IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Lecture notes of G. Q. Maguire Jr.

KTH Information and Communication Technology

For use in conjunction with:

Henry Sinnreich and Alan B. Johnston, *Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol*, 2nd Edition, Wiley, August 2006, ISBN: 0-471-77657-2.

Last modified: 2013.08.30:12:51

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 1: Introduction

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with :

Henry Sinnreich and Alan B. Johnston, *Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol*, 2nd Edition, Wiley, August 2006, ISBN: 0-471-77657-2.

Last modified: 2013.09.01:14:31

Welcome to the course!

The course should be fun.

We will dig deeper into Voice over IP - with a focus on SIP and related protocols, and will also examine some of the other protocols which are used.

Information about the course is available from the course web page

http://www.ict.kth.se/courses/IK2554/

Staff Associated with the Course

Instructor (Kursansvarig)

prof. Gerald Q. Maguire Jr. <maguire@kth.se>

Goals, Scope and Method

Goals of the Course

- To understand what Voice over IP (VoIP) systems are, their basic architectures, and the underlying protocols
- To be able to read and understand the literature.
- To provide a basis for your own research and development in this area.

Scope and Method

- You are encouraged to examine: SIP Router Project[1], Minisip[2], Open SIP Server (OpenSIPS)[3], …[4]
  - to understand both the details of the system(s) and
  - to abstract from these details some architectural features and examine some places where it can be extended (thus using it as a platform on which you can explore).
- You will demonstrate your knowledge by writing a written report and giving an oral presentation describing your project.

---

1. The source code is available from *http://sip-router.org/*
2. The source code is avialable from *http://www.minisip.org/*
3. The source code is avialable from *http://www.opensips.org/*
4. See *http://www.voip-info.org/wiki/view/Open+Source+VOIP+Software*

Learning Outcomes

Following this course a student should be able to:

- Understand the relevant protocols (particularily SIP, SDP, RTP, and SRTP): what they are, how they can be used, and how they can be extended.
- Enable you to utilize SIP in Presence and event-based communications.
- Understand how SIP can provide application-level mobility along with other forms of mobility.
- Understand how SIP can be used to facilitate communications access for users with disabilities (for example using real-time text, text-to-speech, and speech-to-text) and to know what the basic requirements are to provide such services.
- Understand SIP can be used as part of Internet-based emergency services and to know what the basic requirements are to provide such services.
- Contrast "peer-to-peer" voice over IP systems (i.e., how they differ, how they might scale, what are the peers, ...)
- Know the relevant standards and specifications - both of the protocols and of the requirements (for example, concerning legal intecept).
- Understand the key issues regarding quality-of-service and security

- Evaluate existing voice over IP and other related services (including presence, mobile presence, location-aware, context-aware, and other services)
- Design and evaluate new SIP based services
- Read the current literature at the level of conference papers in this area.
  - While you may not be able to understand all of the papers in journals, magazines, and conferences in this area - you **should** be able to read 90% or more of them and have good comprehension. In this area it is especially important that develop a habit of reading the journals, trade papers, etc. In addition, *you should also be aware of standardization activities, new products/services, and public policy in the area*.
- Demonstrate knowledge of this area both orally and in your writing.
  - By *writing* a paper suitable for submission to conferences and journals in the area.

This course should prepare you for starting a thesis project in this area (for undergraduate students) or beginning a thesis or dissertation (for graduate students).

Prerequisites

- Internetwork (IK1550) **or**
- Equivalent knowledge in Computer Communications (this requires permission of the instructor)

Contents

The focus of the course is on what Voice over IP (VoIP) systems are, their basic architectures, and the underlying protocols. We will primarily focus on the Session Initiation Protocol (SIP) and related protocols.

The course consists of ~10 hours of lectures and a project of ~50 (or more) hours.

Topics

- Session Initiation Protocol (SIP)
- Real-time Transport Protocol (RTP)
- Real-time Streaming Protocol (RTSP)
- SIP User Agents
- Location Server, Redirect Server, SIP Proxy Server, Registrar Server, ... , Provisioning Server, Feature Server
- Call Processing Language (CPL)
- SIP SIMPLE

Examination requirements

- Written and Oral project reports

Grades: A..F (ECTS grades)

- To get an "A" you need to write an outstanding or excellent paper and give an outstanding or excellent oral presentation. (Note that at least one of these needs to be excellent.)
- To get a "B" you need to write a very good paper, i.e., it should be either a very good review or present a new idea; and you have to give a very good oral presentation.
- To get a "C" you need to write a paper which shows that you understand the basic ideas underlying voice over IP and that you understand one (or more) particular aspects at the level of an average masters student. In addition, you must be able to present the results of your paper in a clear, concise, and professional manner - and answer questions (as would be expected at a typical international conference in this area.)

- To get a "D" you need to demonstrate that you understand the basic ideas underlying voice over IP, however, your depth of knowledge is shallow and you are unable to orally answer indepth questions on the topic of your paper.
- If your paper has some errors (including incomplete references) or you are unable to answer any indepth questions following your oral presentation the grade will be an "E".
- If your paper has serious errors or you are unable to answer basic questions following your oral presentation the grade will be an "F".

If your paper or oral presentation are close to passing, but not at the passing level, then you will be offered the opportunity for "komplettering", i.e., students whose written paper does not pass can submit a revised version of their paper (or a completely new paper) - which will be evaluated; similarly students whose oral presentation is unacceptable may be offered a second opportunity to give their oral presentation. If a student fails the second oral presentation, they must submit a new paper on a new topic in order to give an oral presentation on this new topic.

Project

Goals: to gain analytical or practical experience and to show that you have mastered some knowledge in this area and to encourage you to find a topic which interests you (since this will motivate you to really understand the material)

- Can be done in a group of **1 to 3** students (formed by yourself). Each student must contribute to the final written and oral reports.
- Discuss your ideas about topics with the instructor **before** starting.

Assignment Registration and Report

- Registration: Monday 16 September 2013 at 23:59, to <maguire@kth.se>, subject=IK2554 topic
  - Group members, leader; Topic selected
- Written report: a technical paper
  - The length of the final report should be 10 pages (roughly 5,000 words) for each student; it should **not** be longer than 12 pages for each student - papers which are longer than 12 pages per student will be graded as "F".
  - The report may be in the form of a collections of papers, with each paper suitable for submission to a conference or journal
  - Contribution by each member of the group - must be clear (the role of each member of the group must be explained in the overall introduction).
  - The report should clearly describe: 1) what you have done; 2) who did what; if you have done some implementation and measurements you should describe the methods and tools used, along with the test or implementation results, and your analysis.

Final Report: written report due Friday 25 October 2013 at 23:59 and **oral presentations** individually scheduled 30 and 31 October 2013 (from 08:00-18:00)[1] at a location to be annouced.

1. Alternative dates can be scheduled with the instructor's permission.

- Send email with URL link for a **PDF** or **PostScript** file to <maguire@kth.se> and you must submit your Zotero RDF file or BibTeX file of references that you have cited.
- Late assignments will not be accepted
  (i.e., there is no guarantee that they will be graded before the end of the term)

Note that it is OK to start working *well in advance* of the deadlines!

Literature

The course will mainly be based on the book[3]:

- Henry Sinnreich and Alan B. Johnston, Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol, 2nd Edition, Wiley, August 2006, ISBN: 0-471-77657-2

We will refer to other books, articles, and RFCs as necessary. A list of interesting literature will be available on the course web page and in the references and further reading section of each lecture module.

Observe proper academic ethics and properly cite your sources!

You will be searching & reading the literature in conjunction with your projects. Please make sure that you properly reference your sources in your report - keep in mind the **KTH Ethics policies.**

In particular:

- If you use someone else's words - they must be clearly indicated as a **quotation** (***with a proper citation***).
- Note also that individual figures have their own copyrights, so it you are going to use a figure/picture/… from some other source, you need to **both** cite this source & have the copyright owner's permission to use it.

Ethics, Rights, and Responsibilities

There is a policy of zero tolerance for **cheating, plagiarism, etc.** - for details see relevant KTH policies, at http://www.kth.se/en/student/studentliv/studentratt/studentratt-1.307449

From this page you can find the KTH Ethics Policies.

Before starting to work on your paper read the page about **plagiarism** at

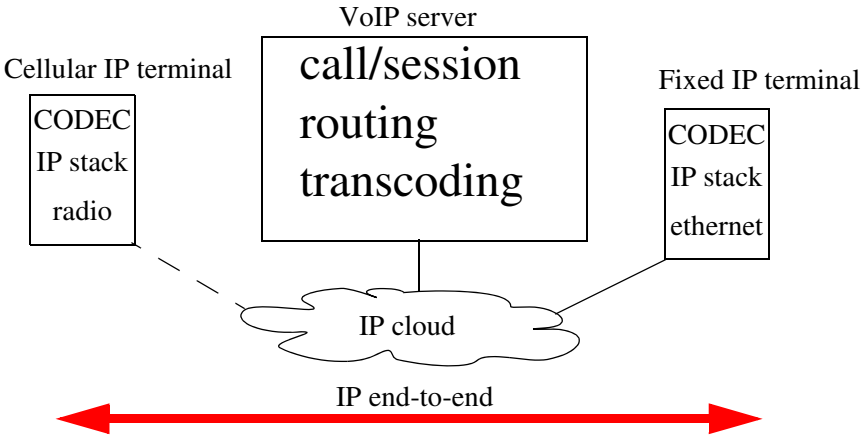
http://www.kth.se/en/student/studentliv/studentratt/fusk-och-plagiering-1.323885

Lecture Plan

- Introduction
  - Course arrangement
  - Set the context of VoIP, both technically and economically
- VoIP details
  - Session Initiation Protocol (SIP)
  - Session Description Protocol (SDP)
  - DNS and ENUM
- Mobility
- Service Creation
- User preferences
- Security, NATs, and Firewalls
- SIP Telephony
- Conferencing
- Mixed Internet - PSTN services
- AAA and QoS
- More than just voice!

Voice over IP (VoIP)

VoIP is an end-to-end architecture[22] which exploits **processing** in the **end points**.



Unlike the traditional Public Switch Telephony Network - where processing is done **inside the network**.

Network Convergence:

In the past, many different networks - *each optimized for a specific use*: POTS, data networks (such as X.25), broadcast radio and television, … and each of these in turn often had specific national, regional, or proprietary implementations)

$\Rightarrow$

(Now) we think about a *converged* network which is a *global* network

Potential Networks

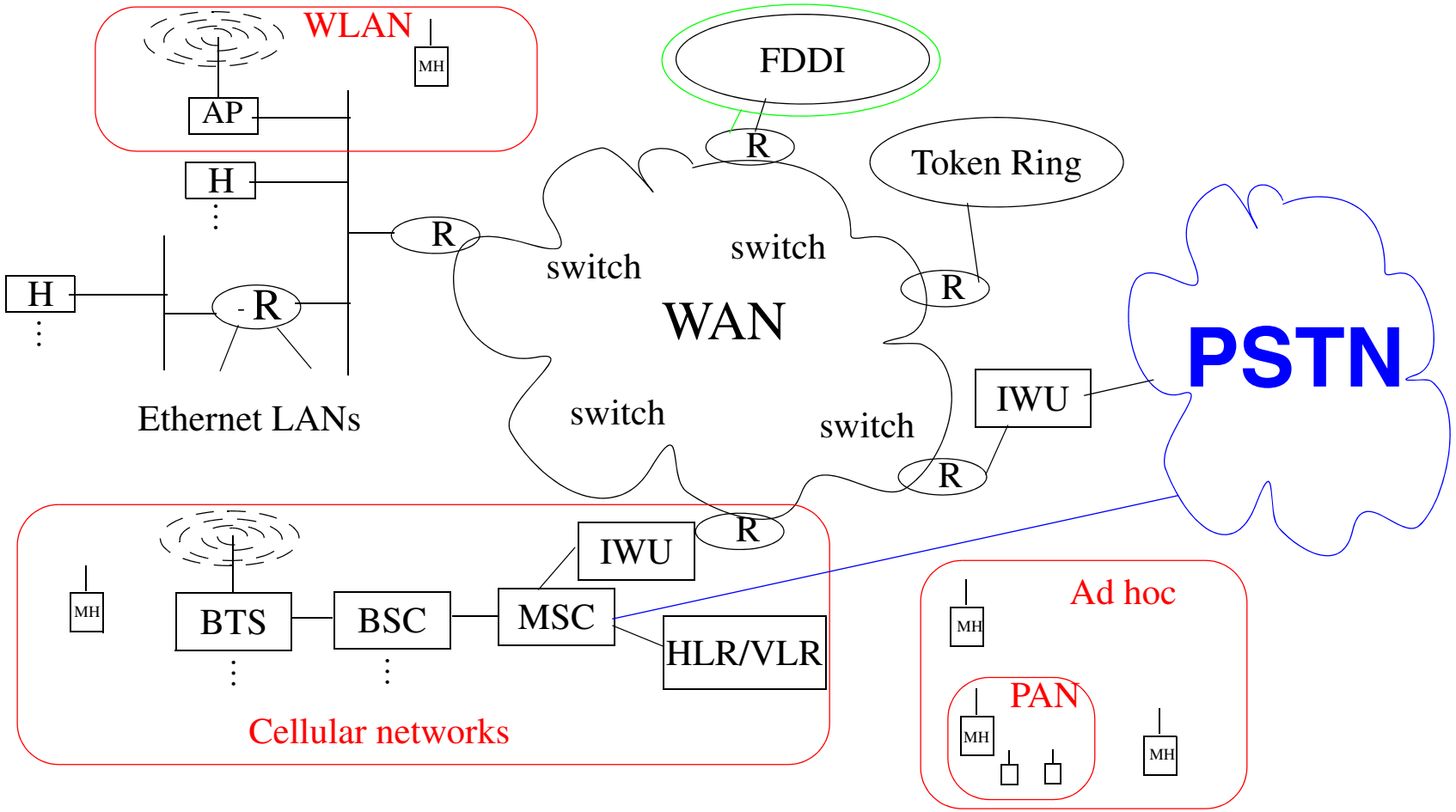


Figure 1: Internet and PSTN

We will focus on VoIP, largely *independently* of the underlying network, i.e., LAN, Cellular, WLAN, PAN, *ad hoc*, … .

Internetworking

Internetworking is

- based on the interconnection (concatenation) of multiple networks
- accommodates multiple underlying hardware technologies by providing a way to interconnect **heterogeneous** networks and makes them inter-operate.

Public Switched Telephony System (PSTN) uses a **fixed** sampling rate, typically 8 kHz and encoded to 8 bits, this results in 64 kbps voice coding; however, VoIP is *not* limited to using this coding and could have **higher** or **lower** data rates depending on the CODEC(s) used, the available bandwidth between the end points, and the user's preference(s).

One of the interesting possibilities which VoIP offers is quality which is:

- better that "toll grade" telephony or
- worse than "toll grade" telephony (but perhaps still acceptable)

This is unlike the *fixed* quality of traditional phone systems.

VoIP a major market

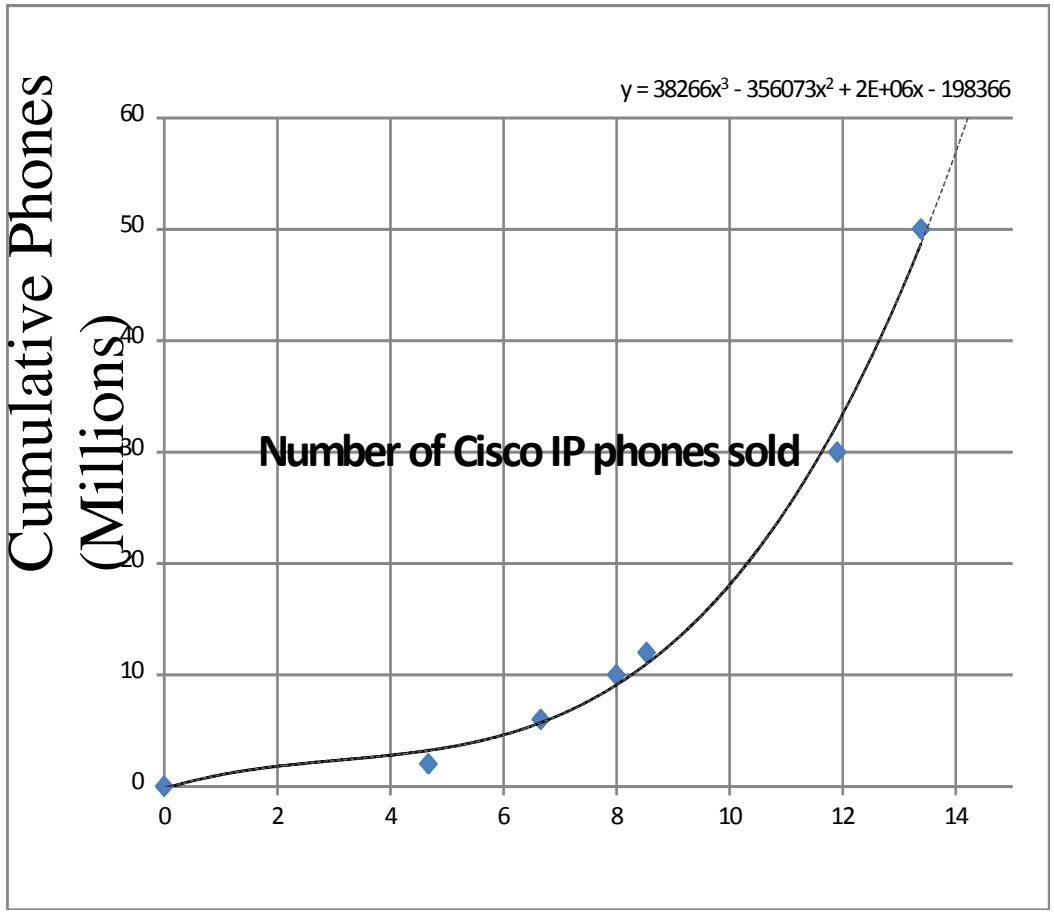
Voice over IP has developed as a major market - which began with H.323 and has now moved to SIP. There are increasing numbers of users and a large variety of VoIP hardware and software on the market. With increasing numbers of vendors, the competition is heating up - is it a maturing market?

> "Cisco began selling its VoIP gear to corporations around 1997, but until the past year, sales were slow. Cisco notes that it took more than three years to sell its first 1 million VoIP phones, but the next 1 million took only 12 months."
>
> Ben Charny , "Is VoIP pioneer Cisco losing momentum?",
> CNET News.com, September 17, 2003, 4:00 AM PT

As of July 30, 2005, Cisco had shipped their 6 millionth IP phone[10], 10 Million by November 2006[17], in 2010, their 30 millionth IP phone[18], in April 2012 their 50 millionth IP phone[19], …

Cumulative number of Cisco IP phones sold

Viewing the data on the previous page as graph gives a better view of the trend (which has been extrapolated into the future in the curve)[1]



1. This trend may or may **not** be realized, it is based simply on a project of the historic data.

Handsets

There are now lots of USB attached VoIP handsets

WLAN Handsets

- starting with Symbol Technologies's NetVision® *Data Phone*
- Vocera Communications Badge http://www.vocera.com/
  - runs speech recognition software in a network attached server
  - unfortunately it uses a proprietary protocol between the handset and their server, but I expect others will make similar devices which will **not** have this **mis-feature.**

VoIP cellular handsets combining IEEE 802.11 (WLAN) with wide area cellular connectivity.

IP DECT phone handsets are available from many vendors - combine DECT's physial and media layers with VoIP.

For more type "SIP handsets" into your favorite search engine!

VoIP Headsets

The maturity of VoIP headsets can be see in the review criteria, for example the following are adapted from [24]:

- **Reviewer Comments**[1]
- **Lowest Price**: $26.90 to $119.00
- **Overall Rating**
- **Ratings**: performance, functionality, features, help & support
- **Performance**: ideal for gaming, mute, noise cancelling microphone, Laser tuned audio drivers[2], certified/optimized for XXXX (where XXXX is some specific software, standard, …)
- **Functionality**: biaural or monaural, 3.5mm jack, headband/neckband, rechargeable batteries, USB, wireless interface, battery operated
- **Features**: adjustable headband, flexible boom, headset audio adjustments, peakstop/sound guard, pivoting ear cushions, voice recognition, Help & support, support community, technical support, troubleshooting, warranty, online downloads of new software or firmware
- **Supported Configurations**: Apple Mac, PC, …

1. Reviwer comments are often important in the decision to purchase a product or not, see for example Yongliang Wu's masters thesis [27] http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/091129-Yongliang_Wu-with-cover.pdf

2. For example, Logitech uses laser scanning of the moving parts of the speaker to analyze the mechanical motion

VoIP Chipsets

Chips from: Broadcom (BCM1103 Gigabit IP Phone Chip), SiTel Semiconductor (SC14461 Green VoIP processor), Zarlink (Legerity VoicePath + VE8910 1FXS chipset), Atmel (AT76C901, AT76C902 for Wi-Fi phones), Centillium (Entropia III >1,000 VoIP channels per chip), Freescale (iMX chip), LSI Corp. (StarPro 2700 multicore media processors), Lantiq (VINETIC-SVIP), DSP Group (XciteR - Vega Firebird Family), Conexant Systems, Inc., Texas Instruments, … .

A common feature is **acoustic** echo cancellation to enable high quality speakerphone.

Deregulation ⇒ New operators

Lots of new actors appeared as operators:

- Verizon/MCI (formerly Worldcom) - http://www.verizon.com/
- Level3 http://www.level3.com/
  - (3)Voice, an IP based long distance service using Softswitch technology
  - Hosted VoIP services for 10 to >100,000 extensions
- Vonage - http://www.vonage.com
  - 2.5 million subscriber lines as of June 30, 2009 [21]
- TringMe - http://tringme.com/
  - Web based VoIP (using Adobe's Flash)
  - VoicePHP (http://voicephp.com/)
- "Voxbone's private global VoIP network carried 2.8 billion minutes of voice traffic" - http://www.voxbone.com/aboutus.jsf
- …

See "VoIP Providers List", last accessed 2013.08.30, http://www.voipproviderslist.com/

VoIP service providers

Skype 40 million simultaneous users as of 10 April 2012

Rebtel (http://www.rebtel.com/) 20 million users [25]

Comcast 8.4 million users (as of 30 Sept. 2010) [26]

Deregulation $\Rightarrow$ New Suppliers

Lots of new actors as equipment suppliers

Traditional telecom equipment vendors buying datacom vendors.

Lots of mergers and acquisitions among datacom vendors.

As of Fall 2002, many of these vendors (similar to operators) were reorganizing, selling off divisions, reducing staffing, … -- due to the Telecom meltdown! However, some have survived (or been reborn) and some have **not** survived.

Let them fail fast!

"We hold that the primary cause of current telecom troubles is that Internet-based end-to-end data networking has subsumed (and will subsume) the value that was formerly embodied in other communications networks. This, in turn, is causing the immediate obsolescence of the vertically integrated, circuit-based telephony industry of 127 years vintage."

Izumi Aizu, Jay Batson, Robert J. Berger, et al.,
Letter to FCC Chairman Michael Powell, October 21, 2002 http://pulver.com/press/powell.html

The extent of this transformation is well described in their complete letter which recommends that the FCC:

- "Resist at all costs the telephone industry's calls for bailouts. The policy should be one of "fast failure."
- Acknowledge that non-Internet communications equipment, while not yet extinct, is economically obsolete and forbear from actions that would artificially prolong its use.
- Discourage attempts by incumbent telephone companies to thwart municipal, publicly-owned and other communications initiatives that don't fit the telephone company business model.
- Accelerate FCC exploration of innovative spectrum use and aggressively expand unlicensed spectrum allocation."

Latency

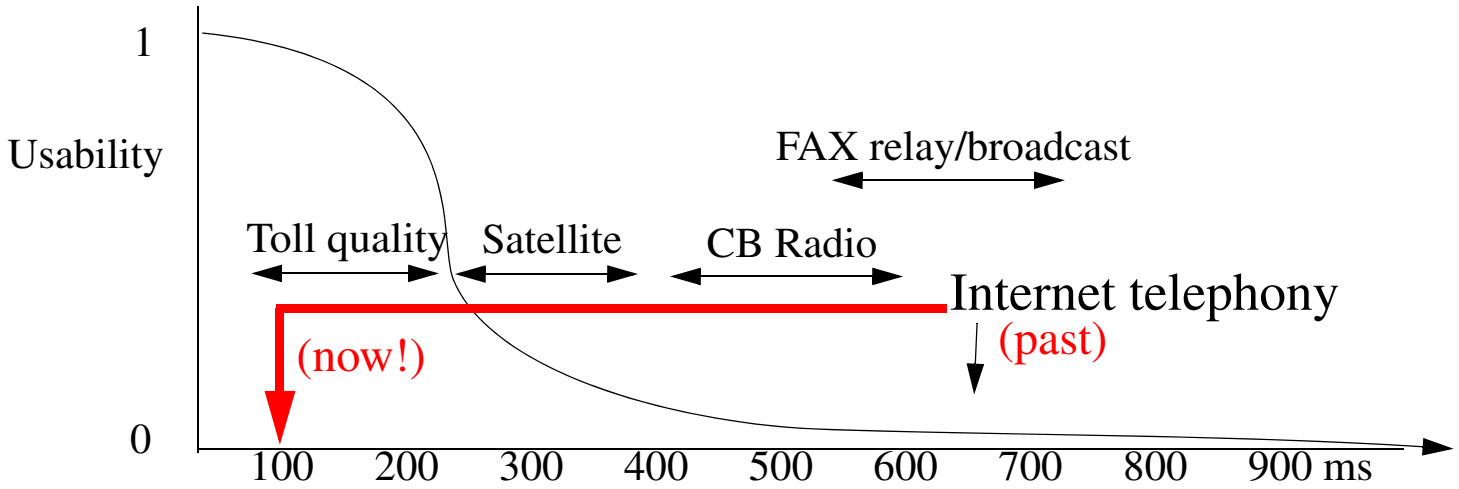


Figure 2: Usability of a voice circuit as a function of end-to-end delay (adapted from a drawing by Cisco[a])

a. This was at http://www.packeteer.com/solutions/voip/sld006.htm

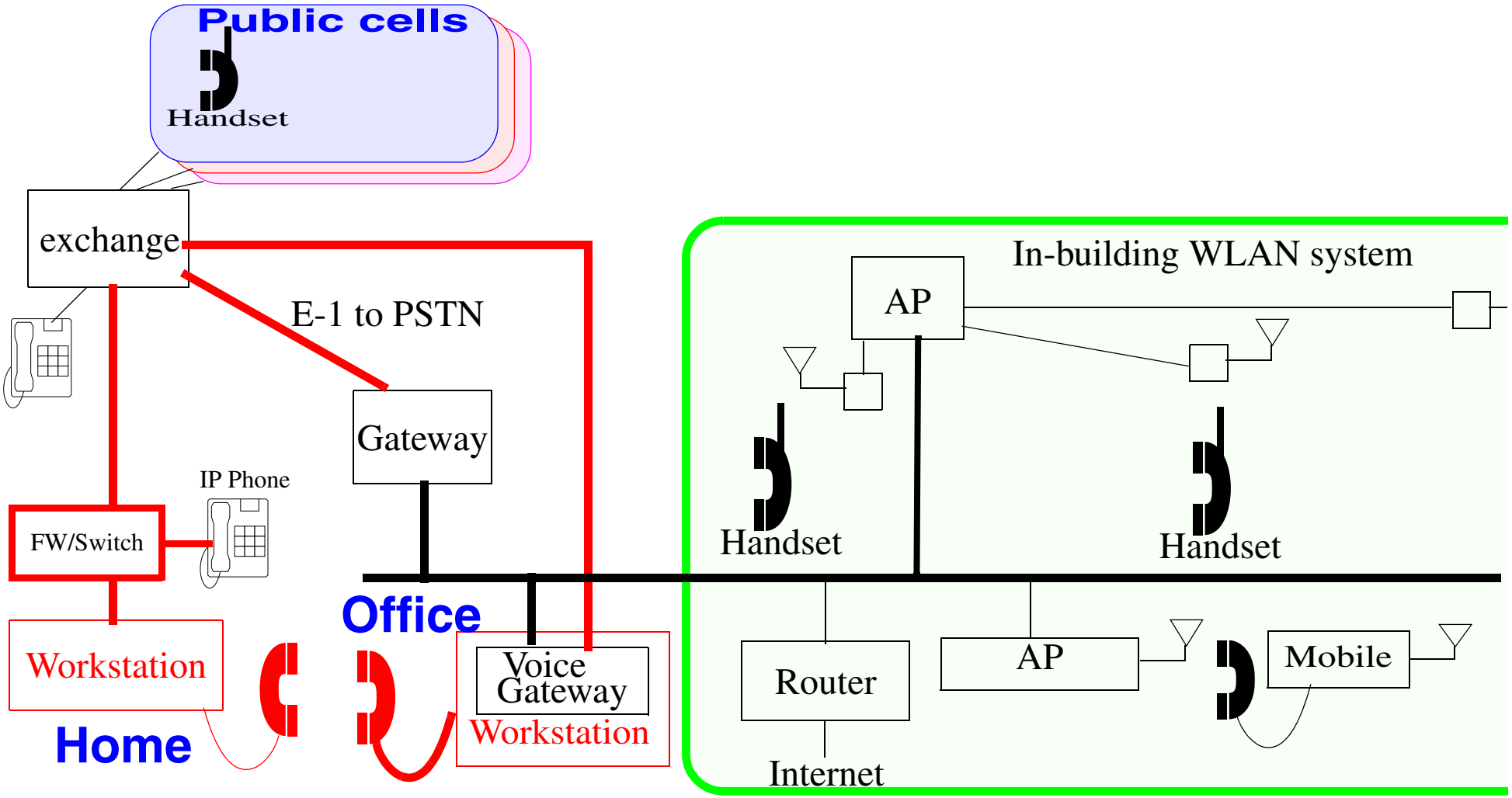
For example:

Round-trip times from 130.237.209.xxx (as of 2013.08.30) for 10 pings (with DNS to IP cached)	min (ms)	avg (ms)	max (ms)	hops
Local LANs (www.wireless.kth.se)	0.443	0.457	0.478	3
to northern Sweden (www.luth.se)	13.298	14.752	17.025	11
From my machine in eastern US (via an VDSL link)	116.936	118.283	122.766	~21
To US west coast (www.stanford.edu)	190.598	190.949	191.937	23
To Australia (www.uow.edu.au) {via the US west coast}	334.845	336.211	339.600	>17

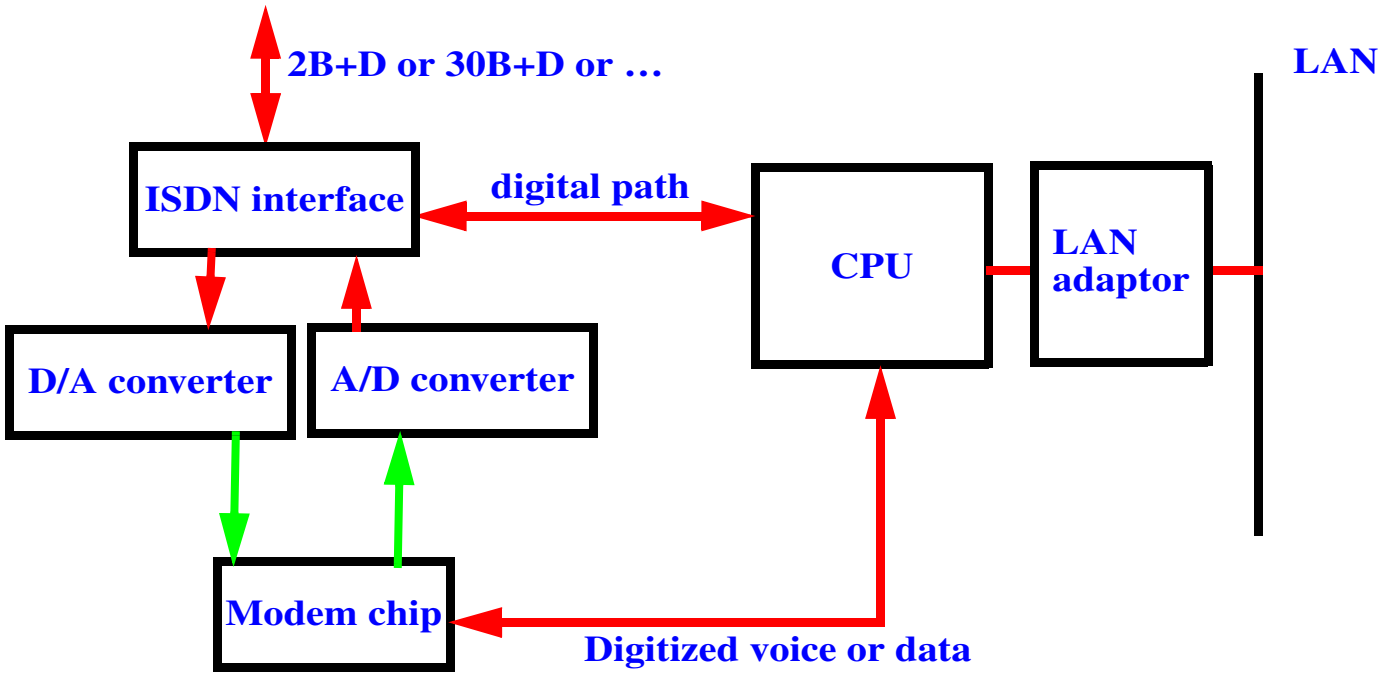
VoIP Modes of Operation

- PC to PC
- PC-to-Telephone calls
- Telephone-to-PC calls
- Telephone-to-Telephone calls via the Internet
- Premises to Premises
  - use IP to tunnel from one PBX/Exchange to another
  - see Time Warner's "Telecom One Solution"
- Premises to Network
  - use IP to tunnel from one PBX/Exchange to a gateway of an operator
- Network to Network
  - from one operator to another or from one operator's regional/national network to the same operator in another region or nation

IP based data+voice infrastructure



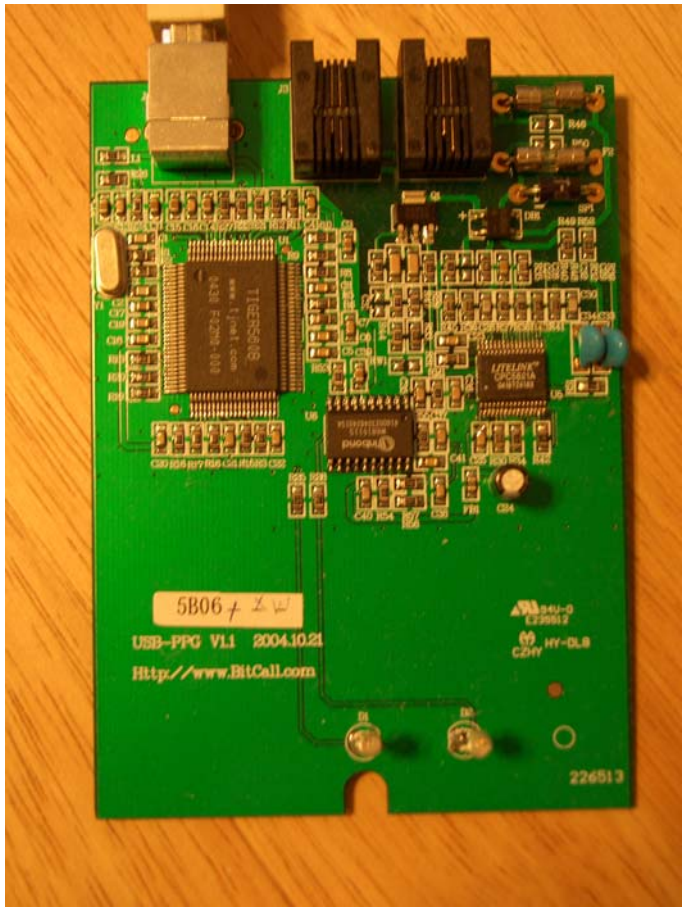
Voice Gateway



Use access servers filled with digital modems (currently (formerly?) used for analog modem pools) as voice gateways or special purpose gateways such as that of Li Wei [5]. (Li Wei created the first E1 to Ethernet gateway that looked like part of a Ericsson PBX - hence all of the services of this distributed PBX were available.)

Many Analog Telephony Adapters (ATAs) exist: Cisco ATA 186, Linksys SPA2102, Linksys SPA3000 or SPA3102 (FXS + FXO port for gatewaying to/from PSTN), … .

Home Telephony Voice Gateway



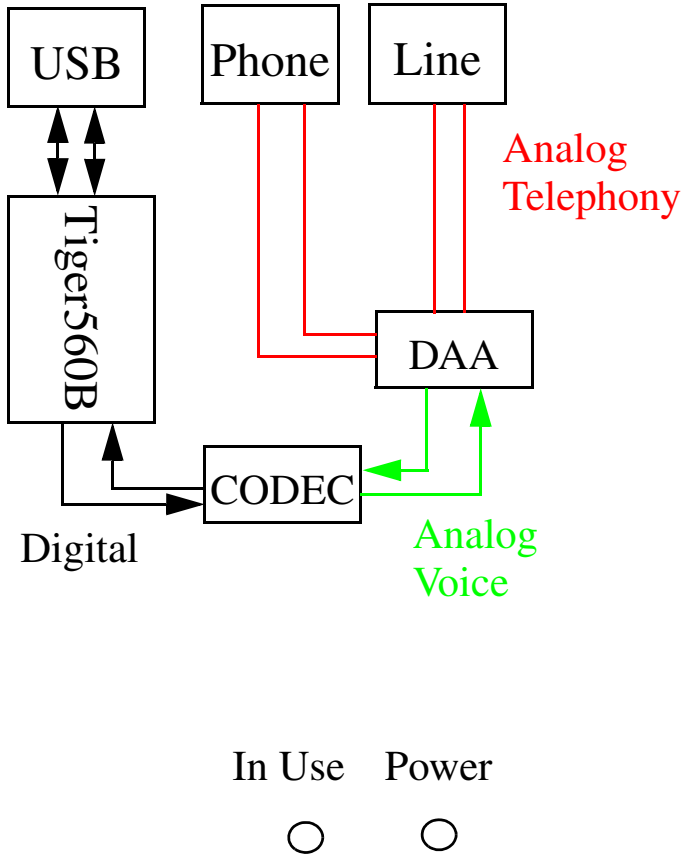


Figure 3: www.BitCall.com USB-PPG V1.1 - a personal phone gateway based upon a Tiger560B chip, Winbond 681511 Single-channel Voiceband CODEC, and a Clare CPC5621A LITELINK III Phone Line Interface IC - Data Access Arrangement (DAA).

Voice over IP (VoIP) Gateways

Gateways not only provide basic telephony and fax services, but can also enable lots of value-added services, e.g., call-centers, integrated messaging, least-cost routing, … .

Such gateways provide three basic functions:

- **Interface between the PSTN network and the Internet**

  Terminate incoming synchronous voice calls, compress the voice, encapsulate it into packets, and send it as IP packets. Incoming IP voice packets are unpacked, decompressed, buffered, and then sent out as synchronous voice to the PSTN connection.

- **Global directory mapping**

  Translate between the names and IP addresses of the Internet world and the E.164 telephone numbering scheme of the PSTN network.

- **Authentication and billing**

Voice representation

Commonly: ITU G.723.1 algorithm for voice encoding/decoding or G.729 (CS-ACELP voice compression).

Signaling

Based on the H.323 or SIP (on the LAN) and conventional signaling will be used on telephone networks.

NB: In conventional telephony networks signalling **only** happens at the *beginning* and *end* of a *call*. See Theo Kanter's dissertation for what can be enabled via SIP so that you can react to **other** events.

Fax Support

Both store-and-forward and real-time fax modes.

- In store-and-forward the system records the entire FAX before transmission.

Management

Full SNMP management capabilities via MIBs (Management Information Base)

- provided to control all functions of the Gateway
- Extensive statistical data will be collected on dropped calls, lost/resent packets, and network delays.

Compatibility

De jure standards:

- ITU G 723.1/G.729 and H.323
- VoIP Forum IA 1.0

De facto standards:

- Netscape's Cooltalk
- Microsoft's NetMeeting (formerly H.323, now SIP)
- Adobe Pacifica - SIP based high quality VoIP for Flash

Session Initiation Protocol (SIP) RFC 2543 [28] is much simpler than H.323

An emerging area is Web Real Time Communication (WebRTC) - see for example http://sipml5.org/ for a HTML5 SIP client uses a WebRTC to SIP proxy (http://webrtc2sip.org/).

