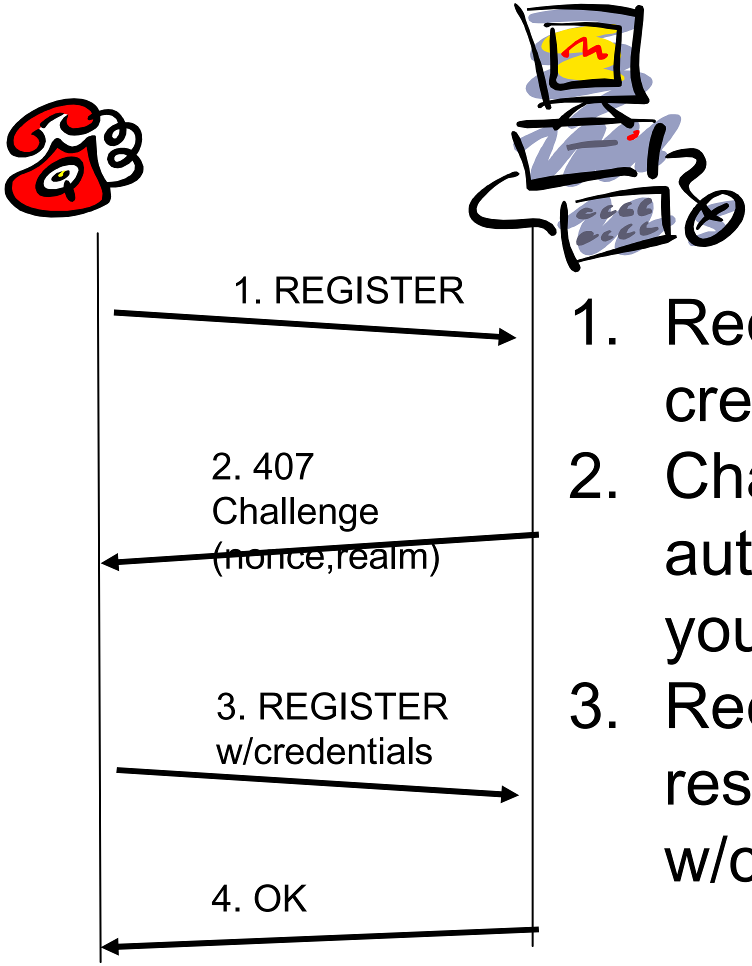
What Security Protocols Can Do For You:

- Privacy/Confidentiality:
  - Making sure that if an attacker can intercept your traffic, it cannot misuse it. → **Encryption**
- Authenticity:
  - Make sure that you know to whom you are speaking (very useful for authorization, accounting, and knowing who is actually calling you) → **Authentication**
- Message Integrity
  - Make sure that no man in the middle has tempered with your message → **Message Integrity Check** (MIC)

RFC 2617

Client’s Authenticity: Digest

- Required for user identification and admission control for services.
- Protocol:
  - challenge-response using MD5 to protect from replay attacks
  - Based on secret shared between client and server
- History: SIP in RFC2542 inherited basic plain-text authentication which was deprecated as too insecure



1. Request w/o credentials
2. Challenge: authenticate yourself
3. Request resubmitted w/credentials

Proxy

Due Diligence of Digest Security

- Executive summary: It is a viable instrument for authentication that can be used for authorization and accounting and can’t be easily compromised by attackers with read-only access to network traffic. But:
- Server MUST unavoidably store plain-text passwords to be able to verify hashed passwords – if authentication database is compromised, there is a great trouble.
  - To lower the risk, servers SHOULD at least hash the plain-text password with realm (domain name typically) so that the revealed password if used many times does not compromise security in other domains
- No message integrity is provided. Attacker who can mangle SIP messages coming from a trusted user may change them. (E.g., to substitute dialed URI with one of a 900 phone number.) If available, auth-int and predictive nonces can be used to improve security.
- A safer challenge-response authentication standard, AKA (RFC4187) developed for use in IMS – see the IMS section.

Conveying Identity: Who Is Really Calling Me?

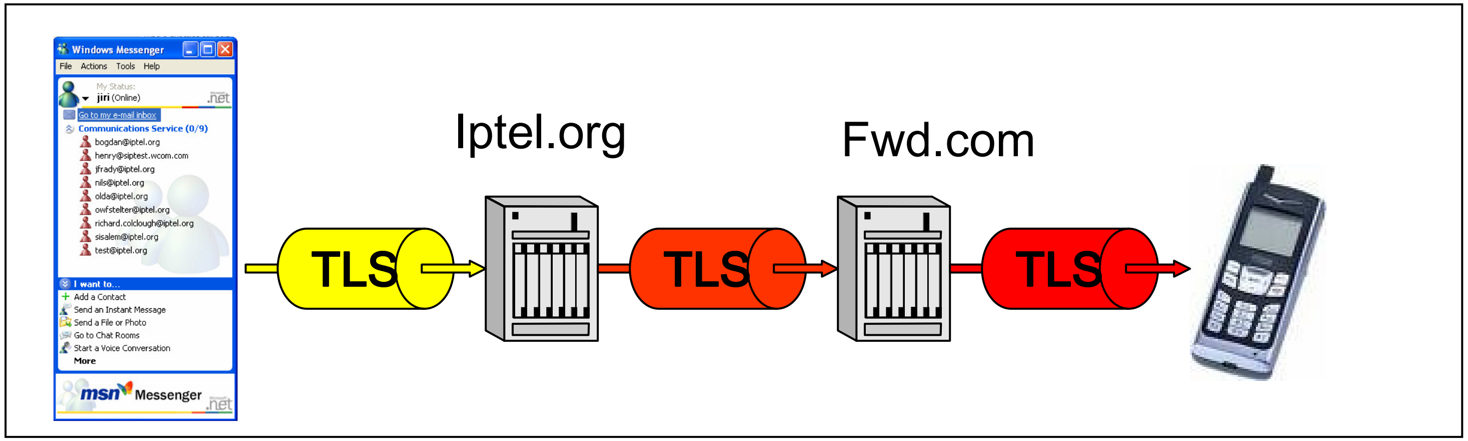
RFC3325
RFC4474

```
INVITE sip:foo@iptel.org SIP/2.0
To: <sip:foo@iptel.org>
From: <sip:GWBush@iptel.org>; tag=c775
Authorization: Digest username="john", realm="iptel.org", algorithm="md5",
   uri="sip:nils@iptel.org", nonce="3edab81b7a8427be362c2a924f3171d215a8f7d3",
   response="4a868f9cbffd2b1f39c778abca78f75b".
P-Asserted-Identity: tel:+14085264000
Identity: "ZYNBbHC…hVn9Yc6U="
```

- #1: From header field content is informational only – the end-device legitimately authenticated as john@iptel.org can put ANYTHING there, including GWBush@iptel.org. → Proxy server must verify From using authenticated identity to avoid confusion of downstream User Agents.
- #2: One identity in From may be insufficient. This is particularly the case when in addition to native email-like URI PSTN number owned by the caller must be displayed → That's what P-asserted-identity (RFC 3325) is used for and appended by proxy servers.
- #3: From is plain-text and trustable only in secured environments – that becomes problematic once a request leaves an administrative domain. Idea: perform light-weighted digest authentication within domain, rubber-stamp identity with domain's certificate and have downstream entities trust your domain as whole. That's done by proxy server appending Identity header field (RFC4474).

SIP Security at Transport Layer

RFC2246



- Suggestion: put the security burden underneath the application in the transport layer: use TLS
- Downside: security "tunnels" are established between invidiual SIP "hops" (typically caller's outbound proxy and callee's inbound proxy). All the servers underway get internally to see the traffic and must be trusted to keep the traffic secure. (Do you trust me???)
- Practical downside: there are not too many clients with TLS support.

SIP Security for Message Body

- Worried about sensitive message body (e.g. if it contains an instant message) and not willing to trust a proxy server not to disclose the content?
- Encrypt the message body end-2-end using S/MIME:
- Downside: some proxy servers may have legitimate reasons to look at message body and if prevented from doing so, traffic may fail → practically unused today

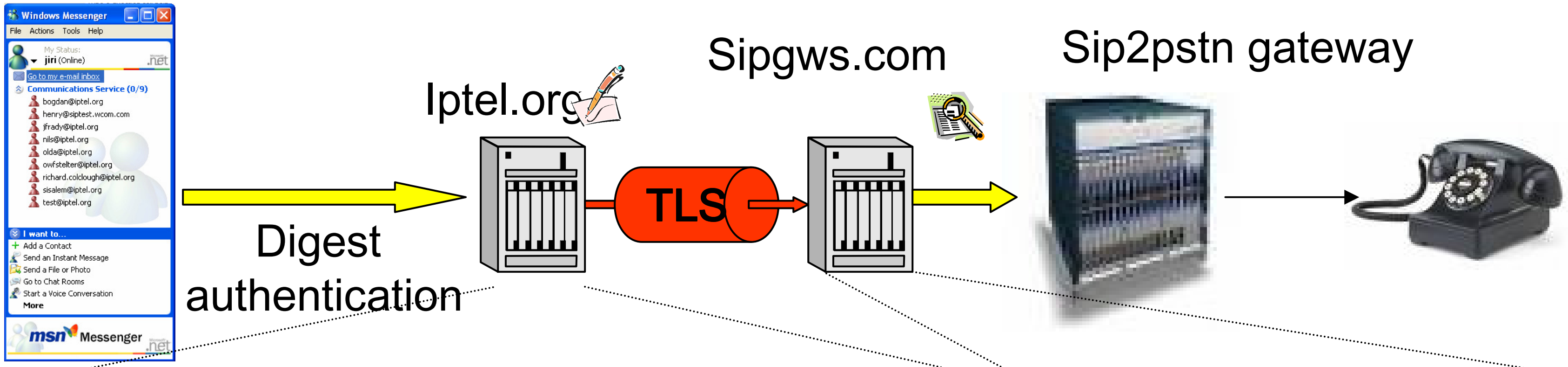
SIP Security Protocol Features

	Digest RFC2617	TLS RFC2246	S/MIME RFC2633
Applicability	UA-2-proxy	Hop-by-hop	UA-2-UA
Security Model	Client-server shared secret authentication.	Transitive trust at transport layer.	End-2-end public-key encryption of payload.
Privacy	☒	☑	☑
Authenticity	☑	☑	☑
Integrity	☒	☑	☑

Putting the Pieces Together

- As you see one CAN do a lot of fascinating things with SIP security protocols, but what the heck does one actually do today?
- Digest authentication to determine caller’s identity for sake of From verification and accounting
- Occasionally TLS is used, mostly for interdomain communication
- Asserted-Identity is appended by proxy servers to convey caller’s PSTN number from trusted SIP proxy servers to PSTN gateways (even though insecure)
- Identity header field, more dense use of TLS and S/Mime still on the radar screen. (At least Identity hopefully not for too long.)

SIP Security BCP in a Single Picture



Security Policy @ iptel.org Proxy Server

•Has Client properly authenticated?

•Does a Client use a proper identity in From?

•Does the client have privilege to call where he is calling?

•If provisioned for caller, append his Asserted-Identity.

•In the (hopefuly near) future: sign by domain certificate.

•If client demands encryption using ‘sips’ protocol discriminator, use TLS to forward downstream.

Security Policy at sipgws.com

Is there a proper certificate from iptel.org domain? If so, trust the content.

draft-zimmermann-avt-zrtp

Security of Media

- A variety of encryption protocols for securing media available, it is just that keying is so troublesome that they hardly get deployed
- New emerging alternative: zRTP (work of PGP author Phil Zimmerman)
  - Works without prior knowledge of keying material and without any change to infrastructure: solely end-device feature
  - Session key is established dynamically using Diffie-Hellman algorithm
  - Encrypted media is transmitted using SRTP

Alternatives for Media Security

- Other solutions being proposed but appear to gain little traction, presumably because of keying complexity.
- Keying typically based on MIKEY (RFC3830) or DTLS (RFC4347)
- For a more complete survey, see: http://www3.ietf.org/proceedings/06mar/slides/raiarea-1/raiarea-1.ppt

What Makes Attacks Easy

- Security incidents caused by errors in carefully designed security protocols are rare despite exciting reports about weaknesses in MD5;
- Attacker motivation unsurprising: money (get free access to expensive numbers, obtain credit card numbers from unknowing users) and fame (make it to news by paralyzing a major VoIP service)
- Attackers have mighty allies:
  - Manufacturers: Code vulnerabilities
  - Operators: Careless mistakes in policy

Code Vulnerabilities

- Despite all manufacturers' diligence it is unreasonable to assume there are no bugs in their SIP software
- The Internet is rough environment: a public services is available for attack to attackers from the whole world. There are many of them, they are smart and they have tools!
  - Port scanners: smap, http://www.wormulon.net/files/misc/
  - Dictionary attacks: sipcrack, http://codito.de/
  - Buffer overflow tools: protos, http://www.ee.oulu.fi/research/ouspg/protos/
- Recommendations:
  - Devise careful firewall policy
  - For public services that must be fully available on the Internet, be ahead of attackers. Put effort in testing your environment, seek vulnerabilities proactively, apply security patches early. There is no magic bullet – work on it!

Getting Security Policy Right

- Getting security policy right is laborious and thus error-prone procedure too. You have to:
  - Define adequate firewall policy and network design
  - Identify all scare resources such as 900 calls and required privileges for accessing them
  - Assign proper privileges to users
  - Avoid SIP's built-in traps if possible: looping and forking "amplifiers", preloaded routes, misguided BYEs for avoiding proper CDR or call termination
  - Choose a proper mix of security protocols.
  - Proper SIP server configuration (e.g., way of storage of shared secrets)
- Status of the affairs: the problem has been recognized but no auditing tools available yet.
- Recommendation: Operators still have to rely on smart admins and professional security reviewers.

True Horror Story: Plain-Text Password (June 2006)

- Use of plain-text password made it easy for the attacker Pena, 23, to route his customer's calls and have them charged to unknowing third parties
- Damage size: 10 million minutes, 500,000 unathorized calls, aggregate routing cost of $300.000 per provider
- Attack steps: hacking third party sides, using them to mount brute-force attack on prefixes used as wholesale passwords and later using them to relay calls.
- Full story: http://newark.fbi.gov/dojpressrel/2006/nk060706.htm

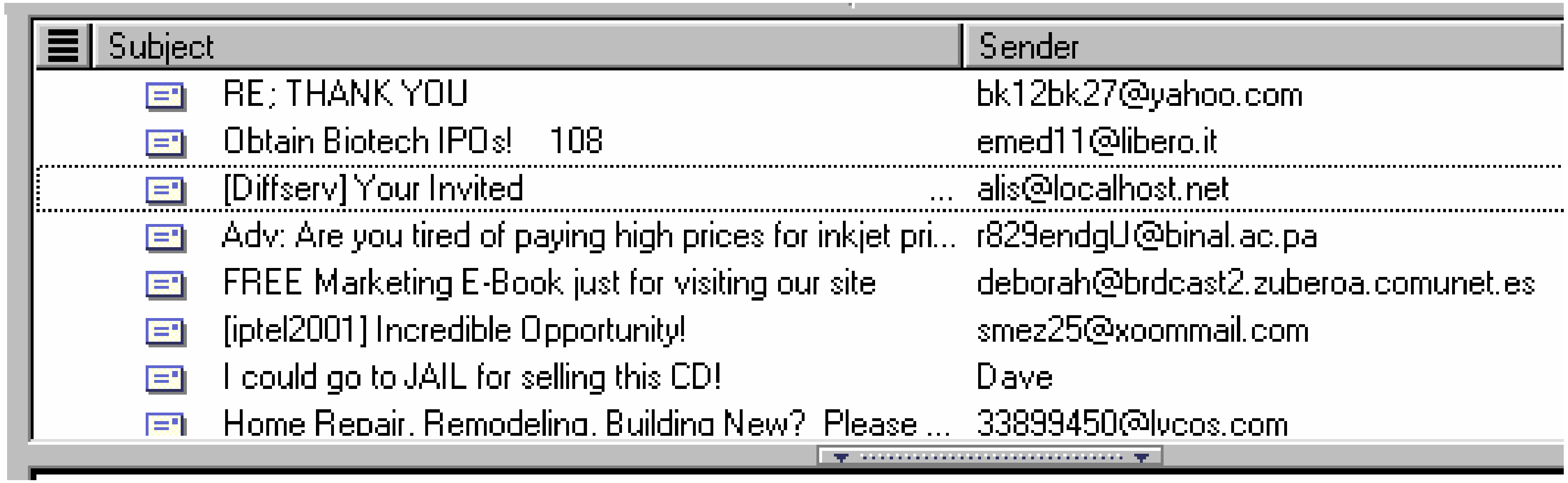
Denial of Service

- Different DoS attack mutations: paralyze servers, paralyze clients, annoy subscribers, “careless attacks” by misconfiguration.
- So far ‘incidental’ DoS occurrences have been reported
  - 2004: an Asian manufacturer of predictive diallers chose to use our site as testing target → 200 calls reached our secretariat on that day
  - 2005: major IAD vendor’s firmware was upgraded to re-REGISTER at 3AM → resulting SIP avalanche put most of sites lame
- Reasonable SIP servers come with tools for detection of unusual traffic patterns (e.g., SER/pike), innovation underway (www.snocer.org, http://www.iptego.de/solutions/VSP/)
- Still: we are in infancy and human effort is needed to deal with the invasion days
- Recommendation: deploy monitoring tools and analyze traffic regularly

draft-ietf-sipping-spam

SPIT (Spam over Internet Telephony)

- This is really discomforting image: world’s telemarketers offering you their goods over the Internet at virtually no cost for them.



Subject	Sender
RE: THANK YOU	bk12bk27@yahoo.com
Obtain Biotech IPOs! 108	emed11@libero.it
[Diffserv] Your Invited ...	alis@localhost.net
Adv: Are you tired of paying high prices for inkjet pri...	r829endgU@binal.ac.pa
FREE Marketing E-Book just for visiting our site	deborah@brdcast2.zuberoa.comunet.es
[iptel2001] Incredible Opportunity!	smez25@xoommail.com
I could go to JAIL for selling this CD!	Dave
Home Repair, Remodeling, Building New? Please ...	33899450@lycos.com

Dave: I could go to jail for selling this CD!

- Just look at some of the things you can do with this CD ...
- Save hundreds or even thousands of dollars on your taxes by using the secret tax tips contained in this package.
- Find out where your EX is hiding their money to avoid alimony, child support, or divorce settlements.
- If your EX is coming after your money, stay one step ahead of the lawyers and keep their greedy hands off your loot. Find out how to hide your money where it will never be found. Then get your hands on that money. Bleed 'em dry! Private investigators charge thousands of dollars for this service, but you can do it with a computer and an internet conection when you buy the Banned CD!
- Learn how to use offshore money havens and asset protection trusts to avoid lawsuits, judgments, and fool the most aggressive tax collector!
- Find out where to buy "forbidden products" on the Internet. Further elaboration should not be necessary; just use your imagination.
- Get a better job by purchasing a college degree (including a Phd!) for a very low fee. No study required!

We Should Really Do Something About It Before It Is Too Late!!!

- Legally
  - Telephone Consumer Protection Act of 1991 puts restrictions on telemarketers: do-not-call lists, 8am-9pm, no automatic dialing systems, no junk fax, etc.
  - hard to identify the physical sender in the Internet: anonymous accounts, IP addresses not fixed, application-layer addresses spoofed
- By economic means
  - paying for Internet calls unlikely to get acceptance
- Beat'em: Strike-Back
  - illegal
  - you never know whom you strike
  - you disclose more about you

Defeating Spam (cont.)

- “Please, remove me”
  - you disclose more about you
  - your address and 50 000 others will be sent to other spammers with instructions “these addresses ought not receive mass e-mail”
- Prevent Spammers From Getting Your Address Easily
  - advertise your address as GIF
  - generate mailto: in JavaScript
  - doesn’t work if you post to archived mailing lists
- **Filtering**
  - requires least user’s effort: setting up a filter; the effort can be easily delegated to local or a 3-rd party site
  - filtering criteria may include but are not limited to: presence on IP black-list, presence on application-layer black-list, application-layer address not matching IP address

What Shall I Pick to Protect Myself From SPIT?

- We don’t really know the patterns yet – in any case a prerequisite for filtering unwanted traffic is accountability. For which we need notion of identity (see previous slides).

Note Well: Every List is Too Short for All Attacks

- This section was mostly about protocol security: still attackers can be very inventive and can find easier ways to break in than cracking crypto-algorithms:
- Exploiting careless administrative practices: weak passwords, too generous administrative access, infrequent updates with security patches, insecure way of storing passwords, etc.
- Accessing paid services with stolen credit card numbers.
- Physical security violation (e.g., wiretap administrative network)
- Misuse of privileges (e.g., revenge of a fired administrator)
- VOIPSA lists a long list of possible threats
  - http://www.voipsa.org/Activities

Security Summary

- Today’s BCP (digest+identity+TLS) provides a reasonable mix of SIP security to achieve proper and viable service access control, accounting, identity. Cryptographic identity as a prerequisite for traceability and accountability emerging.
- Media security still emerging. ZRTP most appealing candidate because of its simplicity.
- As long as SIP still young, deployments’ security (DoS protection, policy making, SPIT avoidance, …) by large does rely on human effort of skilled professionals: review and test firewall policies, audit proper use of security protocols, verify SIP Access Control Lists, monitor traffic, keep applying OS security patches.

SIP Services

- Service space
- Internet Services (messaging, presence, …)
- PBX-services
- Service Programming

Service Space

- Traditional “PBX services”
  - Some reproducible with SIP 1:1, such as call forwarding
  - Some hard to reproduce, such as call parking
  - Some reproducible in different ways, such as voicemail by E-mail
- Native Internet Services, e.g.
  - Instant messaging and presence
  - Web integration such as click-to-dial
- Killer applications
  - … and other nonsense is out-of-scope of this tutorial.