Cisco's Voice Over IP

Cisco 3600 series routers[1] to carry live voice traffic (e.g., telephone calls and faxes) over an IP network. (This was the first of the Cisco routers to support VoIP.)

They state that this could be used for:

- Toll bypass
- Remote PBX presence over WANs
- Unified voice/data trunking
- POTS-Internet telephony gateways

Uses Real-Time Transport Protocol (RTP) for carrying packetized audio and video traffic over an IP network.

1. The Cisco 3600 series was introduced in 1996 and their end of life was 31 December 2003. So this representes *ancient* history, but illustrates the many issues that have to be addressed by a gateway in order to support existing users and devices.

Cisco 3600 supports a selection of CODECs:

- G.711 A-Law 64,000 bits per second (bps)
- G.711 u-Law 64,000 bps
- G.729 8000 bps

Cisco 3800 supports even more CODECs:

- ITU G.726 standard, 32k rate
- ITU G.726 standard, 24k rate
- ITU G.726 standard, 16k rate
- ITU G.728 standard, 16k rate (default)
- ITU G.729 standard, 8k rate

By using Voice Activity Detection (VAD) - you only need to send traffic if there is something to send {Note: telecom operators like this because it enables even higher levels of statistical multiplexing}.

An interesting aspect is that users worry when they hear *absolute* silence, so to help make them comfortable it is useful to play noise when there is nothing useful to output. Cisco provide a "**comfort-noise** command to generate background noise to fill silent gaps during calls if VAD is activated".

Cisco 3600 series router can be used as the voice gateway with software such as Microsoft NetMeeting.

Cisco 3800 also supports “fax-relay” - at various rates either current voice rate or 2,400/4,800/7,200/9,600/14,400 bps fax rates.

(Formerly further information was at http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_1/voip/config.htm)

Intranet Telephone System

On January 19, 1998, Symbol Technologies (now part of Motorola, Inc.) and Cisco Systems announced that they had combined the Symbol Technologies' NetVision™ wireless LAN handset and Cisco 3600 to provide a complete wireless local area network telephone system based on Voice-Over-IP technology.

The handset uses a wireless LAN (IEEE 802.11) infrastructure and a voice gateway via Cisco 3600 voice/ fax modules. The system conforms to H.323.

> "I believe that this is the first wireless local area network telephone based on this technology" -- Jeff Pulver

Seamless roaming via Symbol's pre-emptive roaming algorithm with load balancing.

Claims each cell can accommodate ~25 simultaneous, full-duplex phone calls.

Ericsson partnered with Symbol, using Ericsson's WebSwitch2000.

Wireless LANs

"The wireless workplace will soon be upon us[1]

Telia has strengthened its position within the area of radio-based data solutions through the acquisition of Global Cast Internetworking. The company will primarily enhance Telia Mobile's offering in wireless LANs and develop solutions that will lead to the introduction of the wireless office. A number of different alternatives to fixed data connections are currently under development and, *later wireless IP telephony will also be introduced.*

…

The acquisition means that Telia Mobile has secured the resources it needs to maintain its continued expansion and product development within the field of radio-based LAN solutions. *Radio LANs are particularly suitable for use by small and medium-sized companies as well as by operators of public buildings such as airports and railway stations.*

Today's radio-LAN technology is based on *inexpensive products that do not require frequency certification*. They are *easy to install* and are often used to replace cabled data networks in, for example, large buildings.

…"

[*emphasis* added by Maguire]

1. Telia press annoucement: 1999-01-25

Femto cell and UMA

Unlicensed Mobile Access (UMA) providing local telephone access via Wi-Fi/Bluetooth/other unlicensed wireless link technology. (These are also referred to as uncoordinated cells - since they are not directly controlled by a macro/micro cellular operator.)

Being embraced by a number of major telecom operators: British Telecom, TeliaSonera, Orange/France Telecom, T-Mobile US, Netcom, and others.

VoIP vs. traditional telephony

As of 2003 approx. 14% of International traffic to/from the US is via VoIP, based on 24 billions minutes vs. 170.7 billion minutes via PSTN [11] (the article cites the source of data as TeleGeography Research Group/Primetrica Inc.)

According to the TeleGeography Report, in 2011 the international voice traffice was roughly 320 billion minutes of TDM and 144 billion minutes of VoIP traffic[1] - see: http://www.telegeography.com/research-services/telegeography-report-database/index.html Note their 2013 figure: Where Did the Growth Go?: The Skype Effect

As of March 2007, commercial VoIP calling plans for **unlimited** North American traffic cost ~US$24.99/month.

Traditional operators replacing their exchanges with IP telephony, see Niels Herbert and Göte Andersson, "Telia ersätter all AXE med IP-telefoni", Elektronik Tidningen, #3, 4 March 2005, page 4.

For information about the development of the AXE switches see [12].

1. These numbers are estimated based upon their plot entitled "International Call Volumes and Growth Rates".

Economics

"Can Carriers Make Money On IP Telephony?" by Bart Stuck and Michael Weingarten, Business Communication Review, Volume 28, Number 8,August 1998, pp. 39-44.

> "What is the reality in the battle over packet-versus-circuit telephony, and what is hype?
>
> Looking at the potential savings by cost element, it is clear that in 1998, access arbitrage is the major economic driver behind VOIP. By 2003, we anticipate that switched-access arbitrage will diminish in importance, as the ESP exemption disappears and/or access rates drop to true underlying cost.
>
> However, we believe that the convergence between voice and data via packetized networks will offset the disappearance of a gap in switched access costs. As a result, VOIP will continue to enjoy a substantial advantage over circuit-switched voice. Indeed, as voice/data convergence occurs, we see standalone circuit-switched voice becoming economically nonviable."

Note: Enhanced Service Provider (ESP) exemption means that ISPs do not pay access charges to local phone companies {since the ISP just **receives** calls from users}

VoIP vs. traditional telephony

Henning Schulzrinne in a slide entitled "Why should carriers worry?"[1] nicely states the threats to traditional operators:

- Evolution from application-specific infrastructure ⇒ **Content-neutral** bandwidth delivery mechanism - takes away the large margins which the operators are used to (and **want**!):
  - "GPRS: $4-10/MB, SMS: >$62.50/MB, voice (mobile and landline): $1.70/MB"
- Only operators can offer services ⇒ Anybody can offer phone services
- SIP only needs to handle signaling, not media traffic
- High barriers to entry ⇒ No regulatory hurdles[2]

In addition to this we can add:

- Only vendors can create services ⇒ anybody can create a service

NB. These new services can be far broader than traditional telephony services.

---

1. Henning Schulzrinne, "When will the telephone network disappear?", as part of Intensive Graduate Course "Internet Multimedia", University of Oulu, 3-6 June 2002.

2. see "Regulations in Sweden" on page 98

Patents

Mixing voice and data in the LAN goes back to at least this patent:

US 4581735 :	Local area network packet protocol for combined voice and data transmission
INVENTORS:	Lois E. Flamm and John O. Limb
ASSIGNEES:	AT&T Bell Laboratories, Murray Hill, NJ
ISSUED:	Apr. 8 , 1986
FILED:	May 31, **1983**

ABSTRACT: In order to control the transfer of packets of information among a plurality of stations, the instant communications system, station and protocol contemplate first and second oppositely directed signal paths. At least two stations are coupled to both the first and the second signal paths. A station reads one signal from a path and writes another signal on the path. The one signal is read by an arrangement which electrically precedes the arrangement for writing the other signal. Packets are transmitted in a regular, cyclic sequence. A head station on a forward path writes a start cycle code for enabling each station to transmit one or more packets. If a station has a packet to transmit, it can read the bus field of a packet on the forward path. Responsive thereto, a logical interpretation may be

made as to whether the forward path is busy or is not busy. If the path is not busy, the packet may be written on the path by overwriting any signal thereon including the busy field. If the path is busy, the station may defer the writing until the path is detected as not busy. In order to accommodate different types of traffic, the head station may write different start cycle codes. For example, a start-of-voice code may enable stations to transmit voice packets; a start-of-data code may enable stations to transmit data packets, etc. for the different types of traffic. Further, the start cycle codes may be written in a regular, e.g., periodic, fashion to mitigate deleterious effects, such as speech clipping. Still further, the last station on the forward path may write end cycle codes in packets on a reverse path for communicating control information to the head station. Responsive to the control information, the head station may modify the cycle to permit the respective stations to, for example, transmit more than one packet per cycle or to vary the number of packet time slots, which are allocated to each of the different types of traffic.

Deregulation ⇒ Trends

- replacing multiplexors with Routers/Switches/… << 1/10 circuit switched costs
- Standard telco interfaces being replaced by datacom interfaces
- New Alliances:
  - telecom operators & vendors working with traditional data & data communications vendors
- future developments building on VoIP
  - ♦ Fax broadcast, Improved quality of service, Multipoint audio bridging, Text-to-speech conversion and Speech-to-Text conversion, Voice response systems, …
  - ♦ Replacing the wireless voice network's infrastructure with IP:
    U. C. Berkeley's *ICEBERG*: Internet-based core for CEllular networks BEyond the thiRd Generation

See the Univ. of California at Berkeley ICEBERG project report:

http://iceberg.cs.berkeley.edu/release/

⇒Telecom (only) operators have no future

⇒Telecom (only) companies have no future

Carriers offering VoIP

"Equant, a network services provider, will announce tomorrow that it is introducing voice-over-frame relay service in 40 countries, ... The company says customers can save 20% to 40% or more by sending voice traffic over its frame relay network. "This is the nearest you're going to get to free voice," says Laurence Huntley, executive VP of marketing for Equant Network Service. … Equant isn't alone in its pursuit to send voice traffic over data networks. Most of the major carriers are testing services that would send voice over data networks. ... ."[1]

- October 2002:
  - Verizon offering managed IP telephony via **IPT Watch** for US$3-4/month
  - WorldCom offering SIP based VoIP for DSL customers for US$50-60/month for unlimited local, domestic long distance, and data support {price does **not** include equipment at US$200-300 per phone and DSL/Frame relay/ATM connection} The Service Level Agreement (SLA) specifies >99.9% network availability, <55ms round trip latency, and >99.5% packet delivery.
- December 2004:
  - Verizon offering VoiceWing - with unlimited calling within the US for US$34.95/month
  - "As we see the industry fundamentals continue to shift, the future will be about the convergence of computing and telecommunications. And where these two worlds meet is where MCI will be." -- Michael D. Capellas, MCI CEO [2]
- August 2009: Verizon, TeliaSonera (529 SEK/month for 8 simultaneous calls), ... offering SIP trunks

---

1. Mary E. Thyfault, Equant To Roll Out Voice-Over-Frame Relay Service, InformationWeek Daily, **10/21/98**.
2. Formerly available from: http://global.mci.com/about/publicpolicy/voip/

MCI[1] Connection

Previously

- 3 or more separate networks (often each had its own staff!)
- Duration/geography-based pricing
- Expensive moves, adds, and changes (typically 1^{+} move/person/year)
- Standalone applications - generally expensive
- Closed PBX architecture

After convergence

- via gateway to the PSTN, service expands beyond the LAN to the WAN
- centralized intelligence is offered; customers utilize a Web browser to control and manage their network
- MCI incurs the costs of buying major equipment, thus limiting customer's risk and capital investment
- **One** source for all services
- Easy mobility
- Choice of vendors for Customer Premises Equipment (CPE)

1. Formerly WorldCom, now part of Verizon

Level 3 Communications Inc.

Introduced (3)VoIP Toll Free service: “a toll-free calling service across the United States, rounding out its local and long distance voice over Internet protocol offerings.”

Antone Gonsalves, E-BUSINESS: Level 3 Rounds Out VoIP Offerings, Internetweek.com, January 13, 2004, http://www.internetweek.com/e-business/showArticle.jhtml?articleID=17300739

Level 3 sells services to carriers, who then offer VoIP and data services to their customers.

Uses **softswitch** networking technology to convert voice signals from the PSTN to IP packets and conversely converts packets to voice signals when a call is routed to the public switched network.

TeliaSonera Bredbandstelefoni

February 5th, 2004 TeliaSonera annouces their *residential* broadband telephony service using server and client products from Hotsip AB {Now part of Oracle, Inc.}. In addition to telephony, the service includes: video calls, presence, and instant messaging.[7]

- The startup cost (2004) was 250 kr and the monthly cost 80 kr[1].
- Calls to the fixed PSTN network are the same price as if you called from a fixed telephone in their traditional network.
- Customers get a telephone number from the "area/city" code 075 (i.e., +46 75-15xxxxxxx)
- They do **not** support calls to "betalsamtal" (0900-numbers)

Today: broadband telephony from **any** internet access network with ≥128kbps, with a +46 y xxxxxxx number; no longer a limitation to having the phone number in a specific area/city code, but the default value is based upon where you "live".

1. Montly cost in August 2009 was from 59 SEK/month.

Emulating the PSTN

Many people feel that VoIP will really only "take off" when it can really emulate all the functions which users are used to in the PSTN:

- Integration with the web via: Click-to-connect
- "Dialing" an e-mail address or URL {digits vs. strings}
- Intelligent network (IN) services:
  - Call forward, busy
  - Call forward, no ans.
  - Call forward, uncond.
  - Call hold
  - Call park
  - Call pick-up
  - Call waiting
  - Consultation hold
  - Do not disturb
  - Find-me
  - Incoming call screen/Outgoing call screen
  - Secondary number in/Secondary number out
  - Three-way conference
  - Unattended transfer

- additional PBX features (which in Sweden means providing functions such as “I’m on vacation and will not return until 31 August 2010”)
- Computer-Telephony Integration (CTI), including Desktop call management, integration with various databases, etc.
- PSTN availability and reliability (thus the increasing use of Power over Ethernet for ethernet attached IP phones - so the wall outlet does not have to provide power for the phone to work)
- Roaming - both **personal** and **device** mobility
- **Phone number** portability
- E911 service {How do you handle **geographic** location of the station?}

Calling and Called Features

- **Calling** feature - activated when placing a call
  - e.g., Call Blocking and Call Return
- **Called** feature - activated when this entity would be the target of a call
  - Call Screening and Call Forward

Beyond the PSTN: Presence & Instant Messaging

- **Presence**, i.e., Who is available?
- **Location**, i.e., Where are they?: office, home, traveling, …
- **Call state**: Are they busy (in a call) or not?
- **Willingness**: Are they available or not?
- **Preferred medium**: text message, e-mail, voice, video, …
- **Preferences** (*caller* and *callee* preferences)

See Sinnreich and Johnston's Chapter 11 (Presence and Instant Communications).

Presence-Enabled Services

- Complex call screening
  - Location-based: home vs. work
  - Caller-based: personal friend or business colleague
  - Time-based: during my “working hours” or during my “personal time”
- Join an existing call ⇒ Instant Conferencing, group chat sessions, …
- Creating a conference when a specific group of people are all *available* and *willing* to be called
- New services that have **yet** to be invented!
- SIP Messaging and Presence Leveraging Extensions (SIMPLE) Working Group was formed in March 2001 - concluded in March 2011

  http://www.ietf.org/html.charters/simple-charter.html

Three major alternatives for VoIP

Concept	Implementation
Use *signalling* concepts from the traditional telephony industry	H.323
Use *control* concepts from the traditional telephony industry	Softswitches
Use an internet-centric *protocol*	Session Initiation Protocol (SIP)

SIP ⇒ a change from telephony's "calls" between handsets controlled by the network to "sessions" which can be between **processes** on **any** platform **anywhere** in the Internet and with both **control** and **media content** in *digital* form and hence can be easily manipulated.

- thus a separate voice network is **not** necessary
- open and distributed nature enables lots of innovation
  - since **both** *control* and *media* can be manipulated and
  - "events" are no longer restricted to start and end of calls

Negatives

Although VoIP equipment costs less than PBXs:

- the technology is new and thus upgrades are frequent (this takes time and effort)
- PBXs generally last ~10 years and public exchanges ~30yrs; while VoIP equipment is mostly computer equipment with a ~3 year ammortization

Deregulation ⇒ New Regulations

"I am preparing legislation to preserve the free regulatory framework that has allowed VoIP applications to reach mainstream consumers," Sununu, Republican from New Hampshire, said in a statement. "VoIP providers should be free from state regulation, free from the complexity of FCC regulations, free to develop new solutions to address social needs, and free to amaze consumers."

E-BUSINESS: New Hampshire Senator Readies, "Hands-Off VoIP" Bill,
Internetweek.com, January 12, 2004
http://www.internetweek.com/e-business/showArticle.jhtml?articleID=17300570

Regulations in Sweden

Magnus Sjöstedt and Oskar Bergquist, VoIP regulatory issues, M.Sc. Thesis, June 2003 [8]

Programmable “phone”

Programming environments: Symbian, Java, Linux, Andoid, Microsoft Wndows Mobile, …

Avoids lock-in driven by operators and telecom equipment vendors

Greatly increases numbers of developers

⇒ more (new) services

⇒ more security problems

- see for example: David Nasaw, “Viruses Lurk as a Threat to ’Smart’ Cellphones”, Wall Street Journal, 18 March 2004, p. B4. [9]

- See Google’s Android - an Open Handset Alliance Project (*http://www.openhandsetalliance.com/*)
  - *https://developers.google.com/android/*

Conferences

Interoperability testing:

- SIP development community's interoperability testing event is called Session Initiation Protocol Interoperability Test (SIPit) http://www.sipit.net/ [1]. Note: The SIPit event is **closed** to the public and press, and no information is released about which products **fail** to comply with the standard.
  - Why have it closed? So that the testing can be done wthout risk of public embarrasment.
- Interoperability is one of the most important aspects of wide deployment using multiple vendors products[6].
- Proper handing of server failover is considered by some to be the most critical interoperability issue at present[6].

1. The 12th SIPit event in Stockholm, Sweden occurred February 24-28, 2003. SIPIT 17 was in Stockholm, Sweden, September 2005, SIPit 26 was in Kista in 17-21 May 2010!

Not with out problems

It is not necessary a smooth transition to VoIP. Numerous organizations have faced problems [14] and there remain vast areas where further work is needed.

Potential for Spam over Internet Telephony (SPIT), Denial of Service, …

VoIP PBXs

Goce Talaganov in his 2012 thesis ‘Green VoIP?: A SIP Based Approach’ - examines how one can use a Cisco Linksys WRT54GL + Asterisk + cloud to make a low power PBX replacement

Auto-provisioning a VoIP user agent

The user scans a QR code with their camera and Zopier's "Zoiper Mobile" application converts this into the address of the user's SIP registrar, their username, their password, … .[29]

Examples of using this application, the format of the URL which a SIP provider can send a customers, and the web page that can be filled out to create a QR code are shown at [30].

Seven Myths About Voice over IP[20]

"1. VoIP is free

2. The only difference between VoIP and regular telephony is the price

3. Quality of service isn't an issue nonadways, because there's plenty of bandwidth in the network

4. VoIP can't replace regular telephony, because it still can't guarantee quality of service

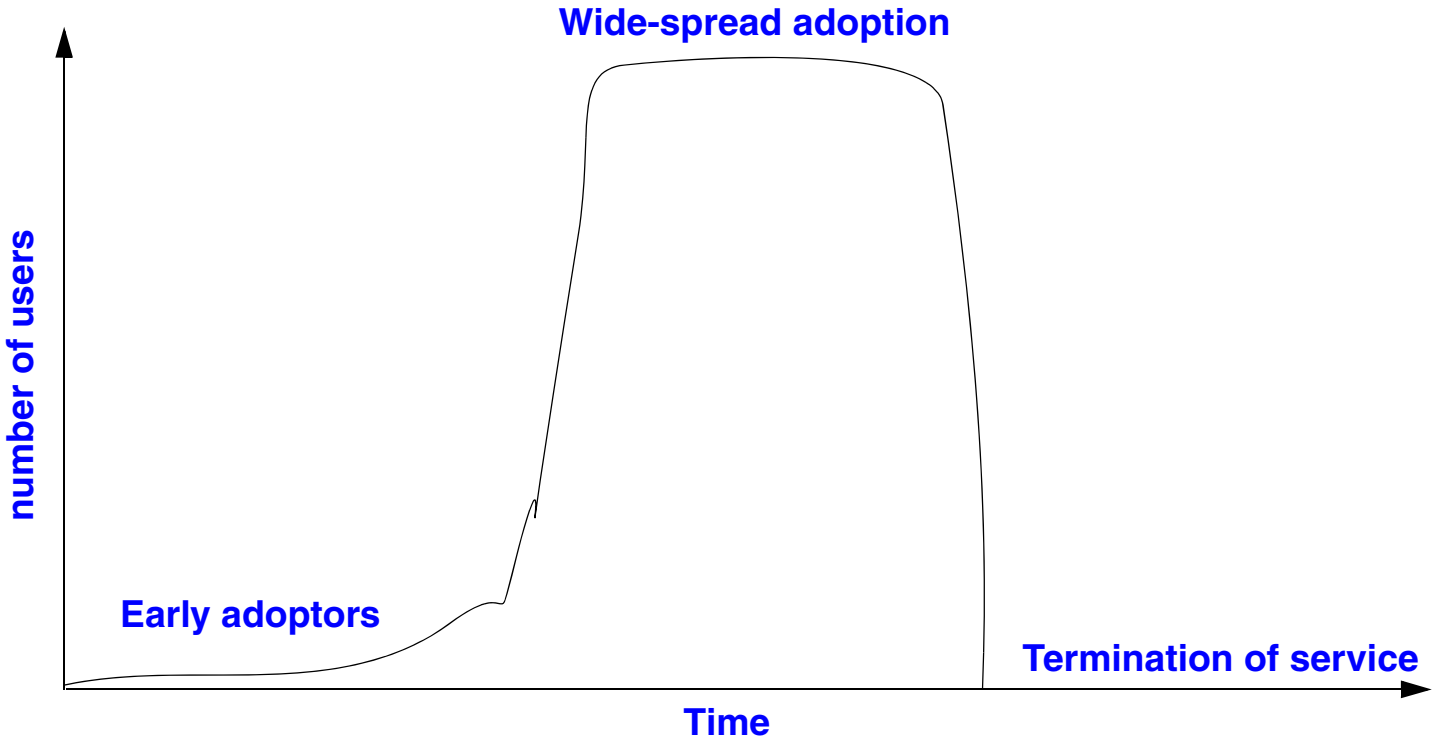
5. VoIP is just another data application

6. VoIP isn't secure

7. A Phone is a Phone is a Phone"

Steven Cherry, "Seven Myths About Voice over IP: VoIP is turning telephony into just another Internet application - and a cheap one at that", IEEE Spectrum, V.42 #3, March 2005, pp. 52-57

S adoption curve + shut-down



References and Further Reading

- SIP Forum http://www.sipforum.org
- VoIP-Info.org

[1] Luan Dang, Cullen Jennings, and David Kelly, *Practical VoIP: Using VOCAL*, O'Reilly, 2002, ISBN 0-596-00078-2.

[2] Henry Sinnreich and Alan B. Johnston, *Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol*, Wiley, 2001, ISBN: 0-471-41399-2.

[3] Henry Sinnreich and Alan B. Johnston, *Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol*, 2nd Edition, Wiley, August 2006, ISBN: 0-471-77657-2

[4] William E. Witowsky, "IP Telephone Design and Implementation Issues", a white paper, Telogy Networks, Inc. A Texas Instruments Company, July 1998, Version 2.2, SPEY004. was at http://www.telogy.com/our_products/golden_gateway/pdf/IP_Telephone.pdf

[5] Li Wei, “Gateway between Packet and Switched Networks for Speech Communication”, M.Sc. Thesis, KTH/Teleinformatics, September 1994.

[6] Carolyn Duffy Marsan, “Convergence / SIP rollouts hit variety of snags”, Network World, 02/02/04 http://www.nwfusion.com/news/2004/0202sip.html

[7] Telia, “Telia lanserar bredbandstelefoni”, Pressrelease - 880445927, 5 Feb. 2004 14:02:01 +0100.

[8] Magnus Sjöstedt and Oskar Bergquist, VoIP regulatory issues, M.Sc. Thesis, KTH, June 2003

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/030627-Magnus_Sjostedt-and-Oskar_Bergquist-Report.pdf

[9] David Nasaw, “Viruses Lurk as a Threat to ’Smart’ Cellphones”, Wall Street Journal, 18 March 2004, p. B4.

[10] John T. Chambers, "to our shareholders", Cisco Annual Report 2005,

http://www.cisco.com/web/about/ac49/ac20/downloads/annualreport/ar2005/pdf/ar_2005_complete.pdf

[11] “FCC boosts Web phones, frees them from state rules”, Metro, New York,

10 November, 2004, pg. 9

[12] Mats Fridlund, “Switching Relations: The Government Development Procurement of a Swedish Computerized Electronic Telephone Switching Technology”, Innovation Systems and European Integration (ISE), Report of research project funded by the Targeted Socio-Economic Research (TSER) program of the European Commission (DG XII) under the Fourth Framework Program, European Commission (Contract no. SOE1-CT95-1004, DG XII SOLS), coordinated by Professor Charles Edquist of the Systems of Innovation Research Program (SIRP) at Linköping University (Sweden). Sub-Project 3.2.2: Government Technology Procurement as a Policy Instrument, December, 1997.

http://www.tema.liu.se/tema-t/sirp/PDF/322_6.pdf

[13] Vonage, “About Vonage”, *http://www.vonage.com/corporate/aboutus_fastfacts.php*, Last modified March 12, 2006 13:53:55, accessed on 2006.03.12

[14] J. Nicholas Hoover, VoIP Gotchas, InformationWeek, November 14, 2005

http://www.internetweek.cmp.com/showArticle.jhtml?sssdmh=dm4.158123&articleId=173602687

[15] Cisco Systems Inc. Annual Report 2007,

HTTP://WWW.CISCO.COM/WEB/ABOUT/AC49/AC20/DOWNLOADS/ANNUALREPORT/AR2007/PDF/CISCO_AR2007_COMPLETE.PDF

[16] Cisco Systems Inc. Annual Report 2008,

http://www.cisco.com/web/about/ac49/ac20/downloads/annualreport/ar2008/pdf/cisco_ar2008_complete.pdf

[17] Cisco Systems, Inc. "Bank of America Experiences Operational Efficiencies with Cisco Unified Communications System Deployed by EDS", Press release, November 20, 2006 http://newsroom.cisco.com/dlls/2006/prod_112006.html

[18] Barry O' Sullivan, 30 Millionth Cisco IP Phone!!, Cisco Blog > The Platform, October 27, 2010 at 8:00 am PST,

http://blogs.cisco.com/news/30-millionth-cisco-ip-phone/

[19] Matt Hamblen, Cisco sells 50 millionth IP phone, Computerworld, April 18, 2012, http://www.computerworld.com/s/article/9226334/Cisco_sells_50_millionth_IP_phone

[20] Steven Cherry, "Seven Myths About Voice over IP: VoIP is turning telephony into just another Internet application - and a cheap one at that", IEEE Spectrum, Volume 42, Number 3, March 2005, pp. 52-57

[21] Vonage Holdings Corp., Company Fact Sheet, August 2009 http://ir.vonage.com/factsheet.cfm

[22] B. Carpenter (Editor), "Architectural Principles of the Internet", IAB, Network Working Group, RFC 1958, June 1996, Updated by RFC 3439 [23], http://datatracker.ietf.org/doc/rfc1958/

[23] R. Bush and D. Meyer, "Some Internet Architectural Guidelines and Philosophy", IETF, Network Working Group, RFC 3439, December 2002, Updates RFC 1958, https://datatracker.ietf.org/doc/rfc3439/

[24] VoIP Headset Review 2011 - TopTenREVIEWS, TechMediaNetwork.com, 2011, http://voip-headset-review.toptenreviews.com/

[25] Rebtel, "About Us - What we do", 2013.08.30, http://www.rebtel.com/en/About/

[26] Alex Goldman, How The FCC Killed VoIP, Internet Statistics: Blog Archive, 2011.02.06, http://net-statistics.net/wordpress/2011/02/how-the-fcc-killed-voip/

[27] Yongliang Wu, Aggregating product reviews for the Chinese market, Masters Thesis, School of Information and Communicatin Technology,

Royal Institute of Technology (KTH), Stockholm, Sweden, TRITA-ICT-EX-2009:208, November 2009, http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/091129-Yongliang_Wu-with-cover.pdf

[28] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, "SIP: Session Initiation Protocol", IETF, Network Working Group, RFC 2543, March 1999, Obsoleted by RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3265, http://datatracker.ietf.org/doc/rfc2543/

[29] Tom Keating, 'Auto-Provision VoIP Softphone with QR Code', 10-August-2012. [Online]. Available: http://blog.tmcnet.com/blog/tom-keating/voip/auto-provision-voip-softphone-with-qr-code.asp. [Accessed: 23-August-2012].

[30] Ward Mundy, 'PIONEERS - QRcode Configurator for Zoiper | PBX in a Flash Forum', 09-August-2012. [Online]. Available: http://www.pbxinaflash.com/community/index.php?threads/qrcode-configurator-for-zoiper.13920/. [Accessed: 23-August-2012].

[31] Goce Talaganov, 'Green VoIP?: A SIP Based Approach', Master's thesis,

KTH, Communication Systems, CoS, Stockholm, Sweden, 2012 [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-98795

Acknowledgements

I would like to thank the following people and organizations for their permission to use pictures, icons, …

- Ulf Strömgren <ustromgr@cisco.com> for sending the Cisco 7960 picture on 2002.10.30
- Henry Sinnreich and Alan Johnston, both of WorldCom (at the time), for the wonderful SIP tutorial which Henry sent on 2002.10.30

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 2: VoIP details

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

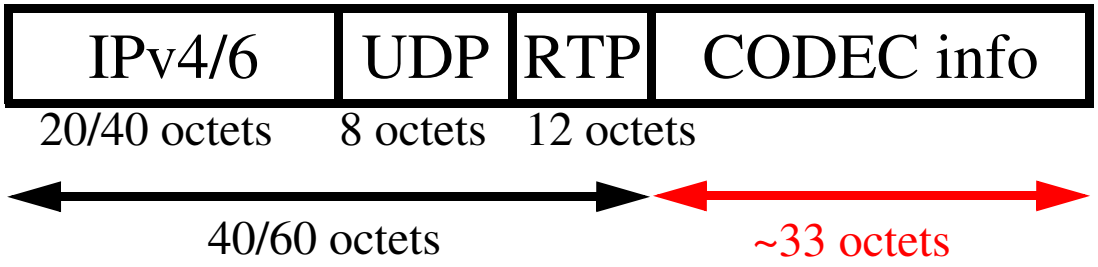
Last modified: 2013.09.01:14:31

Traditional Telecom vs. Datacom

Circuit-switched	Packet-switched
standardized **interfaces**	standardized **protocols** and **packet formats**
lots of internal state (i.e., each switch & other network nodes)	very limited internal state • caches and other state are soft-state and dynamically built based on traffic • no session state in the network
long setup times - since the route (with QoS) has to be set up from end-to-end before there is any further traffic	End-to-End Argument ⇒ integrity of communications is the reponsibility of the end node, **not** the network [22][23]
services: built **into** the network ⇒ hard to add new services • **operators** decide what services users can have • all elements of the net have to support the service before it can be introduced • Application programming interfaces (APIs) are often vendor specific or even proprietary	Services can be added by **anyone** • since they can be provided by **any** node *attached* to the network • users control their choice of services
centralized control	no central control ⇒ no one can easily turn it off
"carrier class" equipment and specifications • target: very high availability 99.999% (5 min./year of unavailability) • all equipment, links, etc. must operate with very high availability	a mix of "carrier class", business, & consumer equip. • backbone target: high availability >99.99% (50 min./year unavailability) • local networks: availability >99% (several days/year of unavailability) • In aggregate - there is extremely high availability because most of the network elements are **independent**
long tradition of slow changes • PBXs > ~10 years; public exchanges ~30yrs	short tradition of very fast change • Moore's Law doublings at 18 or 9 months!
clear operator role (well enshrined in *public law*)	unclear what the role of operators is (or even **who** is an operator)

VoIP details: Protocols and Packets

Carry the speech frame inside an RTP packet



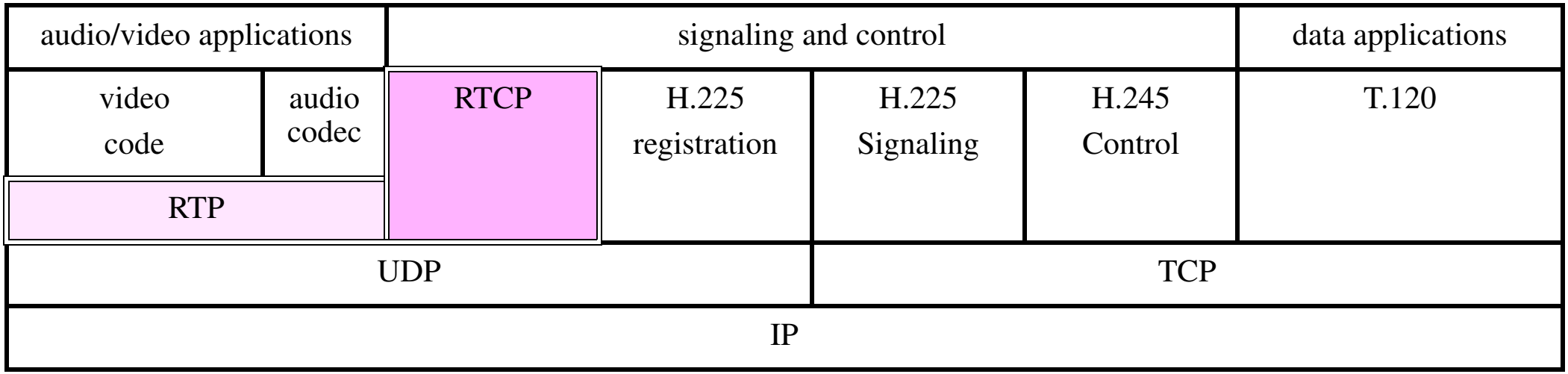
Typical packetization time of 10-20ms per audio frame.

See http://www.ietf.org/html.charters/avt-charter.html (Concluded in 2011)

This should be compared to the durations relevant to speech phenomena:

- "10 µs: smallest difference detectable by auditory system (localization),
- 3 ms: shortest phoneme (plosive burst),
- 10 ms: glottal pulse period,
- 100 ms: average phoneme duration,
- 4 s: exhale period during speech." (from Mark D. Skowronski's slide titled 'What is a "short" window of time?'[49])

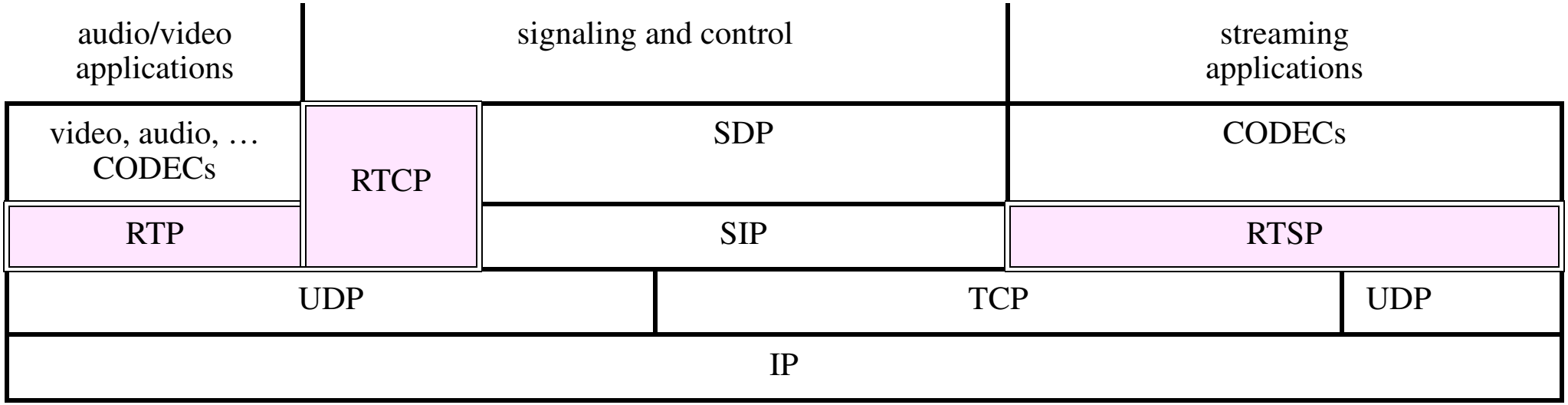
RTP and H.323 for IP Telephony



H.323	framework of a group protocols for IP telephony (from ITU)
H.225	Signaling used to establish a call
H.245	Control and feedback during the call
T.120	Exchange of data associated with a call
RTP	Real-time data transfer
RTCP	Real-time Control Protocol

We will not examine H.323 in much detail, but will examine RTP and RTCP.

RTP, RTCP, and RTSP



Real-Time Delivery

In a real-time application ⇒ data must be delivered with the same time *relationship* as it was created (but with some **delay**)

Two aspects of real-time delivery (for protocols):

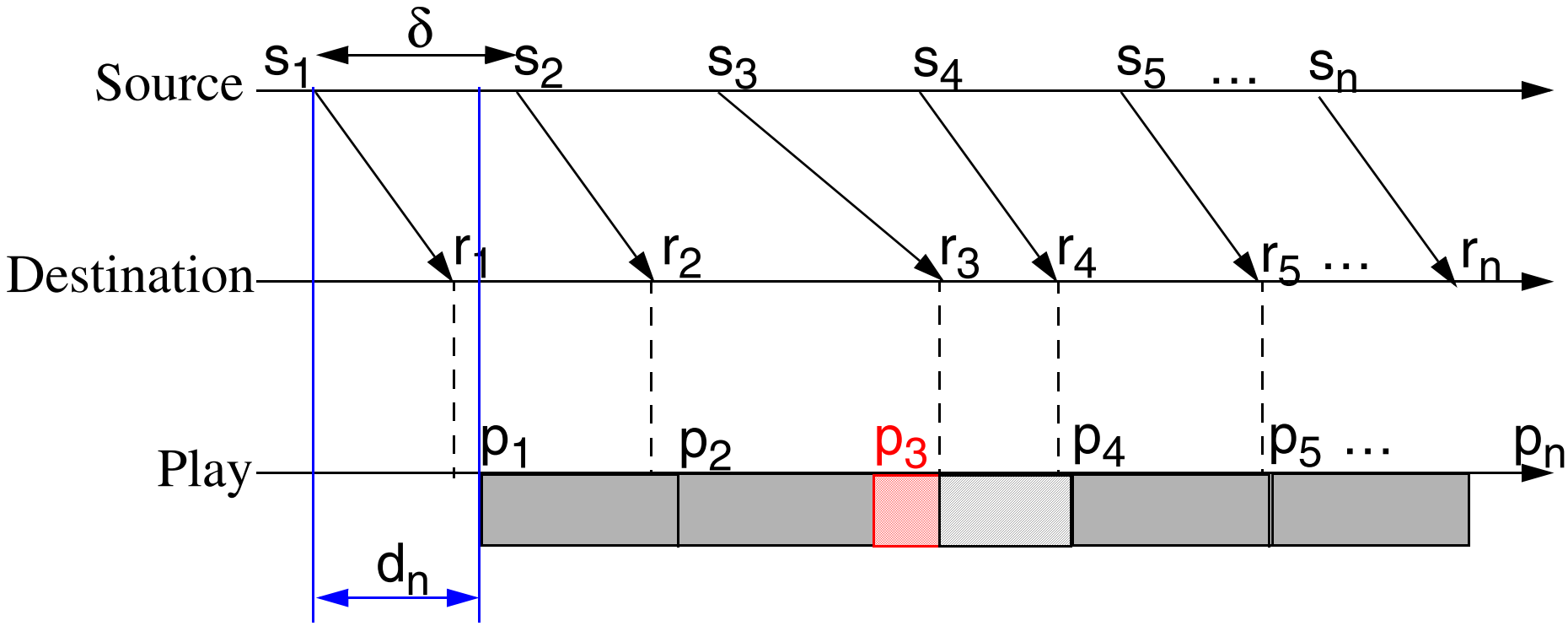
Order	data should be played in the same order as it was created
Time	the receiver must know when to play the packets, in order to reproduce the same signal as was input

We keep these separate by using a **sequence number** for *order* and a **time stamp** for *timing*.

Consider an application which transmits audio by sending datagrams every 20ms, but does silence detection and avoids sending packets of only silence. Thus the receiver may see that the time stamp advances by more than the usual 20ms, but the sequence number will be the *expected* next sequence number. Therefore we can tell the difference between *missing packets* and *silence*.

Packet delay

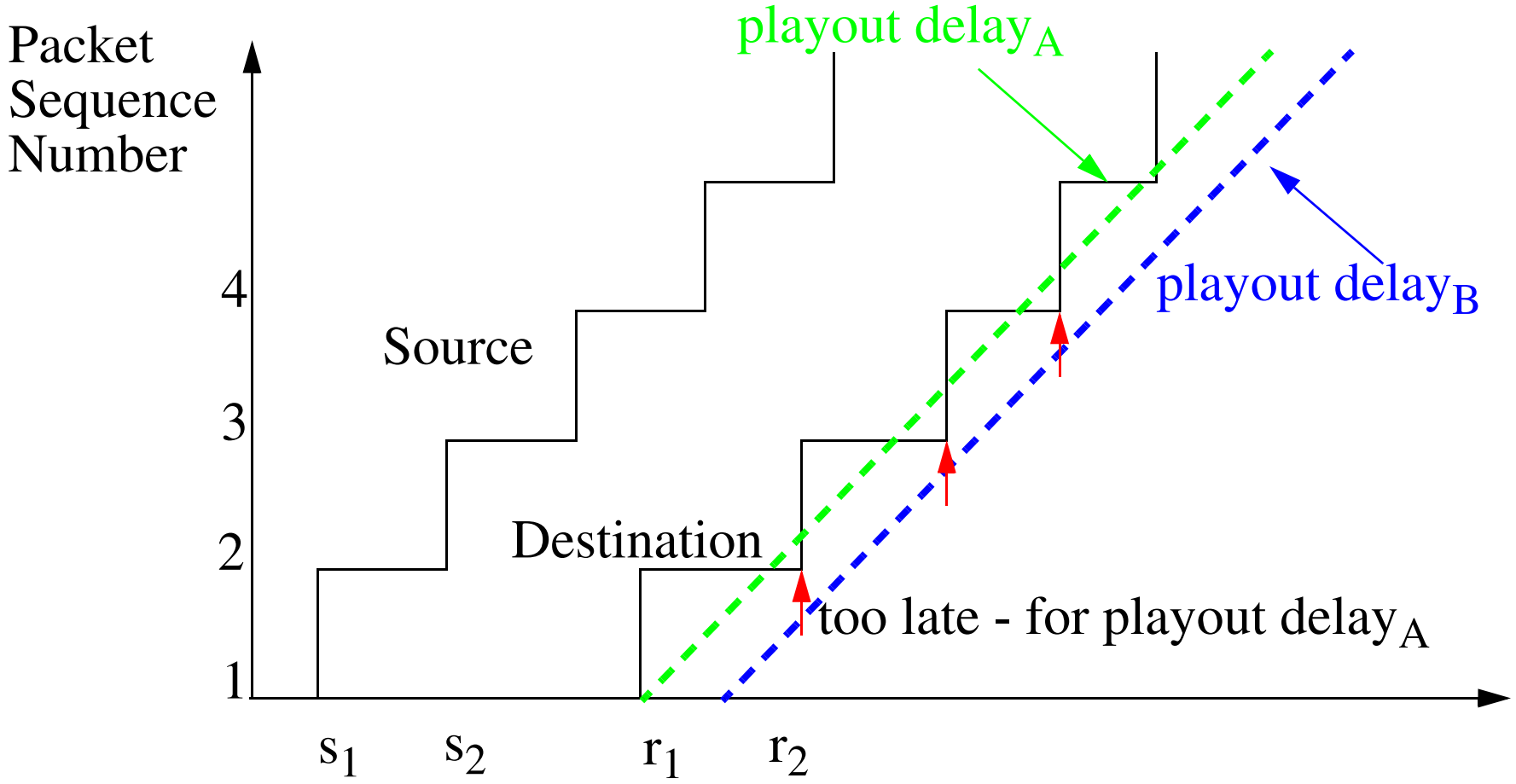
A stream of sampled audio packets are transmitted from the source (s_n), received at the destination (r_n), and played (p_n), thus each packet experiences a delay before playout (d_n)



If a packet arrives too late (r_3 arrives after we *should have* started to play at p_3), then there is a problem (for some or all of the third packet's audio).

Dealing with Delay jitter

Unless packets are lost, if we wait **long enough** they will come, but then the total delay may exceed the threshold required for interactive speech! (~180ms)



Delay and delay variance (jitter)

The end-to-end delay (from mouth to ear - for audio), includes:

encoding, packetization, (transmission, propagation, switching/routing, receiving,)$^{+}$ dejittering, decoding, playing

To hide the jitter we generally use playout buffer **only** in the final receiver.

Note: This playout buffer **adds additional delay** in order to *hide* the delay variations (this is called: **delayed playback**), playback delay > delay variance

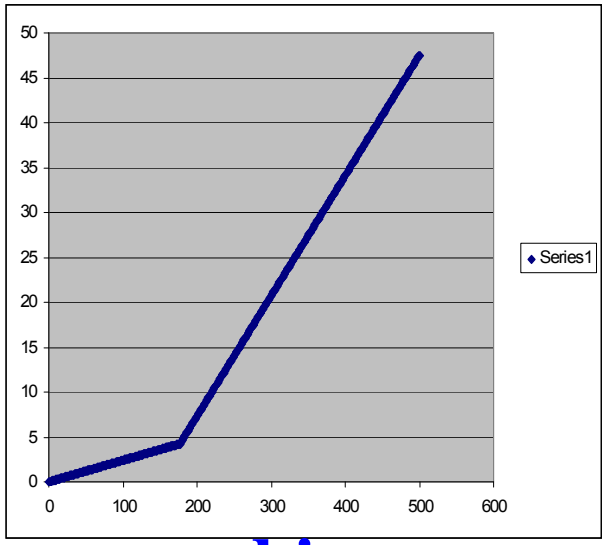
Perceived voice quality

There are very nice studies of the effects of delay on peceived voice quality, see R. G. Cole and J. H. Rosenbluth, "Voice over IP Performance Monitoring"[33].

$$I_d = 0.024d + 0.11(d - 177.3)H(d - 177.3)$$

d = one-way delay in ms

$H(x) = 0$ if $(x < 0)$ else $H(x) = 1$ when $x \geq 0$



The delay impairment (I_d) has roughly two *linear* behaviors, thus for delays less than 177ms conversation is very natural, while above this it become more strained (eventually breaking down $\Rightarrow$ simplex)

Playout delay

- Playout delay should track the network delay as it **varies** *during* a session [39][40]
- This delay is computed for each talk spurt based on *observed* average delay and deviation from this average delay -- this computation is similar to estimates of RTT and deviation in TCP
- Beginning of a talk spurt is identified by examining the timestamps and/or sequence numbers (if silence detection is being done at the source)
- The intervals between talk spurts[1] give you a chance to catch-up
  - without this, if the sender's clock were slightly faster than the receiver's clock the queue would build without limit! This is important as the 8kHz sampling in PC's CODECs is rarely exactly 8kHz (similar problems happen at other sampling rates[2]).

---

1. Average silence duration (~596 ms) combine with the average talk-spurt duration (227ms) ⇒ a long-term speech activity factor of 27.6% [369].

2. A common approach is to sample at a high frequency, such as 48 K samples/second, then down sample (or up sample) digitally in software, thus you can take advantage of the fact that you have multiple subsamples for in the incoming speech (or outgoing speech) to do clever things to time expand or compress the audio. Additionally by using a single high frequency for all of the audio that you are sending to (or receiving from) your audio interface you can mix audio from different sources (for example, plaing high quality music in the background while you listen to a G.711 call). For examples of this see [34]

When to play

The actual playout time is **not** a function of the arrival time, only of the end-to-end delay which can be calculated as shown below:

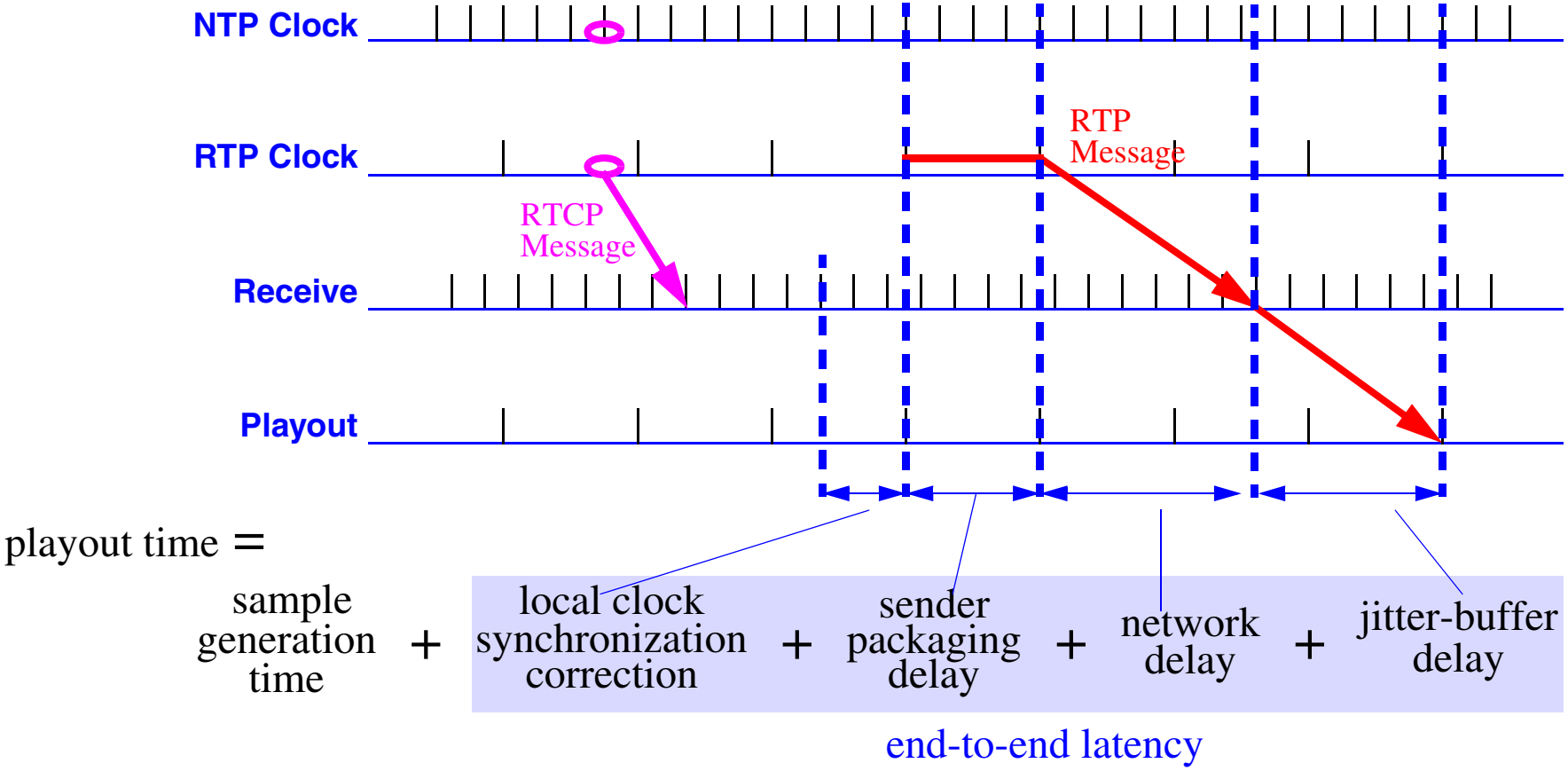


Figure adapted from slide 11 on page 6 of Kevin Jeffay, "Lecture 9: Networking Performance of Multimedia Delivery on the Internet Today", Lecture notes for COMP 249: Advanced Distributed Systems Multimedia, Dept. of CS, Univ. of North Carolina at Chapel Hill, November 9, 1999. http://www.cs.odu.edu/~cs778/jeffay/Lecture9.pdf [41]

Retransmission, Loss, and Recovery

For interactive real-time media we generally don't have time to request the source to retransmit a packet and to receive the new copy ⇒ **live without it** or *recover it using Forward Error Correction (FEC)*, i.e., send sufficient redundant data to enable recovery.

However, for non-interactive media we can use retransmission at the cost of a longer delay before starting playout

If you do have to generate output, but don't have any samples to play:

- audio
  - Comfort noise: play **white nosie** or play noise like in the last samples {as humans get uncomfortable with complete silence, they think the connection is broken!} [35]
  - if you are using highly encoded audio even a BER of 10^{-5} will produce very noticable errors
- video
  - show the same (complete) video frame again
  - you can drop every 100th frame (for a BER of 10^{-2}), but the user will not notice! [36]

There may also be compression applied to RTP see [55].

Patterns of Loss

With simple FEC you could lose *every other* packet and still not be missing content, but if pairs of packets are lost then you lose content.

To understand temporal patterns of speech, various models have been developed, see for example [52].

Loss concealment

There are various techniques for loss concealment (i.e., hiding losses), such as those used in the Robust Audio Tool (RAT):

- Vicky J. Hardman, Martina Angela Sasse, Anna Watson, and Mark Handley, “Reliable Audio for use over the Internet”, in Proceedings or INET95, Honolulu, Hawaii, Sept. 1995. [37]
- Mark Handley, Martina Angela Sasse, and I. Kouvelas, Successful Multiparty Audio Communication over the Internet”, Communications of the ACM, Vol. 41, No. 5, May 1998.[38]
- UCL’s Robust Audio Tool (RAT), was SUMOVER $\Rightarrow$ now AVATS Project UCL Media tools site http://mediatools.cs.ucl.ac.uk/nets/mmedia/

See also [387] and [388].

VoIP need not be “toll quality”

Public Switched Telephony System (PSTN) uses a **fixed** sampling rate, typically 8kHz and coding to 8 bits, this results in 64 kbps voice coding

However, VoIP is *not* limited to using this coding and could have **higher** or **lower** data rates depending on the CODEC(s) used, the available bandwidth between the end points, and the user’s preference(s).

One of the interesting possibilities which VoIP offers is quality which is:

- better that “toll grade” telephony or
- worse than “toll grade” telephony (but perhaps still acceptable)

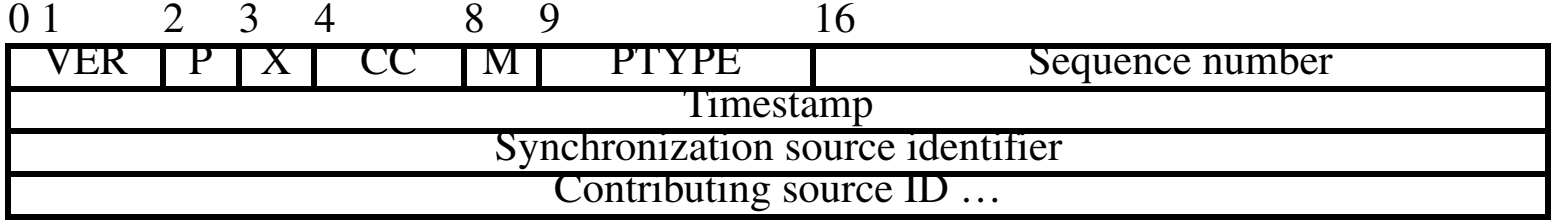
This is unlike the *fixed* quality of traditional phone systems.

To assess the quality of a call, see standards such as ITU-T’s Methods for Subjective Determination of Transmission Quality, Recommendation P.80 [51].

RTP: Real-Time Transport Protocol

- First defined by RFC 1889, now defined by RFC 3550 [43]
- Designed to carry a variety of real-time data: audio and video.
- Provides two key facilities:
  - Sequence number for order of delivery (initial value chosen randomly)
  - Timestamp (of first sample) - used for control of playback

Provides no mechanisms to ensure timely delivery.



- VER - version number (currently 2)
- P - whether zero padding follows the payload
- X - whether extension or not
- M - marker for beginning of each frame (or talk spurt if doing silence detection)
- PTYPE - Type of payload - first defined as Profiles in RFC 1890 now defined in RFC 3551

We will address the other fields later.

Payload types

Payload types (PT) for standard audio and video encodings (Adapted from Tables 4 and 5 of RFC3551 [44])

PT	encoding name	audio (A)	clock rate (Hz)	channels (audio)
0	PCMU	A	8,000	1
1	reserved	A	8,000	1
2	reserved	A	8,000	1
3	GSM	A	8,000	1
4	G723	A	8,000	1
5	DVI4	A	8,000	1
6	DVI4	A	16,000	1
7	LPC	A	8,000	1
8	PCMA	A	8,000	1
9	G722	A	8,000	1
10	L16	A	44,100	2
11	L16	A	44,100	1
12	QCELP	A	8,000	1
13	CN	A	8,000	1
14	MPA	A	90,000	see RFC
15	G728	A	8,000	1
16	DVI4	A	11,025	1
17	DVI4	A	22,050	1
18	G729	A	8,000	
19	reserved	A		
20..23	unassigned	A		

PT	encoding name	video (V)	clock rate (Hz)
24	unassigned	V	
25	CelB	V	90,000
26	JPEG	V	90,000
27	unassigned	V	
28	nv	V	90,000
29	unassigned	V	
30	unassigned	V	
31	H.261	V	90,000
32	MPV	V	90,000
33	MP2T	AV	90,000
34..71	unassigned		
72..76	reserved	N/A	N/A (N/A = Not Applicable)
77..95	unassigned		
96..127	dynamic		

Dynamic assignment of mapping between a payload type and an encoding is defined by SDP or H.323/H.245 mechanisms; these start with 96 - but can use lower numbers, if more than 32 encodings are needed - see RFC3551 [44].

RFC3551 says no new static assignments are to be made.

Audio Encodings

Properties of Audio Encodings (adapted from Table 1 of RFC1990 and updated by RFC3551 [44])

encoding	encoding	sample/frame	bits/sample	ms/frame
DVI4	Interactive Multimedia Assoc.'s DVI ADPCM Wave Type	sample	4	
G722	ITU's G.722: 7 kHz audio-coding within 64 kbit/s	sample	8	
G723	ITU's G.723: Dual-rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s	frame	N/A	30.0
G726	ITU's G.726	frame	N/A	
G728	ITU's G.728: 16 kbit/s using low-delay CELP	frame	N/A	2.5
G729	ITU's G.729: 8 kbit/s using conjugate structure-algebraic code excited linear prediction (CS-ACELP)	frame	N/A	10.0
GSM	GSM 06.10: RPE/LTP (residual pulse excitation/long term prediction) coding at a rate of 13 kb/s	frame	N/A	20.0
L8	8 bit linear	sample	8	
L16	16 bit linear	sample	16	
LPC	Linear Predictive Coding	frame	N/A	20.0
MPA	MPEG-I or MPEG-II audio encapsulated as elementary streams, from ISO standards ISO/IEC 11172-3 & 13818-3	frame	N/A	
PCMA	G.711 A-law	sample	8	
PCMU	G.711 mu–law	sample	8	
QCLEP		frame	variable	20.0
VDVI	variable-rate version of DVI4	sample	variable	

See also internet Low Bitrate Codec (iLBC) http://www.ilbcfreeware.org/ [53] (now WebRTC project (webrtc.org). See also wideband CODECs, such as Extended Adaptive Multi-Rate Wideband (AMR-WB+) Audio Codec [56], [57], [58]

Other important types of data

Dual Tone Multifrequency (DTMF) digits and telephony tones & signals

To convey signaling information in the audio channel channel dual tone multifrequency signaling is often used.

FAX

Another use of telephony connections is for FAX.

See RFC 4733[46] and RFC 4734[47].

Why is FAX still important?

Timestamps

The *initial* timestamp is to be chosen *randomly* (just as the initial sequence number is selected randomly):

- to avoid replays
- to increase security (this assumes that the intruder does not have access to all the packets flowing to the destination)

The timestamp *granularity* (i.e., the units) are determined by the payload type {often based on the sampling rate}

Stream translation and mixing

mixing	combining several RTP streams to produce a single stream
translation	converting from one encoding to another (also know as **transcoding**)

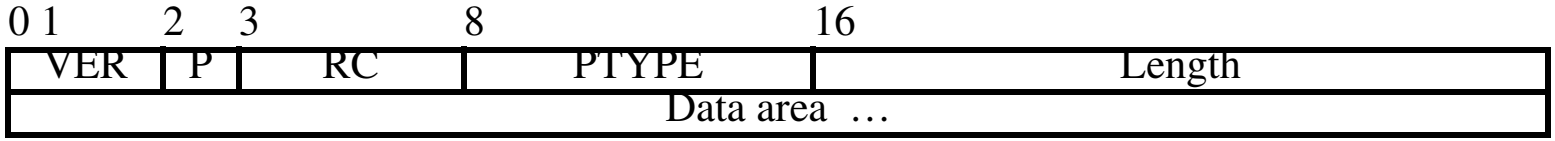
Each source has a unique 32 bit **Synchronization Source Identifier**.

When several sources are mixed the new stream gets its own unique **Synchronization Source Identifier** and the IDs of the contributing sources are included as **Contributing Source IDs**, the number of which is indicated in the 4-bit **CC** field of the header.

RTP Control Protocol (RTCP)

[upward] enables endpoints to provide meta-information to the source - this enables the sources to be adaptive to the endpoints. For example, by using an adaptive coding algorithm the source can accommodate the actually data rate of packets arriving at the endpoint.

[downward] enables sources to send the endpoints information about a session



- VER - version number (currently 2)
- P - whether **padding** follows the payload (last octet indicates how much was added)
- RC - **R**eport **C**ount - specifies the number of reports in this packet[1]
- PTYPE - Type of payload

Name	Type		Meaning
Sender Report	SR	200	Time information for each synchronization source and a count of data octets sent
Receiver Report	RR	201	Report of packet loss and jitter, information for timing and round-trip estimation
Source Description	SDES	202	Description of who owns the source
Goodbye	BYE	203	Receiver leaving the session
Application	APP	204	Application-specific report

1. RTCP uses compound packets with multiple RTCP messages in a single packet.

Compound Reports

If and only if (IFF) the compound packet is to be encrypted: it is prefixed by a random 32-bit quantity selected for each compound packet transmitted.

The first RTCP packet in the compound packet must always be a report packet (either Receiver Report or Sender Report). Followed by upto 30 more report packets (as **R**eport **C**ount is only 5 bits).

This is followed by an Source Description (SDES) packet containing a CNAME item (other information such as NAME, EMAIL, PHONE, LOC {geographic location},TOOL, NOTE, and PRIV {private extension to SDES} are optional).

BYE should be the last packet sent with a given SSRC/CSRC.

Proposed RTCP Reporting Extensions

See RFC 3611 RTP Control Protocol Extended Reports (RTCP XR)[54]

VoIP Metrics Report Block - provides metrics for monitoring VoIP calls.

0	8	16	24
BT=64	reserved	length=7	
loss rate	discard rate	burst duration	
burst density	gap duration		gap density
round trip delay		end system delay	
signal power	doubletalk	noise level	Gmin
R factor	ext. R factor	MOS-LQ	MOS-CQ
RX Config	JB Nominal	JB Maximum	JB Abs Max

block type (BT)	the constant 64 = 0x40
reserved	8 bits - MUST be set to zero unless otherwise defined.
length	length of this report block in 32-bit words minus one, including the header; constant 6.
loss rate	fraction of RTP data packets from the source lost since the beginning of reception, as a fixed point number with the binary point at the left edge of the field[a]
discard rate	fraction of RTP data packets from the source that have been discarded since the beginning of reception, due to late or early arrival, under-run or overflow at the receiving jitter buffer, in binary fixed point
burst duration	mean duration of the burst[b] intervals, in milliseconds
burst density	fraction of RTP data packets within burst intervals since the beginning of reception that were either lost or discarded, in binary fixed point
gap duration	mean duration, expressed in milliseconds, of the gap intervals that have occurred
gap density	fraction of RTP data packets within inter-burst gaps since the beginning of reception that were either lost or discarded, in binary fixed point
round trip delay	most recently calculated round trip time between RTP interfaces, in milliseconds
end system delay	most recently estimated end system delay, in milliseconds
signal level	voice signal relative level is defined as the ratio of the signal level to overflow signal level, expressed in decibels as a signed integer in two's complement form
doubletalk level	defined as the proportion of voice frame intervals during which speech energy was present in both sending and receiving directions
noise level	defined as the ratio of the silent period back ground noise level to overflow signal power, expressed in decibels as a signed integer in two's complement form

R factor	a voice quality metric describing the segment of the call that is carried over this RTP session, expressed as an integer in the range 0 to 100, with a value of 94 corresponding to "toll quality" and values of 50 or less regarded as unusable; consistent with ITU-T G.107 and ETSI TS 101 329-5
ext. R factor	a voice quality metric describing the segment of the call that is carried over an external network segment, for example a cellular network
MOS-LQ	estimated mean opinion score for listening quality (MOS-LQ) is a voice quality metric on a scale from 1 to 5, in which 5 represents excellent and 1 represents unacceptable
MOS-CQ	estimated mean opinion score for conversational quality (MOS-CQ) defined as including the effects of delay and other effects that would affect conversational quality
Gmin	gap threshold, the value used for this report block to determine if a gap exists
RX Config	PLC - packet loss concealment: Standard (11)/enhanced(10)/disabled (01)/ unspecified(00); JBA - Jitter Buffer Adaptive: Adaptive (11) / non-adaptive (10) / reserved (01)/ unknown (00). Jitter Buffer is adaptive then its size is being dynamically adjusted to deal with varying levels of jitter;JB Rate - Jitter Buffer Rate (0-15)
Jitter Buffer	nominal size in frames (8 bit)
Jitter Buffer Maximum	size in frames (8 bit)
Jitter Buffer Absolute Maximum	size in frames

a. Here after simply referred to as a binary fixed point number.

b. A burst is defined as a longest sequence of packets bounded by lost or discarded packets with the constraint that within a burst the number of successive packets that were received, and not discarded due to delay variation, is less than some value Gmin.

RTP translators/mixers

Translator	changes transport (e.g., IPv4 to IPv6) or changes media coding (i.e., transcoding)
Mixer	combines multiple streams to form a **combined** stream

Connect two or more transport-level "clouds", each cloud is defined by a common network and transport protocol (e.g., IP/UDP), multicast address or pair of unicast addresses, and transport level destination port.

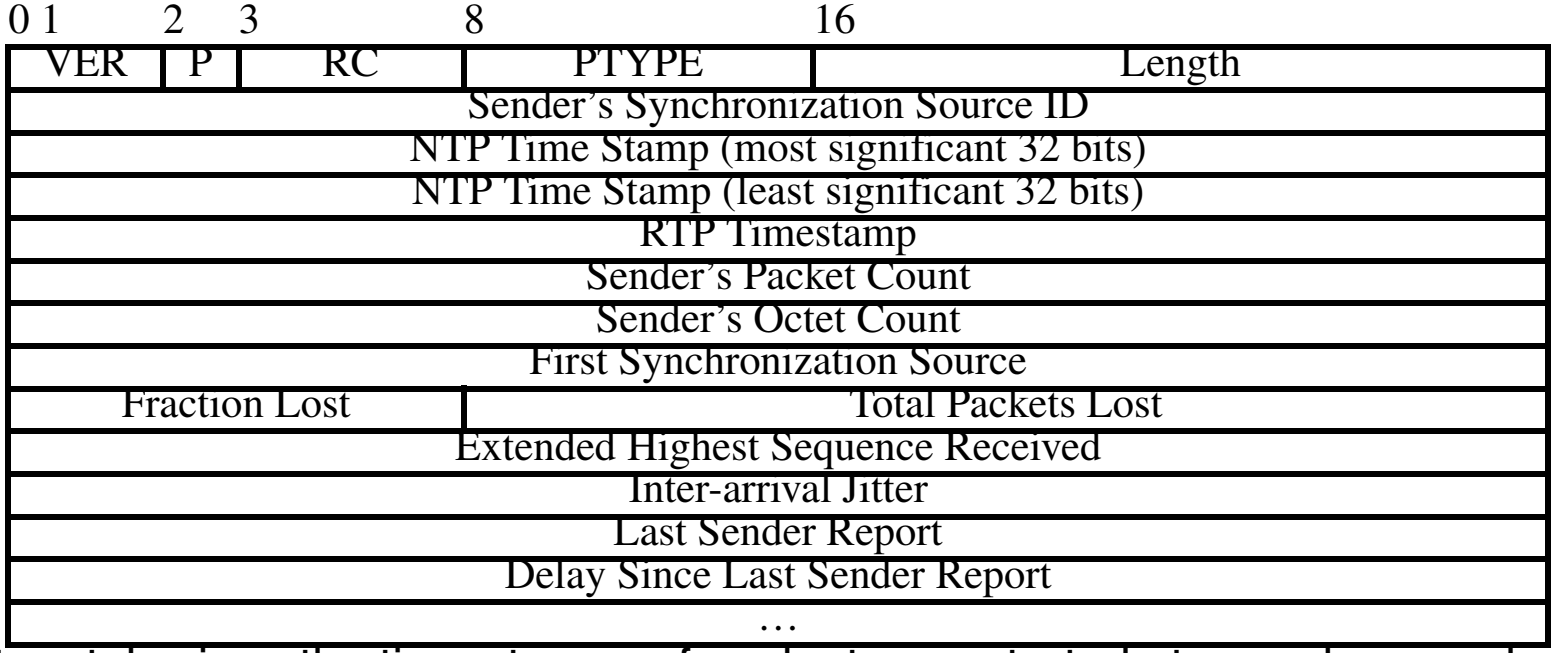
To avoid creating a loop the following rules must be observed:

- "Each of the clouds connected by translators and mixers participating in one RTP session either must be distinct from all the others in at least one of these parameters (protocol, address, port), or must be isolated at the network level from the others.
- A derivative of the first rule is that there must not be multiple translators or mixers connected in parallel unless by some arrangement they partition the set of sources to be forwarded."

From §7.1 General Description of RFC 1889

Synchronizing Multiple Streams

One of the interesting things which RTP supports is synchronization of multiple streams (e.g., audio with a video stream)



- Unfortunately since the time stamps of each stream started at a random number we need some other method to synchronize them!
- Thus use Network Time Protocol (NTP) based time stamps $\Rightarrow$ an absolute timestamp
- Since we now include the stream timestamps we can correlate these to absolute time (and hence from one stream to another)

RTP Transport and Many-to-many Transmission

RTP uses a connectionless transport (usually UDP):

- Retransmission is undesirable (generally it would be too late)
- Since RTP handles flow control and sequencing we don't need this from the transport protocol
- RTP is packet oriented
- Enables us to easily use multicast (when there are many endpoints that want the same source stream)
  - multicast identifed a **group**
  - these multicast groups can be *dynamic*

Sessions, Streams, Protocol Port, and Demultiplexing

Session	All traffic that is sent to a given IP address, port
Stream	a sequence of RTP packets that are from a single synchronization source

Demultiplexing:

session demultiplexing	occurs at the transport layer based on the port number
stream demultiplexing	occurs once the packet is passed to the RTP software, based on the synchronication source identifier - then the sequence number and timestamp are used to order the packet at a suitable time for playback

Further details of RTP and RTCP

See: Chapters 28 and 29 of Douglas E. Comer and David L. Stevens, "Internetworking with TCP/IP, Volume III: Client Server Programming and Applications, Linux/POSIX Version", pp. 467-513 [48].

Note that an important aspect of RTCP is the rate of sending reports.

- "It is RECOMMENDED that the fraction of the session bandwidth added for RTCP be fixed at 5%." [43]
- "It is also RECOMMENDED that 1/4 of the RTCP bandwidth be dedicated to participants that are sending data so that in sessions with a large number of receivers but a small number of senders, newly joining participants will more quickly receive the CNAME for the sending sites." [43]
- Senders can be divided into two groups "… the RECOMMENDED default values for these two parameters would be 1.25% [active senders] and 3.75% [in-active senders] …".[44]
  - $\Rightarrow$ in-active sender $\cong$ receivers should generate at a rate of ~3.75% of the session traffic
  - of course: receivers on receive only links can not generate any reports

Further details of speaking patterns

Professor Deborah Tannen, *You just don't understand: women and men in conversation*. New York: Quill, 2001. There is also a 2007 paperback version: William Morrow Paperbacks, 2007, 352 pages, ISBN-10: 0060959622, ISBN-13: 978-0060959623

Communication involves more than just the words that are uttered.

Real Time Streaming Protocol (RTSP)

Defined in RFC 2326 http://www.ietf.org/rfc/rfc2326.txt

- remote media playback control (think in terms of controlling a remote VCR/DVD/CD player)
- similar to HTTP/1.1, but
  - introduces new methods
  - RTSP servers maintain state
  - data carried out of band (i.e., in RTP packets)
- can use UDP or TCP
- Uses Web security methods (see [60])

Some of the server implementations are: Darwin Streaming server, Helix DNA server, VideoLAN, Microsoft's Windows Media Server, Gstreamer, … .

H. Schulzrinne, A. Rao, R. Lanphier, M. Westerlund, M. Stiemerling (Ed.), Real Time Streaming Protocol 2.0 (RTSP), MMUSIC Working Group, Internet-Draft, April 4, 2013, Expires: October 6, 2013, draft-ietf-mmusic-rfc2326bis-34

http://datatracker.ietf.org/doc/draft-ietf-mmusic-rfc2326bis/

RTSP session description

```
<title>Twister</title>
   <session>
      <group language=en lipsync>
         <switch>
            <track type=audio e="PCMU/8000/1"
                   src="rtsp://audio.example.com/twister/audio.en/lofi">
            <track type=audio e="DVI4/16000/2" pt="90 DVI4/8000/1"
                   src="rtsp://audio.example.com/twister/audio.en/hifi">
         </switch>
         <track type="video/jpeg" src="rtspu://video.example.com/twister/video">
       </group>
   </session>
```

From figure 6: “Sample RTSP session description” of Henning Schulzrinne, “A comprehensive multimedia control architecture for the Internet”

http://www.cs.columbia.edu/~hgs/papers/Schu9705_Comprehensive.pdf

References and Further Reading

[32] Multiparty Multimedia Session Control (mmusic) Working Group, Webpage, http://www.ietf.org/html.charters/mmusic-charter.html

Also important are the measures of delay, delay jitter, throughput, packet loss, etc. IP Performance Metrics (ippm) is attempting to specify how to measure and exchange information about measurements of these quantities.

[33] R. G. Cole and J. H. Rosenbluth, "Voice over IP Performance Monitoring", Computer Communications Review, Vol. 21, Number 2, April, 2001, pp. 9-24. http://www.acm.org/sigcomm/ccr/archive/2001/apr01/ccr-200104-cole.html

[34] Ignacio Sánchez Pardo, Spatial Audio for the Mobile User, M.Sc. Thesis, Royal Institute of Technology (KTH), School of Information and Communication Technology, Telecommunication Systems Lab, Stockholm, Sweden, IMIT/TSLab-2005-01, March 2005

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/050307-Ignacio_Sanchez_Pardo-with-cover.pdf

[35] Thomas Mattisson, “Integration of Computer Telephony into Ericsson Corporate Network”, M.Sc. Thesis, Royal Institute of Technology (KTH), Teleinformatics, Stockholm, Sweden, February 1995.

[36] Yang Xiaoning, “A New Controlled Video Frame Loss Scheme for Video Transmission Over High Speed Networks”, M.S. Thesis, National University of Singapore, Dept. of Electrical Engineering, 1994.

[37] Vicky J. Hardman, Martina Angela Sasse, Anna Watson, and Mark Handley, “Reliable Audio for use over the Internet”, in Proceedings of INET95, Honolulu, Hawaii, September 1995 http://info.isoc.org/HMP/PAPER/070/html/paper.html

[38] Mark Handley, Martina Angela Sasse, and I. Kouvelas, Successful Multiparty Audio Communication over the Internet”, Communications of the ACM, Vol. 41, No. 5, May 1998.

[39] Miroslaw Narbutt and Liam Murphy, “Adaptive Playout Buffering for Audio/Video Transmission over the Internet”, University College Dublin, Department of Computer Science, Dublin, Ireland, 2001 http://www.eeng.dcu.ie/~narbutt/UKTS_2001.pdf

[40] Sue B. Moon, Jim Kurose, and Don Towsley, “Packet audio playout delay adjustment: performance bounds and algorithms”, Multimedia Systems (1998) 6:17-28. http://www.cs.unc.edu/Courses/comp249-s02/readings/packet-audio-playout.pdf

[41] Kevin Jeffay, “Lecture 9: Networking Performance of Multimedia Delivery on the Internet Today”, Lecture notes for COMP 249: Advanced Distributed Systems Multimedia, University of North Carolina at Chapel Hill, Department of Computer Science, November 9, 1999. http://www.cs.odu.edu/~cs778/jeffay/Lecture9.pdf

RTP and RTCP

[42] IETF AVT Working Group Charter http://www.ietf.org/html.charters/avt-charter.html

[43] H. Schulzrinne, S. Casner, and R. Frederick, “RTP: A Transport Protocol for Real-Time Applications”, IETF, Network Working Group, RFC 3550, July 2003, Updated by RFC 5506 and RFC 5761, http://datatracker.ietf.org/doc/rfc3550/

[44] H. Schulzrinne and S. Casner, “RTP Profile for Audio and Video Conferences with Minimal Control”, IETF, Network Working Group, RFC 3551, July 2003, Updated by RFC 5761, http://datatracker.ietf.org/doc/rfc3551/

[45] H. Schulzrinne and S. Petrack, "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals", IETF, Network Working Group, RFC 2833, May 2000, Obsoleted by RFC 4733 and RFC 4734,

http://datatracker.ietf.org/doc/rfc2833/

[46] H. Schulzrinne and T. Taylor, "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals", IETF, Network Working Group, RFC 4733, December 2006, Updated by RFC 4734 and RFC 5244, Obsoletes RFC 2833, https://datatracker.ietf.org/doc/rfc4733/

[47] H. Schulzrinne and T. Taylor, "Definition of Events for Modem, Fax, and Text Telephony Signals", IETF, Network Working Group, December 2006, RFC 4734, Obsoletes RFC 2833 and Updates RFC 4733,

https://datatracker.ietf.org/doc/rfc4734/

[48] Douglas E. Comer and David L. Stevens, *Internetworking with TCP/IP, Volume III: Client Server Programming and Applications, Linux/POSIX Version*, Prentice Hall, Upper Saddle River, NJ, 2001, 601 pages, ISBN-13: 978-0130320711.

[49] Mark D. Skowronski, “Windows Lecture”, from the course EEL 6586: Automatic Speech Processing, University of Florida, Computational Neuro-Engineering Lab, 10 February 2003.

http://www.cnel.ufl.edu/~markskow/papers/windows.ppt

[50] CCITT, Methods for Subjective Determination of Transmission Quality, CCITT, Recommendation P.80, 1998, A later version of the standard is ITU-T Recommendation P.80, 1993, Section 7: Subjective Opinion Tests, paragraph 3.1.2.3 Silence (gap) characteristics,

http://starlet.deltatel.ru/ccitt/1988/ascii/5_1_06.txt

[51] ITU-T, Methods for Subjective Determination of Transmission Quality, ITU-T, Recommendation P.80, March 1993.

[52] M. Y. Kim and W. B. Kleijn, “Rate-Distortion comparisons between FEC and MDC based on Gilbert channel model”, in Proceedings of the IEEE International Conference on Networks (ICON), 2003, Sydney, Australia, pp. 495 - 500.