Instant Messaging and Presence

- Idea: Use the same signaling vehicle for more services
- SIP already supports:
  - Notion of presence and user location mechanisms
  - Application-layer routing (incl. forking) and message processing (e.g., CPL)
  - Security: authentication

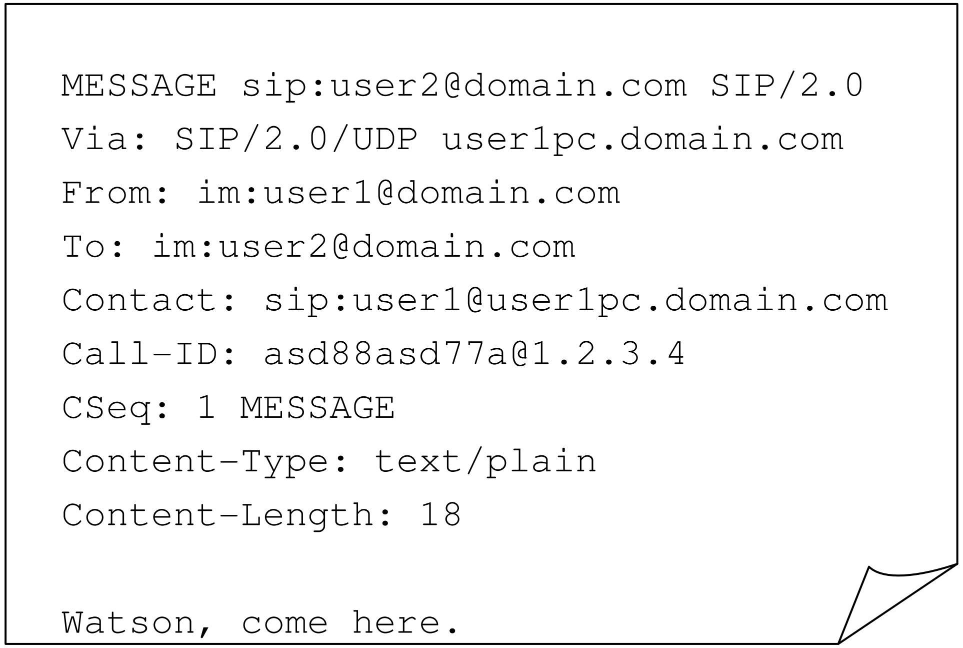
Example of Native Internet Convenience Services

- Applications demanded and deployed are mostly about service integration:
  - E-mail: replacement of IVR annoyance with voicemail-2-e-mail
  - Web: read list of missed calls from your webpage (both off-line and on-line)
  - Web: online phonebook, click-to-dial
  - Instant Messaging and Presence, Notification services (T-storm alarm), SMS delivery
  - Telephony: conferencing
- Technical challenge: make service programming easy

RFC3428
RFC3682

Instant Messaging

- Goal: deliver short messages rapidly
- SIP Extension: “MESSAGE” Method
  - Message body of any MIME type (including Common Profile for Instant Messaging, RFC2682)
- MESSAGE requests are routed and processed by proxy servers like INVITEs are – no special treatment required



```
MESSAGE sip:user2@domain.com SIP/2.0
Via: SIP/2.0/UDP user1pc.domain.com
From: im:user1@domain.com
To: im:user2@domain.com
Contact: sip:user1@user1pc.domain.com
Call-ID: asd88asd77a@1.2.3.4
CSeq: 1 MESSAGE
Content-Type: text/plain
Content-Length: 18

Watson, come here.
```

RFC3265

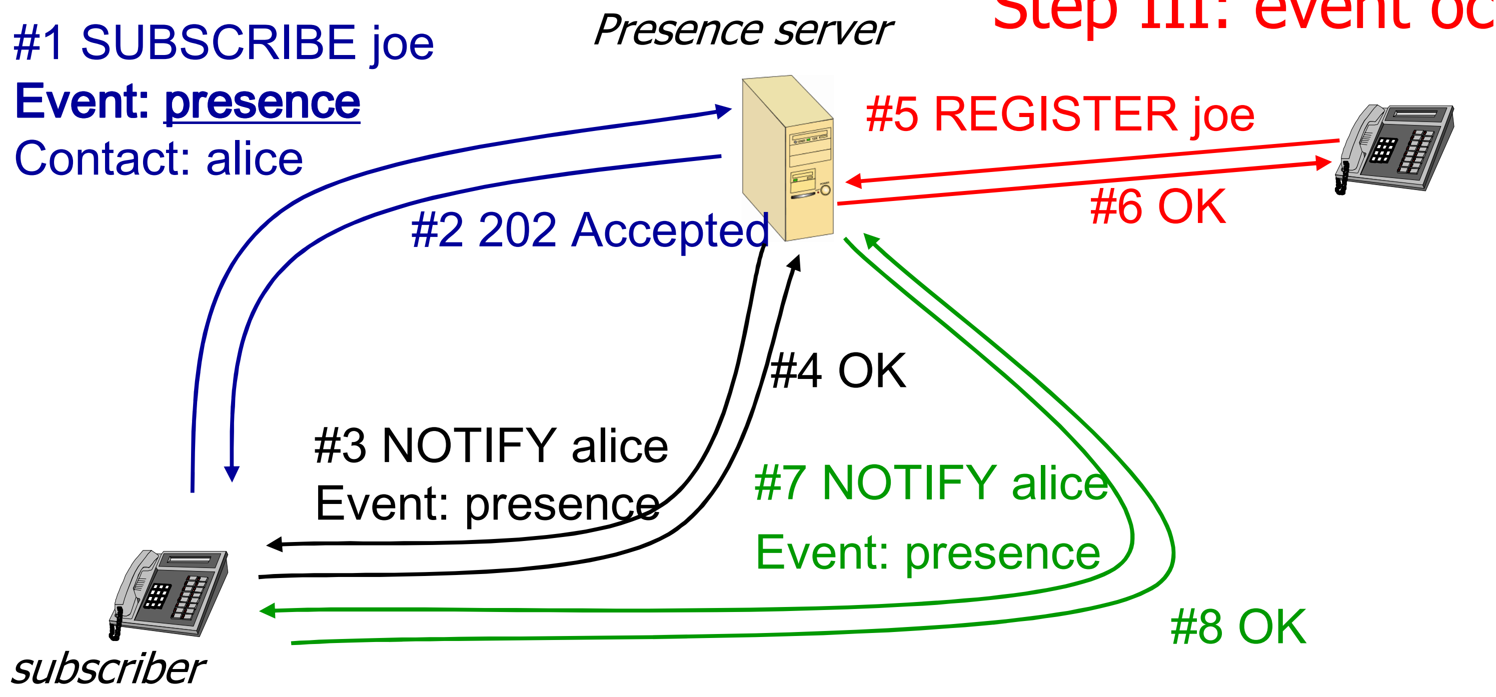
Subscribe-Notify

- Goal: ability to be notified when a condition occurs
- Applications:
  - User presence and related applications
  - Call-back (notify when the other party becomes available)
  - VoiceMail Notification (notify when a voicemail message is stored) *[RFC3842]*
  - Traffic Alerts (notify on traffic jam)
- Extensions: “SUBSRIBE” and “NOTIFY” methods, “Event” and “Allow-Events” headers define application, “489 Bad Event” Response Codes define error behaviour
- Subscription designed soft-state: subject to expiration similarly to how REGISTER is.
- Note: there is competing SIP-free standard based on Jabber/XMPP

Subscribe-Notify For Presence Services

RFC3856

Step I: subscription to a condition



#1 SUBSCRIBE joe
Event: presence
Contact: alice

Step III: event occurs

Step IV: subscriber is notified whenever condition changes

Step II: subscriber is immediately notified on current condition

Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

Presence Is More Than SUB-NOT…

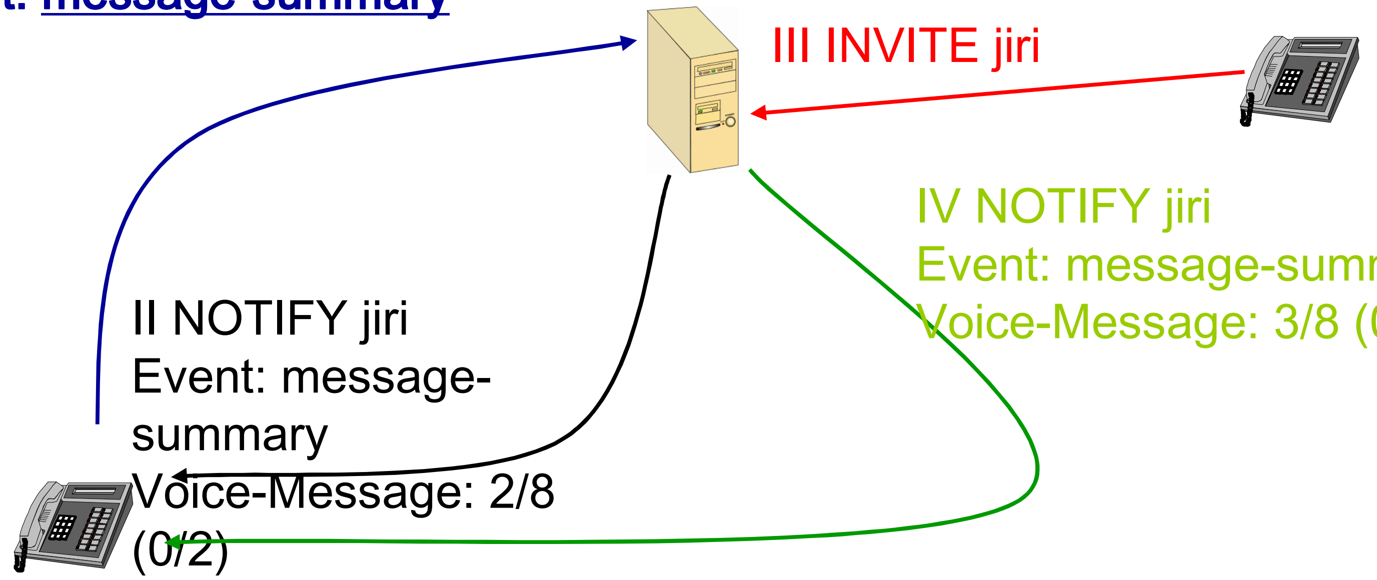
- Provisioning of authorization lists, buddy-lists, and other data
  - XCAP (draft-ietf-simple-xcap)
- Data
  - PIDF: Presence Information Data Format/PIDF (RFC3863)
  - RPID: Rich Presence Extensions to PIDF (RFC4480)
  - Data Model (RFC4479)
- More
  - See http://www.ietf.org/html.charters/simple-charter.html

Subscribe Notify for Message Waiting Indication (MWI)

RFC3842

Step I: subscription to a condition

I. SUBSCRIBE jiri@voicemail
Event: <u>message-summary</u>



Step III: event occurs: someone leaves a voicemail

Step IV: subscriber is notified whenever condition changes

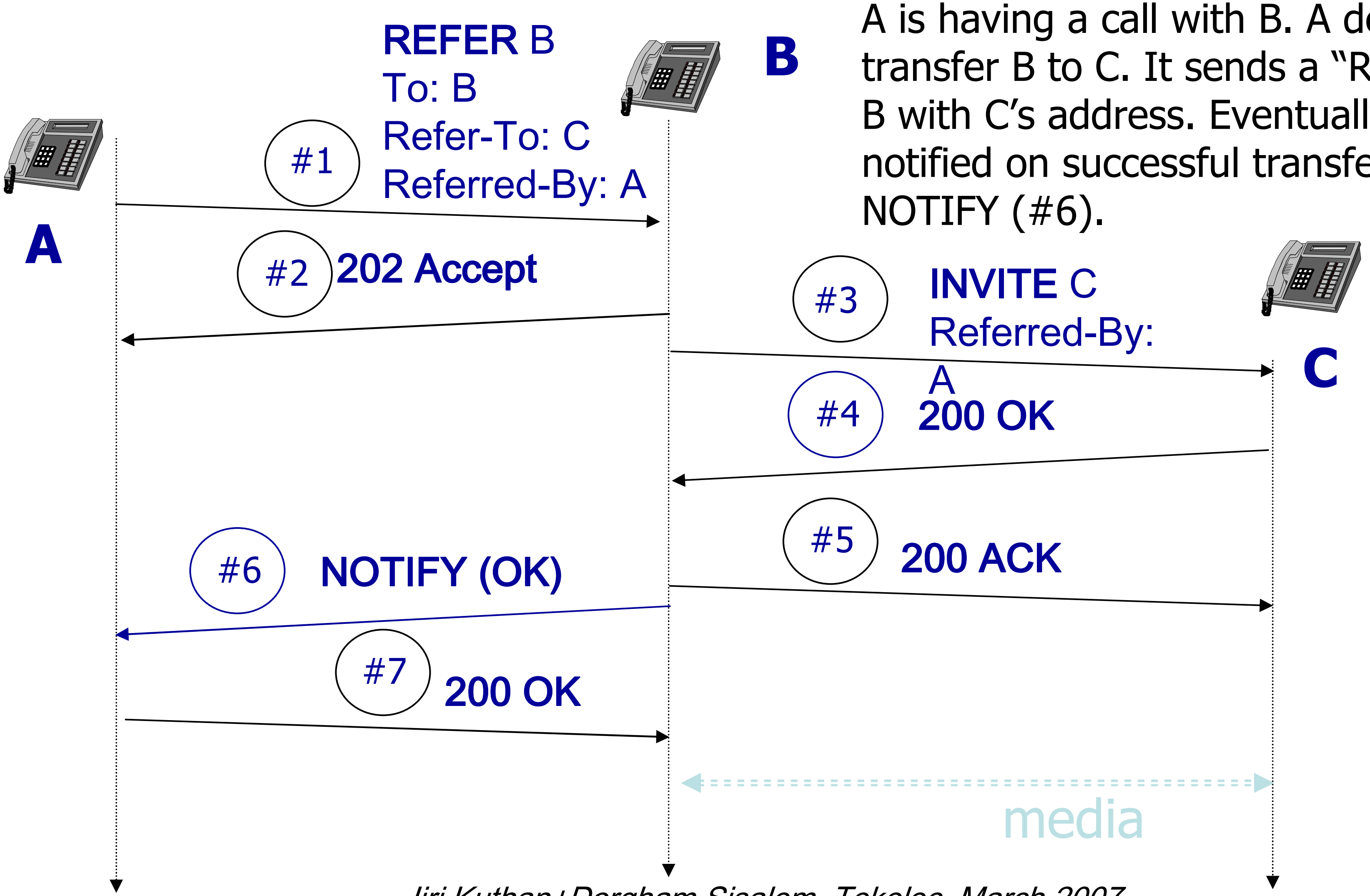
Step II: subscriber is immediately notified on current condition

More PBX-like Services with SIP

- Most of PBX services are implemented with SIP; some in servers (S), some in clients (C)
  - MWI (C and S)
  - (Un)conditional call forwarding (S)
  - abbreviated dialing (C or S)
  - Screening (S)
  - distinctive ringing (C or S)
  - call distribution (S)
  - call transfer (C: REFER)
  - Conferencing (C or S)
  - Call-on-hold (C: re-INVITE)
  - Call-waiting (C)
  - Redial (C or C+S)
  - Follow-me (forking) S
  - Caller-ID (built-in)
  - DND (C or S)
- Sometimes, implementation logic may completely differ.
  - Televoting and IVRs likely to be replaced by Web in the long run.
  - Missed-call keypad sequences (#*…) better served by instant messaging and email

Example:
Call Transfer Call Flow

A is having a call with B. A decides to transfer B to C. It sends a "REFER" to B with C's address. Eventually, A is notified on successful transfer using NOTIFY (#6).

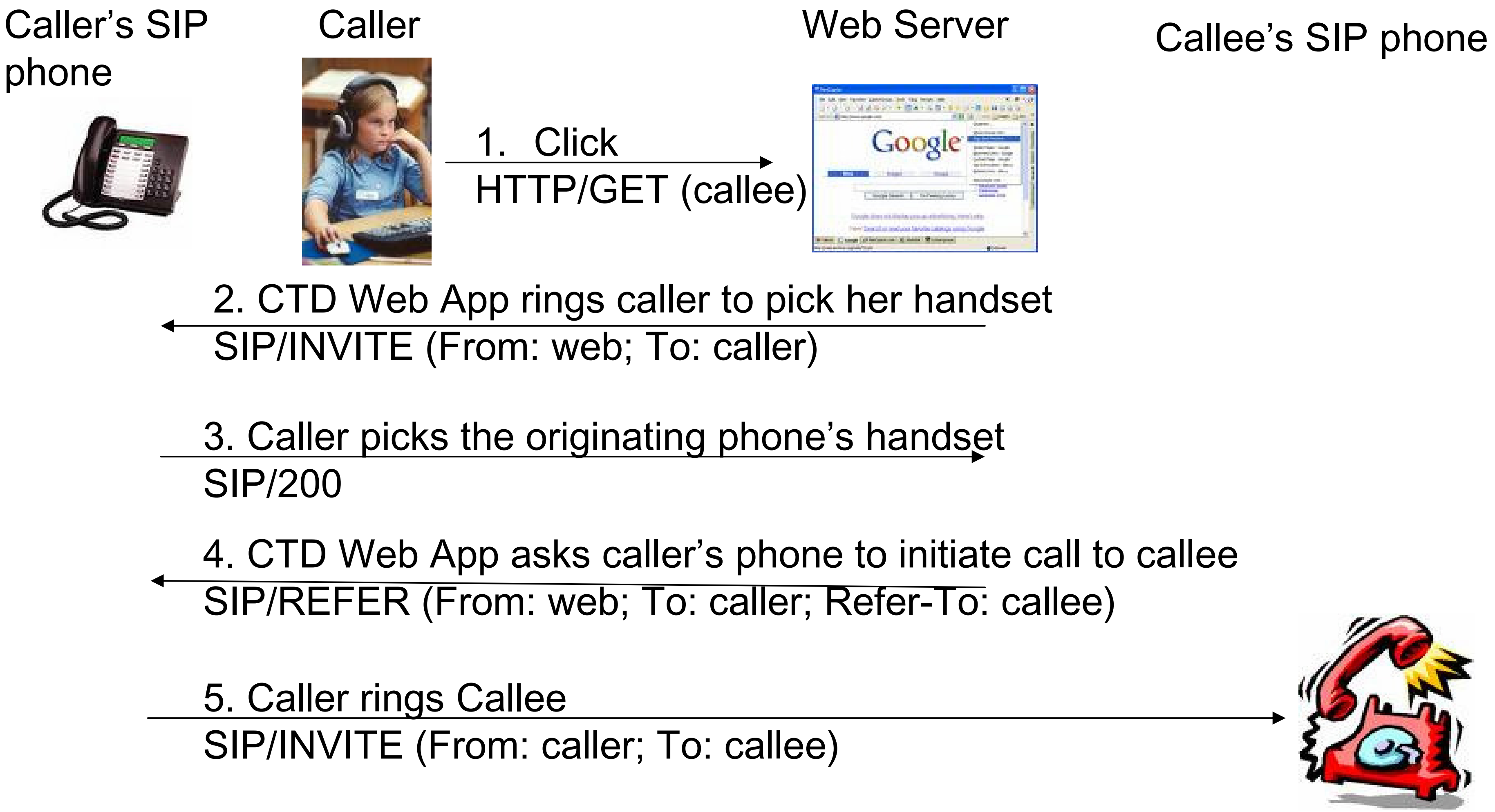


Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

Call Transfer/REFER

- Accomplished using the REFER method.
- The REFER method indicates that the recipient (identified by the Request-URI) should contact a third party using the contact information provided in the method.
- New header fields: Refer-To, Refer-By.
- NOTIFY method used to report on result of referral.
- Note: No changes to proxy behavior required.
- Variants:
  - With Consultation Hold (SIP Hold and unattended transfer)
  - Attended Transfer, I.e., with a short conference
- REFER is a general method to have a phone called someone else, other applications than call transfer possible.

Click-to-Dial Using REFER



Caller's SIP phone

Caller

Web Server

Callee's SIP phone

1. Click
HTTP/GET (callee)

2. CTD Web App rings caller to pick her handset
SIP/INVITE (From: web; To: caller)

3. Caller picks the originating phone's handset
SIP/200

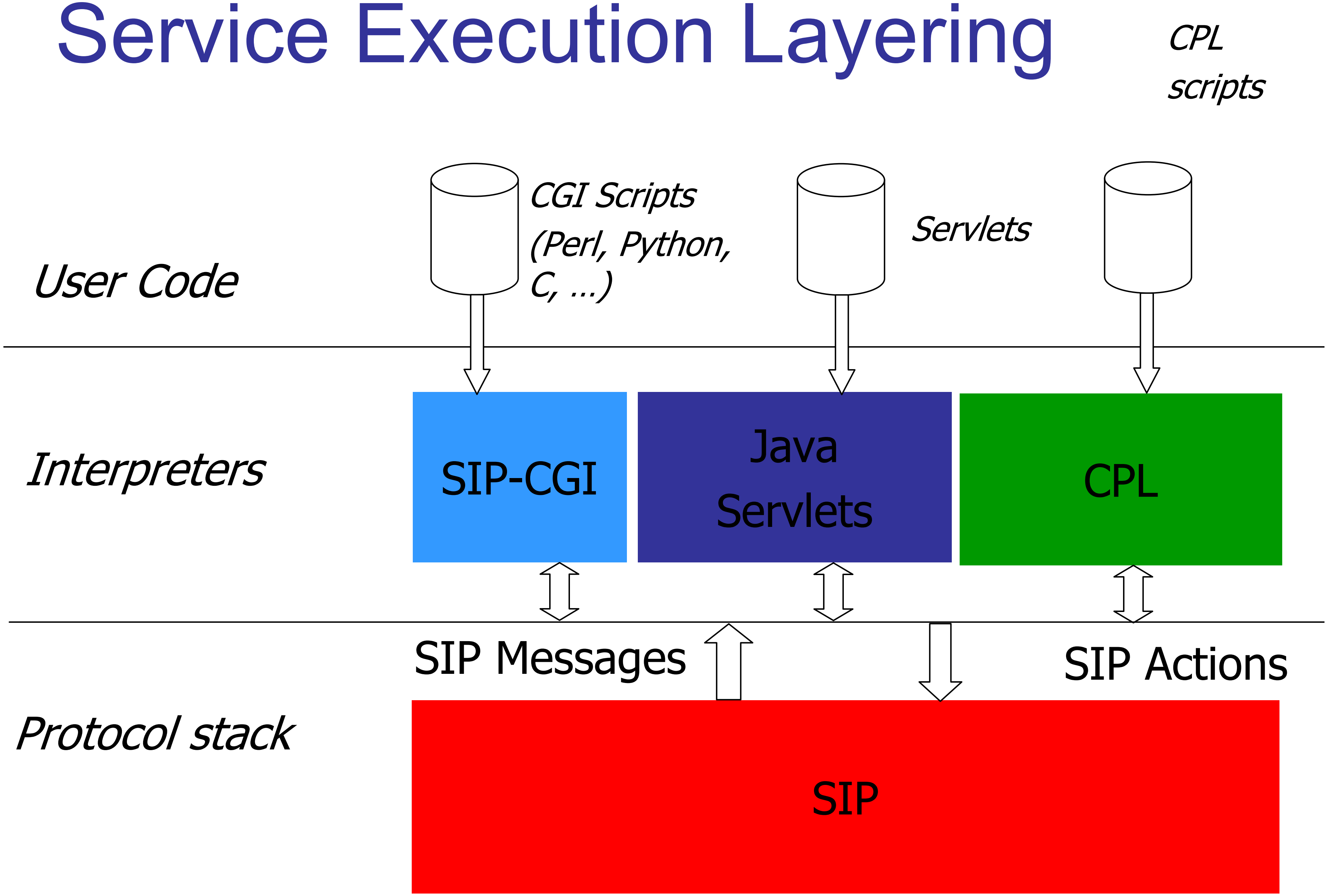
4. CTD Web App asks caller's phone to initiate call to callee
SIP/REFER (From: web; To: caller; Refer-To: callee)

5. Caller rings Callee
SIP/INVITE (From: caller; To: callee)

Programming Network Services

- Desires
  - Introduce new services, say “welcome-message” to new subscribers, on a quick notice
  - Allow users to “co-define” the services by inexpensive “self-service” tools
  - Don’t impair existing infrastructure and services when introducing new services
- General Concept:
  - create a “sandbox” on top of basic SIP server logic which can help to implement new logic in server without impairing existing logic.
  - If remaining concern about availability of the core infrastructure still high, its programmable logic may be limited to forwarding to specialized application servers (e.g., presence servers, message stores, voicemail, etc.)

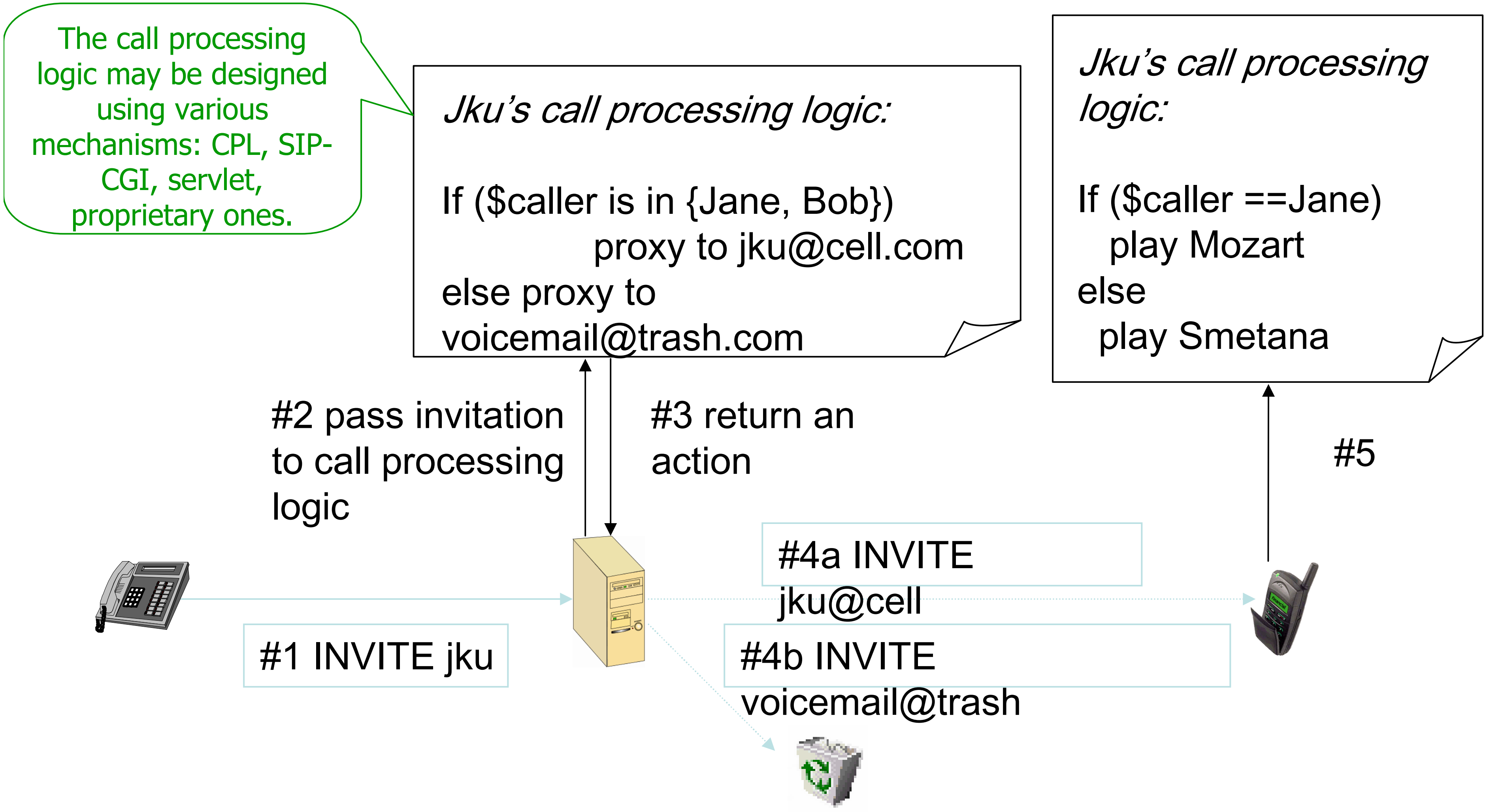
Service Execution Layering



“Sandbox Power Trade-off”

- There is a “sandbox trade-off”:
  - too powerful programming environment (low “sandbox factor”) allows programmers to destroy a service
  - High sandbox factor: programmability constrained in interest of safety
  - Solution to the trade-off: different “sandbox-factor” technologies for different uses
- Sandbox factor high
  - Call Processing Language (RFC3880), CPL, specialized HTML-based limited-purpose language whose constrained environment allows use by laymen without damage
- Sandbox factor: medium
  - JAIN SIP Servlets: “sanbox-factor” configurable in Java Virtual Machine’s sandbox; for use by professionals (www.sipservlet.org)
- Sandbox factor: low
  - SIP-CGI (RFC3050): completely unlimited access to system resources; only for use by professionals
- Other proprietary service programming environments also exist with various sandbox factors

Call Processing Logic Example



The call processing logic may be designed using various mechanisms: CPL, SIP-CGI, servlet, proprietary ones.

Jku’s call processing logic:

```
If ($caller is in {Jane, Bob})
            proxy to jku@cell.com
else proxy to
voicemail@trash.com
```

Jku’s call processing logic:

```
If ($caller ==Jane)
   play Mozart
else
  play Smetana
```

#2 pass invitation to call processing logic

#3 return an action

#5

#4a INVITE jku@cell

#1 INVITE jku

#4b INVITE voicemail@trash

RFC 3050

SIP Common Gateway Interface (CGI)

- Follows Web-CGI. Unlike Web-CGI, SIP-CGI supports proxying and processes responses as well.
- Language-indpendent (Perl, C, ...)
- Communicates through input/output and environment variables.
- CGI programs unlimited in their power. Drawback: Buggy scripts may affect server behavior easily.
- Persistency token (cookie) is passed between SIP server and CGI to keep state across requests and related responses.

SIP-CGI I/O

- Script input: environment variables (AUTH_TYPE, CONTENT_LENGTH, REQUEST_URI, etc.) and SIP message on stdin
- Script output: set of messages consisting of action lines, CGI header fields and SIP header fields on stdout
- Action lines:
  - Generating a response: status line
  - Proxying:
    - `CGI-PROXY-REQUEST <dest-url> <sip-version>`
    - Additional header fields may be followed – they will be merged with the original request.
  - Forward response: `CGI-FORWARD-RESPONSE <token> <sip-version>`
  - Set cookie for subsequent messages: `CGI-SET-COOKIE <token> <sip-version>`
  - Determine if the script should be called for the next message belonging to the same transaction: `CGI-AGAIN ("yes" | "no") <sip-version>`

RFC3880

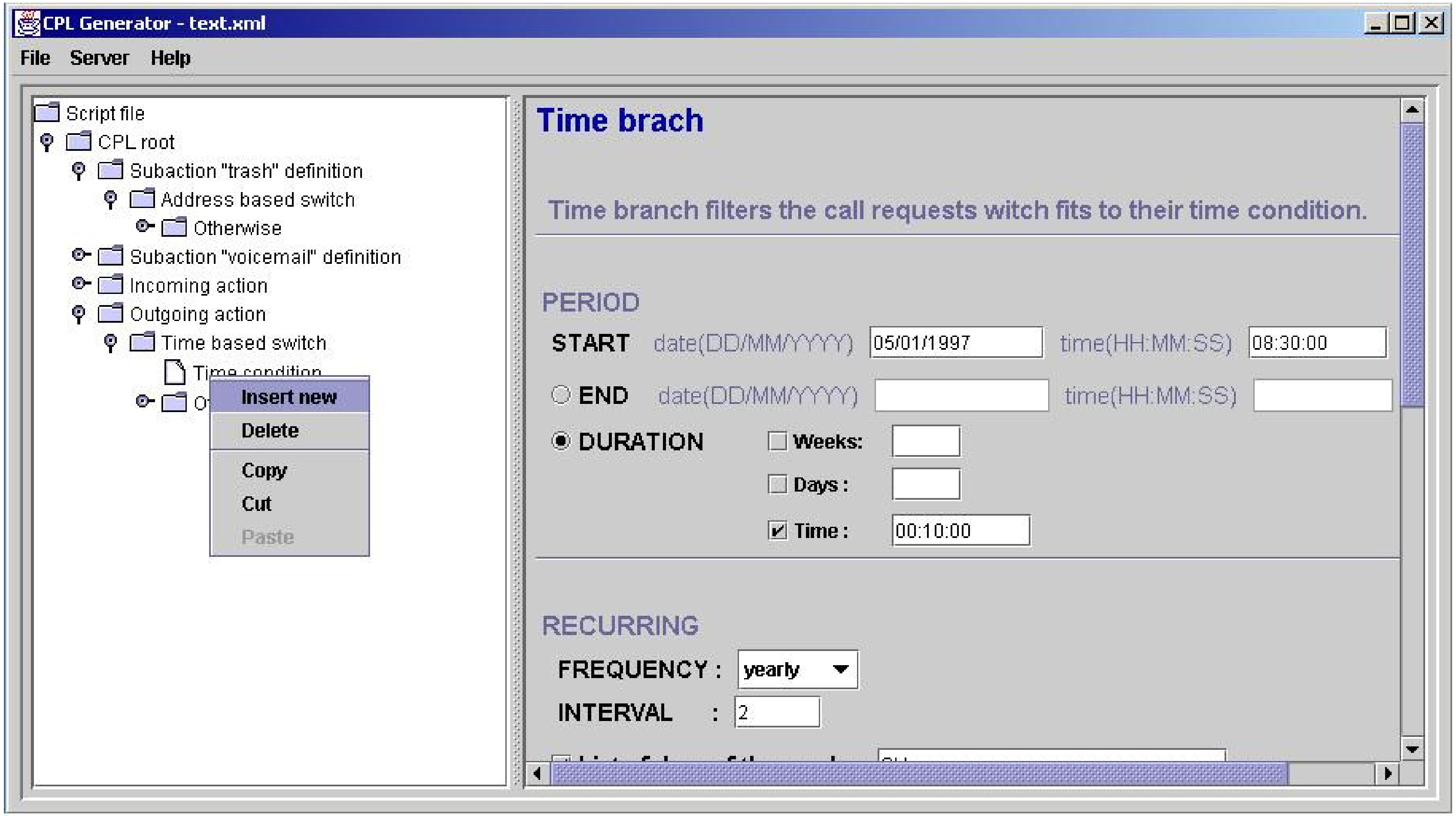
Call Processing Language

- Special-purpose call processing language.
- CPL scripts define a decision tree which may result in signaling (proxy, redirect, reject) or non-signaling (mail, log) action.
- CPL scripts triggered by SIP messages.
- Target scenario: users determine call processing logic executed at a server. The CPL scripts are generated by a convenient web interface.
- Limited languages scope makes sure server’s security will not get compromised.
- Portability allows users to move CPL scripts across servers.

CPL Example

```
<incoming>
      <address-switch field="origin" subfield="host">
                <address subdomain-of="example.com">
                <location url="sip:jones@example.com">
                <proxy timeout="10">
                         <busy> <sub ref="voicemail" /> </busy>
                         <noanswer> <sub ref="voicemail" /> </noanswer>
                         <failure> <sub ref="voicemail" /> </failure>
                </proxy>
                </location>
        </address>
        <otherwise>
                <sub ref="voicemail" />
        </otherwise>
      </address-switch>
 </incoming>
```

Example: Creating CPL Scripts



- Script file
  - CPL root
    - Subaction "trash" definition
      - Address based switch
        - Otherwise
    - Subaction "voicemail" definition
    - Incoming action
    - Outgoing action
      - Time based switch
        - Time condition
        - O

Time brach

Time branch filters the call requests witch fits to their time condition.

PERIOD

START date(DD/MM/YYYY) 05/01/1997 time(HH:MM:SS) 08:30:00

○ END date(DD/MM/YYYY) time(HH:MM:SS)

● DURATION ☐ Weeks: ☐ Days : ☑ Time : 00:10:00

RECURRING

FREQUENCY : yearly

INTERVAL : 2

iptel.org: CPL Composer

Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

Summary SIP Services

- There are both native Internet services based on SIP as well as such mimicking PBX behavior
- Some of services may be implemented in different ways (e.g., server-based versus client-based conferencing).
- To allow for programmability of services, there are both standardized (SIP-CGI, CPL, JAIN) and proprietary techniques. They primarily differ in their security and powerfulness.

Black-Belt SIP: Short Overview of Some Advanced Techniques

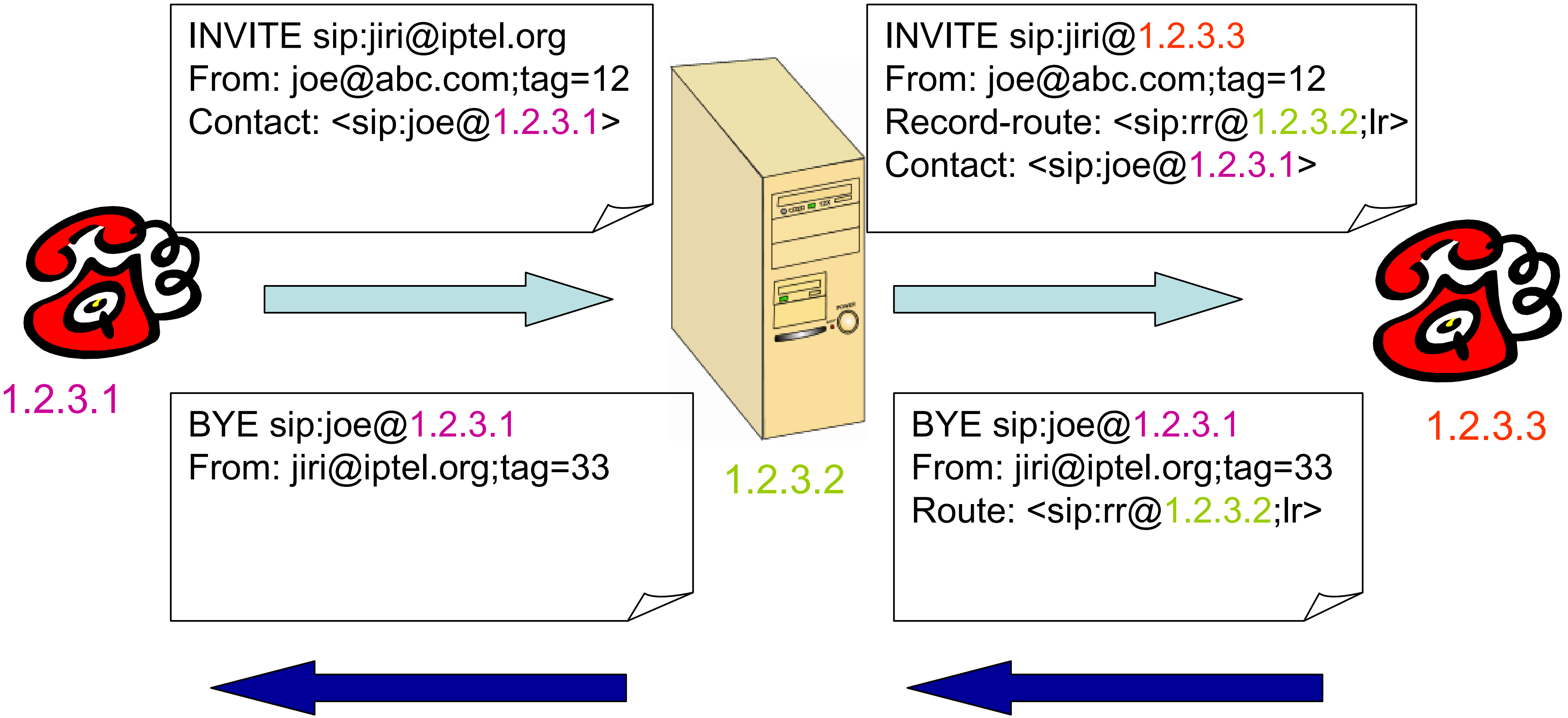
- •Record-routing
- •Session-timer
- •SigComp
- •Peer-2-peer

Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

Record-Routing

- Refresher: by default, only the initial request (INVITE) visits a proxy, subsequent requests (BYE) travel directly to offload servers
- Problems:
  - some applications need to corelate requests with answers (accounting) or “pick” best answer (forking)
  - UAs may live in different protocol realms (TCP vs UDP, IPv4 versus v6) and can communicate only through the proxy server
  - Troubleshooting hard if messages bypass a server under troubleshooter’s control
- Solution: record-routing: proxy servers “sign” themselves in forwarded requests to demand staying in the path for subsequent communication
- BCPs: proxy servers always record-route, the historical leight-weighted “only initial request hits the server” approach used only in special cases

Record-Routing Example



INVITE sip:jiri@iptel.org
From: joe@abc.com;tag=12
Contact: <sip:joe@1.2.3.1>

INVITE sip:jiri@1.2.3.3
From: joe@abc.com;tag=12
Record-route: <sip:rr@1.2.3.2;lr>
Contact: <sip:joe@1.2.3.1>

BYE sip:joe@1.2.3.1
From: jiri@iptel.org;tag=33

BYE sip:joe@1.2.3.1
From: jiri@iptel.org;tag=33
Route: <sip:rr@1.2.3.2;lr>

Another Record-Routing Use

- Record-Routing can be also use to piggy-back session-state in SIP messages to leave server state-less
- Example:
  - A RR-parameter can include timestamp for initial invite
  - When CDRs are generated on receipt of BYE, the call duration is calculated as “current_time()-rr_timestamp_parameter()”
  - Note: In security-sensitive application like above, it is necessary to introduce message integrity

RFC4028

Session Timer

- Typical problem to solve: how does a PSTN gateway make sure that calling SIP phone is not abruptly gone and still charged?
- Answer: test if it is still alive
- Mechanism: negotiate appropriate keep-alive interval and use re-INVITEs (or UPDATEs) to send the actual keep-alives

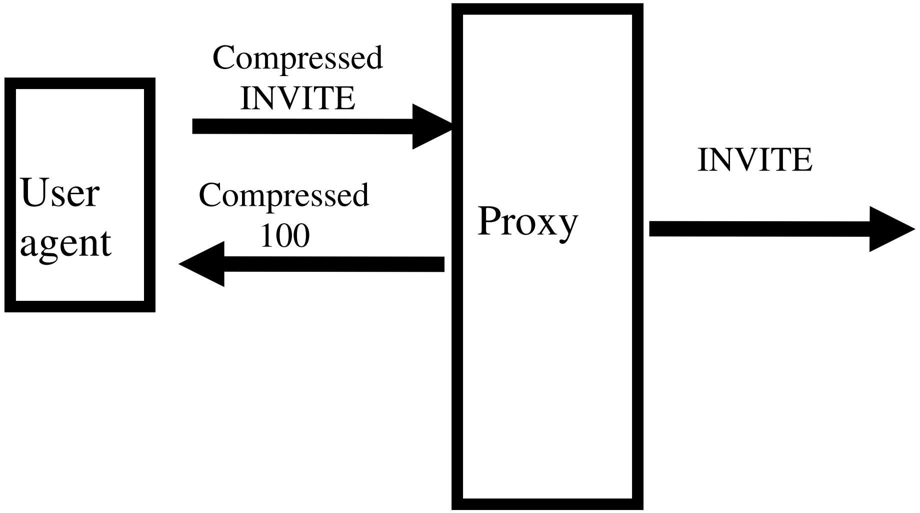
Notion of Dialog

- So far we have vaguely referred to – based on application in question -- calls and session, how is it exactly defined?
- As "**dialog**" – application-independent communication relationship between two UAs, e.g., a VoIP call or a chat session. Dialog is identified by three SIP message elements: CallID, From-tag (caller-generated) and To-tag (callee-generated)
- Always look at the whole triple!
  - Poor client implementations may fail to generate sufficiently unique Call-ID and from-tag
  - Parallel forking may lead to multiple dialogs established by a single call atempt. The dialogs are differentiated only by peer's To-tag!