[53] Alan Duric and Soren Vang Andersen, “Real-time Transport Protocol (RTP) Payload Format for internet Low Bit Rate Codec (iLBC) Speech”, IETF, Network Working Group, RFC 3952, December 2004,

http://datatracker.ietf.org/doc/rfc3952/

[54] T. Friedman, R. Caceres, A. Clark (Editors), “RTP Control Protocol Extended Reports (RTCP XR)”, IETF, Network Working Group, RFC 3611, November 2003, http://datatracker.ietf.org/doc/rfc3611/

[55] T. Koren, S. Casner, J. Geevarghese, B. Thompson, and P. Ruddy, “Enhanced Compressed RTP (CRTP) for Links with High Delay, Packet Loss and Reordering”, IETF, Network Working Group, RFC 3545 , July 2003, http://datatracker.ietf.org/doc/rfc3545/

[56] J. Sjoberg, M. Westerlund, A. Lakaniemi, and S. Wenger, “RTP Payload Format for the Extended Adaptive Multi-Rate Wideband (AMR-WB+) Audio Codec”, IETF, Network Working Group, RFC 4352, January 2006,

http://datatracker.ietf.org/doc/rfc4352/

[57] S. Ahmadi, “Real-Time Transport Protocol (RTP) Payload Format for the Variable-Rate Multimode Wideband (VMR-WB) Audio Codec”, IETF, Network Working Group, RFC 4348, January 2006, Updated by RFC 4424, http://datatracker.ietf.org/doc/rfc4348/

[58] S. Ahmadi, “Real-Time Transport Protocol (RTP) Payload Format for the Variable-Rate Multimode Wideband (VMR-WB) Extension Audio Codec”, IETF, Network Working Group, February 2006, RFC 4424, Updates RFC 4348, https://datatracker.ietf.org/doc/rfc4424/

RTSP

[59] H. Schulzrinne, A. Rao, and R. Lanphier, “Real Time Streaming Protocol (RTSP)”, IETF, Network Working Group, RFC 2326, April 1998, http://datatracker.ietf.org/doc/rfc2326/

[60] Daniel (Högberg) Broms, “Access restrictions in surrogates using Portable Channel Representation”, M.S. thesis, Royal Institute of Technology (KTH), Dept. of Microelectronics and Information Technology, Stockholm, Sweden, October 2002.

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols Fall 2013, Period 1

Module 3: SIP

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:31

Session Initiation Protocol (SIP)

SIP was initially developed by the IETF Multiparty Multimedia Session Control (MMUSIC) working group, from Sept. 1999 in the IETF SIP working group[1].

SIP is a text-based protocol, similar to HTTP and SMTP, for initiating interactive communication sessions between users. Sessions include: voice, video, chat, interactive games, and virtual reality.

SIP working group's charter: "… to maintain the basic model and architecture defined by SIP. In particular:

1. Services and features are provided **end-to-end** whenever possible[2].
2. Extensions and new features must be generally applicable, and not applicable only to a specific set of session types.
3. Simplicity is key.
4. Reuse of existing IP protocols and architectures, and integration with other IP applications, is crucial.

---

1. Now the **Session Initiation Protocol Core (sipcore)** working group - see https://datatracker.ietf.org/wg/sipcore/

2. The use of end-to-end control is the exact opposite of the centralized control in traditional telecommunication networks.

SIP WG's deliverables

- SIP specification
- **callcontrol**: call control specifications, which enables multiparty services, e.g., transfer and bridged sessions
- **callerpref**: caller preferences extensions, enables intelligent call routing services
- **mib**: a MIB for SIP nodes
- **precon**: extensions needed to assure satisfaction of external preconditions, e.g., QoS establishment
- **state**: extensions needed to manage state within signaling, aka SIP "cookies"
- **priv**: extensions for security and privacy
- **security**: security and privacy mechanisms and requirements
- **provrel**: extensions needed for reliability of provisional messages
- **servfeat**: extensions needed for negotiation of server features
- **sesstimer**: Session Timer extension

- **events**: Events extensions (Subscribe/Notify)
- **natfriend**: Extensions for making SIP a NAT-friendly protocol

Related IETF Working groups

- avt (Audio/Video Transport)
- bliss (Basic Level of Interoperability for SIP Services)
- codec (Internet Wideband Audio CODEC)
- dispatch (Dispatch)
- drinks (Data for Reachability of INter/tra-Network SIP)
- ecrit (Emergency Context Rsolution with Internet Technologies)
- enum (Telephone Number Mapping)
- geopriv (Geographic Location/Privacy)
- p2psip (Peer-to-peer SIP)
- salud (SIP ALerting for User Devices)
- simple (SIP for Instant Messaging and Presence Legeraging Extensions)
- sipclf (SIP Common Log Format)
- sipcore (SIP Core)
- siprec (SIP recording)

- soc (SIP Overload Control)
- speechsc (Speech Services Control)
- speermint (Session PEERing for Multimedia INTerconnect)
- splices (looSely-couPLed sIp deviCES) [new - for disaggregated media]
- xcon (Centralized conferencing)
- xmpp (Extensible Messaging and Presence Protocol)

Historic

- PSTN and Internet Internetworking (PINT) WG
  - origin of SUBSCRIBE/NOTIFY
- IP telephony (IPTEL) WG
  - Call Processing Language (CPL), Telephony Routing over IP (TRIP)
- SPIRITS (Service in PSTN requesting Internet Services) - SIP as ‘transport’ mechanism for services that originate in the PSTN

Related working groups

- Distributed Call Signaling (DCS) Group of the PacketCable Consortium (http://www.packetcable.com/) for distributed telephony services
- 3rd Generation Partnership Project (3GPP), 3rd Generation Partnership Project 2 (3GPP2), -- 3rd generation wireless network efforts

Session Initiation Protocol (SIP)

- Defined in RFC 3261 [66], updated by RFC 3853[82] & RFC 4320[81]
- provides application layer signaling
  - Used to **establish**, **modify**, and **terminate** multimedia *sessions*
- can utilize UDP, TCP, TLS, SCTP, … for underlying transport
- HTTP-like
  - uses **textual** rather than binary (ala H.323) messages (⇒ humans can read them)
  - uses Uniform Resource Indicators (URIs) to designate calling and called parties
- target applications : voice, video, gaming, instant messaging, presence, call control[1], …

SIP is an alternative to H.323. SIP **only** covers the **signaling** parts of H.323.
SIP does not use RTP itself, but sessions can use RTP.

- SIP provides ability to **discover** remote users and **establish** interactive **sessions**
- Does **not** ensure QoS or deliver large quantities of data

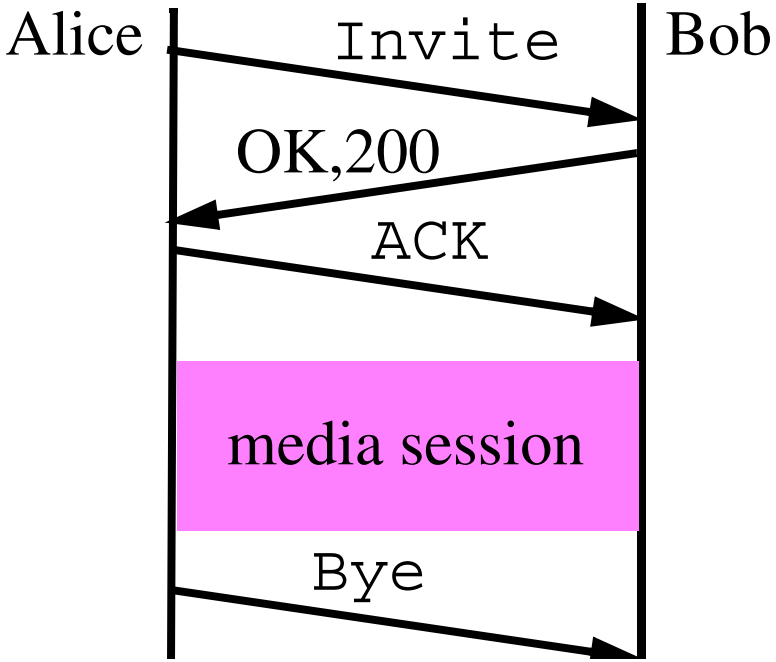
SIP uses SDP (Session Description Protocol) to provide information about a call, such as, the media encoding, protocol port number, multicast addresses, etc.

1. Largely taken from Advanced Intelligent Network (AIN).

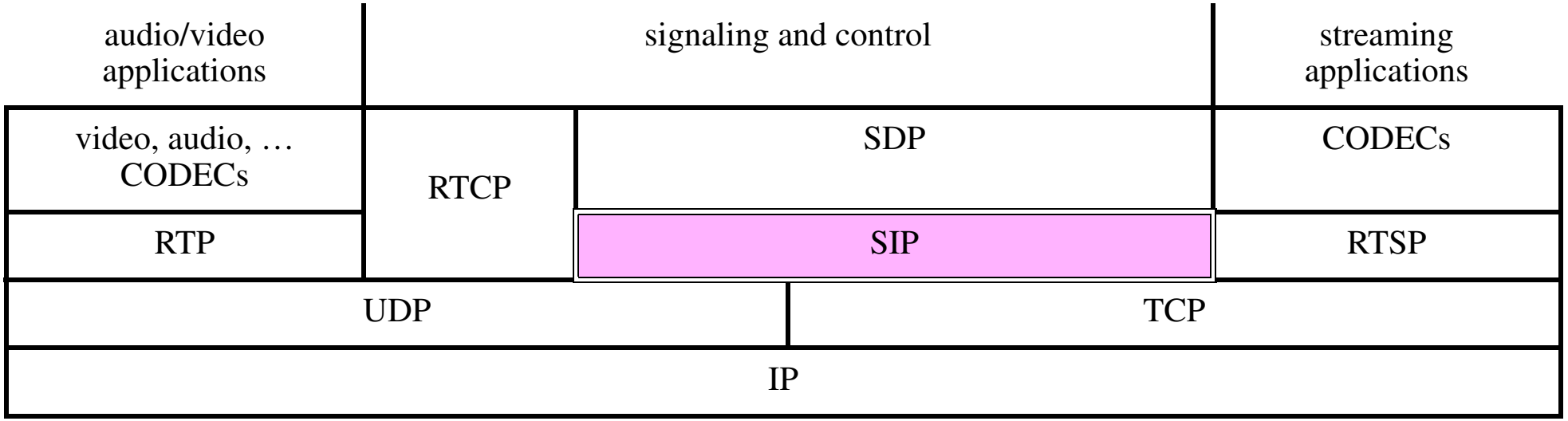
Is SIP simple?

- first 25 related RFCs (for SIP and SDP) - total of 823 pages (SIP alone: 269 pages)
- RFC3261 was longest RFC ever (based on byte count; 663,043 bytes)
- There are claims that one can still build a simple user agent in a (long) evening, but there is **substantial** work required with respect to security (due to TLS, S/MIME, AAA, Denial of Service issues, …)

SIP timeline - showing a simple version of Alice invites Bob to a SIP session:



SIP, RTP, and RTSP



SIP actors

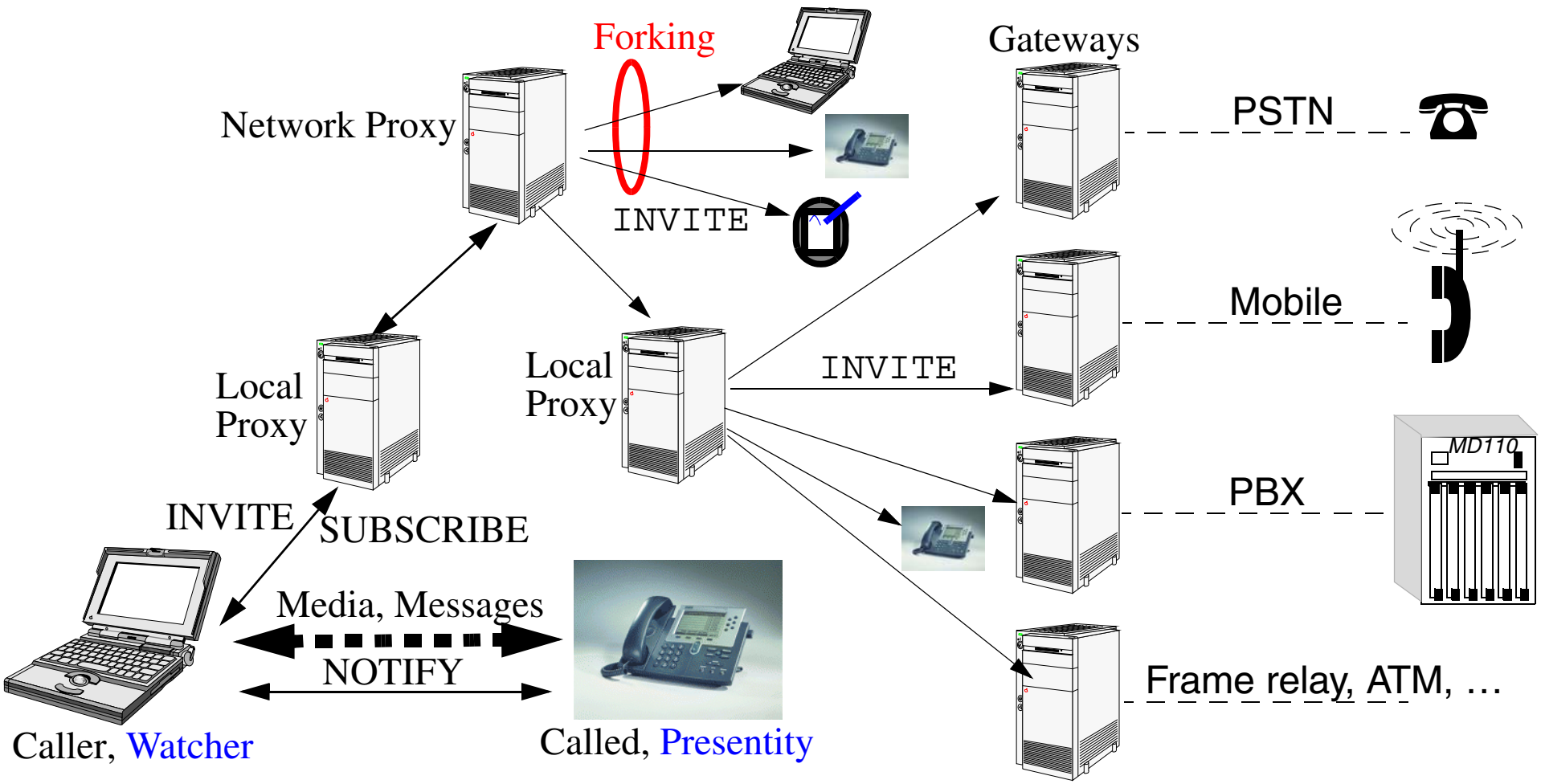


Figure 4: SIP Actors (presense entity names in blue)

SIP Methods and Status Codes

Method	Purpose
INVITE	Invites a user to join a call.
ACK	Confirms that a client has received a final response to an INVITE.
BYE	Terminates the call between two of the users on a call.
OPTIONS	Requests information on the capabilities of a server.
CANCEL	Ends a pending request, but does not end the call.
REGISTER	Provides the map for address resolution, this lets a server know the location of a user.

At least 8 additional methods have been defined see **SIP Method Extensions in other RFCs** on page 199.

SIP Status codes - patterned on and simular to HTTP's status codes:

Code	Meaning
1xx	Informational or Provisional - request received, continuing to process the request
2xx	Final - the action was successfully received, understood, and accepted
3xx	Redirection - further action needs to be taken in order to complete the request
4xx	Client Error - the request contains bad syntax or cannot be fulfilled at this server
5xx	Server Error - server failed to fulfill an apparently valid request (Try another server!)
6xx	Global Failure - the request cannot be fulfilled at any server (Give up!)

SIP Uniform Resource Indicators (URIs)

Two URI schemes - similar to the form of an e-mail addresses: user@domain

- SIP URI - introduced in RFC 2543
  - example: `sip:maguire@kth.se`
- Secure SIP URI - introduced in RFC 3261
  - example: `sips:maguire@kth.se`
  - Requires TLS over TCP as transport for security

Three types of SIP URIs:

- Address of Record (AOR) (identifies a user)
  - example: `sip:maguire@kth.se`
  - Need DNS SRV records to locate SIP Servers for kth.se domain
- Fully Qualified Domain Name (FQDN) (identifies a specific device)
  - examples: `sip:maguire@130.237.212.2` or `sip:maguire@chipsphone.it.kth.se`
  - `sip:+46-8-790-6000@kth.se; user=phone` the main KTH phone number in E.164 format via a gateway; note that the visual separators in a phone number (dashes, dots, etc.) are ignored by the protocol
- Globally Routable UA URIs (GRUU) (identifies an instance of a user at a given UA, for the duration of the registration of the UA to which it is bound)[79]

Issues to be considered

- Address Resolution
- Session Setup
- Media Negotiation
- Session Modification
- Session Termination
- Session Cancellation
- Mid-call Signaling
- Call Control
- QoS Call setup

Address Resolution

The first step in routing the SIP request is to compute the **mapping** between the **URI** and *a specific user* at *a specific host/address*.

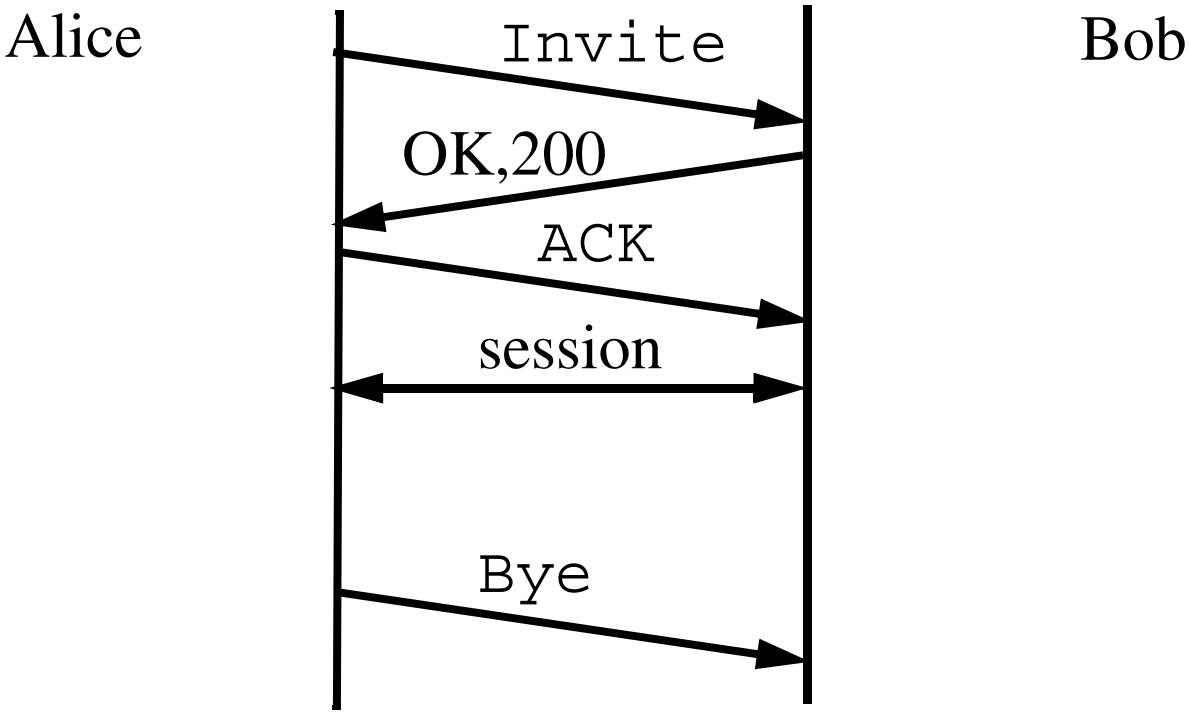
This is a very general process and the source of much of SIP's power.

- providing support for mobility and portability
- Can utilize:
  - DNS SRV lookup
  - ENUM
  - Location Server lookup

We will look at this in detail (see **DNS and ENUM** on page 273), but for now will assume a simple DNS lookup based on the URI.

SIP timeline

Simple version of Alice invites Bob to a SIP session:



We begin by examining the details of session setup. For lots of examples of basic call flows see [76].

SIP Invite[1]

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bK776asdhds
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

SIP is a text-based protocol and uses ISO 10646 character set in UTF-8 encoding (RFC 2279). The message body uses MIME and *can* use S/MIME for security.

The generic form of a message is:

```
generic-message = start-line
                  message-header*
                  CRLF
                  [ message-body ]
```

1. Example adapted from draft-ietf-sip-rfc2543bis-06.ps

Bob's response to Alice's INVITE[1]

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bK776asdhds
Via: SIP/2.0/UDP
bigbox3.site3.atlanta.com:5060;branch=z9hG4bK77ef4c2312983.1
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bKnashds8
To: Bob <sip:bob@biloxi.com>;tag=a6c85cf
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:bob@192.0.2.8>
Content-Type: application/sdp
Content-Length: 131

(Bob's SDP not shown}
```

1. Example adapted from draft-ietf-sip-rfc2543bis-06.ps

ACK

```
ACK sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bK776asdhds
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 ACK
Content-Length: 0
```

A successful set-up sequence was: `INVITE/200/ACK`

A set-up failure would be a sequence such as: `INVITE/4xx`[1]`/ACK`

NB: `INVITE` is the *only* method in SIP that involves a 3-way handshake with ACK

The further setup of the call can proceed **directly** between Alice and Bob, based on the the information (especially that in SDP) which they have exchanged.

Now we will examine the details of these initial SIP messages!

1. or 5xx or 6xx

SIP Invite (method/URI/version)

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bK776asdhds
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

Start Line is the first line of a SIP message which contains:

- method or Request type: `INVITE`
- Request-URI which indicates who the request is for: `sip:bob@biloxi.com`
- SIP version number: `SIP/2.0`

SIP Via

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP proxy.stockholm.se:5060;branch=82.1
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bK776asdhds
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

- **Via** headers show the path the request has taken in the SIP network
  - A Via header is inserted by the User Agent which initiated the request (this will be last in the list of Via headers)
  - Via headers are inserted above this by proxies in the path (i.e., this details the path taken by the request)
- **Via** headers are used to route responses back the same way the request came
  - this allows stateful proxies to see both the requests and responses
  - each such proxy adds the procotol, hostname/IP address, and port number
- The "`branch`" parameter is used to detect loops

Dialog (Call leg) Information

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bK776asdhds
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

- Dialog[1] (formerly "call leg") information is in headers:
  - **To** tag, **From** tag, and **Call-ID** -- all requests and responses in this call will use this **same** dialog information.
  - "**To**" specifies the logical recipient of the message, "**From**" the logical sender
    - the string "Bob" is called a "display name"
- **Call-ID** is unique identifier
  - The Call-ID is an arbitrary number, but it uniquely identifies this call (i.e., **session**), hence all future references to this session refer to this Call-ID
  - usually composed of a pseudo-random string @ hostname or IP Address

1. A Dialog formally begins upon receipt of a response containing a tag. It is called an "Early dialog" when the response was a **18x** provisional response.

SIP CSeq

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bK776asdhds
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

- Command Sequence (**CSeq**) Number
  - Initialized at start of call (1 in this example)
  - Incremented for each subsequent request
  - Used to distinguish a retransmission from a new request
- Followed by the **request type** (i.e., SIP method)

SIP Contact

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bK776asdhds
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

- **Contact** header contains a SIP URL for direct communication between User Agents
  - If Proxies do not Record-Route[1], they can be bypassed
- **Contact** header is also present in the `200 OK` response

1. Note that the Record-Route and Route headers approach of RFC 2543 was found not to work.

SIP Content Type and Length

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bK776asdhds
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

- **Content-Type** indicates the type of message body attachment (others could be text/plain, application/cpl+xml, etc.)
  - Here "**`application/sdp`**" indicates that it is SDP
- **Content-Length** indicates length of the message body in octets (bytes)
  - 0 indicates that there is no message body.

SIP Max-Forwards

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bK776asdhds
Max-Forwards: 30
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142

(Alice's SDP not shown)
```

- Max-Forwards is decremented by each proxy that forwards the request.
- When count goes to zero, request is discarded and `483 Too Many Hops` response is sent.
- Used for stateless loop detection.

Other header fields

- **Content-Encoding**:
- **Allow**:
- **Expires**:
- **In-Reply-To**:
- **Priority**: indicated priority of displaying a message to a user
  - Normal
  - Urgent
  - Non-Urgent
  - Emergency
- **Require**: contains a list of options which the server is expected to support in order to process a request
- **Retry after**: number of seconds after which a requestor should try again
- **Supported**: enumerates all the extensions supported the sender (NB: this differs from a “Require” which requires that a destination supports the given extension)

Several types of SIP Servers

- User agent server runs on a SIP terminal (could be a SIP phone, a PDA, laptop, …) - it consists of two parts:
  - User Agent Client (UAC): initiates requests
  - User Agent Server (UAS): responds to requests
- SIP proxy - interprets (if necessary, rewrites specific parts of a SIP request message) before forwarding it to a server closer to the destination:
  - SIP **stateful** proxy server - remembers its queries and answer; can also forward several queries in parallel (can be **Transaction Stateful** or **Call Stateful**).
  - SIP **stateless** proxy server
  - Proxies ignore SDP and do **not** handle any media (content)
  - Outgoing proxy: used by a user agent to route an outgoing request
  - Incoming proxy: proxy server which supports a domain (receives incoming requests)
- SIP redirect server - directes the client to contact an alternate URI
- Registrar server - receives SIP REGISTER requests updates LS
- Location server (LS) - knows the current binding and queried by Proxies to do their routing
  - SIP can also use DNS SRV (Service) Records used to locate (inbound) proxy.
  - note in RFC 2543: a location server is a generic term for a **database**

SIP Trapezoid[1]

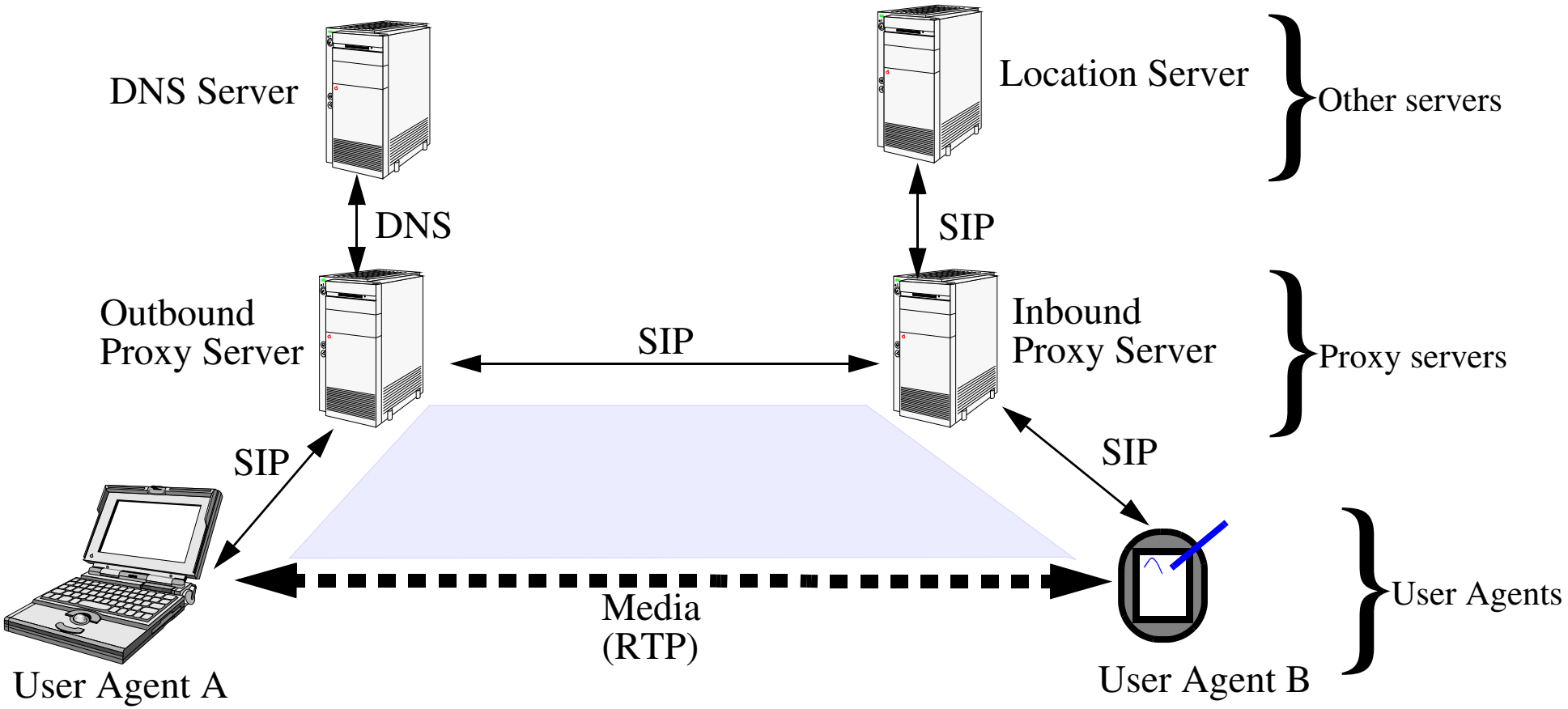


Figure 5: SIP Trapezoid

1. From the lecture notes "SIP Tutorial: Introduction to SIP" by Henry Sinnreich and Alan Johnston, formerly at http://smuhandouts.com/8393/SIPTutorial.pdf

SIP Call Setup[1]

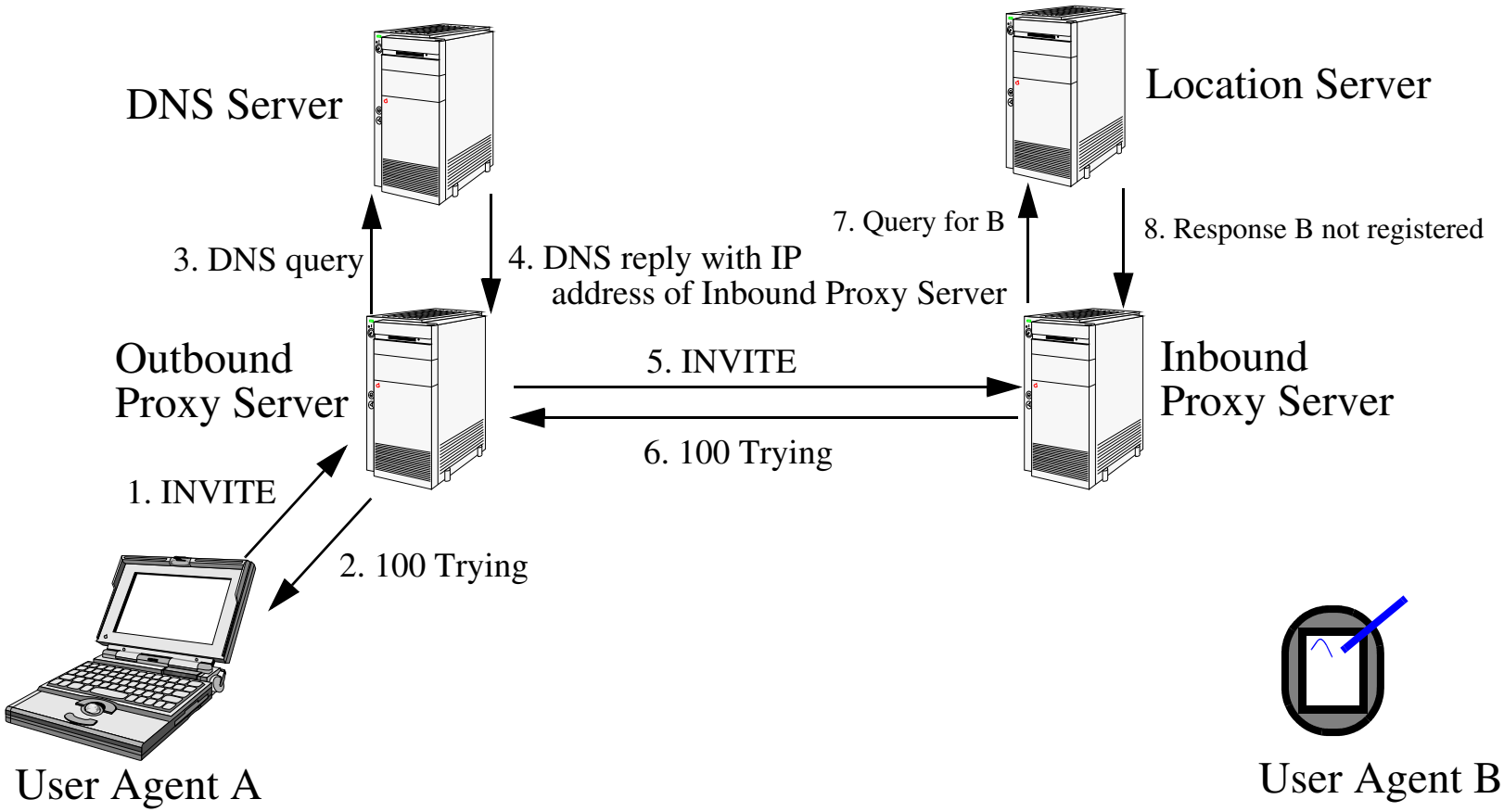


Figure 6: SIP Call Setup - when B has not registered

1. From the lecture notes "SIP Tutorial: Introduction to SIP" by Henry Sinnreich and Alan Johnston, formerly at http://smuhandouts.com/8393/SIPTutorial.pdf

SIP Call Setup Attempt[1]

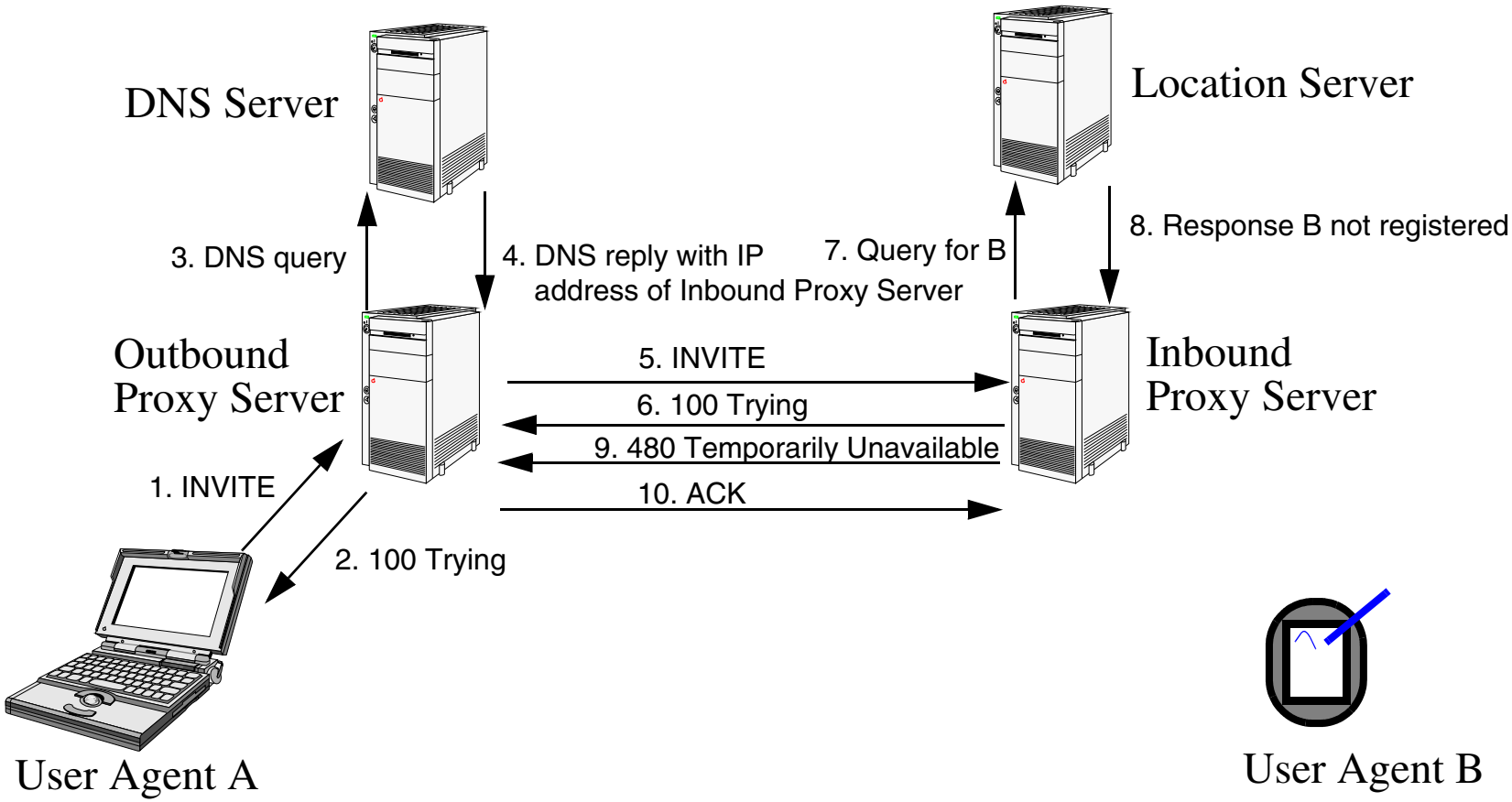


Figure 7: SIP Call Setup Attempt - when B has not registered

1. Adapted from the lecture notes "SIP Tutorial: Introduction to SIP" by Henry Sinnreich and Alan Johnston, formerly at http://smuhandouts.com/8393/SIPTutorial.pdf

SIP Call Setup Attempt[1]

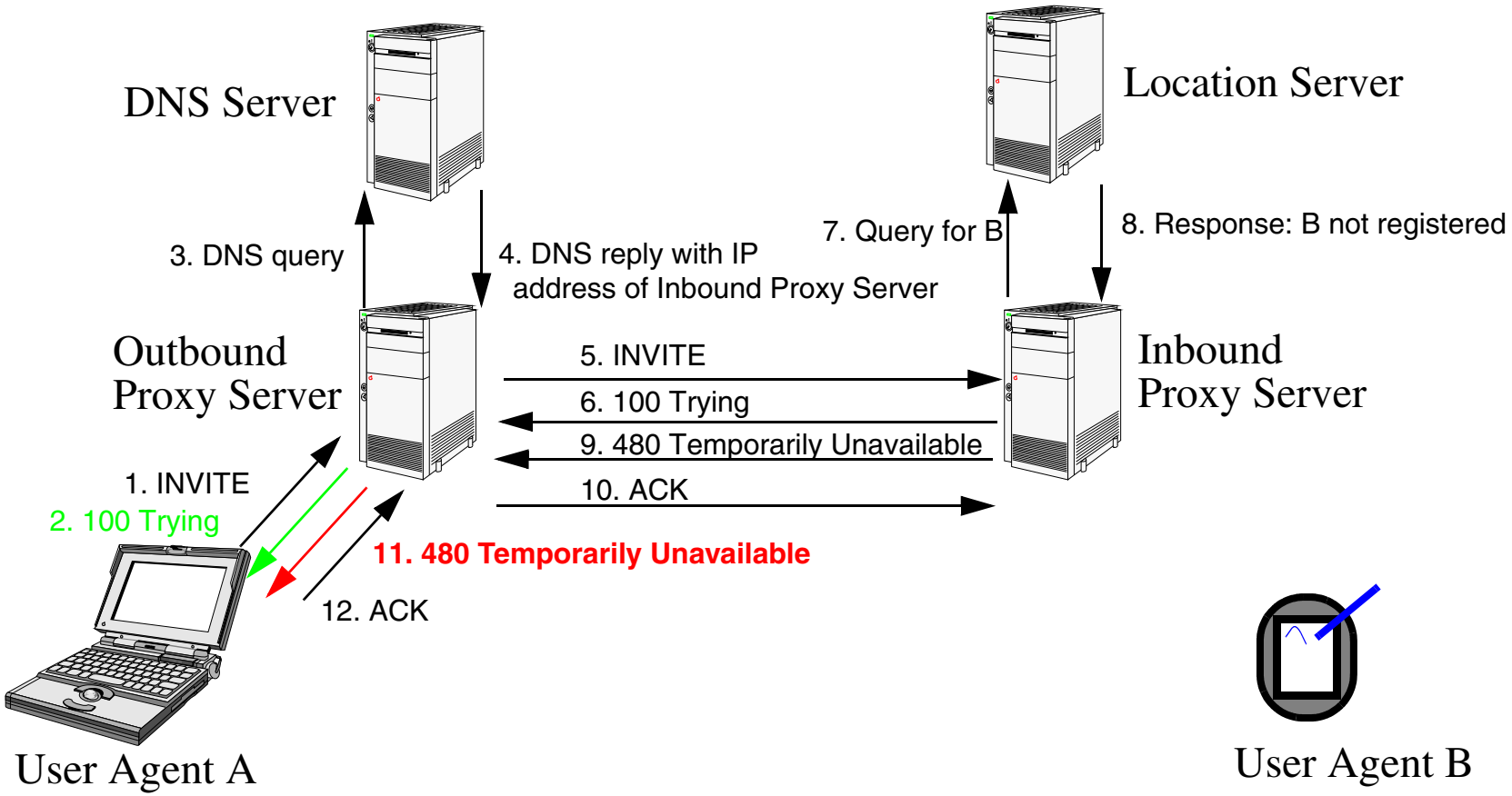


Figure 8: SIP Call Setup Attempt - when B has not registered (continued)