RFC3320

SIGCOMP / SIP

- SIGCOMP – IETF protocol (rfc3320) used for signaling compression
- Designed for speeding up text based signaling (like SIP) on low bandwidth links (e.g. WCDMA)
- Mainstream (SIP for VoIP with basic call setup) case measured in our lab has shown compression down by 70% using deflate algorithm (fixed size Huffman codes)

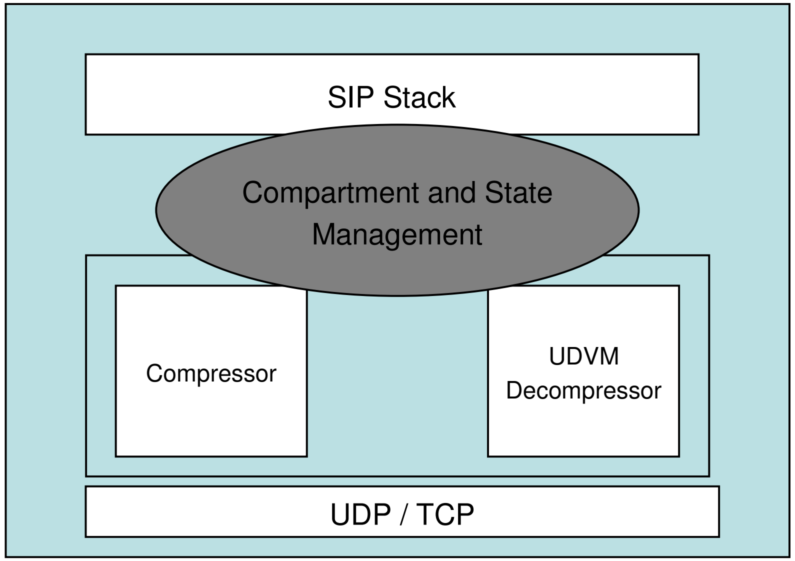


SIGCOMP / SIP

- High compression rates can be attained when using dynamic/stateful compression (up to 3 to 1 for the whole call and 5+ to 1 for certain messages)
- Two approaches for stateful compression:
  - Optimistic (NACK – rfc4077) – assume the remote state was created and use it; if it is not there a NACK will be sent by the remote end
  - Pessimistic (feedback based) – never use a state unless it was acknowledged.

SIGCOMP / SIP

- Decompression is performed using a virtual machine (UDVM)
- Very flexible since compressor sends decompression bytecode along with the compressed data
  - SIP/SDP static-dictionary compression : RFC3485



The peer-2-peer fascination

- Couldn't we save money if we make SIP network serverless? No boxes, no admins, reliability and scalability given by the massive amount of cooperating peers.
  - Partially true. Many features are hard-to-accomplish in fully peer-2-peer way: naming, authentication, PSTN routing, …
- Skype has done that already but … it is deploying a proprietary walled-garden model. With SIP, that can change.
- More information: www.p2psip.org

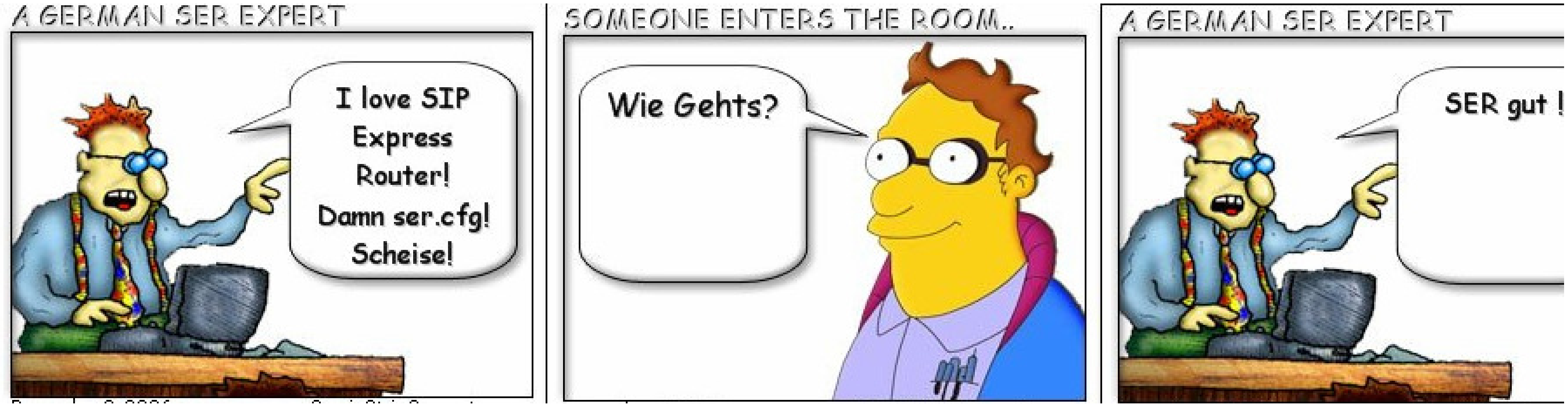
SIP Express Router (SER)

Would you like to get hands on and play with a baby setup?

About SER: iptel.org/ser

- **SER** is free, GPL-ed SIP server with RFC3261 functionality (registrar, proxy, redirect) running on UN*X platforms used by numerous ISPs, ASPs, universities, and others too.
- SER key features are **configurability**, **performance** and **interoperability**. Full feature list: http://iptel.org/ser/features
- These features are its down-side at the same time – experts can greatly leverage those but must first spend time on learning curve to actually become experts.
- To play with basic VoIP services, just download it, configure it, and register a couple of VoIP telephones with it.
- *COMMERCIAL: Tekelec's carrier-grade IMS-ready product,* ***TekCore****, leverages SER, and offers high-available, scalable, proven platform for use by mobile operators.*

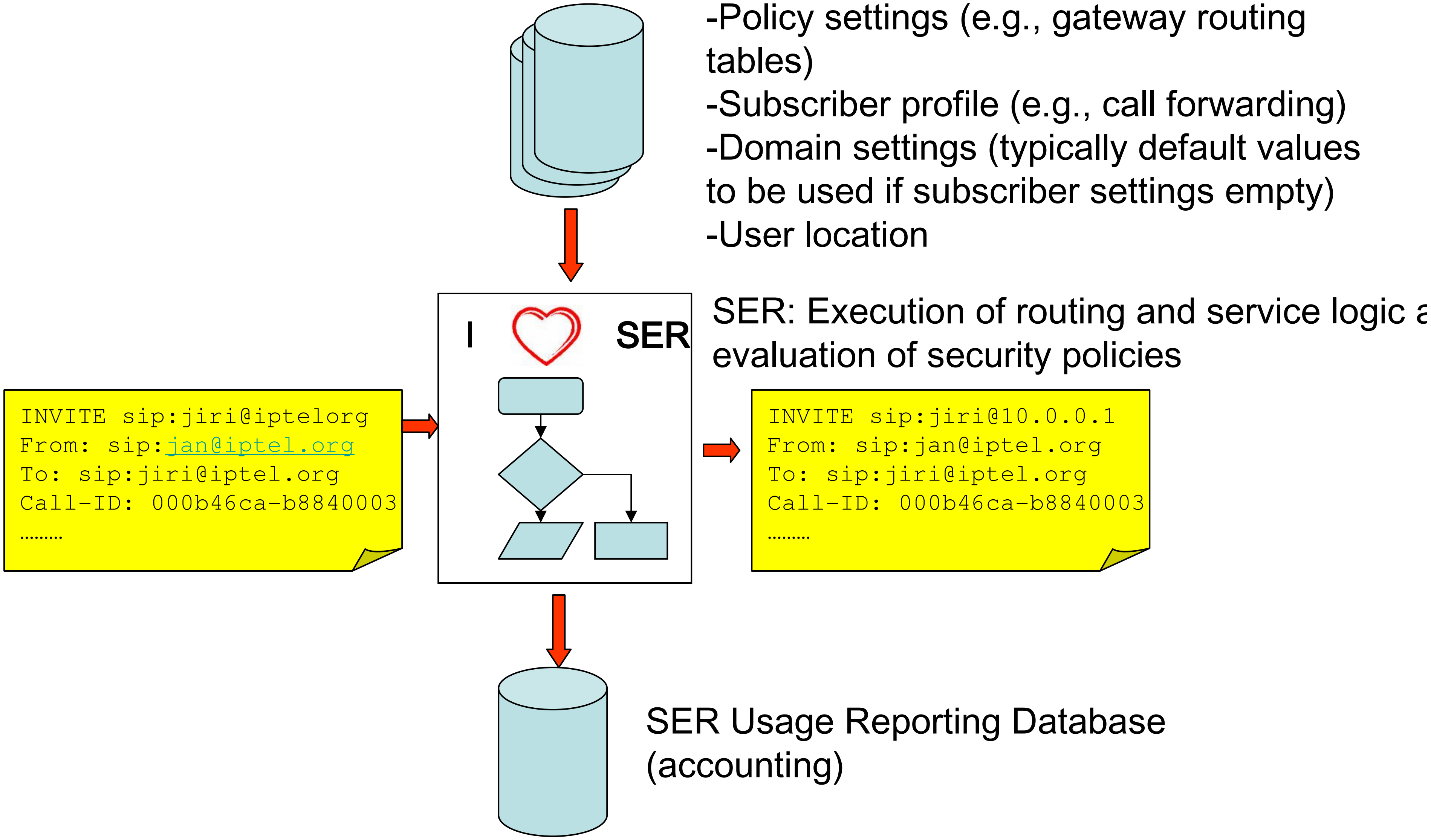
SER is Greatly Configurable


A GERMAN SER EXPERT
I love SIP Express Router! Damn ser.cfg! Scheise!
SOMEONE ENTERS THE ROOM..
Wie Gehts?
A GERMAN SER EXPERT
SER gut !

Picture Courtesy of Alfred E Heggestad

SER's configurability is real pain. The only worse thing that can happen is not to have it.

SER Data Flow



SER Database (provisioned data)
-Policy settings (e.g., gateway routing tables)
-Subscriber profile (e.g., call forwarding)
-Domain settings (typically default values to be used if subscriber settings empty)
-User location

```
INVITE sip:jiri@iptelorg
From: sip:jan@iptel.org
To: sip:jiri@iptel.org
Call-ID: 000b46ca-b8840003
………
```

SER: Execution of routing and service logic a evaluation of security policies

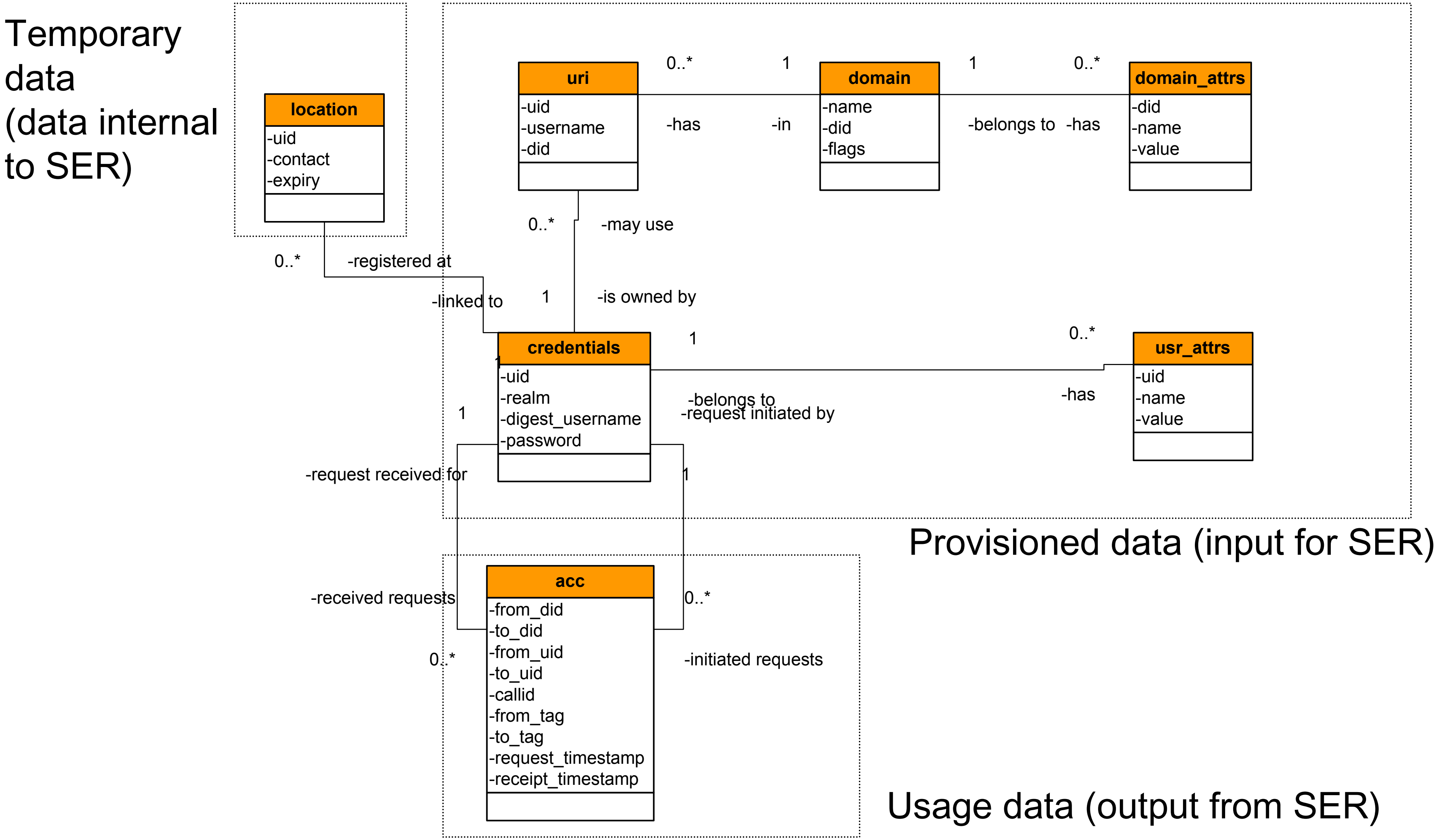
```
INVITE sip:jiri@10.0.0.1
From: sip:jan@iptel.org
To: sip:jiri@iptel.org
Call-ID: 000b46ca-b8840003
………
```

SER Usage Reporting Database (accounting)

World According to SER

- There are **domains** that SER serves
  - Domains are identified by an ID which can have synonymical names (foobar.com, sip.foobar.com) `[domain]`
  - Domains can have attributes associated with them (e.g., default subscriber settings if individual ones are not set) `[domain_attrs]`
- There are **subscribers** identified by a unique number (by default, UUID) and authenticated using a shared password `[credentials]`
  - A subscriber belongs to a served domain
  - Subscribers are associated with one or more URIs (aliases) representing their identity (sip:jiri@iptel.org, sip:jiri.kuthan@iptel.org, tel:+49179501234) `[uri]`
  - Further arbitrary parameters can be associated with subscribers (e.g., call-forwarding options, postal address, foobar parameter, just anything) `[usr_attrs]`
  - Subscribers can have none, one or many contacts of online SIP telephones (temporary “session data”) `[location]`

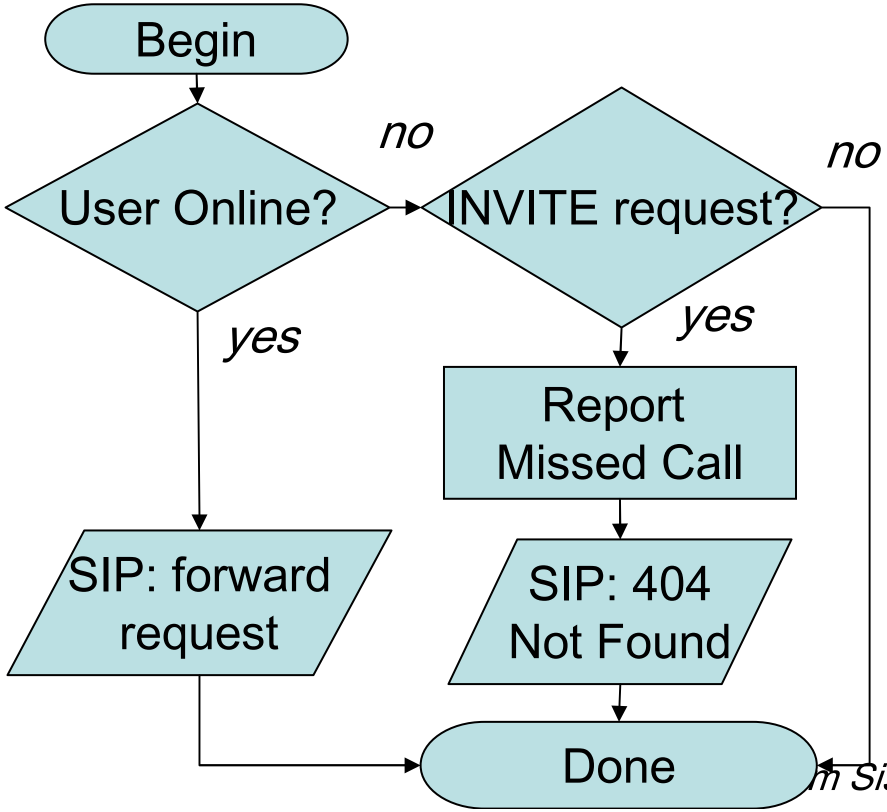
SER Data Model (simplified)



Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

Routing Language

- Request routing flexibility needed to link SIP components (voicemail, PSTN gateway, logging facility, etc.) together
- Answer: request routing language (features conditions, URI-rewriting, request modification, replying, etc.)
- Example: reporting missed calls



Begin

User Online?

no

INVITE request?

no

yes

yes

Report Missed Call

SIP: forward request

SIP: 404 Not Found

Done

SER Routing Language

```
/* user online ? */
if (lookup(“location”)) {
     t_relay();
     break;
};
if (method==“INVITE”) {
     /* report to syslog */
     log(“ACC: missed call\n”);
};
sl_send_reply(“404”,”Not Found”);
```

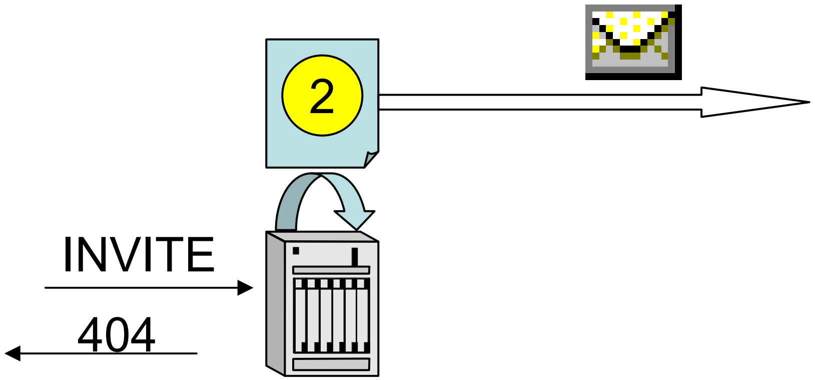
Extensibility: Modules

- Existing modules: RADIUS accounting, digest authentication, regular expressions, presence agent, nat traversal helper, multidomain support, etc., etc..... (about 40 today).

```
# SER script: challenge any user
# claiming our domain in From header
# field; good anti-spam practise; it
# uses module actions for RegExp and
# digest authentication

# apply a regular expression
if (!search(“From:.*iptel\.org”)
{
   # verify credentials
   if (!proxy_authenticate(
         "$fd.digest_realm" ,
         “credentials”)) {
        # challenge if credentials poor
        append_to_reply(
            "%$digest_challenge");
        sl_reply("407", "Proxy
                 Authentication
                 Required");
        break;
   }
}
```

Exec Module – Link to More Apps

- Exec module: starting external applications on request receipt; *(similar to but simpler than SIP CGI-BIN)*
- Features:
  - ability to use existing UN*X tools (mail, sed & awk, wget, …)
  - Language-independency
- Interface:
  - Request URI and header fields passed as environment variables to the applications
  - Whole request passed on standard input
  - Optionally, application's output evaluated as new request's URI (e.g., unconditional forwarding)



```
# SER script: execute an external
# command for off-line users
if (!lookup(“location”)) {
   /* log(“missed call”); */
   exec_msg(“/tmp/notify.sh”);
}
```

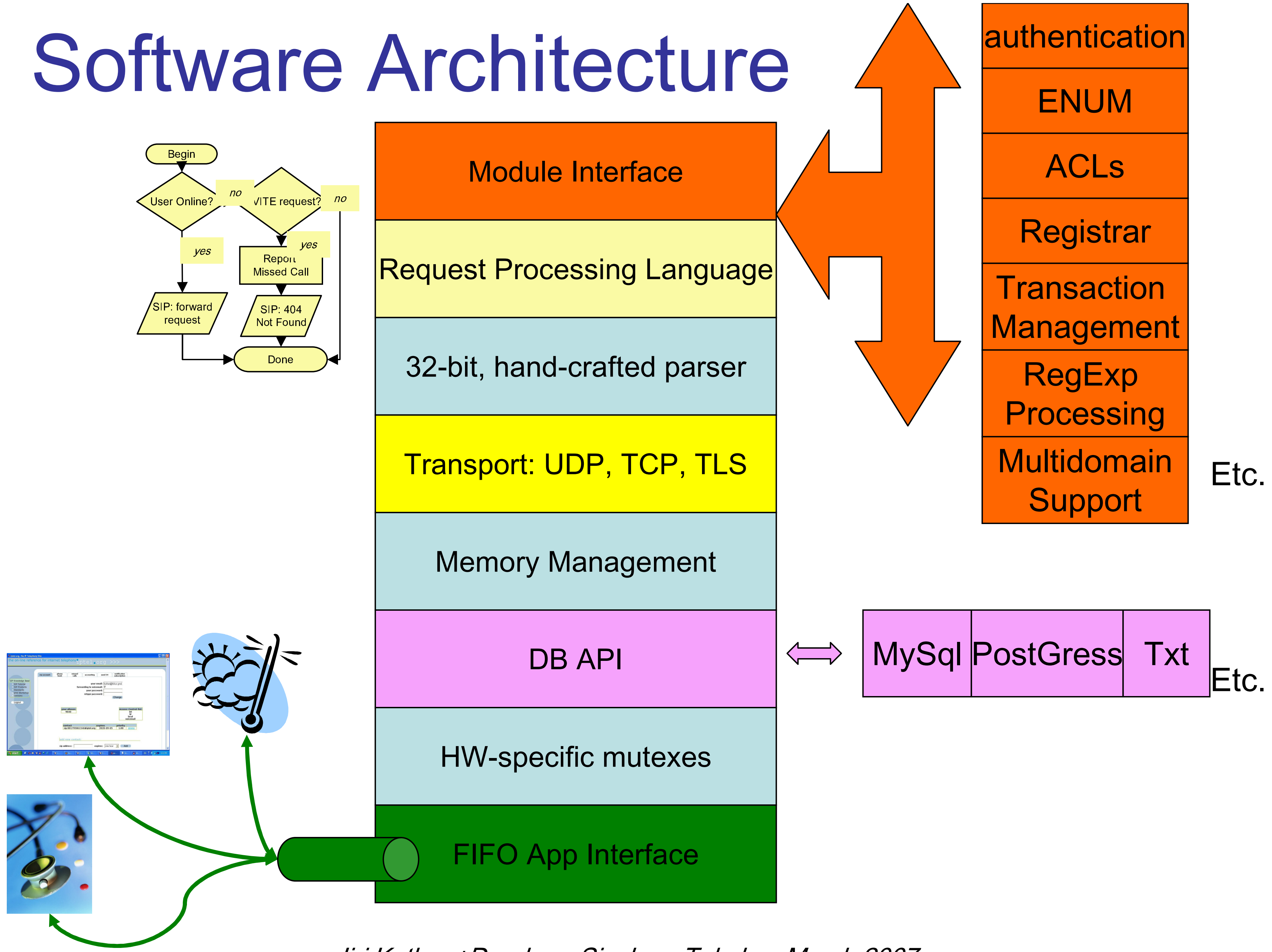
```
# shell script: send email
# notification

MAILTO=`user2email $SIP_USER`
printf “User %s called” \
  “$SIP_HF_FROM” |
  mail -s “Missed Call” $MAILTO
```

2

Interoperability: SER is de-facto Standard

- SER interop-tested in SIPITs since 2002
- Complete list of tested products counts more than 200 SIP devices!

Software Architecture



Module Interface

Request Processing Language

32-bit, hand-crafted parser

Transport: UDP, TCP, TLS

Memory Management

DB API

HW-specific mutexes

FIFO App Interface

authentication

ENUM

ACLs

Registrar

Transaction Management

RegExp Processing

Multidomain Support

Etc.

MySql

PostGress

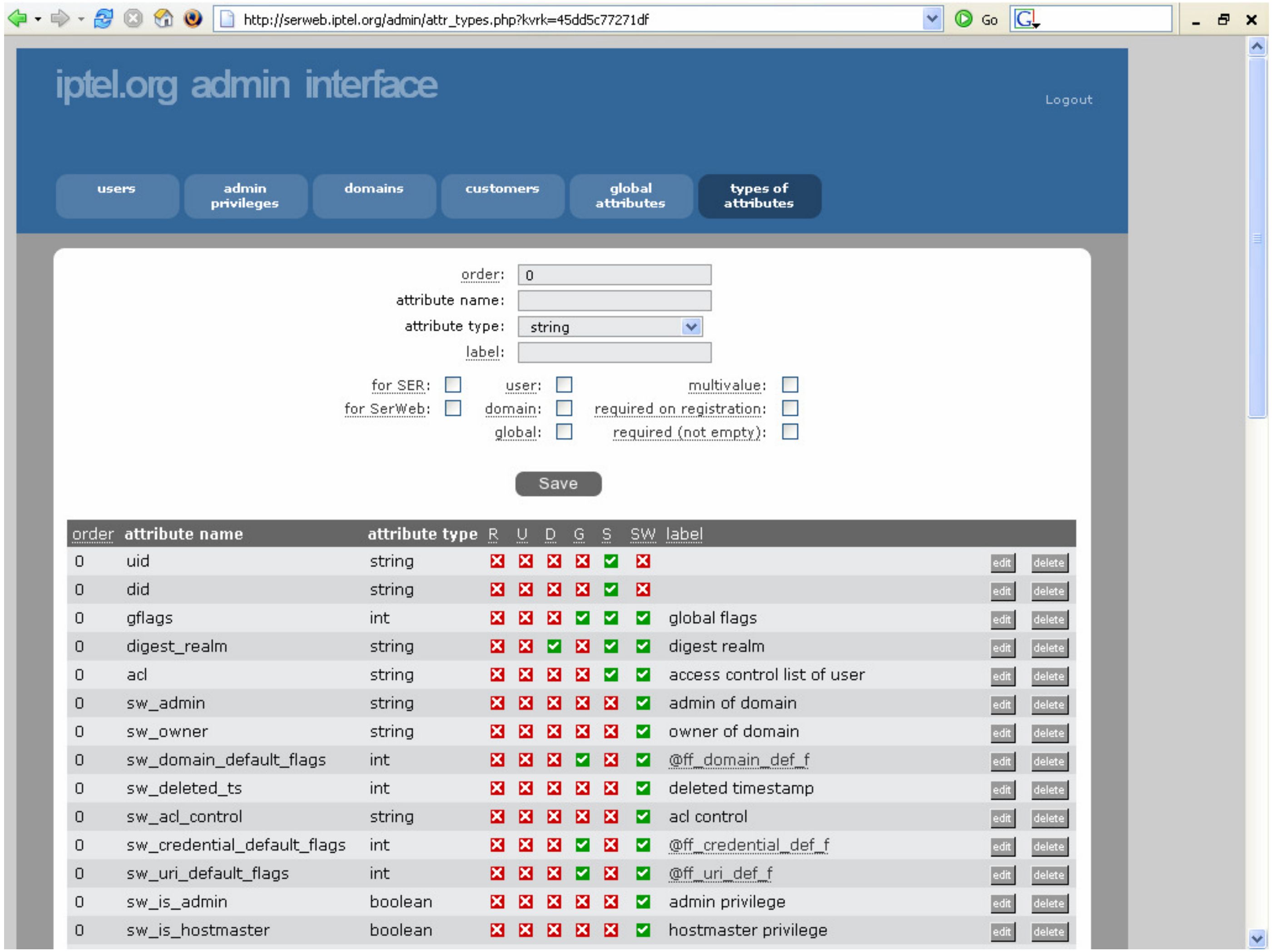
Txt

Etc.

SER Jump Start

- Complexity comparable to that of sendmail or apache – basic setup easy, changes to it take knowledge. Good knowledge of UN*X administration and IP networks required!
- Equip yourself with: Linux PC with DNS name and mysql and apache on it, two SIP telephones, Ethernet network, and time.
- Familiarize yourself with administrative documentation: http://www.iptel.org/ser/doc/
- Download SER from http://iptel.org/downloads
- Provision name of your domain and the first subscriber
- Configure the phones and make first calls.
- If you wish, install provisioning web front-end, serweb, too

Serweb snapshot



http://serweb.iptel.org/admin/attr_types.php?kvrk=45dd5c77271df
Go
iptel.org admin interface
Logout
users
admin privileges
domains
customers
global attributes
types of attributes

order:	0
attribute name:	
attribute type:	string
label:	

for SER: □ user: □ multivalue: □

for SerWeb: □ domain: □ required on registration: □

global: □ required (not empty): □

order	attribute name	attribute type	R	U	D	G	S	SW	label		
0	uid	string	☒	☒	☒	☒	☑	☒		edit	delete
0	did	string	☒	☒	☒	☒	☑	☒		edit	delete
0	gflags	int	☒	☒	☒	☑	☑	☑	global flags	edit	delete
0	digest_realm	string	☒	☒	☑	☒	☑	☑	digest realm	edit	delete
0	acl	string	☒	☒	☒	☒	☑	☑	access control list of user	edit	delete
0	sw_admin	string	☒	☒	☒	☒	☒	☑	admin of domain	edit	delete
0	sw_owner	string	☒	☒	☒	☒	☒	☑	owner of domain	edit	delete
0	sw_domain_default_flags	int	☒	☒	☒	☑	☒	☑	@ff_domain_def_f	edit	delete
0	sw_deleted_ts	int	☒	☒	☒	☒	☒	☑	deleted timestamp	edit	delete
0	sw_acl_control	string	☒	☒	☒	☒	☒	☑	acl control	edit	delete
0	sw_credential_default_flags	int	☒	☒	☒	☑	☒	☑	@ff_credential_def_f	edit	delete
0	sw_uri_default_flags	int	☒	☒	☒	☑	☒	☑	@ff_uri_def_f	edit	delete
0	sw_is_admin	boolean	☒	☒	☒	☒	☒	☑	admin privilege	edit	delete
0	sw_is_hostmaster	boolean	☒	☒	☒	☒	☒	☑	hostmaster privilege	edit	delete

SER Summary

- SER is the best SIP server ever!!! *(note that presenters co-authored SER, their opinion may be subjective and may or may not be shared by others)*
- **SER is really the best SIP server ever!!!**
- For sake of thorough SIP self-education, there can't be better way to learn than playing with SER.
- Next steps: try to change SER configuration, try to play with media server (SEMS), try to install PSTN gateway (Asterisk), look at other prominent free SIP software: http://www.iptel.org/3rdpsip

Self-test

Self-Test

- Q: What is the impact on ongoing call if a proxy server is shut down?
  - None. Media flow is not affected by IP Server.
- Q: What hast to be done in a proxy server if a client begins to emit a new request type, with a brand-new payload (e.g., some gaming data)?
  - Nothing. Proxy servers don’t care about payload.

Self-test

- Q: Why doesn’t RTP run over TCP?
  - Because of voice quality concerns due to TCP’s flow control.
- Q: Could digest authentication use nonces generated by client to avoid the first message exchange?
  - No. Such could be intercepted and replayed by attackers. One-way nonces randomly chosen by server are hard to replay.

Self-test

- Q: what happens if a SIP phone is terminated abruptly and a call comes in?
  - – Within remaining registration period, proxy tries to reach the phone and times out
  - – When the registration expires, proxy answers indicating that the phone is off-line

Self-test

- Q: How would you make sure that accounting of calls to PSTN is accurate even if client abruptly disappears?
  - Use session-timer emitted by gateway to detect dead clients and terminate call if dead client detected.

Self-test

- Q: Which of the following services can be implemented in client and/or network?
  - Call-forwarding-busy (CFB)
  - Call-forwarding offline (CFO)
  - On-hold (OH)
- A: CFB in both, CFO in network (kind of hard to have an offline device executed a service), OH is in SIP client-feature (re-INVITE)

Self-test

- Q: can be a registrar separated from proxy server?
  - It can, but the proxy server must have read access to registrar's user location database if it shall be used for routing to dynamically registered subscribers

-The End –

Information Resources

SIP Information Resources

- Authors: jiri.kuthan@tekelec.com, dorgham.sisalem@tekelec.com
- SIP Express Router: http://www.iptel.org/ser/
- SIP Products: http://www.iptel.org/views/Product_Database
- This Tutorial: http://www.iptel.org/sip/
- SIP Site: http://www.cs.columbia.edu/sip/

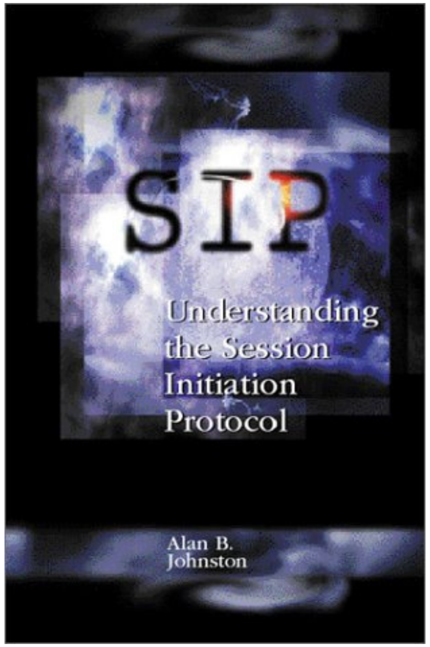
More SIP Information Resources

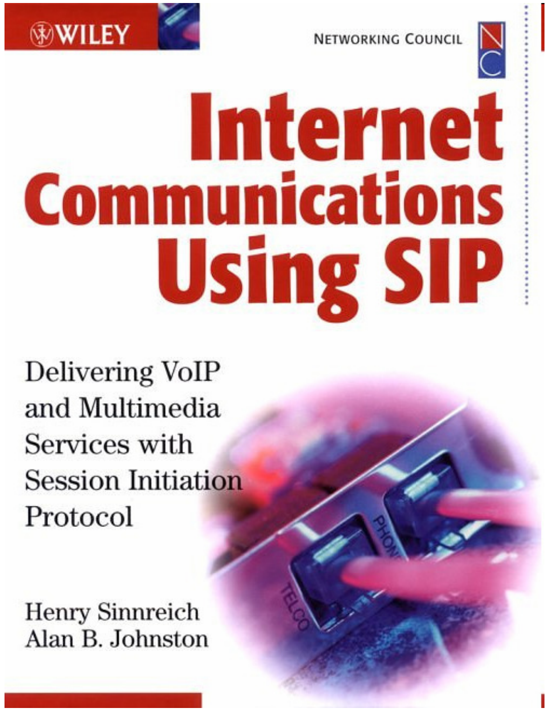
- RFC 3261 – core SIP specification
- draft ietf sip hitchhikers guide – SIP Roadmap
- Learn by Example: call flows
  - SIP PSTN Call Flows: RFC 3666
  - SIP Basic Call Flows: RFC 3665
  - SIP Service Examples: draft-ietf-sipping-service-examples

Even More SIP Information Resources: Knowledge Portals

- http://www.tech-invite.com/ (excellent!)
- http://voip-info.org/

There Are SIP Books!



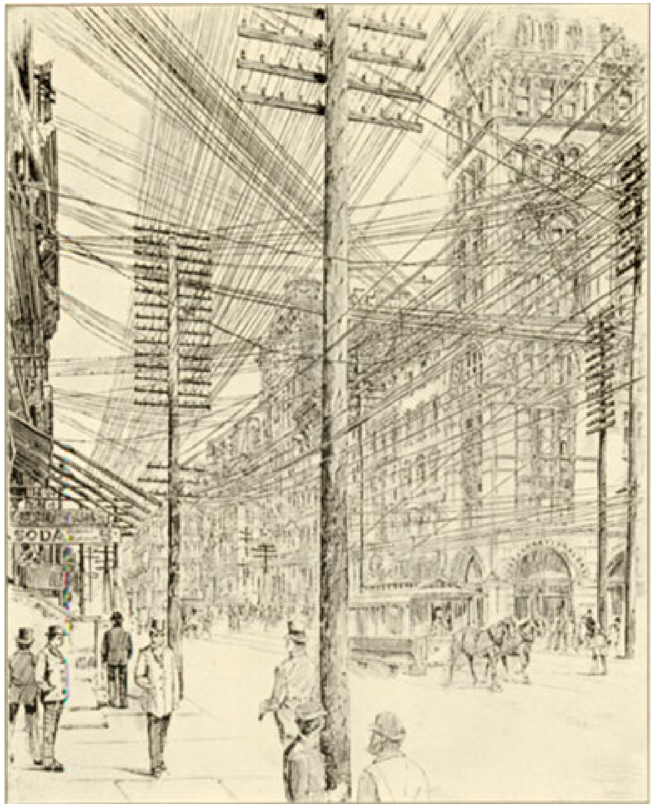

WILEY
Networking Council
Internet Communications Using SIP
Delivering VoIP and Multimedia Services with Session Initiation Protocol
Henry Sinnreich
Alan B. Johnston

- Alan B. Johnston: “SIP: Understanding the Session Initiation Protocol”
- Artech House 2001

- Henry Sinnreich, Alan Johnston: Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol
- John Wiley & Sons, 2001

Going Mobile: IP Multimedia Subsystem (IMS)

Wireless Has Been Striven for Long…



Left-hand picture: Broadway, 1890: Book of Old New York, Henry Collins Brown,1913.

Right-hand picture showing Bell Labs' voice based radio phone in 1924. Source: www.privateline.com/mt_digitalbasics/

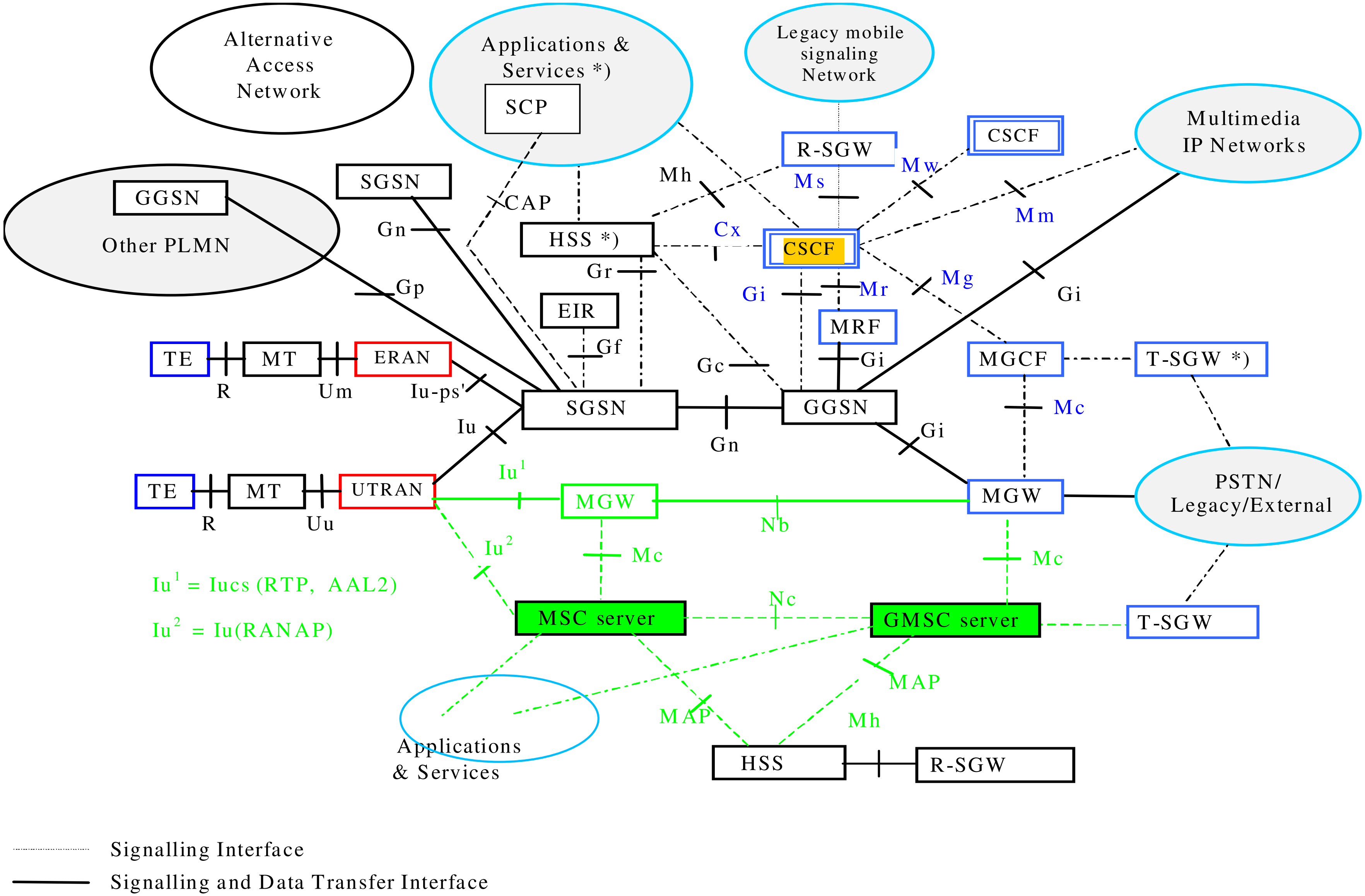
IMS History

- Back in ‘98, mobile world has realized that migration to all-IP would help to globalize the telecommunication market and launched 3GPP effort (www.3gpp.org)
- In early ’00s, 3GPP made SIP part of the All-IP mobile standard under the codename IMS – Internet Multimedia Subsystem
- The key extensions were added under the desire to port existing mobile network architecture to IP world:
  - → Lot of focus on charging, roaming, security
  - Lot of focus on specifying usage guidelines for IETF’s protocol-only specs and documenting in detail a specific network architecture.
- Critiques of IMS pick over-specification and “walled-garden model” (which is in fact not a technological feature of IMS but operator policy)

Introduction

- 3GPP consortium consists of ETSI, ARIB, TTA, T1 and CWTS
- UMTS R5 is an All-IP architecture with support for CS terminals
  - We are in Rel4
  - Rel 5, R6 frozen, currently working on Rel 7.
- Architecture based on GPRS with multimedia enhancements
- Support for integration of intelligent services (SIP based, OSA, CAMEL)
- Based on IETF protocols
  - SIP is used for establishing and terminating IP communication sessions
  - RTP/RTCP for media transport
  - SDP for capability negotiation
  - DIAMETER for AAA
  - COPS for policy based QoS control
  - IP-SEC for inter-domain trust relations
  - H.248 (MEGACO) is used for gateway control
- First trials in labs of mobile providers

3GPP: Architecture



Requirements

- Use IETF protocols (SIP, SDP) and request any additions to be standardized by IETF
- Efficient use of radio interface
  - Signal compression
- Minimum session setup time
  - Higher registration overhead and session based security
- IPv6 support
  - Not so much now though
- Network initiated de-registration and session termination
- QoS support
  - Correlation of session and bearer establishment

Requirements

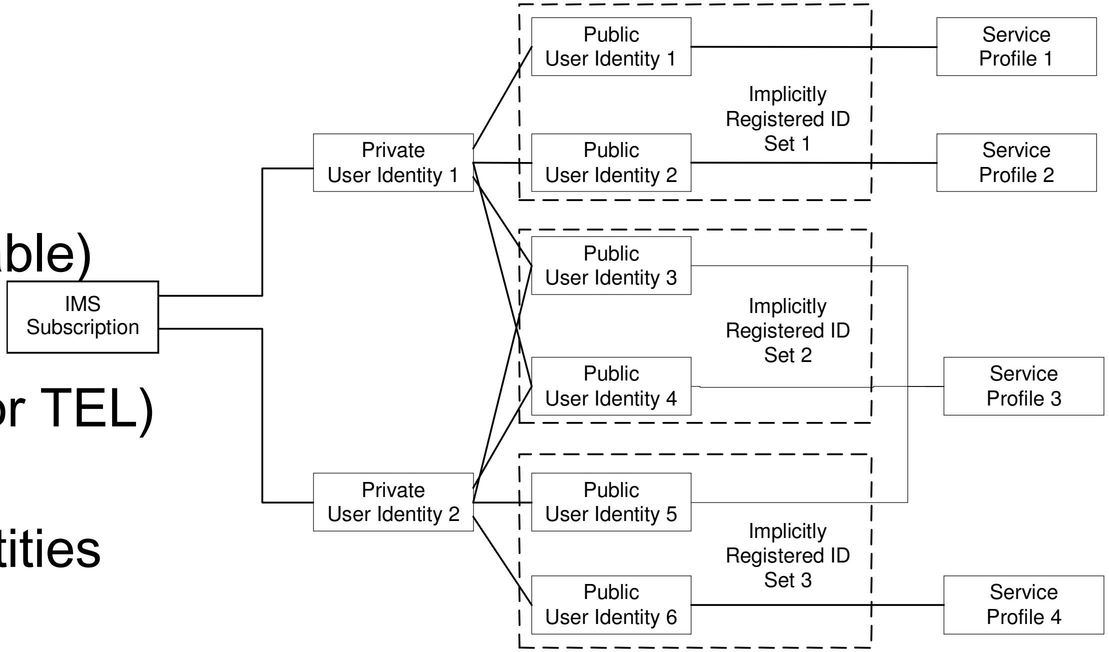
- Access and admission control
  - Policy based control
- Private/Public user identity
- Hiding of network topology
  - More components in the path
- Emergency services
- Remote identity presentation, hiding and assertion
- Charging
  - Support for pre- and post-paid
  - Correlation between session and media
- DTMF and early media

IMS and SIP

- A few headers more
  - P-Headers are used to convey information not included in standard SIP
  - PATH and Service-Route
- Additions to some headers
  - WWW-Authenticate and Authorize
  - VIA, Route ..
- Stricter routing paths (e.g., P-CSCF to S-CSCF to I-CSCF to S-CSCF to P-CSCF)
- XML body used for transporting information from HSS to the SIP elements (emergency)
- Specification of timer values (request retransmission ..)
- More intensive use of some of SIP and SDP extensions (PRACK, UPDATE, qos, offer-answer ...)