1. Adapted from the lecture notes "SIP Tutorial: Introduction to SIP" by Henry Sinnreich and Alan Johnston, formerly at http://smuhandouts.com/8393/SIPTutorial.pdf

SIP Presence[1]

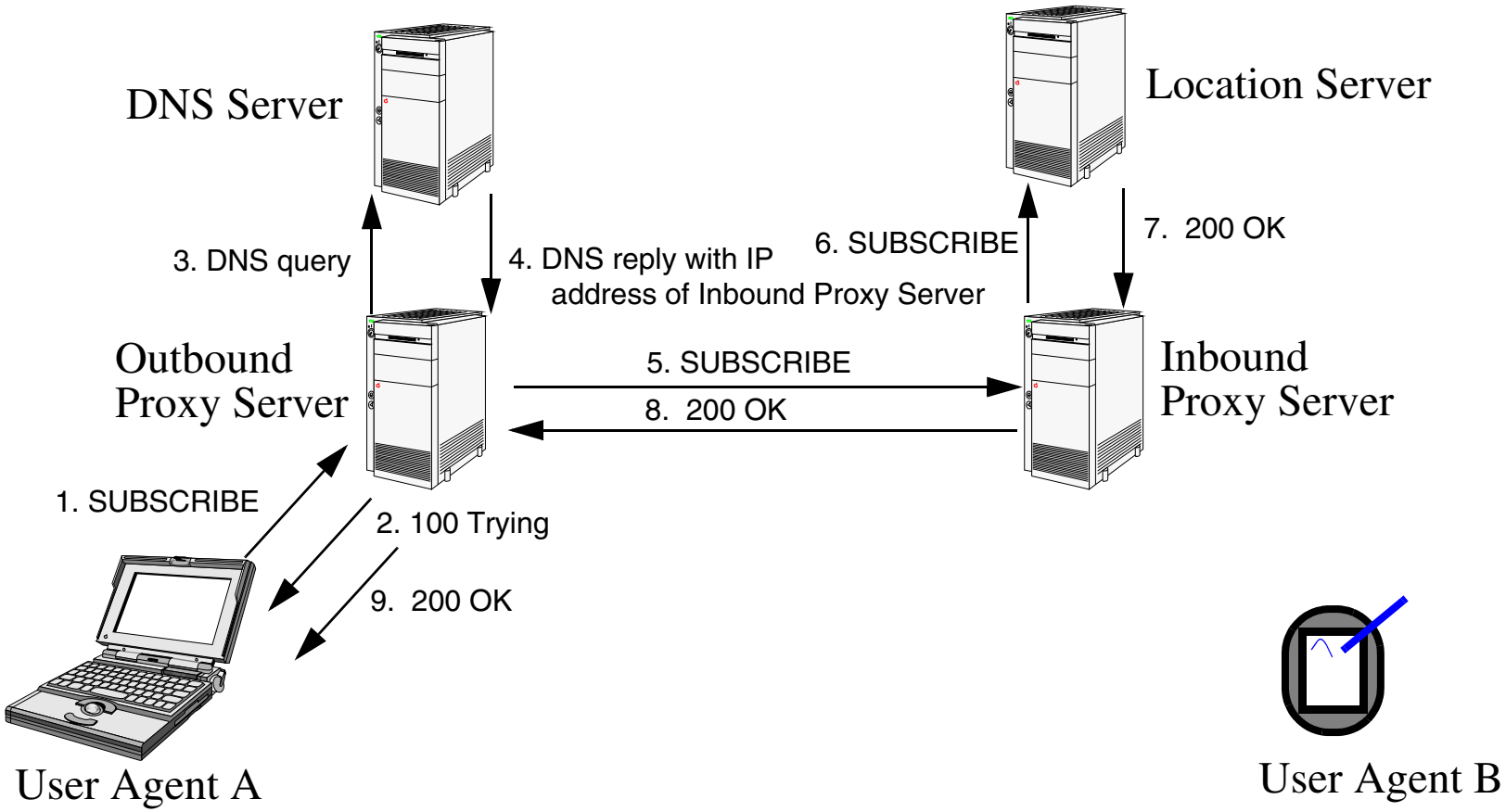


Figure 9: SIP Presence: A asks to be told when B registers

1. Adapted from the lecture notes "SIP Tutorial: Introduction to SIP" by Henry Sinnreich and Alan Johnston, formerly at http://smuhandouts.com/8393/SIPTutorial.pdf

SIP B not Present[1]

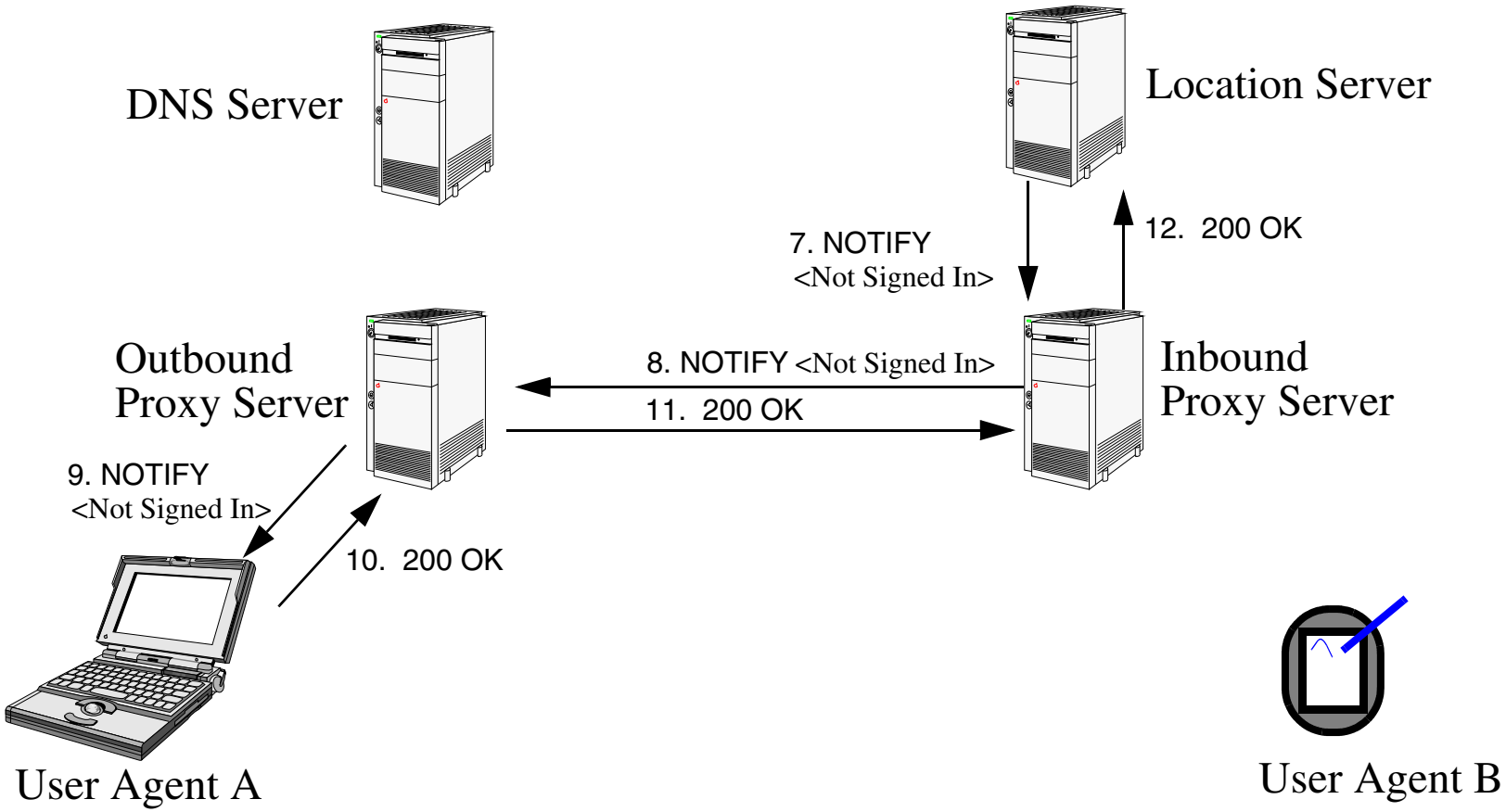


Figure 10: NOTIFY A that B has <Not Signed In>

1. Adapted from the lecture notes "SIP Tutorial: Introduction to SIP" by Henry Sinnreich and Alan Johnston, formerly at http://smuhandouts.com/8393/SIPTutorial.pdf

SIP Registration Example[1]

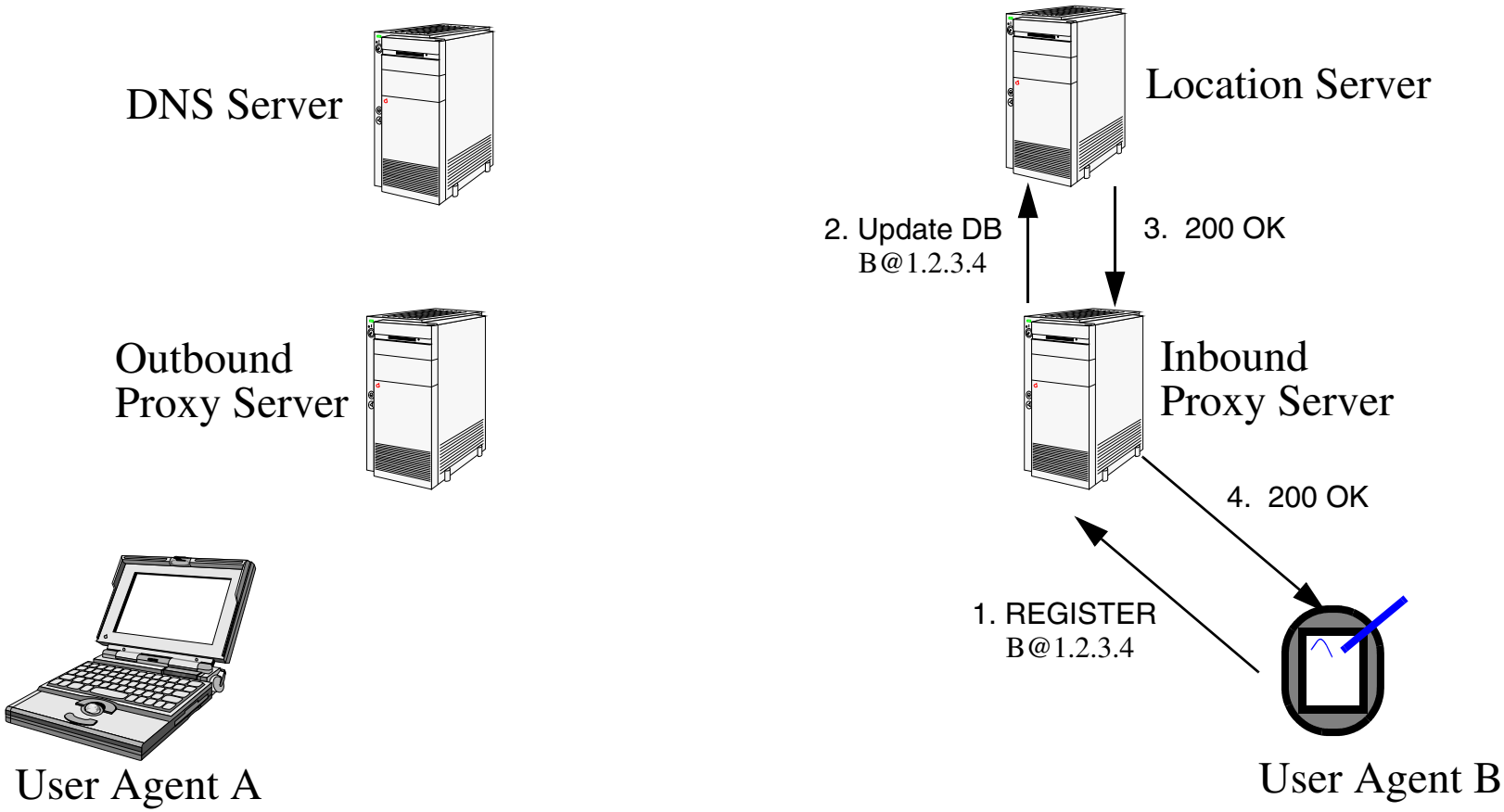


Figure 11: B registers

1. Adapted from the lecture notes "SIP Tutorial: Introduction to SIP" by Henry Sinnreich and Alan Johnston, formerly at http://smuhandouts.com/8393/SIPTutorial.pdf

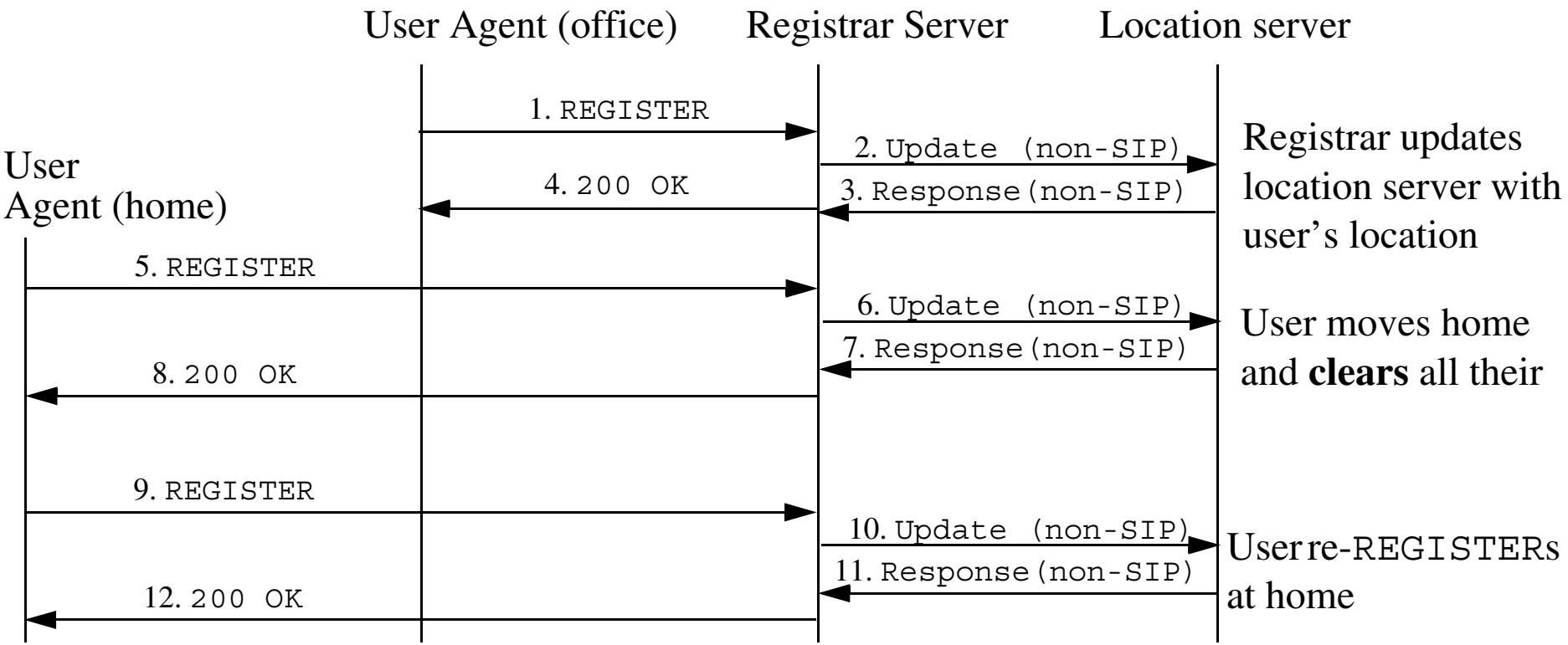
Purpose of registration

User B registers in order to establish their current **device** and **location**

- Only ***their*** location server need know
  - The location server need not disclose this location to "just anyone", but can apply various polices to decide who can learn of it, i.e., their location server can decide **who** can ask for B's location and **when** they can ask (perhaps even limiting it to **where** they can ask from).
  - This has significant privacy implications.
- This scales well - as B only has to update ***their*** location server, rather than having to inform all *possible* callers.

To learn about proxies between the user agent and the Registrar - see [69].

REGISTERing



REGISTER request includes one or more Contact headers:

```
Contact: <sip:UserA@4.3.2.1>;class=personal
Contact: <sip:UserA-msg-depot@voicemail.provider.com>;feature=voicemail
Contact: <sip:+13145551212@gateway.com;user=phone>;class=business
Contact: <sip:+13145553333@cellphone.com;user=phone>;mobility=mobile
Contact: <tel:+13145551212>
Contact: <mailto:UserA@hotmailer.com>
```

Details at: Sinnreich & Johnston, pp. 78-79 and **User Preferences** on page 421.

SIP Call Setup Attempt[1]

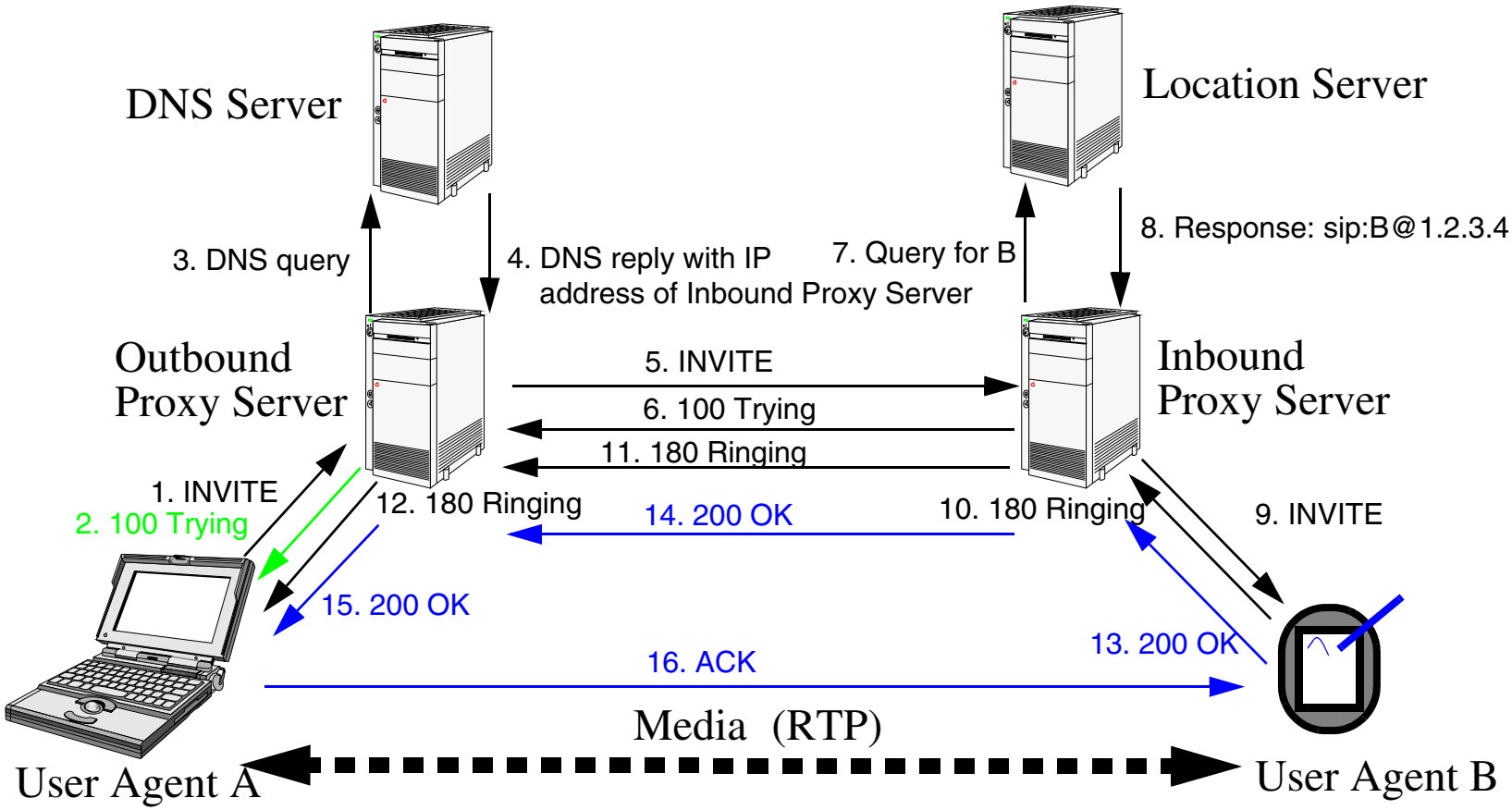
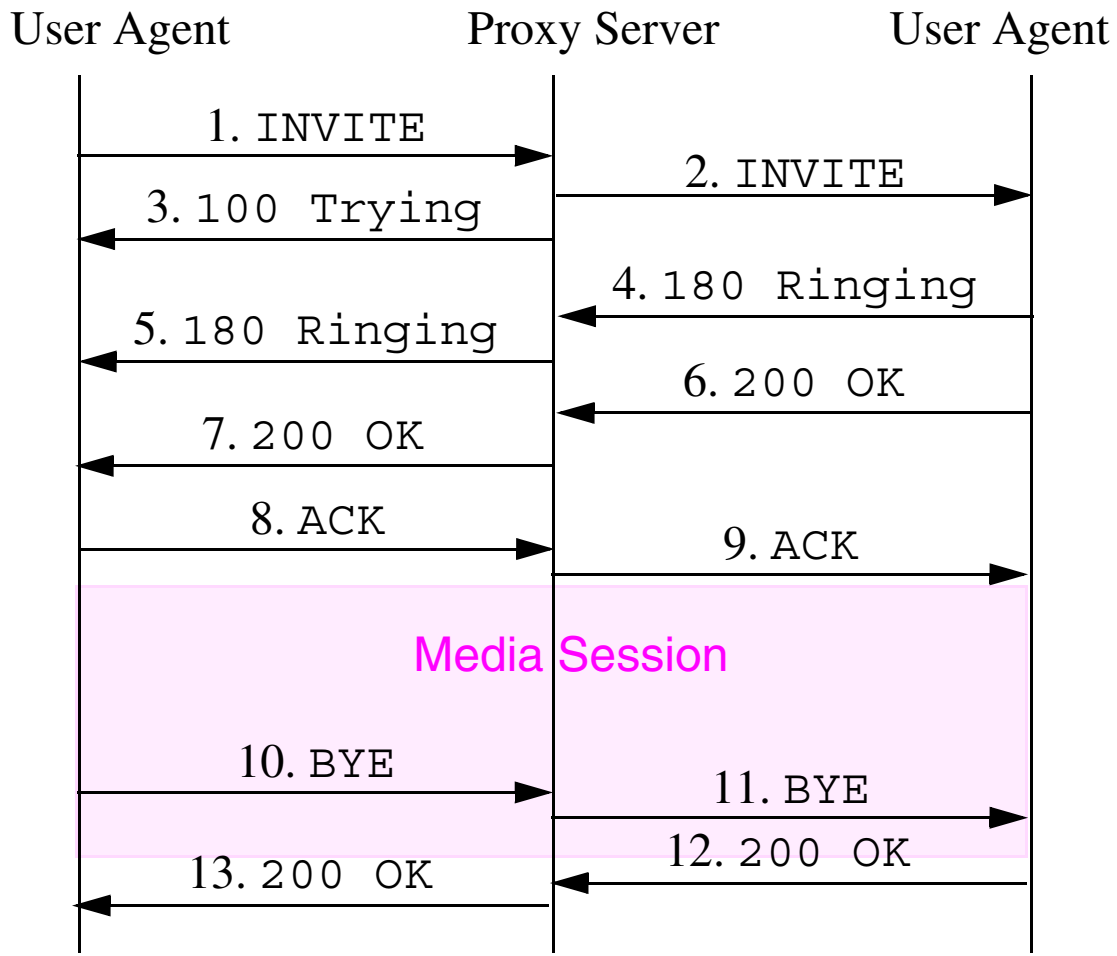


Figure 12: SIP Call Setup Attempt - when B has registered

1. Adapted from the lecture notes "SIP Tutorial: Introduction to SIP" by Henry Sinnreich and Alan Johnston, formerly at http://smuhandouts.com/8393/SIPTutorial.pdf

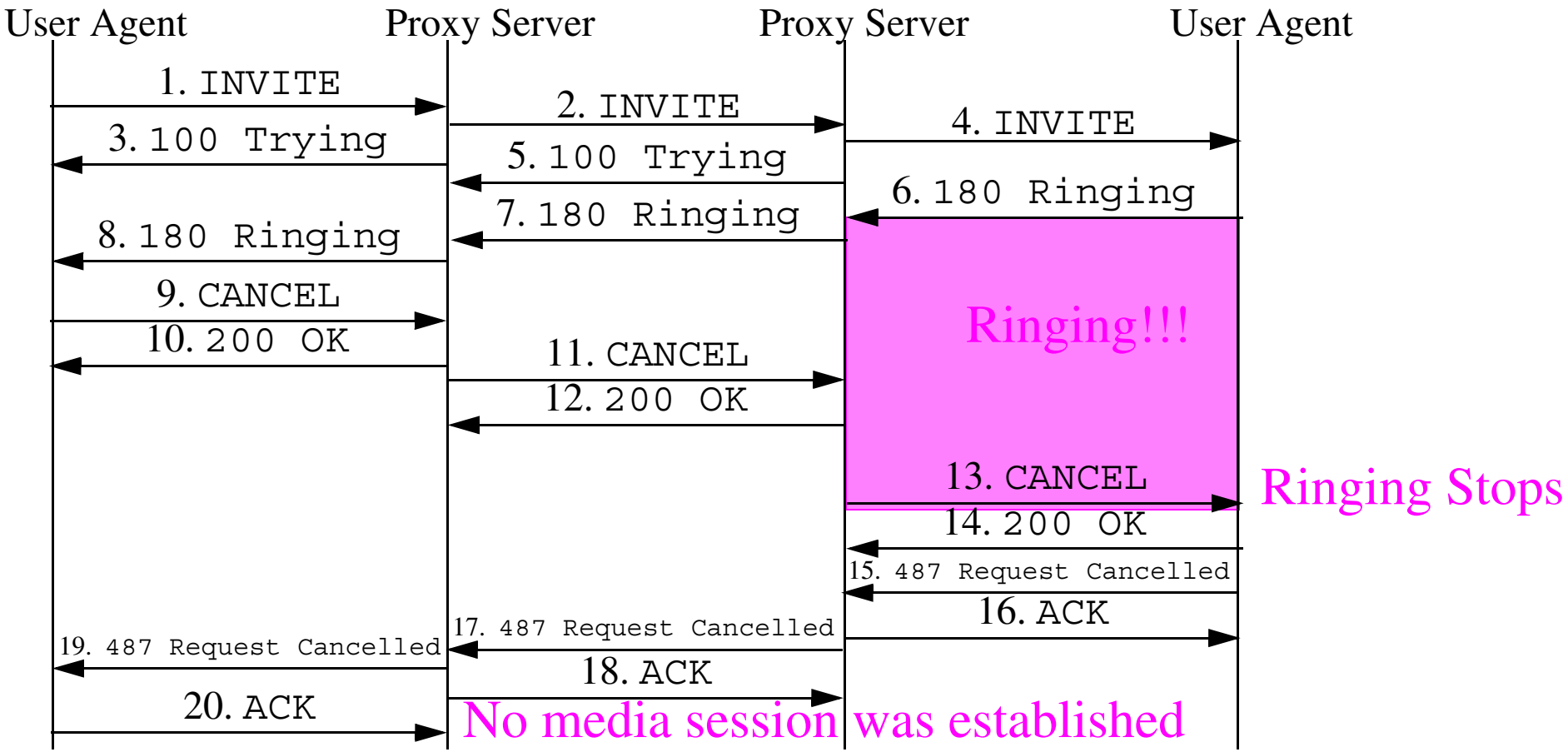
SIP Session Termination using BYE



BYE causes the media session to be torn down.

Note: BYE like INVITE is an **end-to-end** method.

SIP Session Termination using CANCEL



`CANCEL` causes the session to be cancel. Note: If a reply is `481 Transaction Unknown`, then the user agent may need to send a `BYE` since the `CANCEL` was received **after** the final reponse was sent (there was a **race condition**).

CANCEL and OPTIONS

CANCEL

- In addition to canceling a pending session
- CANCEL can also be sent by a proxy or user agent
  - for example, when a parallel fork has been done, once you have a successful match, then you can cancel the others

OPTIONS

- Used to query a server or user agent for its capabilities
- sometimes used for very simple presence information

Unsuccessful final responses are hop-by-hop

Unsuccessful final responses (`3xx`, `4xx`, `5xx`, `6xx`) are **always** acknowledged on a *hop-by-hop* basis.

Only `200 OK` is *end-to-end*.

Authentication

Builds upon authentication schemes developed for HTTP (see RFC 2716), for example challenge/response, digest, …

Two forms:

- user agent-to-user agent
  - `401 Unauthorized` ⇒ Authentication Required
- user agent-to-server
  - `407 Proxy Authentication Required` ⇒ Authentication Required (reponse sent by a proxy/server)

Note: Any SIP request can be challenged for authentication.

Note: There is **no** *integrity* protection, for additional information see **SIP Security, NATs, and Firewalls** on page 431.

SIP Method Extensions in other RFCs

See "Guidelines for Authors of Extensions to the Session Initiation Protocol (SIP)"[71]

- INFO - Call signaling information during a call
  - RFC 2976: The SIP INFO Method, October 2000.
- PRACK - Reliable ACK
  - RFC 3262: Reliability of Provisional Responses in Session Initiation Protocol (SIP), June 2002
- SUBSCRIBE/NOTIFY
  - RFC 3265: Session Initiation Protocol-Specific Event Notification, June 2002.
- REFER
  - RFC 3515: The Session Initiation Protocol (SIP) Refer Method, April 2003 [72]
  - RFC 3892: The Session Initiation Protocol (SIP) Referred-By Mechanism, Sept. 2004 [73]
- MESSAGE
  - RFC 3428: Session Initiation Protocol Extension for Instant Messaging, December 2002 [74]
- UPDATE - Early media and preconditions
  - RFC 3311: The Session Initiation Protocol (SIP) UPDATE Method. October 2002 [75]

SIP Extensions and Features

- Method Extensions
  - Unknown methods rejected by User Agent using `405` or `501` response
  - Listed in `Allow` header field
  - Proxies treat unknown methods as a non-`INVITE`
- Header Field Extensions
  - Unknown header fields are ignored by user agents and proxies
  - Some have feature tags registered, these can be declared in a `Supported` or `Require` header field
- Message Body Extensions
  - Unknown message body types are rejected with a `406` response
  - Supported types can be declared with an `Accept` header field
  - `Content-Disposition` indicates what to do with it
- Extension must define failback to base SIP specification.

$\Rightarrow$ No Profiling is needed

- unlike for example, Bluetooth!

SIP Presence - Signed In[1]

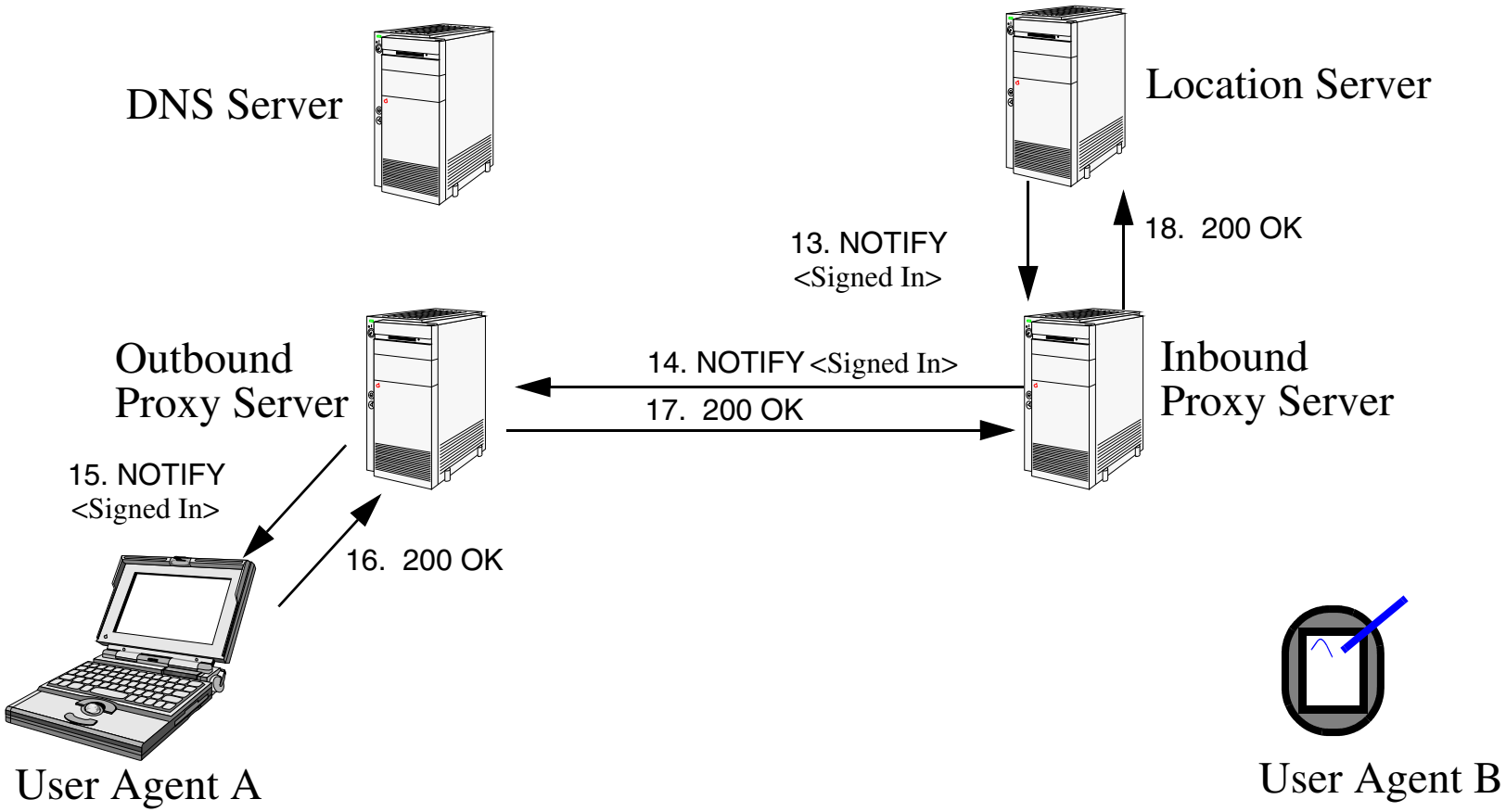
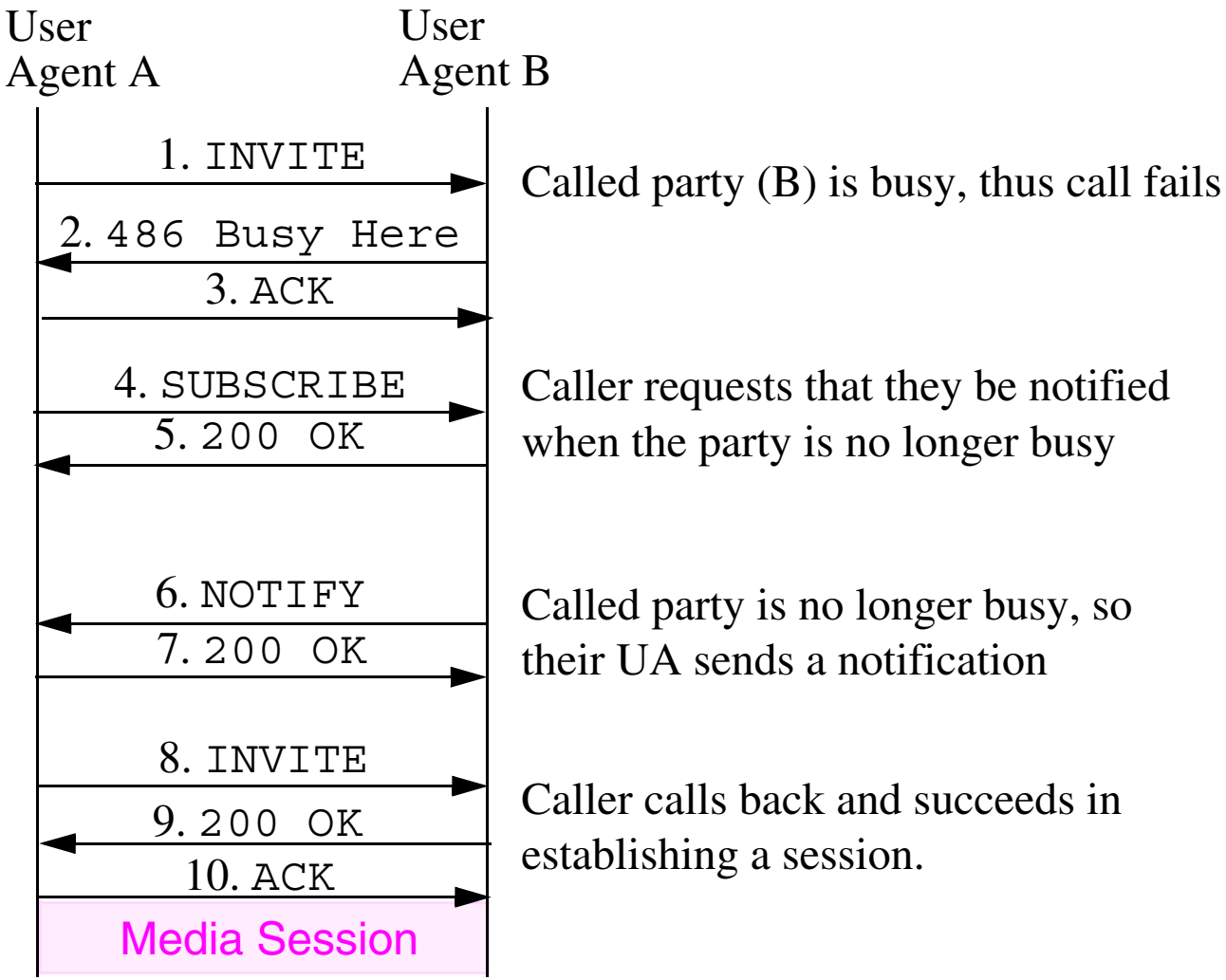


Figure 13: NOTIFY A that B has <Signed In>

1. Adapted from the lecture notes "SIP Tutorial: Introduction to SIP" by Henry Sinnreich and Alan Johnston, formerly at http://smuhandouts.com/8393/SIPTutorial.pdf

SUBSCRIBE and NOTIFY



If user B's agent does not wish to provide user A's agent with a notification it sents a `603 Decline` response.