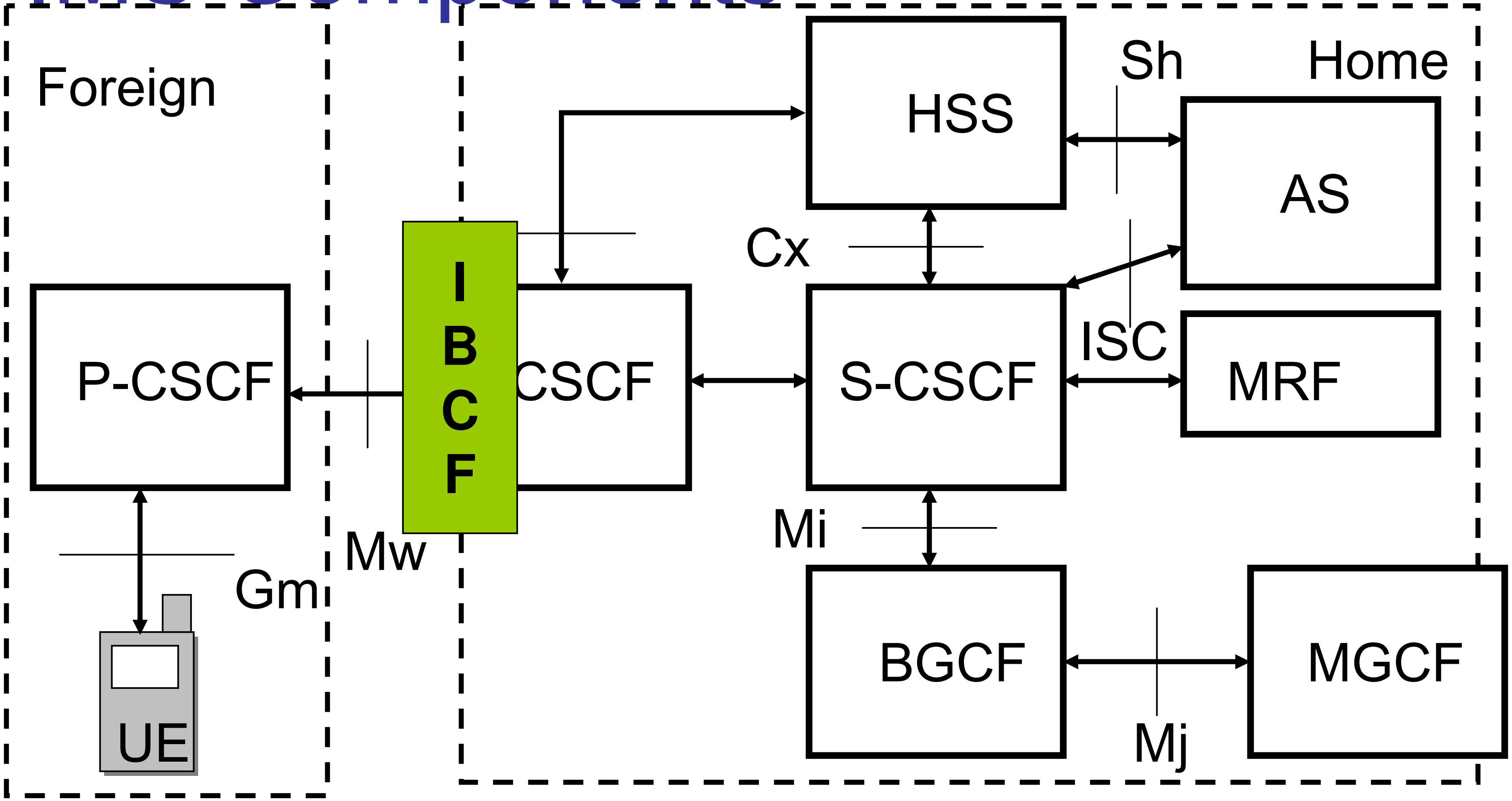
User Identity

- Private identity
  - Issued by home provider
  - Used for AAA
  - Saved on ISIM (not modifiable)
- Public identity
  - Normal SIP address (URI or TEL)
  - Identifies the user publicly
  - User has one or more identities
  - Used for routing
  - Can be grouped into implicit registration sets
    - If one of the set is registered then the others are as well
  - At least one is stored on ISIM
    - In case no ISIM is provided
      - Use a temporary identity derived from USIM during initial registration (derived from IMSI)
      - PIDs are then provided by the S-CSCF in its reply to the registration



Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

IMS Components



Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

User Equipment (UE)

- Contains the SIP user agent
- Establishes a GPRS PDP context for
  - Signaling (either dedicated or a general one)
  - Media transport
- Contains ISIM for authentication
  - Public and private user id
  - User Network address
  - Security algorithms and keys
  - At least a USIM
- Correlate between session control and QoS reservation

Proxy Call Session Control Function (P-CSCF)

- First contact point for the UE (outbound proxy)
  - Forward registration to I-CSCF
  - Forward requests to S-CSCF (or I-CSCF)
  - Forward replies and incoming requests to UE
- Maintain security association with UE
- Responsible for compression/decompression
- Maintain session and registration information
  - Can terminate registrations or sessions if deemed necessary
- Correlation between SIP and QoS
- Enforce local policies
- Generate CDRs
- Possibly support routing to local service infrastructure
  - Emergency call handling
- Discovered through DHCP or during GPRS PDP establishment

Interrogating Call Session Control Function (I-CSCF)

- Contact point within an operator
  - Discovered through DNS
- Assign S-CSCF to a user by contacting the HSS
- May act as a THIG (Topology Hiding Inter-Network Gateway
  - Always on the path (RR and Service-Route) of any message leaving the network
  - Encrypt all entries added by the hiding network in outgoing messages

```
Via: SIP/2.0/UDP icscf1_s.home1.net,
SIP/2.0/UDP Token( SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP
 pcscf1.home1.net)@home1.net;tokenized-by=home1.net,
 SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
```

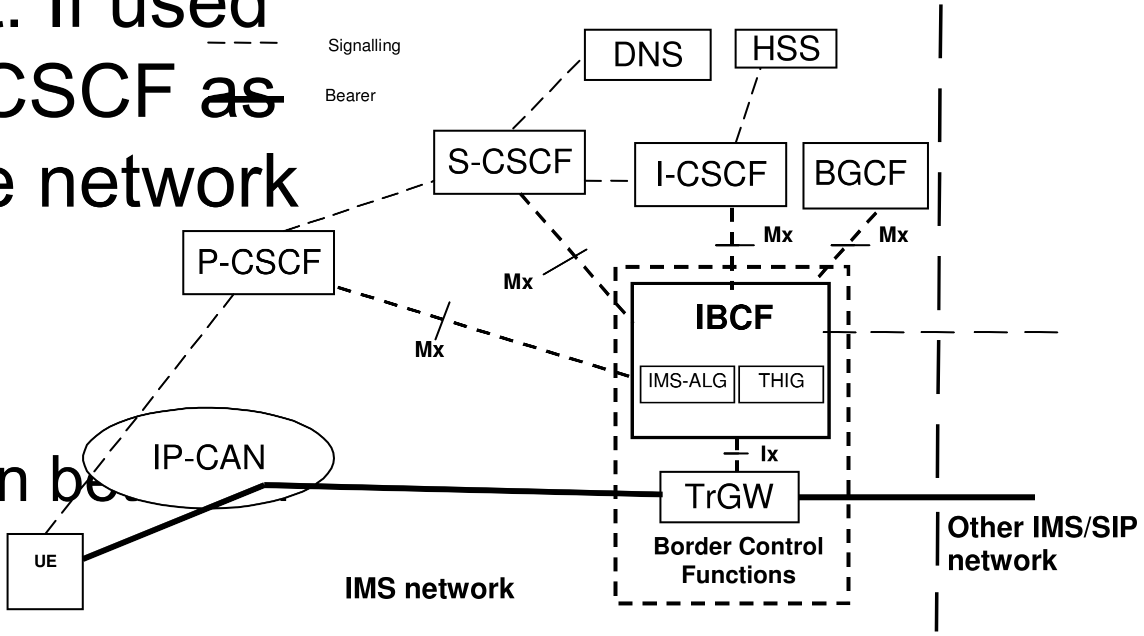
  - Starting with release 7 this functionality has moved to IBCF
- Generate CDRs

Serving Call Session Control Function (S-CSCF)

- Acts as a registrar
- Acts as a SIP proxy (forward messages ..)
- Allocated to a user during registration
- Always on the path of the user‘s SIP messages (use Service-Route and RR)
- Enforces service policies based on the user‘s subscription profile
- Collects session information for billing
- Interacts with application service platform
  - Chose the appropriate AS based on user profile (initial filter criteria –IFC)
  - Forward to AS using ISC interface
- Acts as user agent when required (Notifications about de-registrations and re-authentications, call termination)

Interconnect Border Control Function (IBCF)

- Optional component. If used then replaces the I-CSCF as the entry point to the network
- Support
  - Topology hiding
  - IMS ALG: Translation be IPv4 and IPv6
  - Packet screening:
    - •Is source/destination address OK
    - •Is SIP content OK
  - CDR generation
- Usually built as a B2BUA



Breakout Gateway Control Function (BGCF)

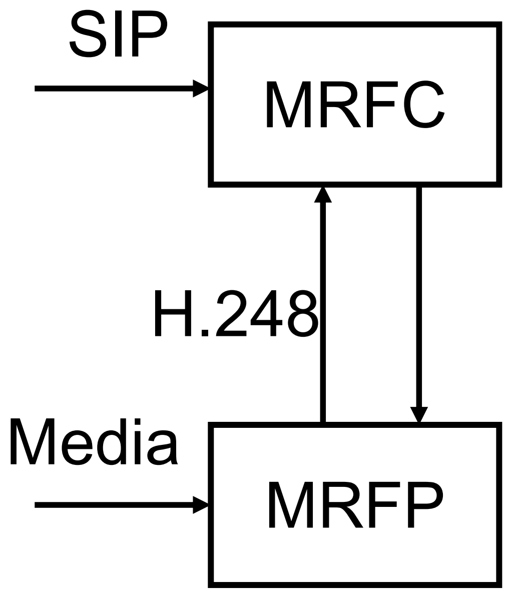
- Select PSTN/CS domain to forward call to
  - Local MGCF
  - Another BGCF
- How to choose an MGCF is not specified
  - Configuration
  - TRIP or similar

Media Gateway Control Function (MGCF)

- Gateway to PSTN networks
  - Translate SIP messages in appropriate PSTN signals and vice versa
  - Establish bearer with appropriate code
  - Possibly translate codec
  - Act as UA (but no registration required)

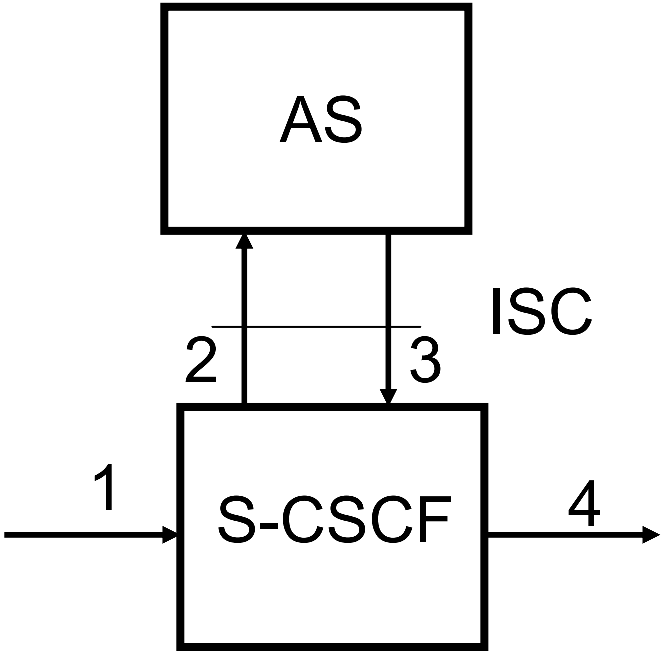
Media Resource Function (MRF)

- Provide conferencing and announcement services
- Multimedia Resource Control Function (MRFC)
  - Interpret information from S-CSCF and AS
    - Conference booking and floor control from AS for example
  - Control MRPF
- Multimedia Resource Processor Function (MRPF)
  - Establish bearers based on MRFC requests
  - Media mixing and distribution
  - Media streaming for announcements
- Use H.248 (MEGACO) between the two components



Application Server (AS)

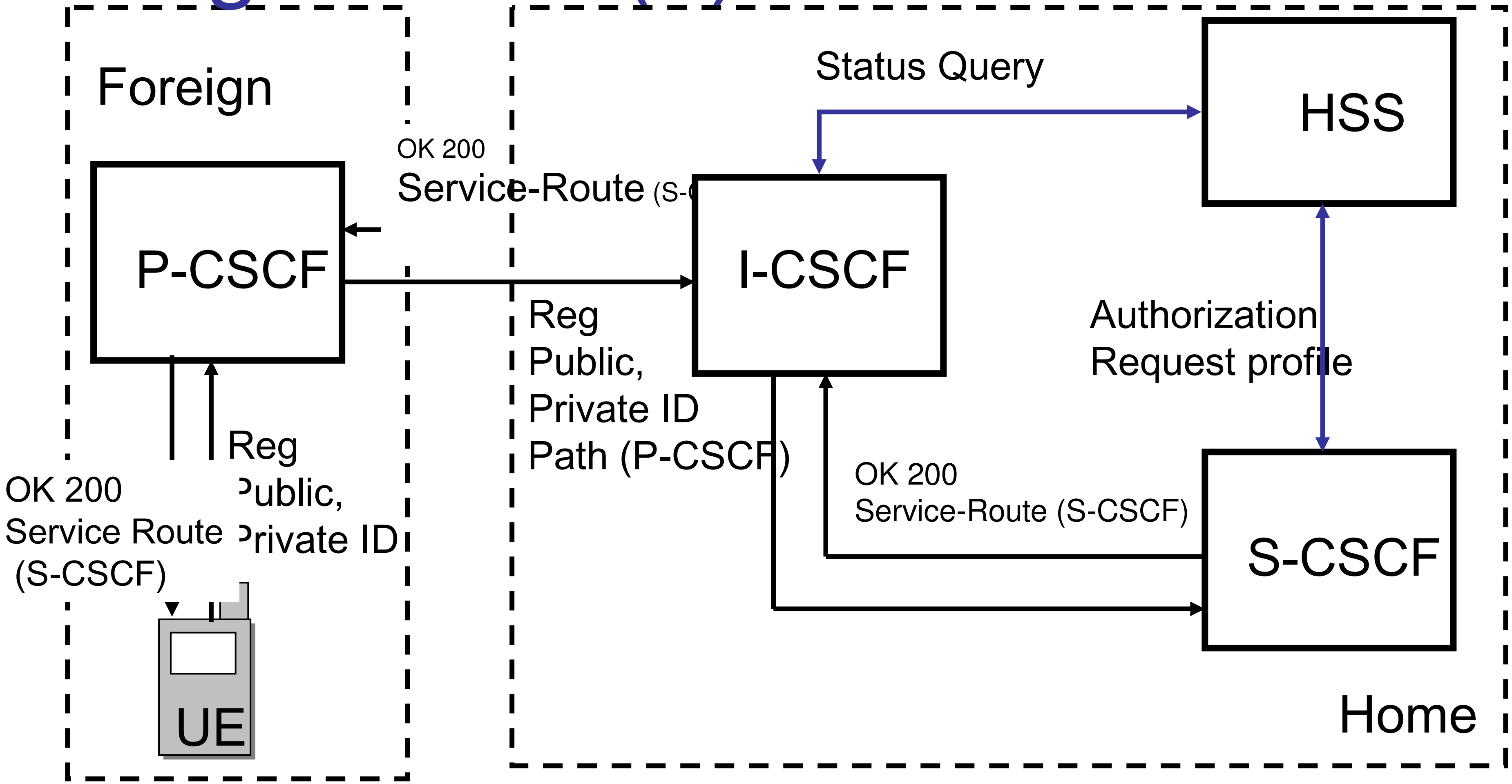
- Services include third party CC, personalized routing, PTT, presence, ...
- Services are offered by home, visited or third party provider
- S-CSCF forwards requests to AS base (possible received from HSS)
- Results of AS sent back to S-CSCF
- AS can act as UA, redirect or proxy
- CAMEL and OSA optional
- ISC
  - SIP and SIMPLE
  - S-CSCF could add charging information
  - S-CSCF could add information to allow the distinction between incoming and outgoing messages



Home Subscription Server (HSS)

- Contains user profile information indicating
  - Private and public identities of the user
  - Authentication information
  - Which services and medias the user is eligible for using
  - Filtering criteria for choosing appropriate AS
- Assist I-CSCF in choosing the appropriate S-CSCF
- Maintain subscription information about the user
- Enforce provider policies
  - De-register users with invalid subscription
- Connected through Cx interface to S-CSCF and I-CSCF (DIAMETER)
- Connected also to AS (Sh interface)
  - Provide user service information
- Allow multiple instances by using SLF (Subscription Location Function)
  - I-CSCF asks over Dx the SLF which HSS is responsible for the user

Registration (1)



Registration: Request handling

- P-CSCF behavior
  - UE adds private and public identity in the REGISTER message
  - P-CSCF adds a PATH header with its address to the REGISTER message
  - P-CSCF adds P-Visited-Network-Identity to the message
  - Discover the I-CSCF of the user using DNS
- I-CSCF behavior
  - Determine the right S-CSCF
    - Ask an HSS (Cx Interface with DIAMETER)
    - Ask an SLF about which HSS to use (Dx Interface with DIAMETER)
    - Use a local database –Tekcore without HSS
  - If it is to stay in the path of future requests then adds itself to the PATH list
- S-CSCF
  - Download the user profile from the HSS
  - Save contents of PATH
  - Generate reply
  - Forward to AS if needed

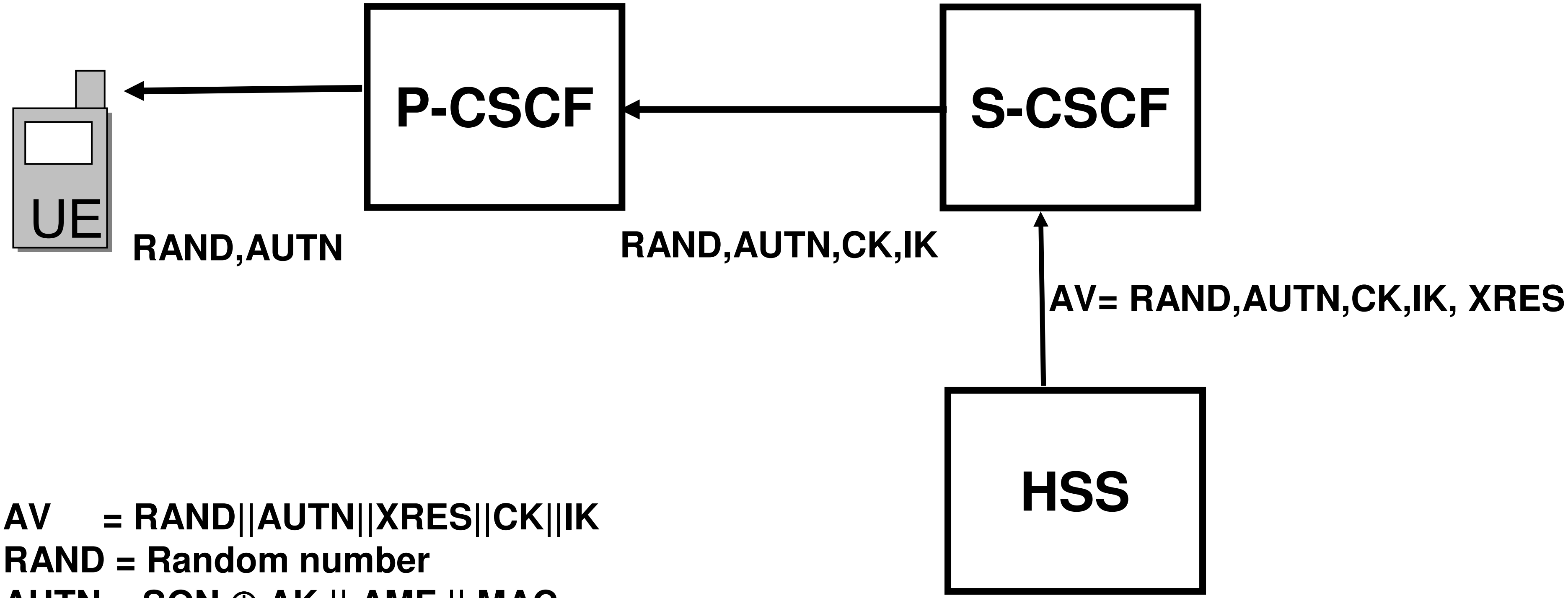
Registration: Reply handling

- S-CSCF behavior
  - Add “service-route” to reply with the address of the S-CSCF
- I-CSCF behavior
  - If it is to stay in the path of future requests then adds itself to the “service-route” list
- P-CSCF
  - Store content of “service-route”
  - Store the public user identities found in the P-Associated-URI

Access Security in IMS

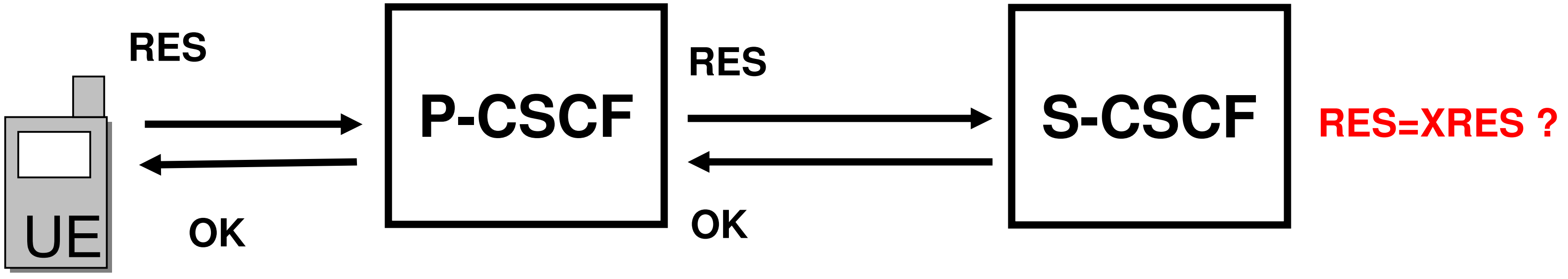
- UE (ISIM) and HSS (AuC) share a secret K
- Based on AKA which provides
  - Mutual authentication between user and network
  - Temporary shared key between UE and P-CSCF
    - Used for establishing an IPSEC tunnel between UE and P-CSCF
- In case of reregistration, the P-CSCF indicates whether the registration was received in a secure manner.

Access Security in IMS



AV = RAND||AUTN||XRES||CK||IK
RAND = Random number
AUTN = SQN ⊕ AK || AMF || MAC
MAC = Message authentication code
AMF = Authentication Management Field
AK = Anonymity key
XRES = Result
CK = Cipher key = f3(K, RAND)
IK = Integrity key = f4(k,RAND)

Access Security in IMS



RES

UE

OK

P-CSCF

RES

OK

S-CSCF

RES=XRES ?

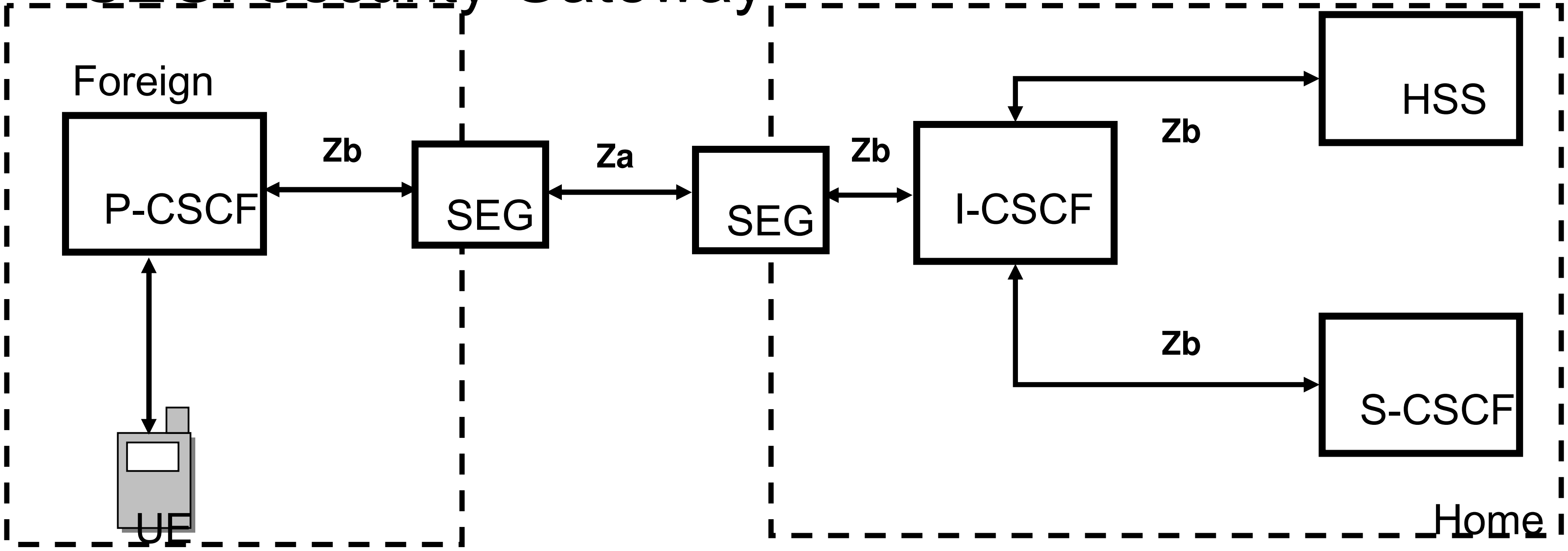
AK = f5(K, RNAD)
SQN = AK(AUTN)
XMAC = f1(K,(SQN|RAND|AMF)

XMAC = MAC ?
RES = f1(K,RAND)

CK = f3(K, RAND)
IK = f4(k,RAND)

Authentication and Security

- Support two interfaces
  - Za: IPSEC connection between different networks
  - Zb: IPSEC connection between components of the same network
- SEG: Security Gateway



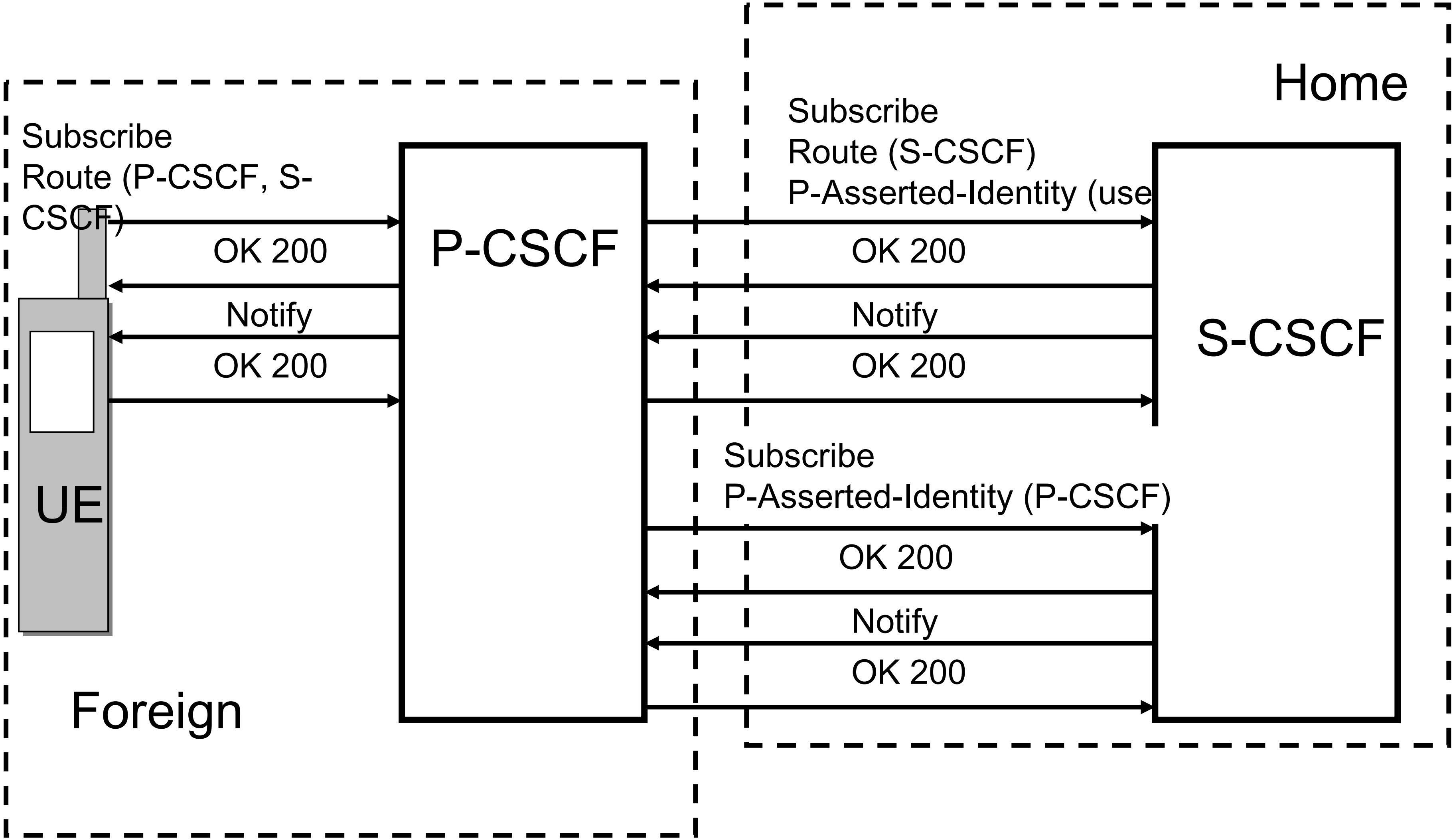
State Information

- S-CSCF:
  - P-CSCF (PATH)
  - User Profile
  - Authentication data
  - Session data
- P-CSCF
  - S-CSCF (possibly also THIG) (Service-Route)
  - Security association with the UE
    - Allows for checking the integrity and authenticity of the messages
    - Allows issuing a network asserted identity
      - P-Asserted –Identity
      - Used for hop-by-hop trust relations
  - Sigcomp compartments
  - Session data (if session termination is to be supported)
  - Registered public ID and the set of public IDs that were received in the P-Associated-URI header
  - Subscription to registration state of PID
- I-CSCF
  - Could cache a PID-2-S-CSCF translation

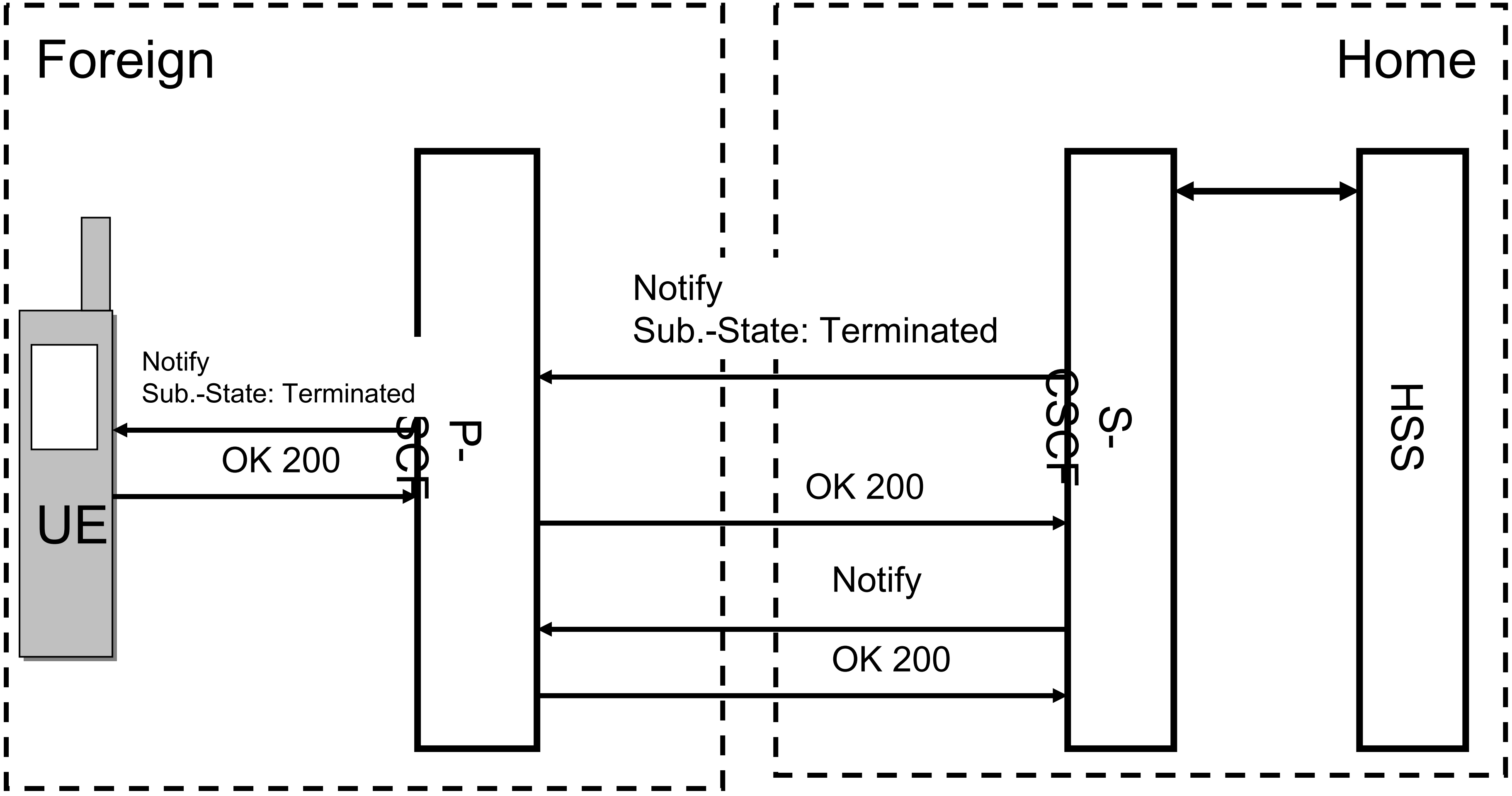
Network Initiated De-Registration

- Registration might time out
- Subscription ends or some other changes in the user‘s profile
- User might roam into another network without clearing the old registration
- Decision taken by S-CSCF, HSS or P-CSCF
- Network initiated re-authentication is similar

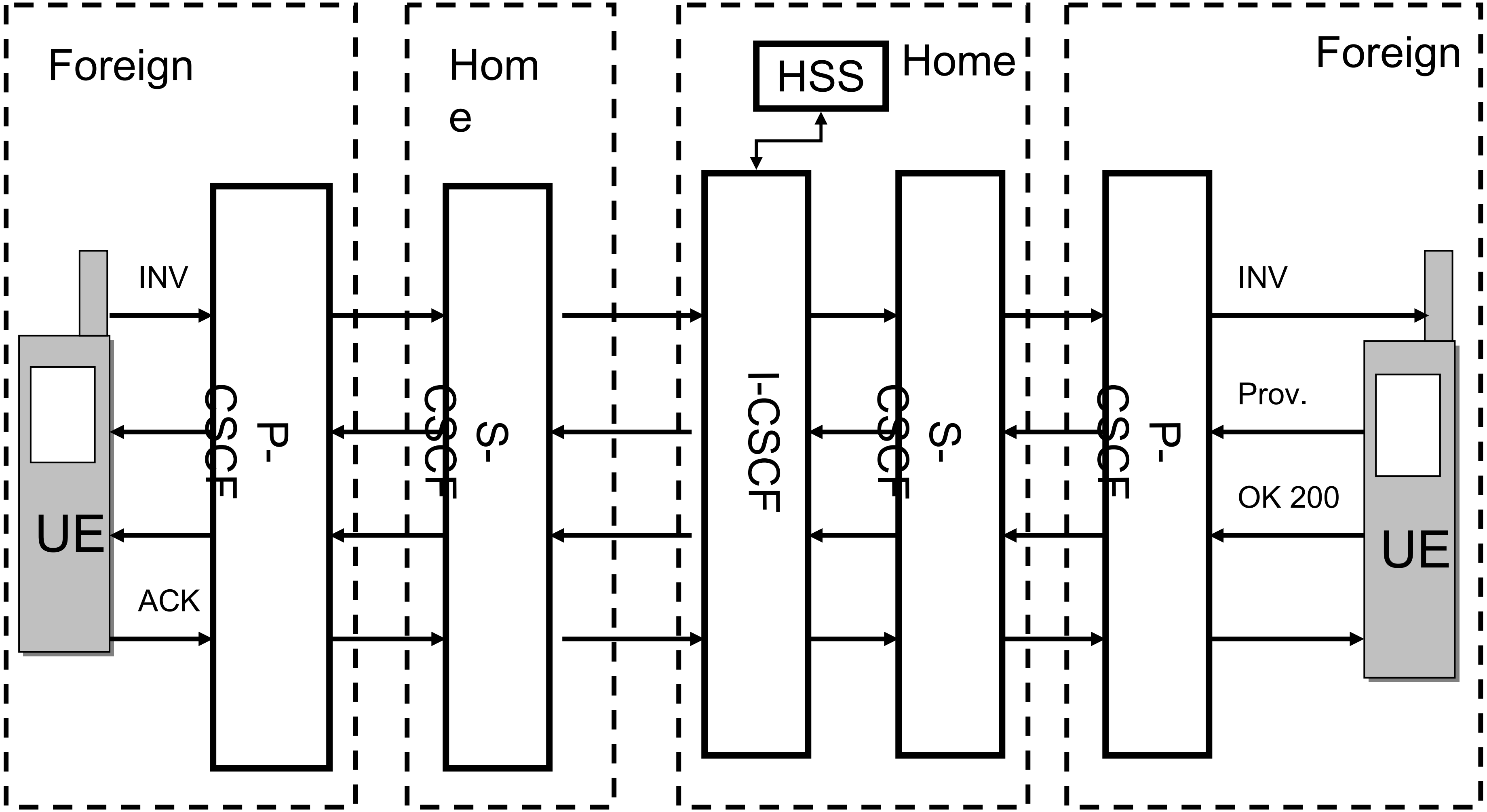
De-Registration: Subscription Phase



De-Registration: De-Registration Phase



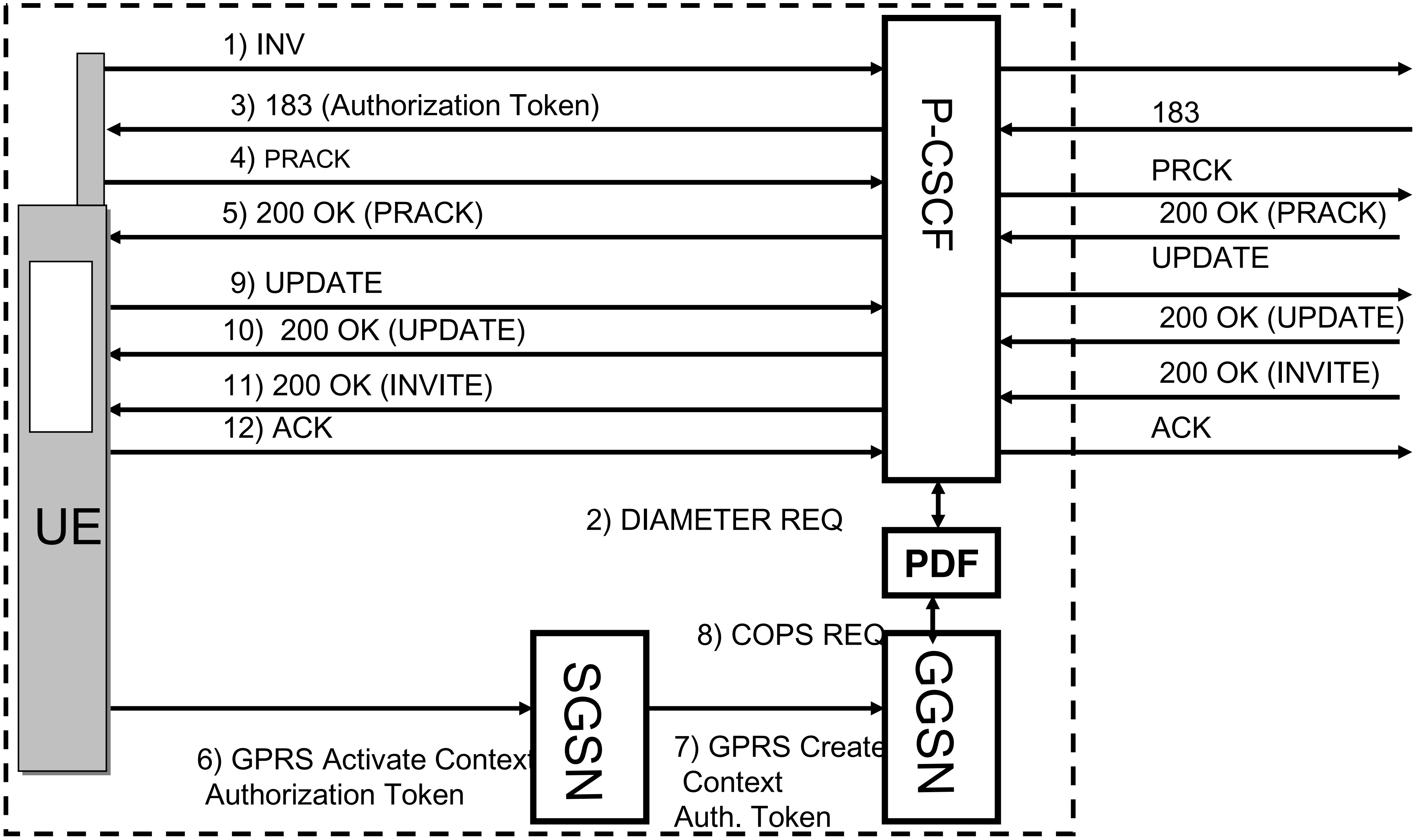
Session Establishment



QoS in IMS

- UMTS can offer different QoS for different kinds of media
  - Conversational, streaming, interactive and background
  - Different classes offer different delay guarantees
- Different PDP contexts are used for media and signaling
- Sessions are allocated resources based on SDP
  - Use bandwidth parameter
  - Use local policies regarding used media