SIP Instant Messaging Example[1]

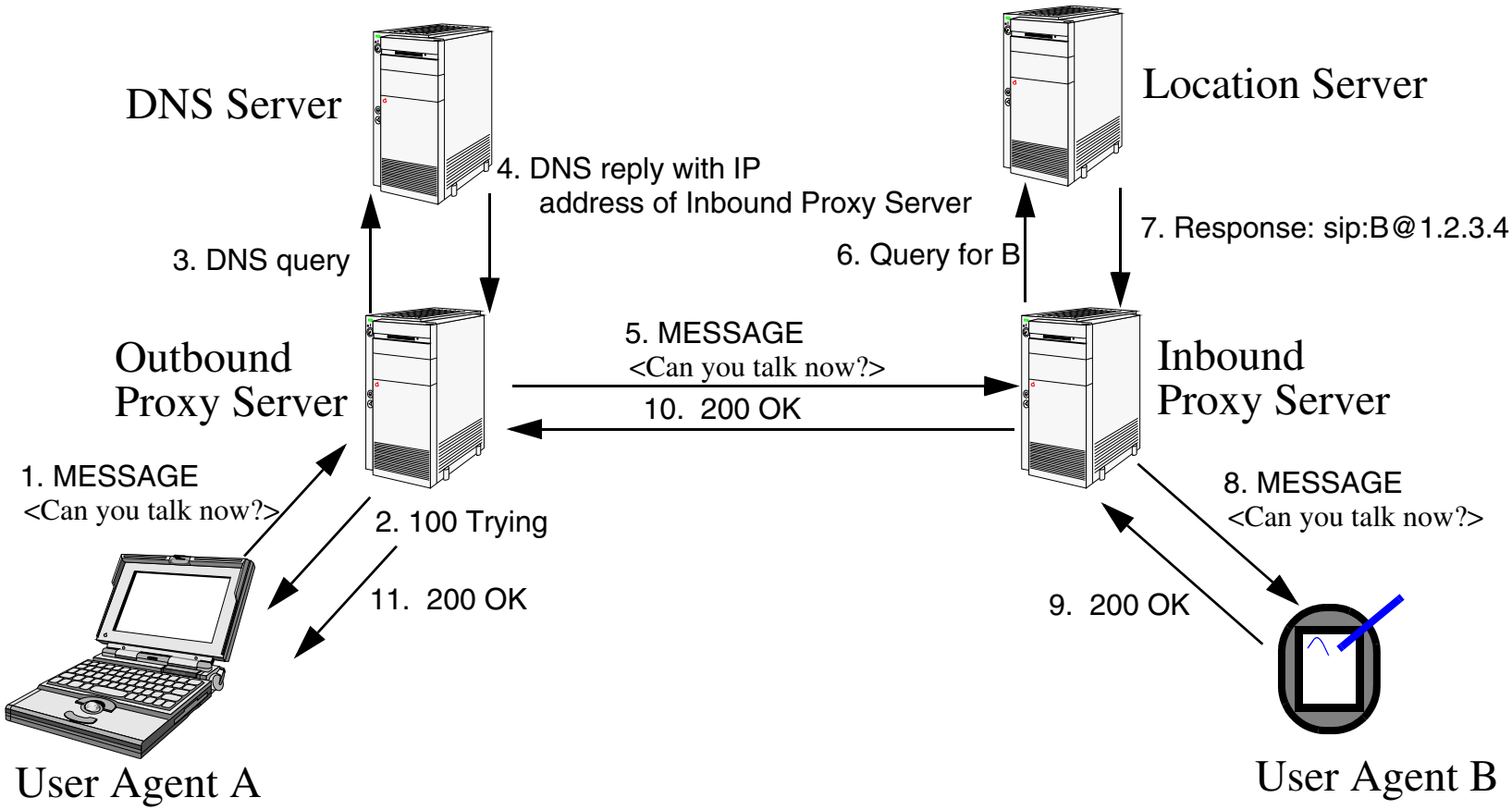


Figure 14: A sends a message to B

1. Adapted from the lecture notes "SIP Tutorial: Introduction to SIP" by Henry Sinnreich and Alan Johnston, formerly at http://smuhandouts.com/8393/SIPTutorial.pdf

SIP Instant Messaging Example (continued)[1]

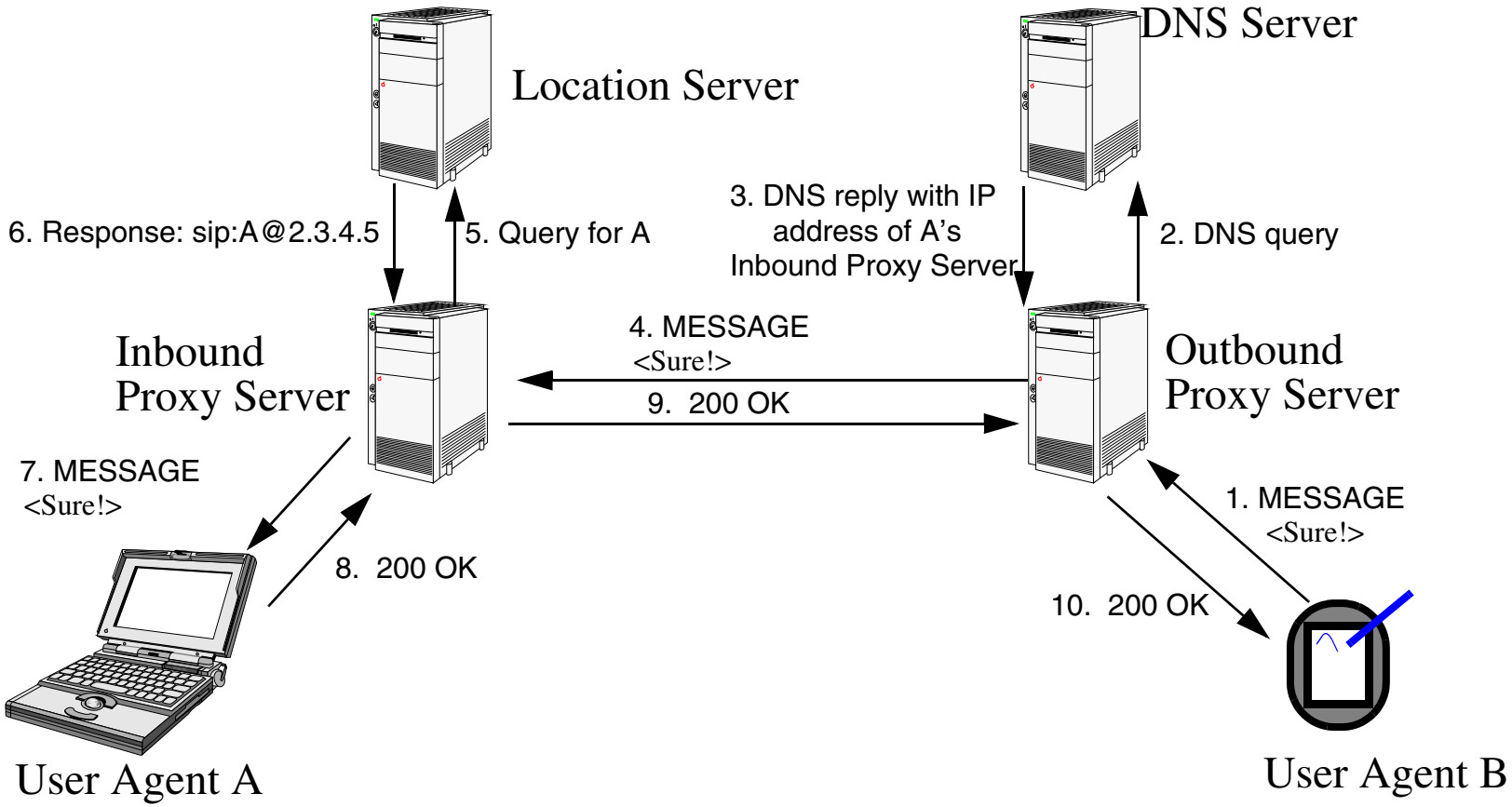


Figure 15: B sends a message to A

1. Adapted from the lecture notes "SIP Tutorial: Introduction to SIP" by Henry Sinnreich and Alan Johnston, formerly at http://smuhandouts.com/8393/SIPTutorial.pdf

Message example

A simple Instant Message (IM) as SIP:

```
MESSAGE im:UserB@there.com SIP/2.0
Via: SIP/2.0/UDP 4.3.2.1
To: User B <im:UserB@there.com>
From: User A <im:UserA@here.com>
Call-ID: a5-32-43-12@4.3.2.1
CSeq: 1 MESSAGE
Content-type: text/plain
Content-Length: 16

Hi, How are you?
```

The response will be a `200 OK` from B.

Note: the example uses IM URIs instead of SIP URIs.

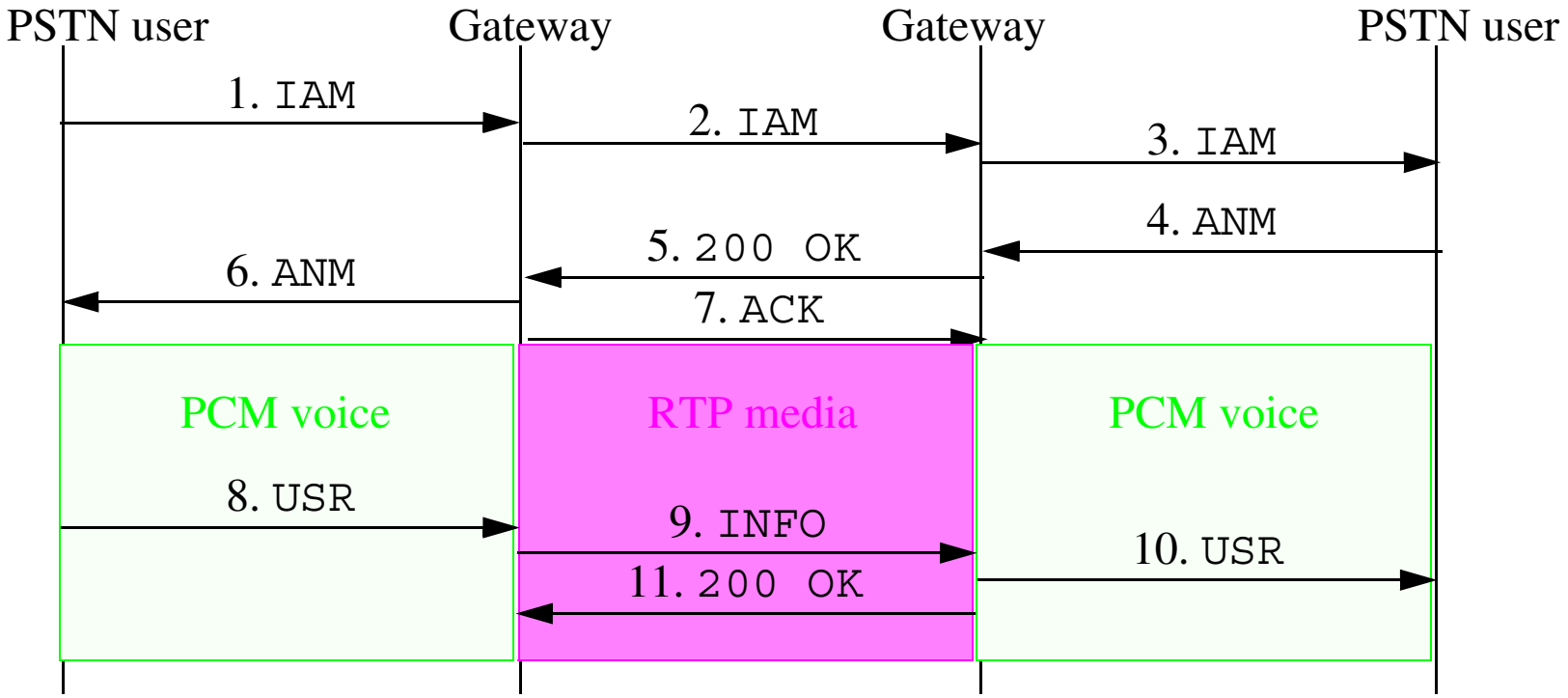
A `MESSAGE` request can be sent at anytime (even without a session).

For futher information about the work of the IETF working group on Instant Messaging and Presence Protocol (impp) see

http://www.ietf.org/html.charters/impp-charter.html (Concluded 2004)

Midcall signaling

Midcall signaling used when the session parameters don't change, to exchange information between two user agents via the body of an `INFO` message. If the session parameters did change then you would use a re-`INVITE`.



Note in the above figure the ISUP messages: IAM (Initial address message), INM (Answer message), and USR (user-to-user message).

Call Control

SIP is peer-to-peer -- thus a proxy cannot issue a `BYE`, only end devices (UAs) can.

To methods for third party call control:

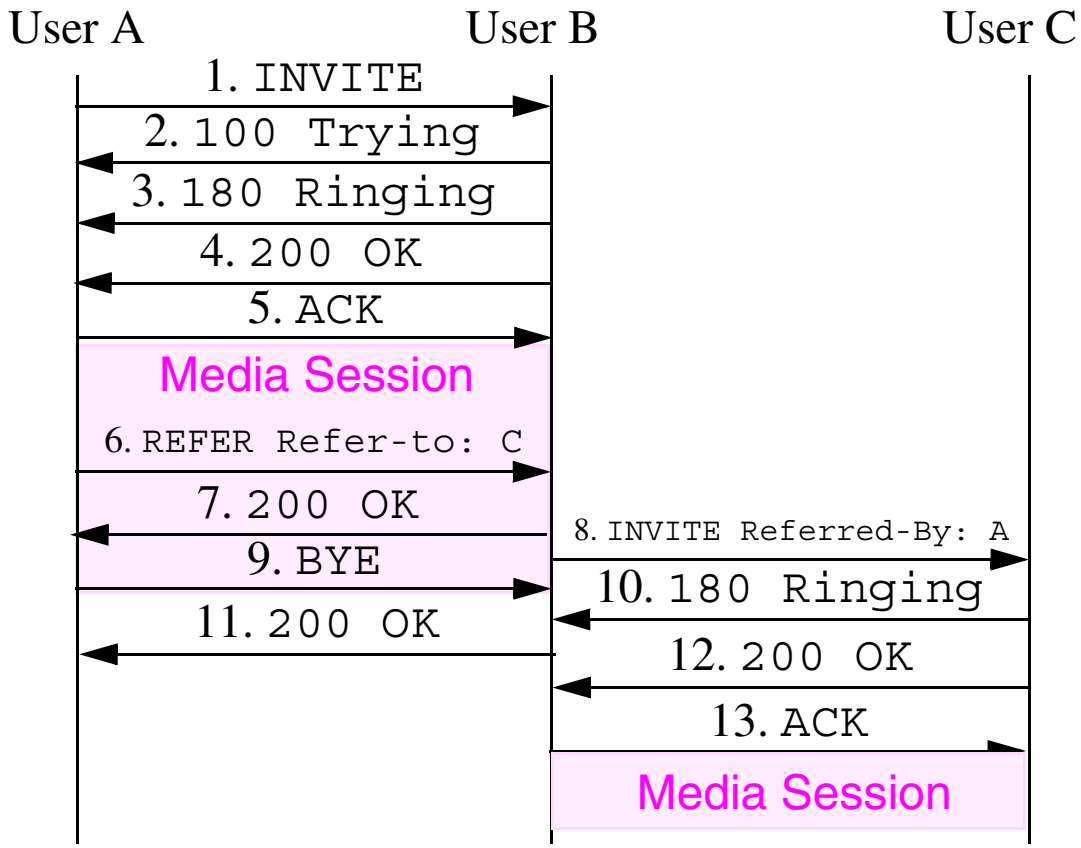
- A proxy passes an invite on, but **stays in the signaling path**
- Use `REFER` to initial third party control (the third party is no longer in the signaling path).

Useful for:

- click-to-call
- Automatic Call Distribution (ACD)
- web call center
- …

Example of using REFER

Third party call control, by User A to set up a session between Users B and C.



Note: the use by A of an `INVITE` with a `Refer-to` header and the user by B of an `INVITE` with a `Referred-By` header.

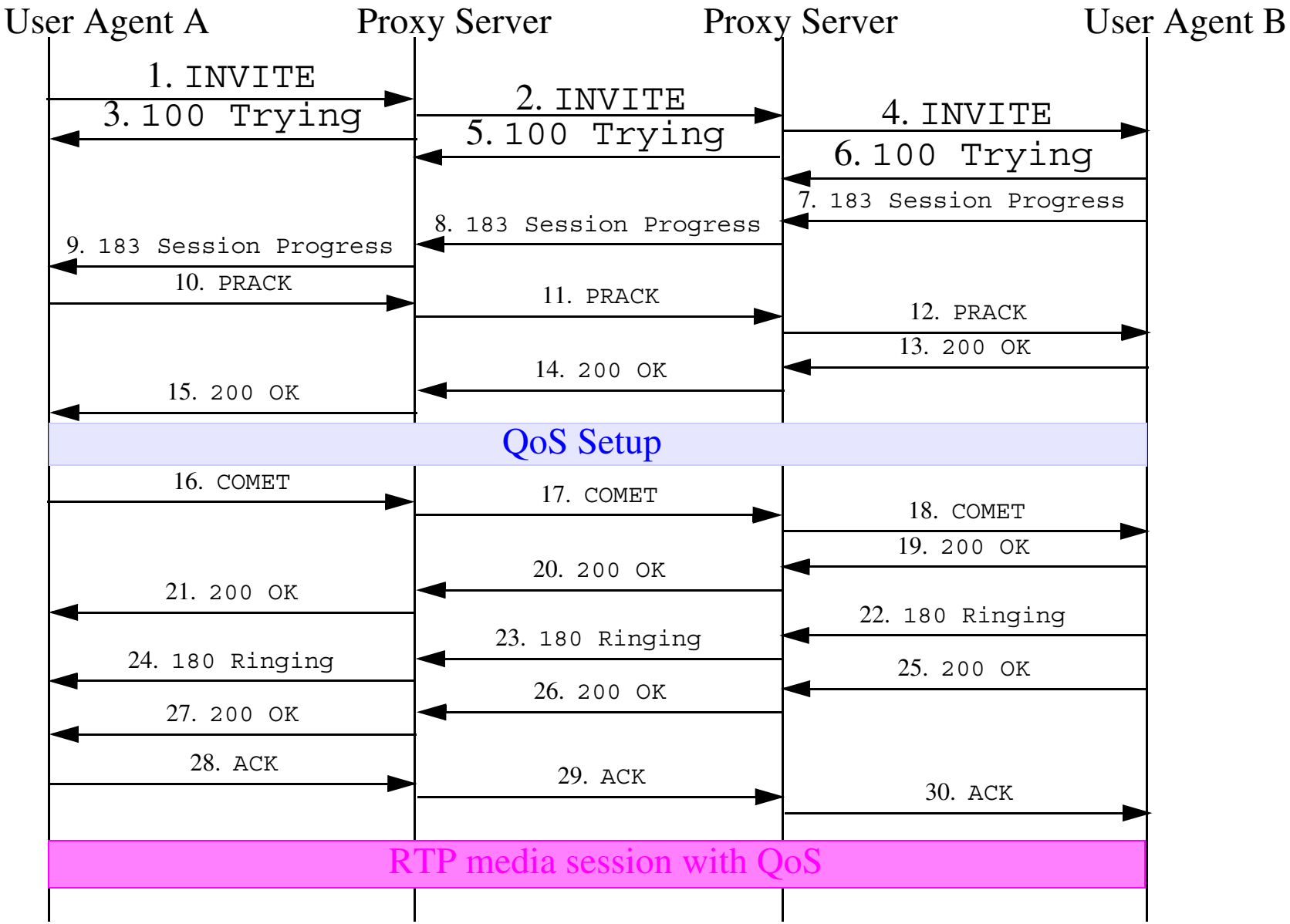
QoS and Call Setup

The path which SIP takes may be different that the media path, thus new extensions were added to enable more handshaking:

- Early Media - by allowing SDP to be included in the `183 Session Progress` response (allows establishment of QoS requirements before call is answered) - may also enable one-way RTP {hence the name “early media”}, formally: “media during early dialog”
- Reliable Provisional Responses extension allows detection of a lost `183 Session Progress` response based on using Provisional Response Acknowledgement (`PRACK`)
- UAs can use preCOnditions MET (COMET) method to indicate that the QoS requirements can be met and that the user can be alerted by ringing the phone.

SDP in the `INVITE` contains an attribute-value pair: "`a=qos:mandatory`".

For further details see: RFC3312 [67] and RFC3262 [68]; more about SDP in the next lecture module.


User Agent A
Proxy Server
Proxy Server
User Agent B
1. INVITE
2. INVITE
4. INVITE
3. 100 Trying
5. 100 Trying
6. 100 Trying
7. 183 Session Progress
8. 183 Session Progress
9. 183 Session Progress
10. PRACK
11. PRACK
12. PRACK
13. 200 OK
14. 200 OK
15. 200 OK
QoS Setup
16. COMET
17. COMET
18. COMET
19. 200 OK
20. 200 OK
21. 200 OK
22. 180 Ringing
23. 180 Ringing
24. 180 Ringing
25. 200 OK
26. 200 OK
27. 200 OK
28. ACK
29. ACK
30. ACK
RTP media session with QoS

SIP Message retransmission

Timer	default	Purpose
T1	500ms	Set when SIP request is first sent
T2	4 sec.	Longer timeout when a provisional response has been received

If a request is lost, then timeout T1 will generate a retransmission of the request.

If a request is received and a provisional response is received, then sender switches to timeout T2 (to wait for the final response).

`INVITE` is different:

- receiving a provisional response stops all re-transmissions of the `INVITE`;
- however, the sender of the provisional response starts a T1 timer when it sends its final response and if it does not get an ACK in time it retransmits the final response.

If you want/need acknowledgement of provisional responses use `PRACK`. {For some problems with timeouts for non-INVITE transactions see [80][81].}

RFC 3261 - Routing Changes

- Introduced “loose routing” vs. RFC 3543’s “strict routing”
  - Examples:
    - Pre-loaded (initial `INVITE`) `Route` header can be used instead of the default outbound proxy (DOP)
    - Pre-loaded `Route` header can be used to invoke “home proxy” services (when you are roaming)
    - Additional proxies can be added as needed (for example, adding routing during a call)
- All elements must insert `branch` paramater as a transaction ID in `Via` header fields
- `Contact` header required in all requests that establish a dialog
- `From` and `To` tags are now mandatory
- Recommend users of Fully Qualified Domain Name (FQDN) instead of IP addresses
- `Via` loop detection no longer required of proxies
  - Use of `Max-Forwards` is now manadatory
- `Via` hiding is deprecated (i.e., should no longer be used)
  - because it turned out not to be secure or useful

RFC 3261 - New Services

- Customized ringing
  - A trusted proxy can insert an `Alert-Info` header field into an `INVITE`
- Screen Pops
  - A trusted proxy can insert an `Call-Info` header field into an `INVITE`
  - URI can be HTTP and can contain call control “soft keys”
- Callback
  - Reply-to and In-Reply-To header - to assist in returning calls
- Annoucement handling
  - UAS or proxy need not make a decision about playing an early media annoucement
    - Error response contains new `Error-Info` header field which contains the URI of the annoucement
  - UAC makes a decision based on the user’s interface

Compression of SIP

As textual protocols, some might thing that SIP and SDP are too verbose, hence RFC 3486 [78] describes how SIP and SDP can be compressed. RFC 3485 [77] describes a static dictionary which can be used with Signaling Compression (SigComp) to achieve even higher efficiency.

Intelligent Network service using SIP

ITU has defined a set of service features (think of them as primitives which can be use to construct more complex services). These are divided into two sets:

- Capability Set 1: Service Features
- Capability Set 2

J. Lennox, H. Schulzrinne, and T. F. La Porta, “Implementing Intelligent Network Service with the Session Initiation Procol” [84] addresses Capability Set 1:

Abbreviated Dialing (ABD)
Attendant (ATT)
Authentication (AUTC)
Authorization code (AUTZ)
Automatic callback (ACB)
Call distribution (CD)
Call forwarding (CF)
Call forwarding on busy/don’t answer (CFC)
Call gapping (GAP)
Call hold with announcement (CHA)
Call limiter (LIM)
Call logging (LOG)
Call queueing(QUE)
Call transfer (TRA)
Call waiting (CW)
Closed usergroup(CUG)
Consultation calling (COC)
Customer profile management (CPM)
Customer recorded announcement (CRA)
Customized ringing (CRG)
Destinating user prompter (DUP)
Follow-me diversion (FMD)
Mass calling (MAS)
Meet-me conference (MMC)
Multi-way calling (MWC)
Off-net calling (ONC)
One number (ONE)
Origin dependent routing (ODR)
Originating call screening (OCS)
Originating user prompter (OUP)
Personal numbering (PN)
Premium charging (PRMC)
Private numbering plan (PNP)
Reverse charging (REVC)
Split charging (SPLC)
Terminating call screening (TCS)
Time dependent routing (TDR)

Capability Set 1: Services

Abbreviated dialling (ABD)

Account card calling (ACC)

Automatic alternative billing (AAB)

Call distribution (CD)

Call forwarding (CF)

Call rerouting distribution (CRD)

Completion of calls to busy subscriber (CCBS)

Conference calling (CON)

Credit card calling (CCC)

Destination call routing (DCR)

Follow-me diversion (FMD)

Freephone (FPH)

Malicious call identification (MCI)

Mass calling (MAS)

Originating call screening (OCS)[

Premium rate (PRM)

Security screening (SEC)

Selective call forwarding on busy/don't answer (SCF)

Selective call forwarding

Call forwarding on busy

Call forwarding on don't answer (no reply)

Split charging (SPL)

Televoting (VOT)

Terminating call screening (TCS)

Universal access number (UAN)

Universal personal telecommunications (UPT)

User-defined routing (UDR)

Virtual private network (VPN)

Capability Set 2

- Wireless services
- Inter-network services
- Multimedia
- Call pick-up
- Calling name delivery

Features

List of features adopted from http://www.miercom.com/survey - augmented with my own notes with respect to SIP supporting this feature:

SIP	Feature	Description
✢	911/E-911 support	Emergency services
	Audible message waiting	An audible indicator when there is a new message
	Automated attendant	Answers and routes calls automatically based on caller responses; e.g., via Interactive Voice Response (IVR) or DTMF prompts
✔	Automatic alternate routing	Routes calls automatically based on user-defined routing parameters, priorities, and failover/availability decisions.
✔	Automatic call back	Calls an extention back automatically when a busy signal or no answer is encountered. Also known as Camp on.
	Bridged call appearance	Allows the same phone number to appear and be answered on multiple phone sets.
✔	Call blocking	Selectively blocks calls from user-defined origins

SIP	Feature	Description
✢	Call conference	An audio path for multiple parties on a single call, established via user keystrokes and no outside intervention.
✢	Call drop	Terminates a call without hanging up the receiver.
✔	Call forward all	Redirects all calls to another station or location.
✔	Call forward on busy	Redirects all calls to another station or location *when the user's is busy.*
✔	Call forward on no answer	Redirects all calls to another station or location *after a specified number of rings*.
✔	Call hold	Places an incoming call on hold or retrieves a call placed on hold.
✔	Call pick-up	Allows a user to place a call on hold, then resume it from another phone in the system.
✢	Call return	Calls back the last incoming number.
✢	Call transfer	Redirects an answered call to another user. see Rick Dean, Billy Biggs, and R. Mahy, “The Session Inititation Protocol (SIP) ’Replaces’ Header”, Internet Draft, 16 May 2002 -- for ‘Attended Transfer’ and ‘Retrieve from Call Park’
✔	Call waiting	An audible indicator heard when there is another call pending.
✔	Caller ID	Displays the name and/or number of the calling party.

SIP	Feature	Description
	Call Detail Recording (CDR)	Records call data on a specific extension or group of extensions.
	Class of service	Restricts access to features based upon users' privilege level(s).
	Direct inward system access	Dial-in system station appearance.
✔	Direct transfer to voice mail	Automatically redirects all calls to users' voicemail at the push of a button.
	Directory lookup	Allows users to look up an extension from the corporate LDAP directory.
✔	Distinctive ringing	Uses a different ringtone for different call characteristics, for example, internal vs external calls.
✔	Do not disturb	Makes the phone appear to be out of service.
✔	Follow me	Rings multiple, disparate phones simultaneously when one extension is dialed.
✔	Free seating/Hoteling	Allows a user to move from one location to another, accessing all calls, features, button mappings, etc.
	Hot line	Private line automatic ring-down connection between two phones.
	Hunt groups	Diverts calls to busy extensions to any extension in a pre-defined group.

SIP	Feature	Description
✢	Intercom - phone-to-phone	An internal intercom that initiates calls within a predefined group or department.
✢	Intercom - phone-to-multi-phone	An internal intercom that initiates voice paging through the speakers of multiple phone systems.
✢	Intrude	Allows specific users to intrude on calls already in progress. See R. Mahy and D. Petrie, “The Session Inititation Protocol (SIP) ’Join’ Header” [83] - a new header for use with SIP multi-party applications and call control; to logically join an existing SIP dialog, for: ‘Barge-In’, ‘Message Screening’, ‘and Call CenterMonitoring’
✢	Last number redial	Redials the last outgoing call.
✔	Least-cost routing	Routes outbound calls to the least expensive alternative, based on user-defined prioritization.
	Leave word calling	Allows internal users to leave short, pre-programmed messages for other internal users.
	Malicious call trace	Allows users to initiate a call trace.
	Message waiting indicator	Visibly indicates when new voicemail arrives, often via a blinking light.
✢	Missed call indicator	Lists missed calls.

SIP	Feature	Description
	Multiple call appearance	Allows a single phone to have multiple, repeated instances of a single phone extension.
✢	Multiple ring styles	Changes the ringtone based on user preference.
✢	Music on hold	Plays music for the caller when placed on hold.
✢	Mute	Disables the microphone. (This is really just a feature of the client.)
✢	Night service	Changes call coverage based on the time of day, for example, plays a common recording for all calls at night.
✢	One-button send all calls	Automatically redirects all calls to someone else who provides coverage with a single button.
✢	One-button speed dial	Dials a predefined number with a single button.
✔	Personal call routing	Defines routing parameters
	Priority ringing	Uses a different ringtone for specified numbers.
	Recorded announcements	Provides predefined announcements to certain calls, for example, “Your call cannot be completed as dialed”.
✔	System speed dialing	Dials frequently-called numbers using an abbreviated access code.
✢	User directory	Allows any system endpoint to browser a database of names, extensions, etc.

SIP	Feature	Description
	Volume control	Changes the volume individually for the speaker, handset, and ringer.
✢	Whisper page	Allows someone else (such as an assitant) to bridge into a call, allowing only the local party to hear.
✔		Supported by SIP
✢		Supported by SIP + additional methods

Coupling in and invoking services in the PSTN uses a sequence of the form `*SS#` or `*SS*parameter#`, where "SS" and "parameter" are numeric. This is described in ETSI ETS 300 378 [89], with the ”SS” codes enumerated in ETSI TR102 083 [88].

SIP development, evolution, …

In traditional IETF fashion is based on **running code**

- So in your projects you should make sure that what you propose is really feasible by implementing it!
  - should have at least **2 interoperable implementations** for each feature
- See the SIP mailing list (**listen** *until* you have sufficient knowledge to contribute)
- See the SIP Working Group for what is being worked on by others
- See “Guidelines for Authors of Extensions to the Session Initiation Protocol (SIP)” [71]

Gateways

- **Gateway Location Protocol** (GLP) - a protocol used between Location Server (LSs) {similar to BGP}
- **Signaling Gateway** - to convert from the signaling used in one network to that of the other
- **Media Gateway** - to convert the media format from that used in one network to that of the other

Significance

- In July 2002, 3GPP adopted SIP for their signalling protocol (Release5)
- 3GPP adops SIMPLE as instant messaging/presence mechanism (Release6)

While there are some differences between the 3GPP and IETF points of view

From Henning Schulzrinne, "SIP - growing up", SIP 2003, Paris, January 2003, slide 5.

3GPP	IETF
Network does not trust the user	User only partially trusts the network
layer 1 and layer 2 specific	generic
walled garden	open access

Not suprisingly the 3GPP system (called "IMS") for using SIP is rather complex with a number of new components: Proxy Call Session Control Function (P-CSFC), Interrogating Call Session Control Function (I-CSFC), Serving Call Session Control Function (S-CSFC), Home Subscriber Server (HSS), Application Server (AS), Subscription Locator Function (SLF), Breakout Gateway Control Function (BGCF), Media Gateway Control Function (MGCF), and Media Gateway (MGW)

P2P SIP

Peer-to-peer SIP

- http://www.p2psip.org/ (Last modified 2009)
- http://tools.ietf.org/wg/p2psip/ (most recent draft is 2013-07-13)

Using peer-to-peer techniques to create an overlay network of SIP entitites, rather than a fixed infrastructure of SIP registrars, proxies, etc.

Work in progress, with several implementations.

References and Further Reading

[61] VOIP-TELEPHONY.ORG, "Voice over IP (VoIP) IP Telephony, SIP, and ENUM resources",Webpage, 7 May 2008 http://www.voip-telephony.org/

[62] Multiparty Multimedia Session Control (mmusic) Working Group, Webpage, http://www.ietf.org/html.charters/mmusic-charter.html

SIP

[63] Session Initiation Protocol (SIP) Working Group, Webpage, http://www.ietf.org/html.charters/sip-charter.html

[64] Henning Schulzrinne's Session Initiation Protocol (SIP) web page http://www.cs.columbia.edu/sip/

[65] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, "SIP: Session Initiation Protocol", IETF, Network Working Group, RFC 2543, March 1999, Obsoleted by RFC 3261, RFC 3262, RFC 3263, RFC 3264, RFC 3265, http://datatracker.ietf.org/doc/rfc2543/

[66] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler,"SIP: Session Initiation Protocol", IETF, Network Working Group, RFC 3261, June 2002, Updated by RFC 3265, RFC 3853, RFC 4320, RFC 4916, RFC 5393, RFC 5621, RFC 5626, RFC 5630, RFC 5922, http://datatracker.ietf.org/doc/rfc3261/

[67] G. Camarillo, W. Marshall, J. Rosenberg, "Integration of Resource Management and Session Initiation Protocol (SIP)", IETF, Network Working Group, RFC 3312, October 2002, Updated by RFC 4032, RFC 5027, http://datatracker.ietf.org/doc/rfc3312/

[68] J. Rosenberg and H. Schulzrinne, "Reliability of Provisional Responses in the Session Initiation Protocol (SIP)", IETF, Network Working Group, RFC 3262, June 2002, http://datatracker.ietf.org/doc/rfc3262/

[69] D. Willis and B. Höneisen, "Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts", IETF, Network Working Group, RFC 3327, December 2002, Updated by RFC 5626, http://datatracker.ietf.org/doc/rfc3327/

[70] Henning Schulzrinne, “SIP - growing up”, SIP 2003, Keynote speech at SIP 2003, Paris, France, January 2003,

http://www.cs.columbia.edu/~hgs/papers/2003/SIP2003-keynote.ppt

[71] J. Rosenberg and H. Schulzrinne, “Guidelines for Authors of Extensions to the Session Initiation Protocol (SIP)”, IETF, Network Working Group, RFC 4485, May 2006, http://datatracker.ietf.org/doc/rfc4485/

[72] R. Sparks, “The Session Initiation Protocol (SIP) Refer Method”, IETF, Network Working Group, RFC 3515, April 2003,
http://datatracker.ietf.org/doc/rfc3515/

[73] R. Sparks, “The Session Initiation Protocol (SIP) Referred-By Mechanism”, IETF, Network Working Group, RFC 3892, September 2004,

http://datatracker.ietf.org/doc/rfc3892/

[74] B. Campbell (Editor), J. Rosenberg, H. Schulzrinne, C. Huitema, and D. Gurle, “Session Initiation Protocol (SIP) Extension for Instant Messaging”, IETF, Network Working Group, RFC 3428, December 2002,
http://datatracker.ietf.org/doc/rfc3428/

[75] J. Rosenberg, “The Session Initiation Protocol (SIP) UPDATE Method”, IETF, Network Working Group, RFC 3311, September 2002, http://datatracker.ietf.org/doc/rfc3311/

[76] A. Johnston, S. Donovan, R. Sparks, C. Cunningham, and K. Summers, “Session Initiation Protocol (SIP) Basic Call Flow Examples”, IETF, Network Working Group, RFC 3665, December 2003, Also Known As BCP 75, http://datatracker.ietf.org/doc/rfc3665/

[77] M. Garcia-Martin, C. Bormann, J. Ott, R. Price, and A. B. Roach, “The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp)”, IETF, Network Working Group, RFC 3485, February 2003, Updated by RFC 4896, http://datatracker.ietf.org/doc/rfc3485/

[78] G. Camarillo, “Compressing the Session Initiation Protocol (SIP)”, IETF, Network Working Group, RFC 3486, February 2003, Updated by RFC 5049, http://datatracker.ietf.org/doc/rfc3486/

[79] J. Rosenberg, “Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)”, IETF, Network Working Group, RFC 5627, October 2009, http://datatracker.ietf.org/doc/rfc5627/

[80] R. Sparks, “Problems Identified Associated with the Session Initiation Protocol’s (SIP) Non-INVITE Transaction”, IETF, Network Working Group, RFC 4321,January 2006, http://datatracker.ietf.org/doc/rfc4321/

[81] R. Sparks, “Actions Addressing Identified Issues with the Session Initiation Protocol’s (SIP) Non-INVITE Transaction”, IETF, Network Working Group, RFC 4320, January 2006, Updates RFC 3261, http://datatracker.ietf.org/doc/rfc4320/

[82] J. Peterson, “S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)”, IETF, Network Working Group, RFC 3853, July 2004, Updates RFC 3261, http://datatracker.ietf.org/doc/rfc3853/

[83] R. Mahy and D. Petrie, “The Session Initiation Protocol (SIP) "Join" Header”, IETF, Network Working Group, RFC 3911, October 2004, http://datatracker.ietf.org/doc/rfc3911/

ITU Services CS-1 and CS-2

[84] J. Lennox and H. Schulzrinne, and T. F. La Porta, "Implementing Intelligent Network Service with the Session Initiation Protocol, Technical Report, Columbia University, Department of Computer Science, CUCS-002-99, January 1999, http://www.cs.columbia.edu/~hgs/papers/cucs-002-99.pdf

[85] Study Group 11 of the International Telecommunications Union Telecommunications Standards Sector (ITU-T), ITU-T recommendation Q.1211: Introduction to Intelligent Network Capability Set 1, Annex B, March 1993, http://www.itu.int/rec/T-REC-Q.1211-199303-I

[86] Study Group 11 of the International Telecommunications Union Telecommunications Standards Sector (ITU-T), ITU-T recommendation Q.1221: Introduction to Intelligent Network Capability Set 2, September 1997, http://www.itu.int/rec/T-REC-Q.1221-199709-I

[87] J. Rosenberg and H. Schulzrinne, "A Framework for Telephony Routing over IP", IETF, Network Working Group, RFC 2871, June 2000, http://datatracker.ietf.org/doc/rfc2871/

[88] ETSI, “Human Factors (HF); Supplementary service codes for use in public network service”, Technical Report, European Telecommunications Standards Institute (ETSI), TR 102 083 V1.1.1, Sophia Antipolis, France, January 1999, 58 pages, ISBN 2-7437-2725-X

http://www.etsi.org/deliver/etsi_tr/102000_102099/102083/01.01.01_60/tr_102083v010101p.pdf

[89] ETSI, “Telecommunications Management Network (TMN); Q3 interface at the Access Network (AN) for fault and performance management of V5 interfaces and associated user ports; Part 1: Q3 interface specification”, Edition: 1.2.1, European Telecommunications Standards Institute (ETSI), ETSI EN 300 378-1, 1 October 1999, 73 pages.

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 4: Session Announcement Protocol (SAP)

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:31

Session Announcement Protocol (SAP)

Defined in RFC 2974 [90]

Primarily for **multicast** session announcement. It provides the session setup information to *prospective* participants.