QoS and Session Establishment

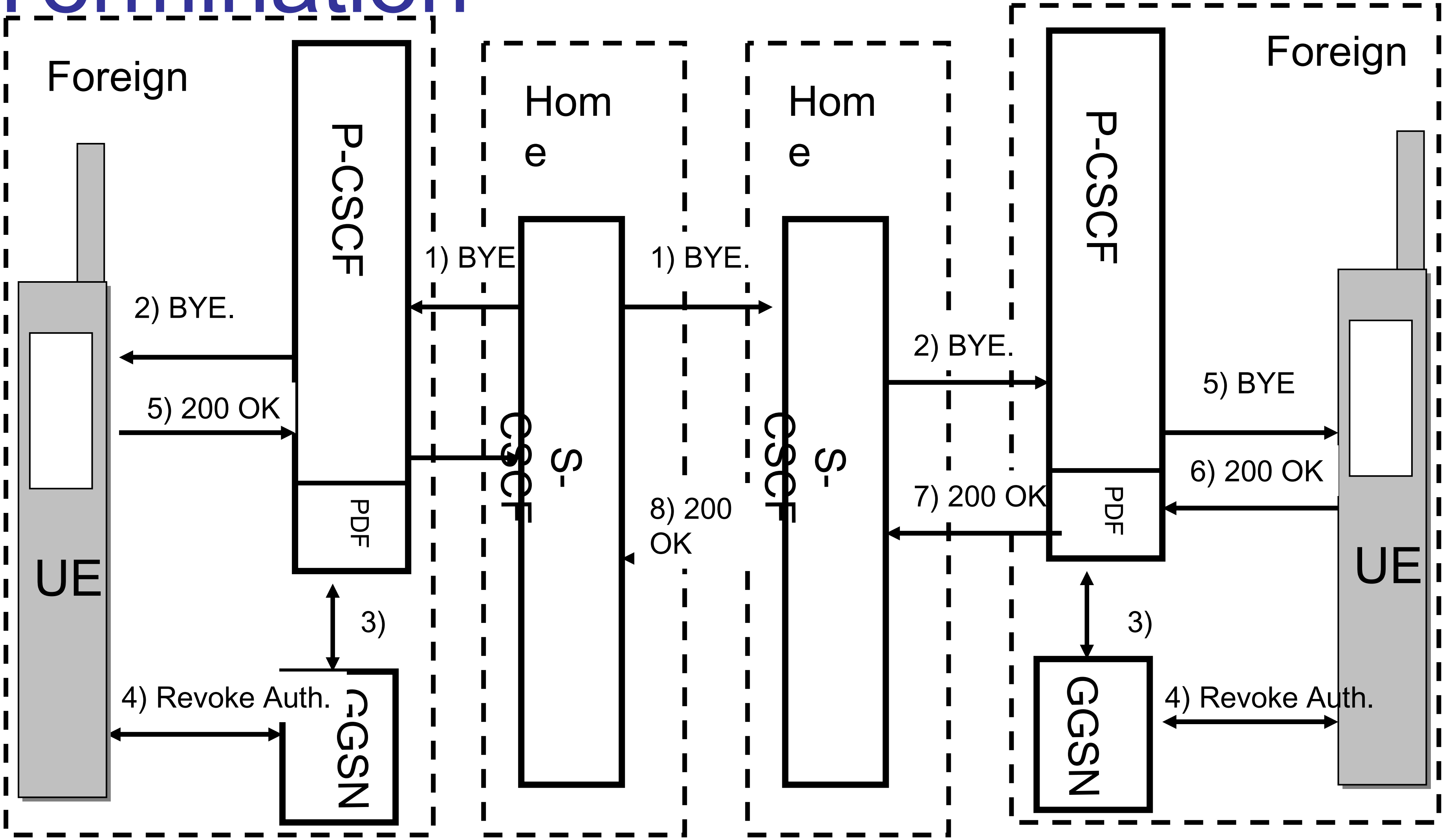


Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

Network Initiated Session Termination

- Termination can occur due to bearer or service related events
- P-CSCF or S-CSCF can decide to terminate a session
  - Act as UA using maintained state information
- P-CSCF (PDF) inform the GGSN to terminate the bearer

Network Initiated Session Termination



Jiri Kuthan+Dorgham Sisalem, Tekelec, March 2007

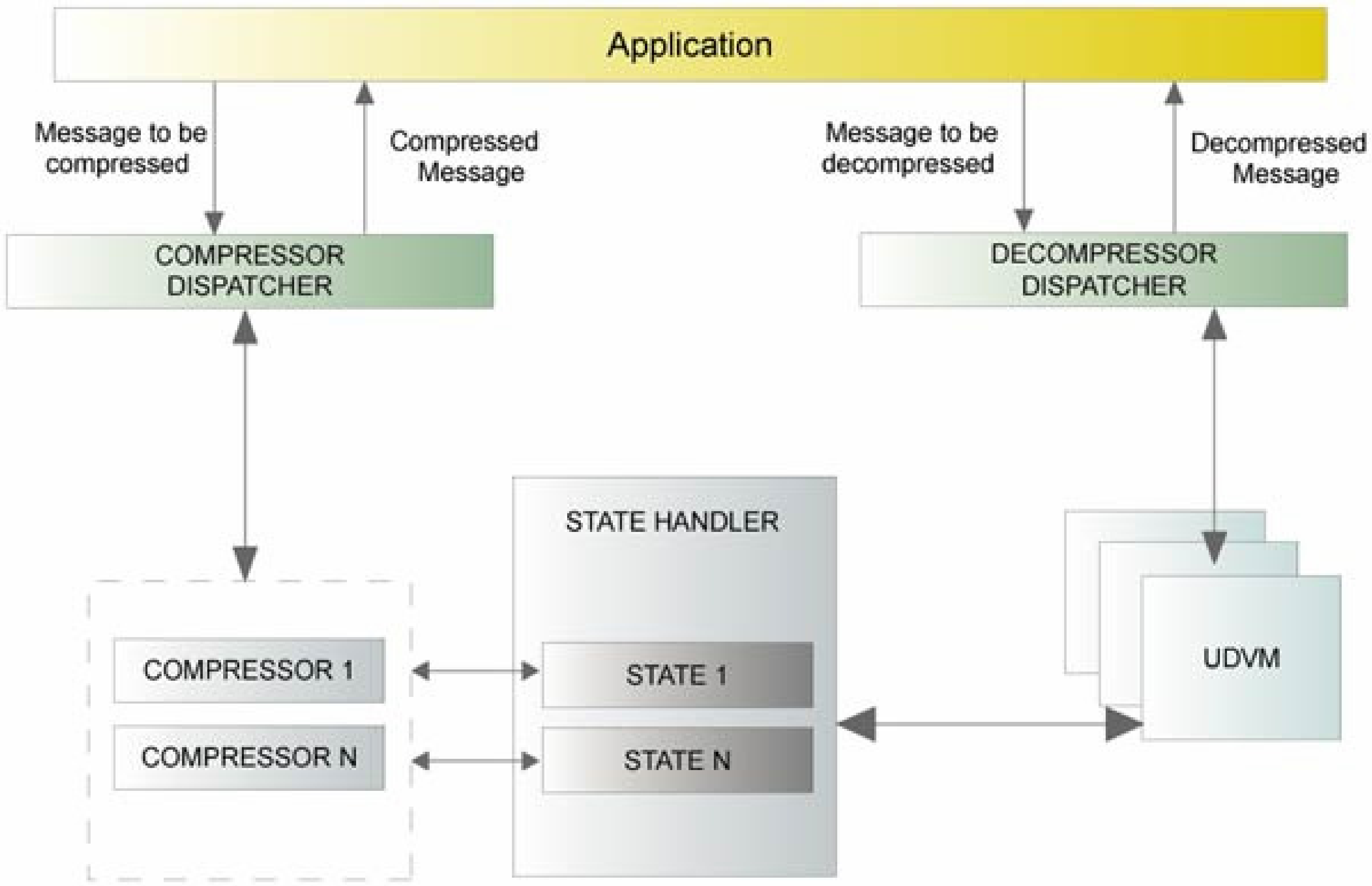
Charging

- Need to correlate bearer resources with IMS session
- GGSN create charging information that is handed over to P-CSCF
  - Describe which resources are used
  - Need to update information based on changes in media PDP context
- P-CSCF include the data as P-Charging-Vector in SIP messages
- Addresses of charging collection functions are also transported in SIP (P-Charging-Function-Address)

SIGCOMP

- SIP messages can become large
  - Long transmission delay
  - High bandwidth usage
- Sigcomp specifies a framework for enabling the compression and decompression of messages with various compression algorithms
  - **Compressor:** Compresses messages and uploads the ByteCode for the corresponding decompression algorithm to the UDVM as part of the SigComp message.
  - **Decompressor (UDVM)**: Uncompress messages by interpreting the corresponding ByteCode received previously
  - **State Handler:** Manages compartments with some information to use between received SigComp messages.
  - Sigcomp itself allows both parties to exchange some status information, and pointers to state to be used

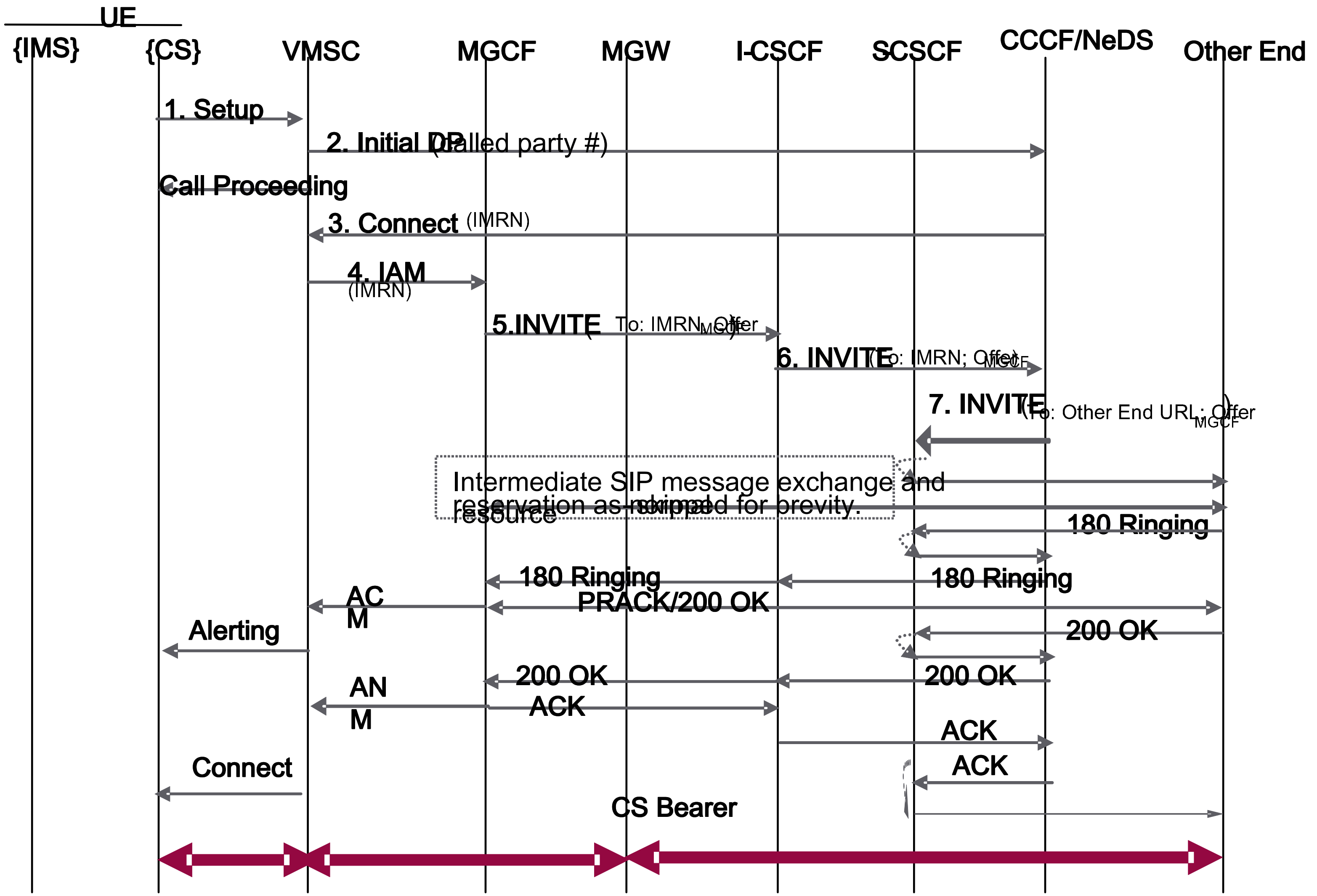
SIGCOMP


Application
Message to be compressed
Compressed Message
Message to be decompressed
Decompressed Message
COMPRESSOR DISPATCHER
DECOMPRESSOR DISPATCHER
STATE HANDLER
COMPRESSOR 1
COMPRESSOR N
STATE 1
STATE N
UDVM

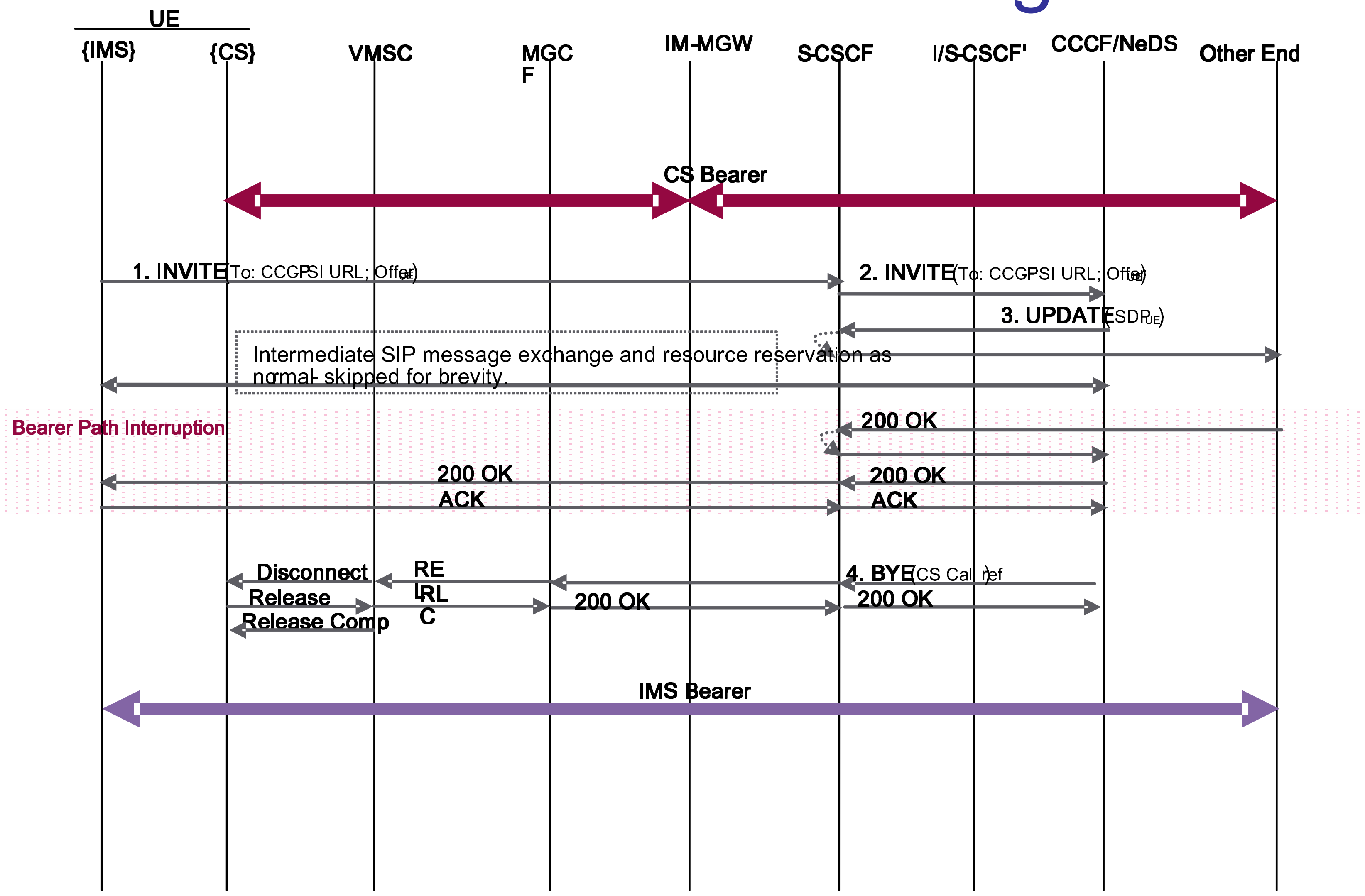
Fixed Mobile Convergence (FMC)

- Enable users to roam from CS to IP networks with no interruption of service
  - E.g., user in WLAN moves to 3G or vice versa
- CCCF (Call Continuity Control Function) mediates between CS and IMS
- IMS anchored model
  - Any calls generated by this user will have to be handled with in the IMS world
  - When a user turns on his mobile he is registered to IMS and/or CS
  - User is an IMS subscriber with a user profile in IMS
  - Call signaling originating from CS are transferred to IMS through CS specific methods (CAMEL, MAP, user signaling –USSD- …)

FMC: Call Handover –CS Originated


UE
{IMS}
{CS}
VMSC
MGCF
MGW
I-CSCF
SCSCF
CCCF/NeDS
Other End
1. Setup
2. Initial DP (Called party #)
Call Proceeding
3. Connect (IMRN)
4. IAM (IMRN)
5.INVITE (To: IMRN; Offer MGCF)
6. INVITE (To: IMRN; Offer MGCF)
7. INVITE (To: Other End URL; Offer MGCF)
Intermediate SIP message exchange and resource reservation as skipped for brevity.
180 Ringing
180 Ringing
180 Ringing
ACM
PRACK/200 OK
Alerting
200 OK
200 OK
200 OK
ANM
ACK
ACK
ACK
Connect
CS Bearer

FMC: Call Handover –IMS Originated



UE

{IMS}

{CS}

VMSC

MGCF

IM-MGW

S-CSCF

I/S-CSCF'

CCCF/NeDS

Other End

CS Bearer

1. INVITE(To: CCCF PSI URL; Offer UE)

2. INVITE(To: CCCF PSI URL; Offer UE)

3. UPDATE(SDP UE)

Intermediate SIP message exchange and resource reservation as normal - skipped for brevity.

Bearer Path Interruption

200 OK

200 OK

200 OK

ACK

ACK

Disconnect

REL

Release

RLC

Release Comp

4. BYE(CS Call ref)

200 OK

200 OK

IMS Bearer

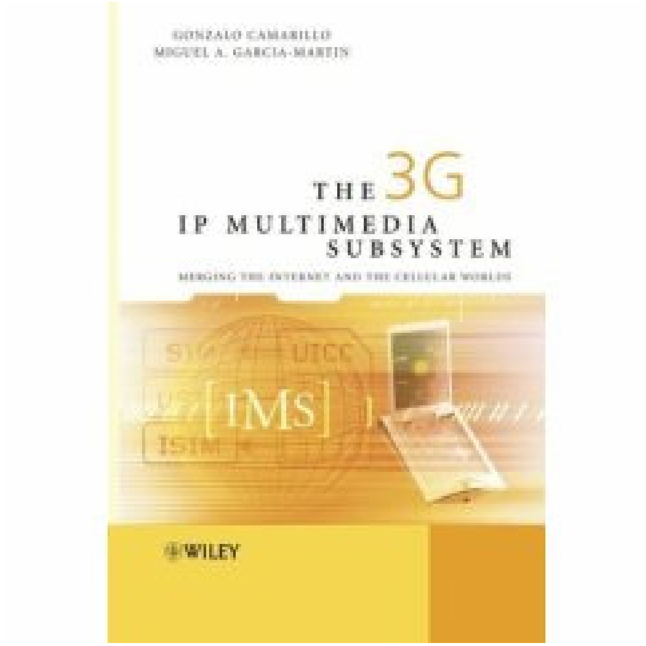
Further Reading

- www.3gpp.org
- TS23.228: General overview of IMS
- TS24.229: Description of what each component does is different scenarios
- TS24.228: All possible signaling flows
- TS33.203: AKA and access control
- TS33.210: Network Security
- TS29.208: QoS signaling (P-CSCF-PDF-GGSN flows)
- TR23.806: FMC

IMS Information Resources

- http://www.3gpp.org/
- http://www.imsbook.com/
- http://www.tech-invite.com/

There Are IMS Books



- Gonzallo Camarillo, Miguel-Angel Garcia-Martin: The 3G IP Multimedia Subsystem

Glossary …

- ACL Access Control List (administrative policy instrument)
- ALG Application-Level-Gateway (firewall/NAT traversal technique)
- ASP Application Service Provider (access-independent provider of applications)
- B2BUA Back-to-Back User Agent (special form of a SIP server)
- BCP Best Current Practice
- CDR Call Detail Record
- CGI Common Gateway Interface (technique for programming services)
- CLID Caller ID
- CPL Call Processing Language (technique for programming services)
- DNS Domain Name System (Internet naming directory)
- DoS Denial of Service (infamous art of attack)
- DTMF Dual Tone Multi-Frequency (technique for transmission of tones used to interact with “voice menus”)
- ENUM Telephone Number Mapping (DNS-based database of Internet addresses associated with PSTN phone numbers)
- ETSI European Telecommunications Standards Institute (telecommunication standardization body)
- ICE Interactive Connection Establishment (methodology used for NAT traversal)
- IETF Internet Engineering Task Force (Internet standardization body)
- ILBC Internet Low Bandwidth Codec (internet-ready codec with built-in loss concealment)
- IMS IP Multimedia Subsystem (standard for use of SIP in wireless networks)

… Glossary

- ISP Internet Service Provider
- ITSP Internet Telephony Service Providers (VoIP-specialized ASP)
- ITU International Telecommunication Union (telecommunication standardization body)
- IVR Interactive Voice Reponse
- JAIN Java APIs for Integrated Network Framework
- LEC Local Exchange Carrier
- LNP Local Number Portability
- NAT Network Address Translation
- MD5 Message Digest 5 (a cryptographic one-way hash function used for authentication in SIP)
- MGCP Media Gateway Control Protocol
- MWI Message Waiting Indication
- OSP Open Settlement Protocol
- PBX Private Branch Exchange
- PSTN Public Switched Telephone Network
- PTT Push-to-talk
- QoS Quality of Service
- RTCP RTP Control Protocol
- RTP Real-Time Transport Protocol
- RTT Round-Trip-Time
- RTSP Real-Time Streaming Protocol
- SBC Session Border Controller
- SDP Session Description Protocol
- SER SIP Express Router
- SIMPLE SIP for Instant Messaging and Presence
- SIP Session Initiation Protocol
- SPIT Spam over IP Telephony
- SS7 Signaling System Nr. 7
- STUN Simple Traversal Underneath NATs (NAT traversal protocol)
- TLS Transport Layer Security
- TRIP Telephony Routing over IP
- URI Uniform Resource Identifier
- VoIP Voice over IP