Each SAP announcer periodically multicasts an announcement:

- to a well known multicast address on port 9875
  - IPv4 global scope sessions use multicast addresses in the range 224.2.128.0 - 224.2.255.255 - their SAP announcements are sent to 224.2.127.254
  - IPv4 administrative scope sessions using administratively scoped IP multicast are defined in [x], the multicast address to be used for announcements is the highest multicast address in the relevant administrative scope zone, e.g., if the scope range is 239.16.32.0 - 239.16.33.255, then SAP announcements use 239.16.33.255
  - IPv6 sessions are announced on the address FF0X:0:0:0:0:0:2:7FFE where X is the 4-bit scope value, e.g., an announcement for a link-local session assigned the address FF02:0:0:0:0:0:1234:5678, is advertised on SAP address FF02:0:0:0:0:0:2:7FFE
- has same scope as the session it is announcing (the use of TTL scoping for multicast is discouraged)
- IP time-to-live of 255

See also [91]

References and Further Reading

SAP

[90] M. Handley, C. Perkins, and E. Whelan, RFC 2974: Session Announcement Protocol, IETF, October 2000 http://www.ietf.org/rfc/rfc2974.txt

[91] H. Asaeda and V. Roca, Requirements for IP Multicast Session Announcement in the Internet, IETF, MBONED Working Group, Internet-Draft, March 8, 2010, **Expired**: September 9, 2010, draft-ietf-mboned-session-announcement-req-03
http://tools.ietf.org/html/draft-ietf-mboned-session-announcement-req-03

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

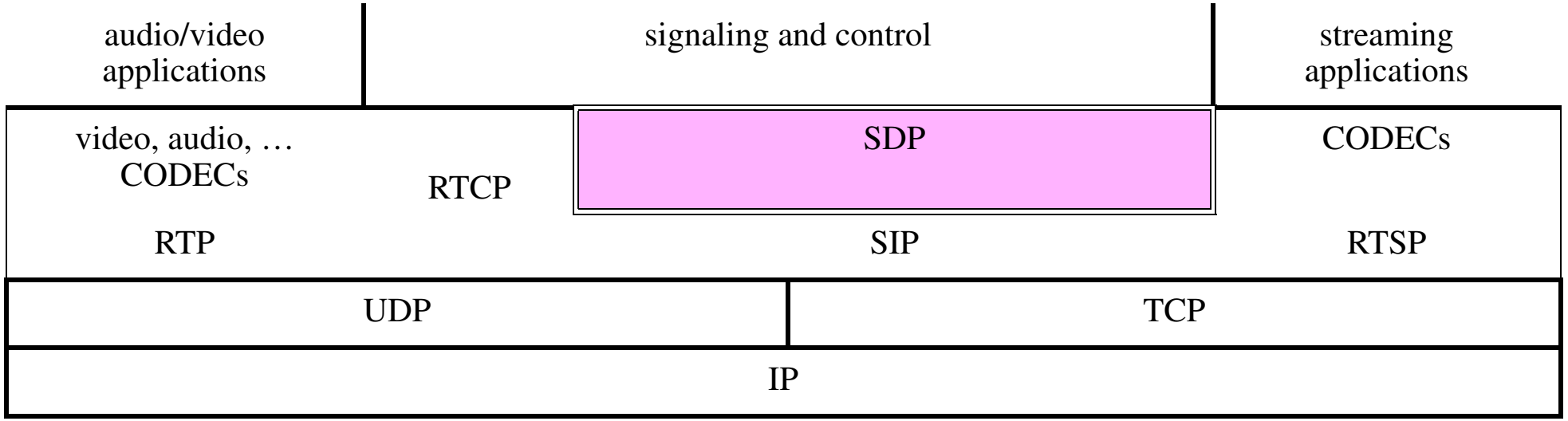
Module 5: Session Description Protocol (SDP)

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:31

Session Description Protocol (SDP)



Session Description Protocol (SDP)

Defined by RFC 2327 [92], later RFC 4566 [93]

- describes media session
- a text-based protocol
- carried in MIME as a message body in SIP messages
- uses RTP/AVP Profiles for common media types [104]

Note: It is more a session description **format** than a **protocol**.

- RFC 3264: An Offer/Answer Model with the Session Description Protocol (SDP) [98]
- RFC 3266: Support for IPv6 in Session Description Protocol [99]
- RFC 3388: Grouping of Media Lines in the Session Description Protocol [100]
- RFC 3407: Session Description Protocol Simple Capability Declaration [102]
- RFC 3485: The Session Initiation Protocol and Session Description Protocol Static Dictionary for Signaling Compression (SigComp) [120]
- RFC 3556: Session Description Protocol Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth [110]
- RFC 3605: Real Time Control Protocol (RTCP) attribute in Session Description Protocol [105]
- RFC 3890: A Transport Independent Bandwidth Modifier for the Session Description Protocol [117]

- RFC 4092: Usage of the Session Description Protocol: Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP) [113]
- RFC 4145: TCP-Based Media Transport in the Session Description Protocol [118]
- RFC 4317: Session Description Protocol Offer/Answer Examples [111]
- RFC 4567: Key Management Extensions for Session Description Protocol and Real Time Streaming Protocol (RTSP) [119]
- RFC 4568: Session Description Protocol Security Descriptions for Media Streams [114]
- RFC 4570: Session Description Protocol Source Filters [109]
- RFC 4572: Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol [121]
- RFC 4574: The Session Description Protocol Label Attribute [112]
- RFC 4579:Session Initiation Protocol Call Control - Conferencing for User Agents [122]
- RFC 4583: Session Description Protocol Format for Binary Floor Control Protocol (BFCP) Streams [123]
- RFC 4796: The Session Description Protocol Content Attribute [115]
- RFC 5027: Security Preconditions for Session Description Protocol (SDP) Media Streams [127]
- RFC 5049: Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP) [128]
- RFC 5112: The Presence-Specific Static Dictionary for Signaling Compression (Sigcomp) [129]
- RFC 5159: Session Description Protocol (SDP) Attributes for Open Mobile Alliance (OMA) Broadcast (BCAST) Service and Content Protection [130]
- RFC 5379: Guidelines for Using the Privacy Mechanism for SIP [131]
- RFC 5898: Connectivity Preconditions for Session Description Protocol (SDP) Media Streams [97]

- RFC 5939: SDP media capabilities Negotiation, now [95]
- RFC 5956: Forward Error Correction Grouping Semantics in the Session Description Protocol
- RFC 6064: SDP and RTSP Extensions Defined for 3GPP Packet-Switched Streaming Service and Multimedia Broadcast/Multicast Service
- RFC 6128: RTP Control Protocol (RTCP) Port for Source-Specific Multicast (SSM) Sessions
- RFC 6189: ZRTP: Media Path Key Agreement for Unicast Secure RTP
- RFC 6193: Media Description for the Internet Key Exchange Protocol (IKE) in the Session Description Protocol (SDP)
- RFC 6236: Negotiation of Generic Image Attributes in the Session Description Protocol (SDP)
- RFC 6332: Multicast Acquisition Report Block Type for RTP Control Protocol (RTCP) Extended Reports (XRs)
- RFC 6337: Session Initiation Protocol (SIP) Usage of the Offer/Answer Model
- RFC 6364: Session Description Protocol Elements for the Forward Error Correction (FEC) Framework
- RFC 6416: RTP Payload Format for MPEG-4 Audio/Visual Streams
- RFC6466: IANA Registration of the 'image' Media Type for the Session Description Protocol (SDP)
- RFC 6642: RTP Control Protocol (RTCP) Extension for a Third-Party Loss Report
- RFC 6849: An Extension to the Session Description Protocol (SDP) and Real-time Transport Protocol (RTP) for Media Loopback’
- RFC 6871: Session Description Protocol (SDP) Media Capabilities Negotiation
- …

SDP Message Details

```
v=0
o=Tesla 289084526 28904526 IN IP4 lab.high-voltage.org
s=-
c=IN IP4 100.101.102.103
t=0 0
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

- Version number (ignored by SIP)
- Origin (not used by SIP)
- Subject (ignored by SIP)
- Connection Data
  - connection: network (IN == Internet), Address type (IPv4), and Address
- Time (ignored by SIP): `start stop`
- Media (type, port, RTP/AVP Profile)
- Attribute (profile, CODEC, sampling rate)

Session description

```
v= protocol version
o= owner/creator and session identifier
s= session name
[i= session information]                          { [xx] ⇒ xx is optional}
[u= URI of description]
[e= email address]
[p= phone number]
[c= connection information- not required if included in all media]
[b= bandwidth information]
<Time description>+                               { <xx>+ ⇒ one or more times}
[z= time zone adjustments]
[k= encryption key]
[a= zero or more session attribute lines]*        { <xx>* ⇒ zero or more times}
<Media descriptions>*
```

Time description

```
t= time the session is active
[r= zero or more repeat times]*
```

Media description

```
m= media name and transport address
[i= media title]
[c= connection information-optional if included at session-level]
[b= bandwidth information]
[k= encryption key]
[a= zero or more media attribute lines]*
```

SDP Offer/Response Example

`v=0`	Version of SDP (0)
`o=`	Origin - not use by SIP
`c=IN IP4 130.237.212.6`	Connection INternet, IPv4, address=130.237.212.6
`t=`	Time - not use by SIP
`m=video 4004 RTP/AVP 14 26`	Media **Video**, port=4004, type=RTP/AVP profile, profiles: 14 and 26
`a=rtpmap:14 MPA/90000`	Attribute for profile 14, codec=MPA, sampling rate=90000
`a=rtpmap:26 JBEG/90000`	Attribute for profile 26, codec=JBEG, sampling rate=90000
`m=audio 4006 RTP/AVP 0 4`	Media **Audio**, port=4006, type=RTP/AVP profile, profiles: 0 and 4
`a=rtpmap:0 PCMU/8000`	Attribute for profile 0, codec=PCMU (PCM µlaw), sampling rate=8000
`a=rtpmap:4 GSM/8000`	Attribute for profile 4, codec=GSM, sampling rate=8000

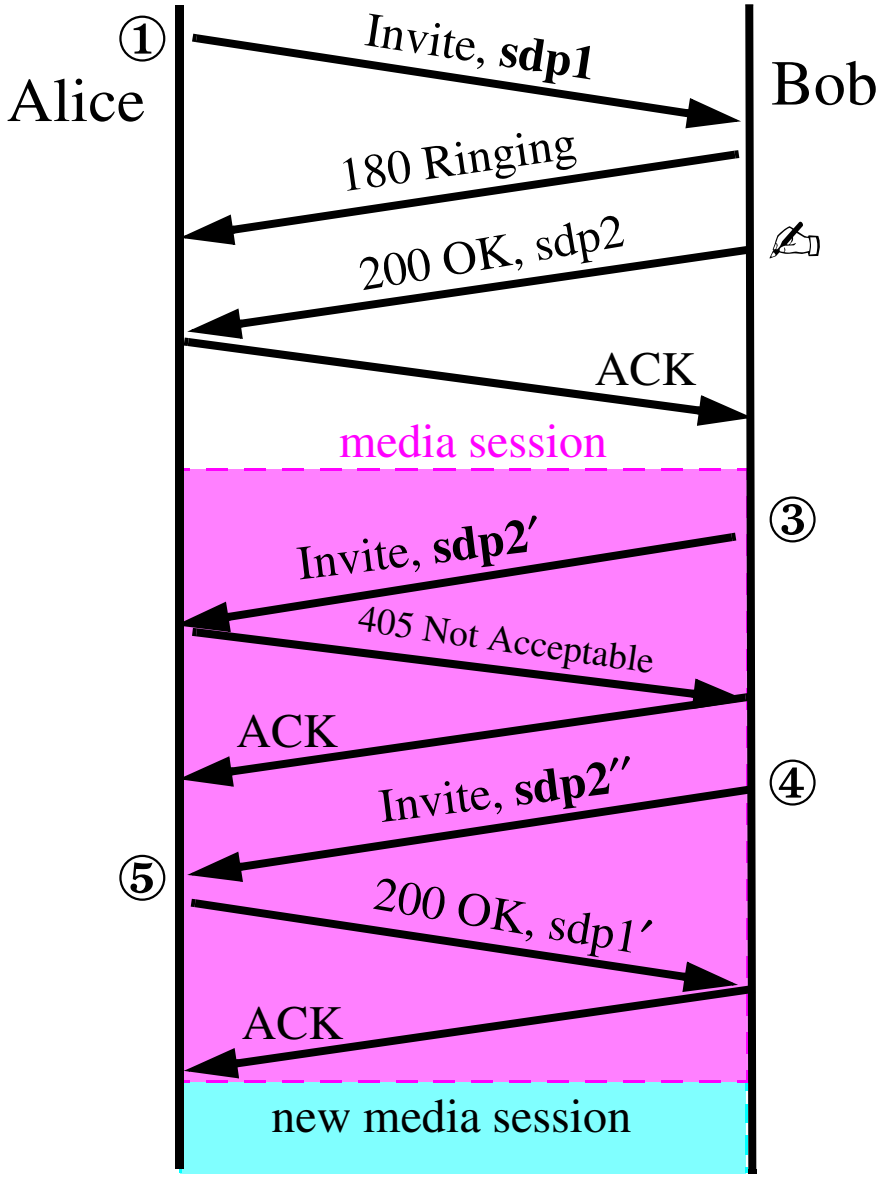
If the RTCP port is not the next port number, then an rtcp-attribute can be specified in the form [105] (this might be useful in conjunction with a NAT):

"a=rtcp:" port [nettype addrtype connection-address] <CRLF>

SDP Response Example

`v=0`	Version of SDP (0)
`o=`	Origin - not use by SIP
`c=IN IP4 130.237.21.87`	Connection INternet, IPv4, address=130.237.21.87
`t=`	Time - not use by SIP
`m=video 0 RTP/AVP 14`	Media **Video**, port=0, type=RTP/AVP profile, profiles: 14 Receiver declines the video, indicated by port = 0
`m=audio 6002 RTP/AVP 4`	Media **Audio**, port=6002, type=RTP/AVP profile, profiles: 4 Receiver declines the PCM coded audio and selects the GSM coded audio
`a=rtpmap:4 GSM/8000`	Attribute for profile 4, codec=GSM, sampling rate=8000

Session Modification



✝① Alice invite's Bob to a session with the parameters in sdp1

✍Bob's modified this in his response sdp2.

They communicate

③ Bob proposes a change in the session (sdp2′), Alice does not accept this change

④ Bob tries with a new proposal (sdp2″)

⑤ Alice accepts with the session description sdp1′

They communication with the new spec.

Session modification (continued)

- The re-`INVITE` could have been done by either party - it uses the same `To`, `From`, and `Call-ID` as the original `INVITE`.
- Note that the re-`INVITE`s do not cause a `180 Ringing` or other provisional messages, since communication between Alice and Bob is already underway.
- Note that the first media session continues despite the SIP signalling, until a new agreement has been reached - at which time the new media session replaces the former session.
- The re-INVITE can propose changes of any of the media characteristics, including adding or dropping a particular media stream.
  - this adding or dropping may be because the user has moved from one wireless cell to another, from one network to another, from one interface to another, from one device to another, …

Start and Stop Times

Enable the user to join a broadcast sessions during the broadcast.

Grouping of Media Lines in the Session Description Protocol (SDP)[100]

Defines two SDP attributes:

- "group" and
- "mid" - media stream identification

Allows grouping several media ("m") lines together. This is to support:

- Lip Synchronization (LS) and
- Flow Identification (FID) - a single flow (with several media streams) that are encoded in different formats (and may be received on different ports and host interfaces)
  - Changing between codecs (for example based on current error rate of a wireless channel)

Note FID does **not** cover the following (but SDP can -- see [100]):

- Parallel encoding using different codecs
- Layered coding

Lip Synchronization

Example adapted from section 6.1 of [100].

A session description of a conference that is being multicast. First and the second media streams MUST be synchronized.

```
v=0
o=Laura 289083124 289083124 IN IP4 one.example.com
t=0 0
c=IN IP4 224.2.17.12/127
a=group:LS 1 2
m=audio 30000 RTP/AVP 0
i=voice of the speaker who speaks in English
a=mid:1
m=video 30002 RTP/AVP 31
i=video component
a=mid:2
m=audio 30004 RTP/AVP 0
i=This media stream contains the Spanish translation
a=mid:3
```

Next generation of SDP (SDPng)

- Designed to address SDP's 'flaws':
  - Limited expressiveness
    - For individual media and combinations of media
    - Often only very basic media descriptions available -- desire for more complex media
  - No real negotiation functionality - as SDP today is a "take it or leave it" proposal
  - Limited extensibility (not nearly as easy to extend as SIP)
  - No semantics for media sessions! Sessions are only implicit.
- SDPng should avoid "second system syndrome"
  - Hence it **should** be simple, easy to parse, extensible, and have limited scope
  - Session Description and Capability Negotiation

SDPng structure

Uses XML syntax - example adapted from Appendix C in [108]:

```
<?xml version="1.0" encoding="UTF-8"?>
   <sdpng xmlns="http://www.iana.org/sdpng"
          xmlns:audio="http://www.iana.org/sdpng/audio"
          xmlns:video="http://www.iana.org/sdpng/video"3
          xmlns:rtp="http://www.iana.org/sdpng/rtp"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation="http://www.iana.org/sdpng       sdpng-base.xsd
                              http://www.iana.org/sdpng/audio sdpng-audio-pkg.xsd
                              http://www.iana.org/sdpng/video sdpng-video-pkg.xsd
                              http://www.iana.org/sdpng/rtp   sdpng-rtp-pkg.xsd"  >
   <cap><audio:codec name="avp:dvi4">
               <audio:encoding>DVI4</audio:encoding>
               <audio:channels>1</audio:channels>
               <audio:sampling>8000 11025 16000 22050</audio:sampling></audio:codec>
        <audio:codec name="avp:l16">
               <audio:encoding>L16</audio:encoding>
               <audio:channels>1 2</audio:channels>
               <audio:sampling>44100</audio:sampling></audio:codec>
        <video:codec name="avp:celb">
               <video:encoding>CelB</video:encoding>
               <video:framerate>4 6 8 12 16 20 24 30</video:framerate></video:codec>
        <rtp:udp name="rtpudpip6">
               <rtp:network>IP6</rtp:network></rtp:udp></cap>
   <def><rtp:udp name="rtp-cfg1" ref="rtpudpip6">
               <rtp:ip-addr>::1</rtp:ip-addr>
                <rtp:rtp-port>9546</rtp:rtp-port></rtp:udp></def>
   <cfg><component>
                <alt>
                     <audio:codec ref="avp:l16"/>
                     <rtp:udp ref="rtp-cfg1"><rtp:pt>0</rtp:pt></rtp:udp></alt></component></cfg></sdpng>
```

For details see appendices A.1 “SDPng Base DTD” and A.2 “SDPng XML-Schema Specification” in [108].

Why XML?

To: "Pete Cordell" <pete@tech-know-ware.com>, <confctrl@ISI.EDU>
Subject: RE: [sdp-ng] Encoding SDPng messages using UMF
From: "Christian Huitema" <huitema@windows.microsoft.com>
Date: Fri, 8 Jun 2001 09:39:27 -0700
Sender: owner-confctrl@ISI.EDU
Thread-Index: AcDvP1amHX72K047Suy+kTYzoya+iAA+DJxA
Thread-Topic: [sdp-ng] Encoding SDPng messages using UMF

[note: paragraphs reformatted to fit on slide]

If, at this date and time, you want to not use XML, then you need an extremely strong case. XML is well understood, there are many support tools, and many more are in development. The W3C is producing a schema description language which is considered adequate for many business applications, many of which are way more complex than SDP.

The talks about ASN.1 are just that -- talks. The only possible advantage of ASN.1 is the size of the messages, but even that is debatable. On the other hand, the cost is very well known: you need specialized parsers and libraries, you cannot easily use text tools for debugging or monitoring purposes, and the syntax is hard to understand and a pain to extend. Most of the proponents of ASN.1 actually propose some variation of it, which is even worse, since it would require even more specific tools.

The main inconvenient of XML is that it can be bulky. I am not convinced that this is an actual problem: SDP is used for describing multimedia sessions, that normally last a few minutes and carry at a minimum several tens of kilobytes of media; the media stream dwarfs the signaling stream by orders of magnitude. If it is an actual problem, then we can indeed use compression. In fact, we can safely assume that other applications will be hurt before us, and that we will get generic XML compression tools sooner or later. All in all, that should not be a big problem.

Let's not be silly. Just pick XML.

-- Christian Huitema

http://bmrc.berkeley.edu/mhonarc/openmash-developers/msg00315.html

SDP today

SDPng petered out with : Dirk Kutscher, Joerg Ott, Carsten Bormann, Session Description and Capability Negotiation, Internet-Draft, February 20, 2005, Expires: August 21, 2005, draft-ietf-mmusic-sdpng-08.txt,

http://tools.ietf.org/html/draft-ietf-mmusic-sdpng-08

SDP is still evolving in IETF drafts from the IETF, MMUSIC Working Group:

- M. Handley, V. Jacobson, C.S. Perkins, and A. Begen, SDP: Session Description Protocol, Network Working Group, Internet-Draft, March 11, 2013, Expires: September 12, 2013, draft-ietf-mmusic-rfc4566bis-08

  http://datatracker.ietf.org/doc/draft-ietf-mmusic-rfc4566bis/

- B. Greevenbosch, Hitchhiker's guide to the Session Description Protocol (SDP), Internet-Draft, mmusic, July 5, 2012, Expired: January 6, 2013, draft-greevenbosch-mmusic-hitchhikersguide-sdp-01

  http://datatracker.ietf.org/doc/draft-greevenbosch-mmusic-hitchhikersguide-sdp/

- P. Capelastegui, 3D Video in the Session Description Protocol (SDP), Internet-Draft, mmusic, April 30, 2012, Expired: November 1, 2012, draft-capelastegui-mmusic-3dv-sdp-00

  http://tools.ietf.org/html/draft-capelastegui-mmusic-3dv-sdp-00
- B. Greevenbosch and Y. Hui, Signal 3D format, Internet-Draft, mmusic, April 9, 2012, Expired: October 11, 2012, draft-greevenbosch-mmusic-sdp-3d-format-00

  https://datatracker.ietf.org/doc/draft-greevenbosch-mmusic-sdp-3d-format/
- B. Greevenbosch and Y. Hui, SDP attribute to signal parallax, Internet-Draft, mmusic, April 9, 2012, Expired: October 11, 2012, draft-greevenbosch-mmusic-sdp-parallax-00

  http://datatracker.ietf.org/doc/draft-greevenbosch-mmusic-sdp-parallax/
- I. Curcio, R. Walsh, J. Peltotalo, S. Peltotalo, and H. Mehta, SDP Descriptors for FLUTE, Internet-Draft, RMT, March 12, 2012, Expired: September 13, 2012, draft-ietf-rmt-flute-sdp-02

  http://www.ietf.org/id/draft-ietf-rmt-flute-sdp-02.txt

- T. Frankkila, M. Westerlund, and B. Burman, Extensible Bandwidth Attribute for SDP, Internet-Draft, MMUSIC Working Group, July 16, 2012, Expired: January 17, 2013, draft-westerlund-mmusic-sdp-bw-attribute-02

  http://www.ietf.org/id/draft-westerlund-mmusic-sdp-bw-attribute-02.txt

- V. Singh, J. Ott, T. Karkkainen, R. Globisch, and T. Schierl, Multipath RTP (MPRTP) attribute in Session Description Protocol, Internet-Draft, MMUSIC Working Group, July 14, 2013, Expires: January 15, 2014 , draft-singh-mmusic-mprtp-sdp-extension-02

  http://tools.ietf.org/html/draft-singh-mmusic-mprtp-sdp-extension-02

- A. Romanow, F. Andreasen, and A. Krishna, Investigation of Session Description Protocol (SDP) Usage for ControLling mUltiple streams for tElepresence (CLUE), Internet-Draft, CLUE, September 11, 2012, Expired: March 15, 2013, draft-romanow-clue-sdp-usage-02

  http://tools.ietf.org/html/draft-romanow-clue-sdp-usage-02

- S. Loreto and G. Camarillo, Stream Control Transmission Protocol (SCTP)-Based Media Transport in the Session Description Protocol (SDP), Internet-Draft, MMUSIC, June 30, 2013, Expires: January 1, 2014, draft-ietf-mmusic-sctp-sdp-04

  http://datatracker.ietf.org/doc/draft-ietf-mmusic-sctp-sdp/

- C. Holmberg, H. Alvestrand, and C. Jennings, Multiplexing Negotiation Using Session Description Protocol (SDP) Port Numbers, MMUSIC Working Group, Internet-Draft, June 14, 2013, Expires: December 16, 2013, draft-ietf-mmusic-sdp-bundle-negotiation-04.txt,

  http://tools.ietf.org/html/draft-ietf-mmusic-sdp-bundle-negotiation-04

- M. Garcia-Martin and S. Veikkolainen, Session Description Protocol (SDP) Extension For Setting Up Audio and Video Media Streams Over Circuit-Switched Bearers In The Public Switched Telephone Network (PSTN), Internet-Draft, MMUSIC WG, June 26, 2013, Expires: December 28, 2013, draft-ietf-mmusic-sdp-cs-21,

  http://tools.ietf.org/html/draft-ietf-mmusic-sdp-cs-21

- M. Garcia-Martin, S. Veikkolainen, and R. Gilman, Miscellanoues Capabilities Negotiation in the Session Description Protocol (SDP), Internet-Draft, MMUSIC WG, July 10, 2013, Expires: January 11, 2014, draft-ietf-mmusic-sdp-miscellaneous-caps-07

  http://tools.ietf.org/html/draft-ietf-mmusic-sdp-miscellaneous-caps-07

- James Polk, Subha Dhesikan, and Paul Jones, The Session Description Protocol (SDP) 'trafficclass' Attribute, Internet-Draft, Network WG, July 14, 2013, Expires: January 14, 2014, draft-ietf-mmusic-traffic-class-for-sdp-04

  http://tools.ietf.org/html/draft-ietf-mmusic-traffic-class-for-sdp-04

- A. Begen, Y. Cai, and H. Ou, Delayed Duplication Attribute in the Session Description Protocol, MMUSIC, Internet-Draft, May 27, 2013, Expires: November 28, 2013, draft-ietf-mmusic-delayed-duplication-02, *http://datatracker.ietf.org/doc/draft-ietf-mmusic-delayed-duplication/*
- A. Begen, Y. Cai, and H. Ou, Duplication Grouping Semantics in the Session Description Protocol, MMUSIC, Internet-Draft, July 11, 2013, Expires: January 12, 2014, draft-ietf-mmusic-duplication-grouping-03

  http://datatracker.ietf.org/doc/draft-ietf-mmusic-duplication-grouping/

- H. Alvestrand, Cross Session Stream Identification in the Session Description Protocol, Network Working Group, Internet-Draft, August 13, 2013, Expires: February 14, 2014, draft-ietf-mmusic-msid-01

  http://datatracker.ietf.org/doc/draft-ietf-mmusic-msid/

- R. Even, J. Lennox, and Q. Wu, The Session Description Protocol (SDP) Application Token Attribute, MMUSIC WG, Internet-Draft, June 28, 2013, Expires: December 30, 2013, draft-even-mmusic-application-token-00.txt

  http://datatracker.ietf.org/doc/draft-even-mmusic-application-token/

- R. Gellens, Negotiating Human Language Using SDP, MMUSIC Working Group, Internet-Draft, July 14, 2013, Expires: January 13, 2014, draft-gellens-mmusic-negotiating-human-language-01

  http://datatracker.ietf.org/doc/draft-gellens-mmusic-negotiating-human-language/

- S. Nandakumar, A Framework for SDP Attributes when Multiplexing, Network Working Group, Internet-Draft, July 15, 2013, Expires: January 16, 2014, draft-nandakumar-mmusic-sdp-mux-attributes-03

  http://datatracker.ietf.org/doc/draft-nandakumar-mmusic-sdp-mux-attributes/

- A. B. Roach, J. Uberti, and M. Thomson, A Unified Plan for Using SDP with Large Numbers of Media Flows, Network Working Group, Internet-Draft, July 15, 2013, Expires: January 16, 2014, draft-roach-mmusic-unified-plan-00

  http://datatracker.ietf.org/doc/draft-roach-mmusic-unified-plan/

- V. Singh, J. Ott, T. Karkkainen, R. Globisch, and T. Schierl, Multipath RTP (MPRTP) attribute in Session Description Protocol, MMUSIC Working Group, Internet-Draft, July 14, 2013, Expires: January 15, 2014, draft-singh-mmusic-mprtp-sdp-extension-02

  http://datatracker.ietf.org/doc/draft-singh-mmusic-mprtp-sdp-extension/

- C.H. Holmberg, M.W. Westerlund, B.B. Burman, and F.J. Jansson, Multiple Synchronization Sources (SSRC) in SDP Media Descriptions, Network Working Group, Internet-Draft, March 27, 2013, Expires: September 28, 2013, draft-westerlund-mmusic-max-ssrc-01.txt

  http://datatracker.ietf.org/doc/draft-westerlund-mmusic-max-ssrc/

…

https://datatracker.ietf.org/doc/search/?name=SDP&rfcs=on&activeDrafts=on&search_submit=

QoS and SDP

"The offer/answer model [RFC3264] for SDP [RFC4566] does not provide any mechanism for endpoints to negotiate the QoS mechanism to be used for a particular media stream. Even when QoS preconditions [RFC3312] are used, the choice of the QoS mechanism is left unspecified and is up to the endpoints.

Endpoints that support more than one QoS mechanism need a way to negotiate which one to use for a particular media stream. Examples of QoS mechanisms are RSVP (Resource Reservation Protocol) [RFC2205] and NSIS (Next Steps in Signaling) [QoS-NSLP]."

RFC 5432: Quality of Service (QoS) Mechanism Selection in the Session Description Protocol (SDP)[116] published in March 2009

Introduces `qos-mech-send` and `qos-mech-recv` attributes for SDP.

Writing code to deal with SDP

Jesper A Nielsen ha written a very informative web page “Introduction to SDP for Java, C# and VB Developers” [126]

References and Further Reading

SDP

[92] M. Handley and V. Jacobson, "SDP: Session Description Protocol", IETF, Network Working Group, RFC 2327, April 1998, Obsoleted by RFC 4566,

http://datatracker.ietf.org/doc/rfc2327/

[93] M. Handley, V. Jacobson, and C. Perkins, SDP: Session Description Protocol, IETF, Network Working Group, RFC 4566, July 2006, Obsoletes RFC 2327 and RFC 3266, http://www.ietf.org/rfc/rfc4566.txt

[94] R. Gilman, R. Even, F. Andreasen, SDP Media Mapabilities Negotiation, IETF, MMUSIC Working Group, Internet-Draft, February 28, 2011, Expires: September 1, 2011,

http://tools.ietf.org/html/draft-ietf-mmusic-sdp-media-capabilities-11

[95] F. Andreasen, Session Description Protocol (SDP) Capability Negotiation, Internet Request for Comments, ISSN 2070-1721, RFC 5939, RFC Editor, September 2010, http://www.rfc-editor.org/rfc/rfc5939.txt

[96] K. Hedayat, N. Venna, P. Jones, A. Roychowdhury, C. SivaChelvan, and N. Stratton, "An Extension to the Session Description Protocol (SDP) for Media Loopback", IETF, MMUSIC Working Group, IETF Draft, 11 March 2011, Expires: September 11, 2011, http://tools.ietf.org/html/draft-ietf-mmusic-media-loopback-15

[97] F. Andreasen, G. Camarillo, D. Oran, and D. Wing, Connectivity Preconditions for Session Description Protocol (SDP) Media Streams, Internet Request for Comments, ISSN 2070-1721, RFC 5898, RFC Editor, July 2010, http://www.rfc-editor.org/rfc/rfc5898.txt

[98] J. Rosenberg and H. Schulzrinne, "An Offer/Answer Model with SDP", IETF, Network Working Group, RFC 3264, June 2002, Obsoletes RFC 2543, http://datatracker.ietf.org/doc/rfc3264/

[99] S. Olson, G. Camarillo, and A. B. Roach, "Support for IPv6 in SDP", IETF, Network Working Group, RFC 3266, June 2002, Obsoleted by RFC 4566, http://datatracker.ietf.org/doc/rfc3266/

[100] G. Camarillo, G. Eriksson, J. Holler, and H. Schulzrinne, Grouping of Media Lines in the Session Description Protocol (SDP), IETF RFC 3388, December 2002 http://www.ietf.org/rfc/rfc3388.txt

[101]G. Camarillo and H. Schulzrinne, “The SDP (Session Description Protocol) Grouping Framework”, IETF, Network Working Group, RFC 5888, June 2010, Obsoletes RFC 3388, http://datatracker.ietf.org/doc/rfc5888/

[102]F. Andreasen, Session Description Protocol (SDP) Simple Capability Declaration, IETF RFC 3407, October 2002. http://www.ietf.org/rfc/rfc3407.txt

[103]A. Li, “Forward Error Correction Grouping Semantics in Session Description Protocol”, IETF, Network Working Group, RFC 4756, November 2006, http://datatracker.ietf.org/doc/rfc4756/

[104] S. Casner and P. Hoschka, "‘‘MIME Type Registration of RTP Payload Formats", IETF RFC3555, July 2003 ftp://ftp.rfc-editor.org/in-notes/rfc3555.txt

[105]C. Huitema, "Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)", IETF RFC 3605, October 2003

http://www.ietf.org/rfc/rfc3605.txt

[106]G. Camarillo and A. Monrad, "Mapping of Media Streams to Resource Reservation Flows", IETF RFC 3524, April 2003 http://www.ietf.org/rfc/rfc3524.txt

[107]M. Handley, V. Jacobson, and C. Perkins, SDP: Session Description Protocol, Internet Request for Comments, ISSN 2070-1721, RFC 4566, RFC Editor, July 2006, http://www.rfc-editor.org/rfc/rfc4566.txt

[108] Dirk Kutscher, Jörg Ott, and Carsten Bormann, "Session Description and Capability Negotiation", IETF Internet-Draft, February 20, 2005, Expired: August 21, 2005 http://www.ietf.org/internet-drafts/draft-ietf-mmusic-sdpng-08.txt

[109]B. Quinn and R. Finlayson, "Session Description Protocol (SDP) Source Filters", IETF, RFC 4570, July 2006 http://www.ietf.org/rfc/rfc4570.txt

[110]S. Casner, "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth", IETF, RFC 3556, July 2003 http://www.ietf.org/rfc/rfc3556.txt

[111]A. Johnston and R. Sparks, "Session Description Protocol (SDP) Offer/Answer Examples", IETF, RFC 4317, December 2005

[112]O. Levin and G. Camarillo, "The Session Description Protocol (SDP) Label Attribute", RFC 4574, August 2006

[113]G. Camarillo and J. Rosenberg, “Usage of the Session Description Protocol (SDP): Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)”, IETF, RFC 4092, June 2005

[114]F. Andreasen, M. Baugher, and D. Wing, “Session Description Protocol (SDP) Security Descriptions for Media Streams”, IETF, RFC 4568, July 2006 http://www.ietf.org/rfc/rfc4568.txt

[115]J. Hautakorpi and G. Camarillo, “The Session Description Protocol (SDP) Content Attribute”, IETF, RFC 4796, February 2007

http://www.ietf.org/rfc/rfc4796.txt

[116]James Polk, Subha Dhesikan, and Gonzalo Camarillo, Quality of Service (QoS) Mechanism Selection in the Session Description Protocol (SDP), IETF, Network Working Group, RFC 5432, March 2009

http://tools.ietf.org/html/rfc5432

[117]M. Westerlund, A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP), Internet Request for Comments, RFC Editor, RFC 3890 (Proposed Standard), ISSN 2070-1721, September 2004 http://www.rfc-editor.org/rfc/rfc3890.txt

[118]D. Yon and G. Camarillo, TCP-Based Media Transport in the Session Description Protocol (SDP), Internet Request for Comments, RFC Editor, RFC 4145 (Proposed Standard), ISSN 2070-1721, September 2005, Updated by RFC 4572 http://www.rfc-editor.org/rfc/rfc4145.txt

[119]J. Arkko, F. Lindholm, M. Naslund, K. Norrman, and E. Carrara, Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP), Internet Request for Comments, RFC Editor, RFC 4567 (Proposed Standard), ISSN 2070-1721, July 2006

http://www.rfc-editor.org/rfc/rfc4567.txt

[120] M. Garcia-Martin, C. Bormann, J. Ott, R. Price, and A. B. Roach, The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp), Internet Request for Comments, RFC Editor, RFC 3485 (Proposed Standard), ISSN 2070-1721, February 2003, Updated by RFC 4896 [124]

http://www.rfc-editor.org/rfc/rfc3485.txt

[121] J. Lennox, Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP), Internet Request for Comments, RFC Editor, RFC 4572 (Proposed Standard)", ISSN 2070-1721, July 2006 http://www.rfc-editor.org/rfc/rfc4572.txt

[122] A. Johnston and O. Levin, Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents, Internet Request for Comments, RFC Editor, RFC 4579 (Best Current Practice), ISSN 2070-1721, August 2006

http://www.rfc-editor.org/rfc/rfc4579.txt

[123] G. Camarillo, Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams, Internet Request for Comments, RFC Editor, RFC 4583 (Proposed Standard), ISSN 2070-1721, November 2006

http://www.rfc-editor.org/rfc/rfc4583.txt

[124] H. Eland, R. Mundy, S. Crocker, and S. Krishnaswamy, Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover, Internet Request for Comments, RFC Editor, RFC 4986 (Informational), August 2007 http://www.rfc-editor.org/rfc/rfc4986.txt

[125]L. Yang and G. Mayer, Session Description Protocol (SDP) Extension for a SIP Connection, Internet-Draft, IETF Network Working Group, June 24, 2010, Expired: December 26, 2010

http://tools.ietf.org/html/draft-yang-dispatch-sip-connection-address-type-01

[126]Jesper A Nielsen, Introduction to SDP for Java, C# and VB Developers, The Code Project, 30 Jul 2010 http://www.codeproject.com/KB/IP/SDPIntroduction.aspx

[127]F. Andreasen and D. Wing, Security Preconditions for Session Description Protocol (SDP) Media Streams, Internet Request for Comments, ISSN 2070-1721, RFC 5027, RFC Editor, October 2007,

http://www.rfc-editor.org/rfc/rfc5027.txt

[128]C. Bormann, Z. Liu, R. Price, and G. Camarillo, Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP), Internet Request for Comments, ISSN 2070-1721, RFC 5049, RFC Editor, December 2007, http://www.rfc-editor.org/rfc/rfc5049.txt

[129]M. Garcia-Martin, The Presence-Specific Static Dictionary for Signaling Compression (Sigcomp), Internet Request for Comments, ISSN 2070-1721, RFC 5112, RFC Editor, January 2008, http://www.rfc-editor.org/rfc/rfc5112.txt

[130]L. Dondeti and A. Jerichow, Session Description Protocol (SDP) Attributes for Open Mobile Alliance (OMA) Broadcast (BCAST) Service and Content Protection, Internet Request for Comments, ISSN 2070-1721, RFC 5159, RFC Editor, March 2008, http://www.rfc-editor.org/rfc/rfc5159.txt

[131]M. Munakata, S. Schubert, and T. Ohba, Guidelines for Using the Privacy Mechanism for SIP, Internet Request for Comments, ISSN 2070-1721, RFC 5379, RFC Editor, February 2010, http://www.rfc-editor.org/rfc/rfc5379.txt

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 6: DNS and ENUM

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:31

Telephony URL and Phone-Context

SIP URIs include Telephony URLs [154].

A Telephony URL looks like:

```
tel: +358-555-1234567  a telephone terminal
fax: +358-555-1234567  a fax machine
```

Digit seperators of "-" or "." are ignored.

A Phone-Context sets the conditions under which the number can be used, e.g.

```
tel: 1-800-555-1234;phone-content:+1 972
```

- a phone number that can only valid within North America (+1) and within the 972 exchange
- the absense of the "+" in the telephone number indicates that this is a local number, rather than a global number -- but the interpretation of these local numbers is problematic (i.e.,there is no assured geographic area **nor** can one depend on 7 digit numbers being local to a Class 5 exchange {the traditional case in North America}) $\Rightarrow$ a proposal to deprecate the use of unqualified local digit strings see [147].

ITU-T E.164

The ITU E.164[132] standard defines the international numbering plan for telephony and related documents list the delegation (allocation of numbers) from this number space[133].

Note that in most countries only telecommunications operators are allocated blocks of numbers, while countries or regions are allocated their country/area prefix by the ITU.

Recommended maximum number of digits is 15. The format is typically:

- Country Code (CC) - 1 to 3 digits
- Identification Code (x) - 1 to 4 digits
- Subscriber Number - 15 - (CC+x) digits

SIP URL

SIP URL used in SIP messages to indicate: originator (From), current destination (Request-URI), final destination (To), and redirection address (Contact)

Examples:

sip:firstname.lastname@company.com	simple example
sip:+1-212-555-1212@gateway.com;user=phone	a call from the Internet to the PSTN E.164 phone number (user=phone is not necessary, but just a hint to parsers that it is a numeric phone number)
sips:+1-212-555-1212@gateway.com;user=phone	a call from the Internet to the PSTN E.164 phone number - the SIP messages should be passd via TLS
sip:+1-212-555-1212@proxy.gateway.com;user=phone	proxy server determines gateway and forwards the request
sip:firstname.lastname@registrar.com;method=register	to register a user at a SIP registrar

ENUM

IETF's E.164 Number Mapping standard uses Domain Name Server (DNS) to map standard International Telecommunication Union (ITU-T) international public telecommunications numbering plan (E.164) telephone numbers to a list of Universal Resource Locators (URL). SIP uses these URL's to initiate sessions.

For example, ENUM DNS [140] converts a telephone number in E.164 format, e.g. +46812345, and returns e.g., a Universal Resource Identifier (URI) SIP:olle.svenson@telia.se

Thus a SIP client makes a connection to the SIP gateway telia.se passing the local part olle.svenson.

ENUM can return a wide variety of URI types.

RFC 3761: The E.164 to URI DDDS Application (ENUM)[141] updates the ENUM specification to be compatible with the Dynamic Delegation Discovery System (DDDS) Application specification in RFC 3401 [135].

In March 2011, RFC 6116: The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM) [142] obsoleted RFC361.

For details of Dial Sequences and Global Switched Telephone Network (GSTN) see [145]. {Dial Sequences include pauses and other signalling in addition to the phone number}

Note that ENUM maintains the nation-state “ownership” of E.164 numbers.

Note there are discussions about adding *virtual* E.164 numbers, see [176].

Why bother with ENUM? {see [149]}

- In order for PSTN/IDSN user to call VoIP users, there must be a way of translating an E.164 number to some way of reach the VoIP user.
  - Since the PSTN user only has a telephone dialing pad - this limits what they can enter (for example '+' entered as '*').
  - However, due to ITU-T Rec. E.105 [152] -- this means that VoIP become a part of the global public telephony service -- hence this translation has to follow at least some of the ITU rules
  - Which gateway should be used?
- For VoIP users to call a PSTN/ISDN user, caller needs to do an ENUM lookup and utilize a VoIP to PSTN/ISDN gateway
  - Which gateway? Can the called user opt-in or opt-out of having calls from the Internet?
- VoIP caller to VoIP callee when the caller dials an E.164 number
  - Does it get routed to the PSTN and back? {I.e., going through two VoIP gateways!}
- Use of Geographic numbers for fixed VoIP terminals
  - easily enables 911 like services for their terminals too
- (Global | National) [non-geographic] personal numbers
  - A personal or global or national number - which can be your single number
- …

One problem is that IP communications is **not** simply IP Telephony, it is VoIP **+** Chat **+** Instant Messaging + Video + … .

DNS

Scales well (due to caching)

ENUM typically uses a 3 layer hierarchy

- Tier 0: ENUM Root Level
  - Top level domain for telephone numbers is: **e164.arpa**
  - DNS look up to find the country for a specific E.164-Country Code (CC)
  - Manager: IAB; Registry: RIPE NCC; Registrar: ITU TSB .e164.arpa
- Tier 1: ENUM CC Level - DNS look up to find the ENUM subscribers
  - Manager: ITU Member State; Registry: choice of Manager; ENUM Registrar: national choice
  - swedish example: 6.4.e164.arpa - registry: NIC-SE (as of 13 Dec. 2002)
- Tier 2: ENUM E.164 Number Level
  - DNS stores a list over different internet based addresses (URIs) in NAPTR records
  - Thus a look up $\Rightarrow$ a list over different internet based addresses associated with each E.164-number
  - Manager: E.164-subscriber; DNS Service Provider: choice of Manger

For details see RFC 3761 ([141] replaced RFC 2916[140]) and RFCs 3401, 3402, 3403, 3404 ([135] to [138] replaced RFC 2915[134]).

NAPTR - Naming Authority Pointer [134]

(As of 2013.08.31) with nslookup:

```
> set querytype=NAPTR
> e164.arpa
Authoritative answers can be found from:e164.arpa
  origin = pri.authdns.ripe.net
  mail addr = dns.ripe.net
  serial = 1373405926
  refresh = 3600
  retry = 600
  expire = 864000
  minimum = 7200
```

With dig `e164.arpa`:

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46745
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;e164.arpa.  IN A
;; AUTHORITY SECTION:
e164.arpa.  3600 IN SOA pri.authdns.ripe.net. dns.ripe.net.
1373405926 3600 600 864000 7200
;; Query time: 49 msec
;; SERVER: 130.237.216.10#53(130.237.216.10)
;; WHEN: Sat Aug 31 15:38:27 2013
;; MSG SIZE  rcvd: 87
```

To find the DNS names for a specific E.164 number

Procedure is:

- Write the E.164 number in its full form, including the countrycode IDDD. Example: +46-8-9761234
- Remove all non-digit characters with the exception of the leading '+'. Example: +4689761234
- Remove all characters with the exception of the digits. Example: 4689761234
- Put dots (".") between each digit. Example: 4.6.8.9.7.6.1.2.3.4
- Reverse the order of the digits. Example: 4.3.2.1.6.7.9.8.6.4
- Append the string ".e164.arpa" to the end. Example: 4.3.2.1.6.7.9.8.6.4.e164.arpa
- Ask the DNS it returns:
  - mailto: foo@kth.se
  - sip: foo@kth.se
  - …

ENUM Services

- NetNumber (www.netnumber.com)
- Neustar (www.neustar.biz)

The ITU-T "List of ITU-T Recommendation E.164 Assigned Country Codes" as of 1 February 2004 can be found at: http://www.itu.int/itudoc/itu-t/ob-lists/icc/e164_763.html

The RIPE list of e-mail concerning the European assignment of ENUMs can be found at http://www.ripe.net/enum/request-archives/

For a summary of the status of ENUM deployment in December 2003 - see [143] and the Post- och telestyrelsen (PTS) final report of 2004 [144]. Leading to the formation of the ENUM Forum - this dissolved in 2008.

For the current status of ENUM according to RIPE's ENUM working group see:

http://enumdata.org/ .

For a summary of the IANA assignments for ENUM services see [164] .. [166].

ENUM Timeline

Sept. 2000	IETF ENUM WG produced RFC2916
2001	Various Workshops (ITU-T, Europe, US, …) to spread the idea
	Swedish PTS releases first ENUM report in April 2001
2002	ITU-T Interim Procedures (IAB, RIPE-NCC)
	ETSI SPAN11 TS "ENUM Administration in Europe"
2003	ETSI SPAN11 TS "Minimum Requirements for Interoperability of European ENUM Trials"
	IETF RFC2916bis
	National and international ENUM Trials using: ♦ different scenarios and numbering resources ♦ different ENUM-enabled products ♦ Swedish PTS releases their ENUM report on 31 July 2003; trial to continue until May 2004, final report due 30 June 2004 (see [156] and [157])
2004	ENUM considered ready for production ⇒ commercial deployments

The IAB instructions regarding ENUM to the RIPE NCC (to whom they had delegated e164.arpa) can be found at: http://www.ripe.net/enum/instructions.html

Sweden ENUM status is described at [148].

Interesting open questions (as described in [148]):

- Should the state have a permanent **operational** role (as opposed to simply an administrative role)
  - important that the subscriber with a given E.164 number also control the associated ENUM domain name {Who is responsible for maintaining this synchronization and validating changes?}
- Who finances the Tier 1 registry?
- Need for regulations? Self-regulation? …
- Privacy: need E.164 subscriber's permission to list them in the DNS
- Are there business opportunities?
- Will ENUM be successful?
- …

Sweden's ENUM Mapping

Approved by ITU TSB on Fri, 29 Nov 2002 12:03:02 +0100

```
Domain Object
domain:          6.4.e164.arpa
descr:           Swedish ENUM Mapping
admin-c:         PTSE46-RIPE
tech-c:          SE194-RIPE
zone-c:          SE194-RIPE
nserver:         a.ns.6.4.e164.arpa
nserver:         b.ns.6.4.e164.arpa
nserver:         c.ns.6.4.e164.arpa
nserver:         d.ns.6.4.e164.arpa
…
Administrative Contact
role:            ENUM Tier 1 Manager
address:         National Post and Telecom Agency
address:         Box 5398
address:         SE-102 49 Stockholm
address:         Sweden
phone:           +46 8 678 55 69
fax-no:          +46 8 678 55 05
e-mail:          pts-enum-admin@localhost
trouble:         enum-test-admin@localhost
nic-hdl:         PTSE46-RIPE
…
```

ENUM in Sweden

The EU directive on number portability means that there will **not** be a separate number space for IP telephony (as users are free to take their number with them from their existing telephony operator to a new operator - who could operate a different type of network: mobile, IP telephony, analog TDM over copper, etc.).[159]

Note that Joakim Strålmark's "Förstudie - Nummerportabilitet för framtida nät, och i samverkan med befintliga nät med aspekter på samtrafik, ENUM och den centrala referensdatabasen" [159] provides an excellent description (in Swedish) of how ENUM works.

Declining interest in “geographic” numbers

An interesting side effect of mobile telephony and IP telephony is that the concept of an “area code” (“riktnummer”) seems to be disappearing[171] - as associating a number with where you “lived” at the time you were assigned the number does not seem to have much meaning. What does this imply in the scope of EU personal mobility? For example, will country codes be replaced by a new region or global code?

Interestingly use of the European Telephony Numbering Space (ETNS) (+388 numbers) ended at the end of 2009, and the number allocation is to be reclaimed by the ITU at the end of 2010!

VISIONng Association

Mission of VISIONng (http://www.visionng.com/): "to provide a framework for the deployment of worldwide inter-domain and multi-vendor IP Communications"

ITU-T has assigned part of the country code for Universal Personal Telecommunication (UPT) to VISIONng for deployment of a UPT Service:

```
+878 10
```

As of May 2002 VISIONng received ITU-TSB permission and an ENUM Delegation from RIPE NCC; BearingPoint Inc. acting as Tier 1 Manager, Telekom Austria acting as Tier 2 DNS.

These E.164 numbers can be used for both: IP-IP and PSTN-IP.

See also [153].

You can register for a number is the +878 10 range via https://www.enum2go.com/

As of 2009.08.20 the cost was £25.85 (including a 1 year registration). As of 2011.08.22 the cost is £12 per year + one time £10 registration fee.

iNum™

International numbers - http://www.inum.net/

+883 5100 international code assigned to Voxbone S. A. by the ITU in 2008

Carrier and user use of ENUM and DNS

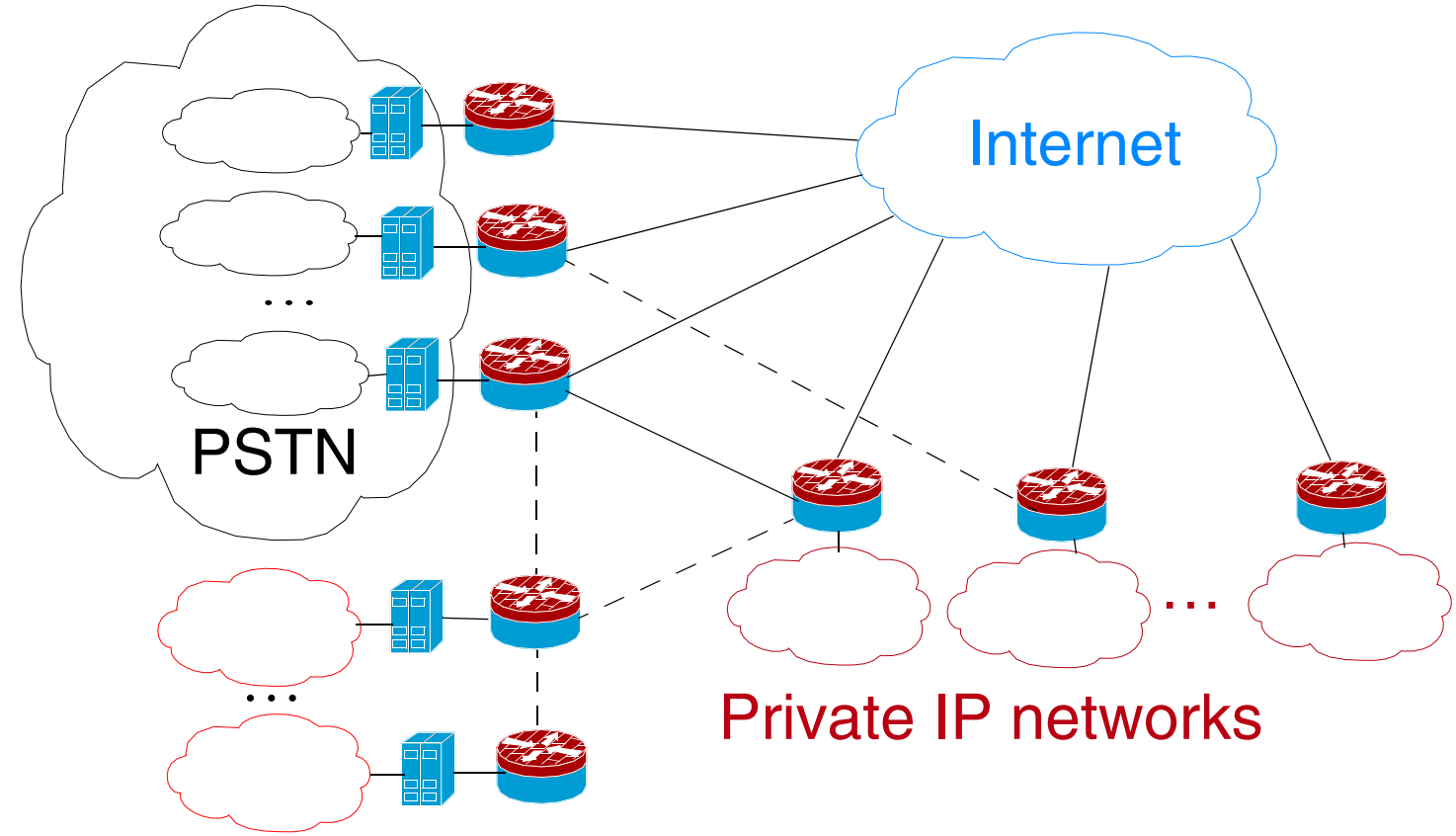
RFC 5526 proposed an “Infrastructure ENUM” parallel to the `e164.arpa` namespace to allow “carriers to provision DNS records for telephone numbers *independently* of those provisioned by end users (number assignees)”[168].

The need for such an infrastructure ENUM are described in RFC 5067[170].

RFC 5527[169] describes how the infrastructure ENUM could be combined in the `e164.arpa` namespace.

For a discussion of the need for including the source SIP URI in an ENUM query see the Internet Draft: “Routing SIP Requests with ENUM” [172].

Mapping and numbering



Where are the mappings between the locally meaningful addresses and the address in the connected network performed? Who provides this mapping? Which mapping should be used? …

NRENum.net

An ENUM service for academia by the National Research and Education Networks (NRENs) organization (via the Trans-European Research and Education Networking Association - http://www.terena.org/).

NRENum.net uses a private dialing plan, as an alternative to the "e164.arpa" zone (known as the Golden ENUM tree).

It is recommended that a VoIP should query *both* the e164.arpa and the nrenum.net trees.

NRENum.net enables universities and research organizaitons:

- to interconnect their VoIP systems - without having to do so through a traditional telephony operators
- to list E.164 numbers and also: telepresense, Global Dialing Scheme (GDS) numbers (a numbering plan for H.323 services), …

For details see https://confluence.terena.org/display/NRENum/About and [176].

SIP goes beyond ENUM

by offering additional features:

- User preferences
- Personal/Service/… mobility[1]
- Easy and secure updating of information by the end-user

A given User Agent need not directly implement call routing, LDAP lookup, …, but can instead utilize a default SIP outgoing proxy (which in turn does the work).

Call Processing Language (CPL) can be used to support rapid changes in user preferences (see **Call Processing Language (CPL)** on page 401)

1. See **SIP Mobility** on page 307.

ENUM for Google Android

Ray Bellis of Nominet UK (the UK Tier 1 operator for +44) released an open source Android ENUM dialer application (called “enumdroid”):

http://code.google.com/p/enumdroid/

Thus everytime you enter a full E.164 number will a “+”, the application does a DNS lookup to see if there is an ENUM mapping - so that you can take advantage of other means of contact this entity, i.e., e-mail, PSTN, SIP, SMS, tel, voice, web, XMPP.

It can also get the “loc” ENUM service information telling you the geo-location associated with the number (if this information exists).

By default it uses resolver1 and resolver2.opendns.com as the DNS server.

ENUM calendaring and other services

See the internet draft: IANA Registration of Enumservices for Internet Calendaring [173], this registers and updates Enumservices for Internet calendaring, specifically for iMIP (iCalendar Message-Based Interoperability Protocol), Calendaring Extensions to WebDAV (CalDAV), and iSchedule (Internet Calendar Scheduling Protocol).

It updates RFC 5333 [174] in preparation for RFC 6118 [175].

In addition to calendaring, there is work on enumervices for FAX, voice mail, voice and video messaging, instant messaging, … .

IANA Enumservice Registrations:

https://www.iana.org/assignments/enum-services/enum-services.xhtml

References and Further Reading

E.164

[132]ITU-T, “The international public telecommunication numbering plan”, International Telecommunication Union, Telecommunication Sector of ITU (ITU-T), Series E: Overall Network Operation, Telephone Service, Service operation, and Human Factors: International operation - Number plan of the internation telephone service, ITU-T E.164, February 2005

[133]ITU-T, “List of ITU-T recommendation E.164 Assigned Country Codes”, International Telecommunication Union, Telecommunication Sector of ITU (ITU-T): Complement to ITU-T Recommendation E.164, Annex to ITU Operational Bulletin No. 835 – 1.V.2005, February 2005.

DNS

[134] M. Mealling and R. Daniel, “The Naming Authority Pointer (NAPTR) DNS Resource Record”, RFC 2915, September 2000, Obsoleted by RFCs 3401, 3402, 3403, 3404. http://www.rfc-editor.org/rfc/rfc2915.txt

[135]M. Mealling, “Dynamic Delegation Discovery System (DDDS) Part One: The Comprehensive DDDS”, Internet Request for Comments, RFC Editor, RFC 3401 (Informational), ISSN 2070-1721, October 2002

http://www.rfc-editor.org/rfc/rfc3401.txt

[136]M. Mealling, “Dynamic Delegation Discovery System (DDDS) Part Two: The Algorithm”, Internet Request for Comments, RFC Editor, RFC 3402 (Proposed Standard), ISSN 2070-1721, October 2002

http://www.rfc-editor.org/rfc/rfc3402.txt

[137]M. Mealling, “Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database”, Internet Request for Comments, RFC Editor, RFC 3403 (Proposed Standard), ISSN 2070-1721, October 2002 http://www.rfc-editor.org/rfc/rfc3403.txt

[138]M. Mealling, “Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI)”, Internet Request for Comments, RFC Editor, RFC 3404 (Proposed Standard), ISSN 2070-1721, October 2002 http://www.rfc-editor.org/rfc/rfc3404.txt

[139]M. Mealling, “Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures”, Internet Request for Comments, RFC Editor, RFC 3405 (Best Current Practice), ISSN 2070-1721, October 2002

http://www.rfc-editor.org/rfc/rfc3405.txt

ENUM

[140]P. Faltstrom, “E.164 number and DNS”, IETF RFC 2916, September 2000, Obsoleted by RFC 3761. http://www.rfc-editor.org/rfc/rfc2916.txt

[141]P. Faltstrom and M. Mealling, “RFC 3761: The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDS) Application (ENUM)”, IETF RFC 3761, Obsoleted by RFC6166, April 2004

http://www.rfc-editor.org/rfc/rfc3761.txt

[142]S. Bradner, L. Conroy, and K. Fujiwara, ‘The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)’, Internet Request for Comments, RFC 6116 (Proposed Standard), Mar. 2011. Available: http://www.rfc-editor.org/rfc/rfc6116.txt

[143]Carsten Schiefner, “ENUM - a snap-shot of current developments”, Deploying IPv6 Networks Conference, Paris, France, 4 December 2003

http://www.ripe.net/ripencc/about/presentations/ipv6-enum-paris-20031204/

[144]Post- och telestyrelsen (PTS), ENUM - Slutrapport, Kommunikationsmyndigheten PTS, PTS-ER-2004:39, ISSN 1650-9862, 22 December 2004

http://www.pts.se/upload/Documents/SE/ENUM_Slutrapport_22%20december_2004_PTS_ER_2004_39.pdf

[145]C. Allocchio, “Text String Notation for Dial Sequences and Global Switched Telephone Network (GSTN) / E.164 Addresses”, RFC 3601, September 2003.

[146]J. Peterson, H. Liu, J. Yu, and B. Campbell, “Using E.164 numbers with the Session Initiation Protocol (SIP)”, IETF RFC 3824, June 2004

http://www.ietf.org/rfc/rfc3824.txt

[147]R. Mahy, “Proposed Clarification of Encoding of Telephone Numbers in SIP URIs”, IETF Internet-Draft, Oct. 2003, Expired: March 31, 2004

http://www.ietf.org/internet-drafts/draft-mahy-sipping-user-equals-phone-00.txt

[148]Joakim Strålmark, “The National Post and Telecom Agency in Sweden (PTS): A Regulator Perspective on ENUM”, RIPE 47 Meeting, 28 January 2004 http://www.ripe.net/ripe/meetings/ripe-47/presentations/ripe47-enum-sweden.pdf

[149]R. Stastny, “Numbering for VoIP and other IP Communications”, IETF IETF-Draft, October 2003, Expired: April 2004

http://www.ietf.org/internet-drafts/draft-stastny-enum-numbering-voip-00.txt

[150]O. Levin, “Telephone Number Mapping (ENUM) Service Registration for H.323”, IETF RFC 3762, April 2004 http://www.ietf.org/rfc/rfc3762.txt

[151]J. Peterson, “enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record”, IETF, RFC 3764, April 2004

http://www.ietf.org/rfc/rfc3764.txt

[152]ITU-T,"InternationalTelephoneService",ITU-TRecommendationE.105, August 1992

[153]Richard Stastny, “Status of ENUM Trials”, SG2 Plenary, Florianopolis, Brazil, October 2003 http://enum.nic.at/documents/AETP/Presentations/Austria/0025-2003-10_SG2_ENUM.ppt

[154]H. Schulzrinne, The tel URI for Telephone Numbers, Internet Request for Comments, ISSN 2070-1721, RFC 3966, RFC Editor, December 2004, Updated by RFC 5341 [155], http://www.rfc-editor.org/rfc/rfc3966.txt

[155]C. Jennings and V. Gurbani, The Internet Assigned Number Authority (IANA) tel Uniform Resource Identifier (URI) Parameter Registry, Internet Request for Comments, ISSN 2070-1721, RFC 5341, RFC Editor, September 2008, http://www.rfc-editor.org/rfc/rfc5341.txt

[156]PTS, Enum - Preliminary report - PTS-ER-2004:11, 2004-05-04

http://www.pts.se/Dokument/dokument.asp?ItemId=3232

[157]PTS, "ENUM: Slutrapport", PTS-ER-2004:39, 22 December 2004, ISSN 1650-9862
http://www.ficora.fi/suomi/document/ENUM_Slutraport_2004.pdf

[158]Robert Shaw, "'ENUM: Country Experiences", International Telecommunication Union, Forum on Telecommunication regulation in Africa, Kampala, Uganda, 3-5 November 2004

http://www.itu.int/osg/spu/presentations/2004/enum-country-experiences-ftra-uganda-rs.pdf&e=10053

[159]Joakim Strålmark, “Förstudie - Nummerportabilitet för framtida nät, och i samverkan med befintliga nät med aspekter på samtrafik, ENUM och den centrala referensdatabasen”, Post- och telestyrelsen (PTS), PTS-ER-2009:7, 2009-02-18

http://www.pts.se/upload/Rapporter/Tele/2009/Nummerportabilitet-i-framtida-nat-PTS-ER-2009-7.pdf

[160]Finnish Communication Regulatory Agency, ENUM web page, published October 22, 2003 http://www.ficora.fi/englanti/tele/enumnd.htm

[161]S. Hollenbeck, E.164 Number Mapping for the Extensible Provisioning Protocol (EPP), Internet Request for Comments, ISSN 2070-1721, RFC 4114, RFC Editor, June 2005, http://www.rfc-editor.org/rfc/rfc4114.txt

[162]Electronic Privacy Information Center, ENUM web page, Last Updated: March 18, 2003 http://www.epic.org/privacy/enum/default.html

[163]Roger Clarke, “ENUM - A Case Study in Social Irresponsibility”, Revised Version of 9 March 2003, published in Privacy Law & Policy Reporter 9, 10 (March 2003) 181-187 http://www.anu.edu.au/people/Roger.Clarke/DV/enumISOC02.html

[164]R. Brandner, L. Conroy, R. Stastny, “IANA Registration for Enumservices

email, fax, mms, ems, and sms", IETF, RFC 4355, January 2006
ftp://ftp.rfc-editor.org/in-notes/rfc4355.txt

[165]R. Brandner, L. Conroy, and R. Stastny, "IANA Registration for Enumservice 'web' and 'ft'", Internet Request for Comments, RFC Editor, RFC 4002 (Proposed Standard), ISSN 2070-1721, February 2005,
http://www.rfc-editor.org/rfc/rfc4002.txt

[166]R. Brandner, L. Conroy, and R. Stastny, "IANA Registration for Enumservice Voice", Internet Request for Comments", RFC Editor, RFC 4415 (Proposed Standard), ISSN 2070-1721, February 2006
http://www.rfc-editor.org/rfc/rfc4415.txt

[167]R. Stastny, R. Shockey, and L. Conroy, "The ENUM Dip Indicator Parameter for the "tel" URI", Internet Request for Comments, RFC Editor, RFC 4759 (Proposed Standard), ISSN 2070-1721, December 2006
http://www.rfc-editor.org/rfc/rfc4759.txt

[168]J. Livingood, P. Pfautz, and R. Stastny, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application for Infrastructure ENUM",

Internet Request for Comments, RFC Editor, RFC 5526 (Informational), ISSN 2070-1721, April 2009 http://www.rfc-editor.org/rfc/rfc5526.txt

[169]M. Haberler, O. Lendl, and R. Stastny, “Combined User and Infrastructure ENUM in the e164.arpa Tree”, Internet Request for Comments, RFC Editor, RFC 5527 (Informational), ISSN 2070-1721, May 2009

http://www.rfc-editor.org/rfc/rfc5527.txt

[170]S. Lind and P. Pfautz, “Infrastructure ENUM Requirements”, Internet Request for Comments, RFC Editor, RFC 5067 (Informational), ISSN 2070-1721, November 2007 http://www.rfc-editor.org/rfc/rfc5067.txt

[171]PTS, Minnesanteckningar från Nummerforum, Kommunikationsmyndigheten PTS Post- och telestyrelsen (PTS), 15 april 2010 http://www.pts.se/upload/Ovrigt/Tele/nummerforum/nrforum-minnesanteckningar-100415.pdf

[172]H. Kaplan, C. Pons, and P. Gorman, Routing SIP Requests with ENUM, IETF Network Working Group, Internet Draft, October 24, 2011, Expired: April 24, 2012, draft-kaplan-enum-sip-routing-04,

http://tools.ietf.org/html/draft-kaplan-enum-sip-routing-04

[173]B. Hoeneisen, IANA Registration of Enumservices for Internet Calendaring, Network Working Group, Internet-Draft, March 11, 2012, Expired: September 12, 2012, draft-hoeneisen-rfc5333bis-01,

https://datatracker.ietf.org/doc/draft-hoeneisen-rfc5333bis/

[174]R. Mahy and B. Hoeneisen, IANA Registration of Enumservices for Internet Calendaring, Internet Request for Comments, ISSN 2070-1721,RFC 5333, RFC Editor, October 2009, Updated by RFC 6118,

http://www.rfc-editor.org/rfc/rfc5333.txt

[175]B. Hoeneisen and A. Mayrhofer, Update of Legacy IANA Registrations of Enumservices, Internet Request for Comments, ISSN 2070-1721, RFC 6118, RFC Editor, March 2011, http://www.rfc-editor.org/rfc/rfc6118.txt

[176]Mihály Mészáros, NRENum.net (update): new developments and service update, RIPE65 - ENUM WG, Budapest, Hungary, 27 Sep 2012,

https://ripe65.ripe.net/presentations/263-ripe65.pdf

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 7: SIP Mobility

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:31

SIP Mobility

- **Terminal mobility**[1] $\Rightarrow$ the **terminal** moves between **subnets**
  - Note: Mobile IP supports this at the network layer, while SIP supports this at the application layer (*without* requiring Mobile IP be underneath)
- **Personal Mobility** $\Rightarrow$ the **person** moves between **terminals**
- **Service mobility** $\Rightarrow$ the **person** has access to the **same services** *despite* their movement between terminals and/or networks
  - note: the service may be reduced in quality or capabilities subject to the current network's capabilities -- but it is the same service
  - this implies that personalization of services must be distributed to the various terminals that the user wishes to use - see the dissertation of Roch Glitho [180]
- **Session mobility** $\Rightarrow$ the **same session** is maintained despite the user changing from one device to another

1. Also known as network-level mobility.

Local Number Portability

In the PSTN this means a complex set of lookups for the number, since the number is no longer tied to an exchange.

In SIP the portability occurs because of the lookup of `name@domain`, which can be mapped to where ever the user wants this mapped to! (i.e., fully qualified domain names are *unique*, but are **not** tied to an underlying network address -- it is the name to address mapping which estabilishes this mapping and it is ***always*** **dynamic**).

For some considerations of tel URIs and number portability see [178] and [179].

For some additional information regarding number portability and the availability of sufficient numbers for all of the entities (people, terminals, “things”, etc.) see [181] .. [186].

References and Further Reading

SIP Mobility

[177]SIP Mobility informal meeting: Unedited Version of SIP-Mobile Minutes, 50th IETF, 730-830pm, March 20th 2001 at Salon A, Minneapolis, Minnesota, http://www.research.telcordia.com/SIP-mobile/sip-mobile-minutes-50.htm

[178]James Yu, “Number Portability Parameters for the "tel" URI”, Internet Request for Comments, RFC Editor, RFC 4694 (Proposed Standard), ISSN 2070-1721, October 2006 http://www.rfc-editor.org/rfc/rfc4694.txt

[179]M. Foster, T. McGarry, and J. Yu, “‘Number Portability in the Global Switched Telephone Network (GSTN): An Overview”, IETF RFC 3482 , February 2003 http://www.ietf.org/rfc/rfc3482.txt

Service Mobility

[180] Roch H. Glitho, “A Mobile Agent Based Service Architecture for Internet Telephony”, Doctoral Dissertation, Royal Institute of Technology (KTH), Microelectronics and Information Technology, TRITA-IT-AVH:02:01, April 2002. http://kth.diva-portal.org/smash/get/diva2:9108/FULLTEXT01

Number portability

[181] Joakim Strålmark, Dirigeringsprefix NP: Framtida portabilitet, Slides, PTS, 23 October 2007 http://www.pts.se/upload/Ovrigt/Tele/NF_Bilaga_4_Dirigeringsprefix_NP_framtiden_NP_071025.pdf

[182] Joakim Strålmark, "NP för framtida nät –Nummerforum", Slides, PTS, 29 April 2009

http://www.pts.se/upload/Ovrigt/Tele/nummerforum/nrforum-bilaga-2-np-for-framtida-nat-090429.pdf

[183] PTS, "NP för framtida nät – Fortsatt arbete", Nummerforum, Slides, PTS, 22 October 2009

http://www.pts.se/upload/Ovrigt/Tele/Nummerfragor/nrforum-bilaga-3-np-framtida-nat-091022.pdf

[184] PTS, "Nätteknisk utveckling för nät som använder telefonnummer – Framtida telefoninummerplan", Slides, PTS, 15 December 2008

http://www.pts.se/upload/Ovrigt/Tele/nummerforum/nrforum-bilaga3-natteknisk-utveckling-081211.pdf

[185] Joakim Strålmark, "Implementering av nummerkapacitet ur telefoninummerplanen", Arbetsgruppens avrapportering, PTS, 24 April 2008

http://www.pts.se/upload/Ovrigt/Tele/nummerforum/nrforum-bilaga2-implementering-nummerkapacitet-080424.pdf

[186] Thomas Florenteng, Nummerserie for M2M, Bilaga, PTS, 16 June 2004

http://www.pts.se/upload/Documents/SE/Nummerserie_for_M2M_Bilaga.pdf

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 8: SIP (Telia) Example

KTH Information and
Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:13:58

Example of IP Telephony (Telia's Broadband Telephony)

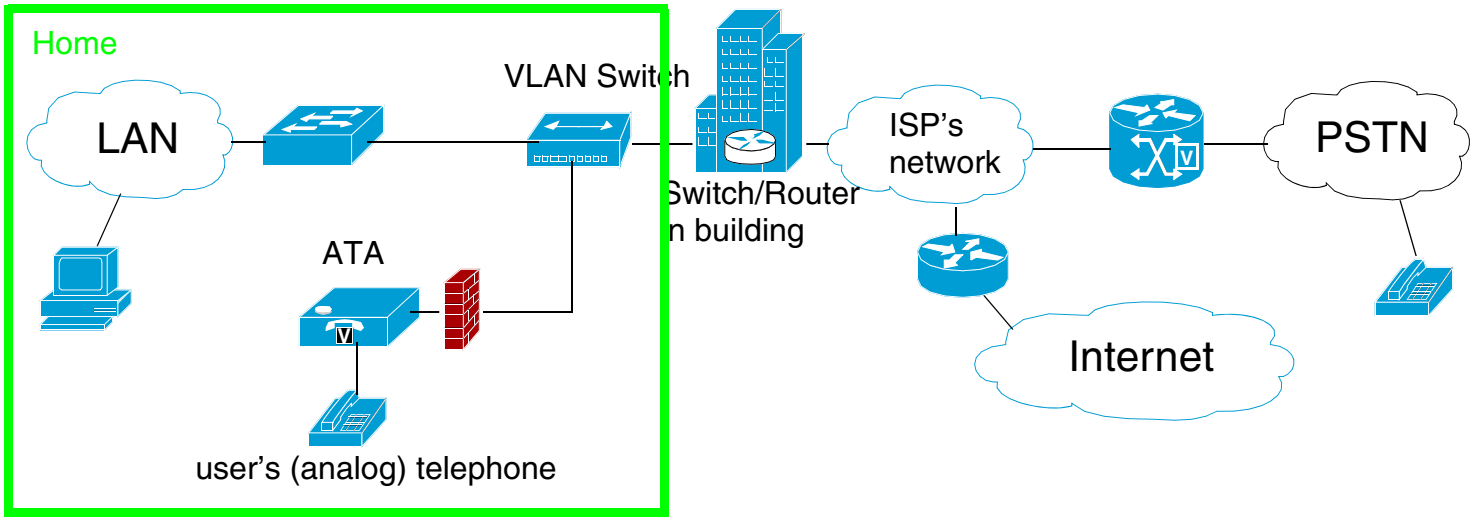


Figure 16: User at home with broadband connectivity and a IP telephone subscription

References and Further Reading

SIP Example

[187]Tilgin AB, web page, las accessed 2010.08.05, http://www.tilgin.com/

[188]TNETV1060 Communications Processor for VoIP Gateway Applications Data Manual, Texas Instruments, Literature Number SPRS255, June 2004, 139 pages http://focus.ti.com/pdfs/vf/bband/tnetv1060_datasheet.pdf

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 9: SIP (Telia) Example

KTH Information and
Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:31

Example of IP Telephony (Telia's Broadband Telephony)

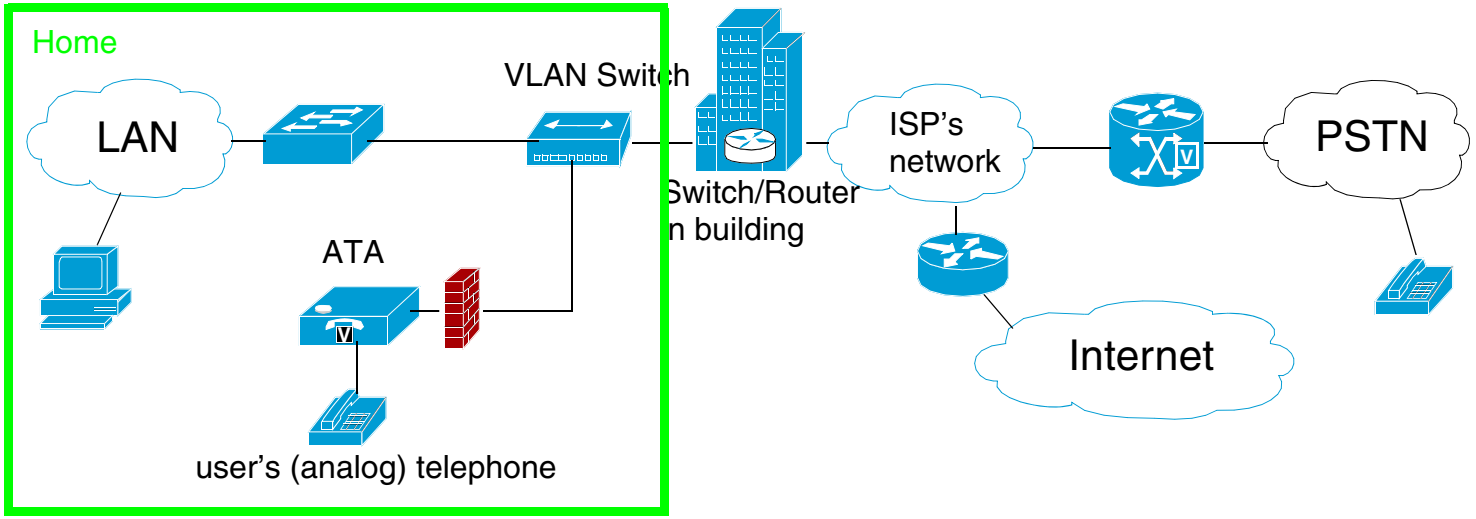


Figure 17: User at home with broadband connectivity and a IP telephone subscription

Sniffing the IP telephony traffic

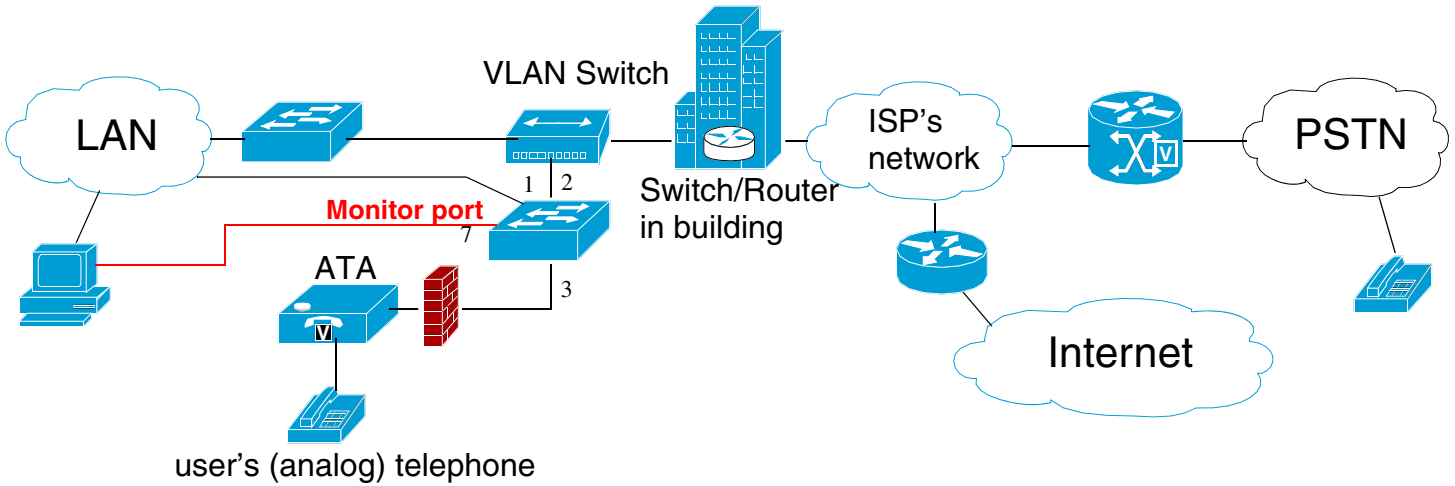


Figure 18: Inserting a switch with monitor port into the IP telephone path in the home

Port 1 of the switch (an HP ProCurve Switch 2524) is connected to the local LAN (at IP address 192.168.1.100)

Port 7 of the switch is set up as a monitor port and connected to a secondary ethernet interface of the PC (at IP address 192.168.3.2)

Ports 2 and 3 of the switch bridge traffic between the VLAN switch and the IP telephony box (which contains a firewall and IP telephony interface).

Switch configuration

To prevent the switch from sending transmissions about its existance, use the console interface (i.e., telnet to the device) to turn off CDP:

```
IP ProCurve Switch 2524# config
IP ProCurve Switch 2524(config)# no cdp run
IP ProCurve Switch 2524(config)#
```

Figure 19: Configure CDP off

Set up a VLAN for the IP telephony traffic

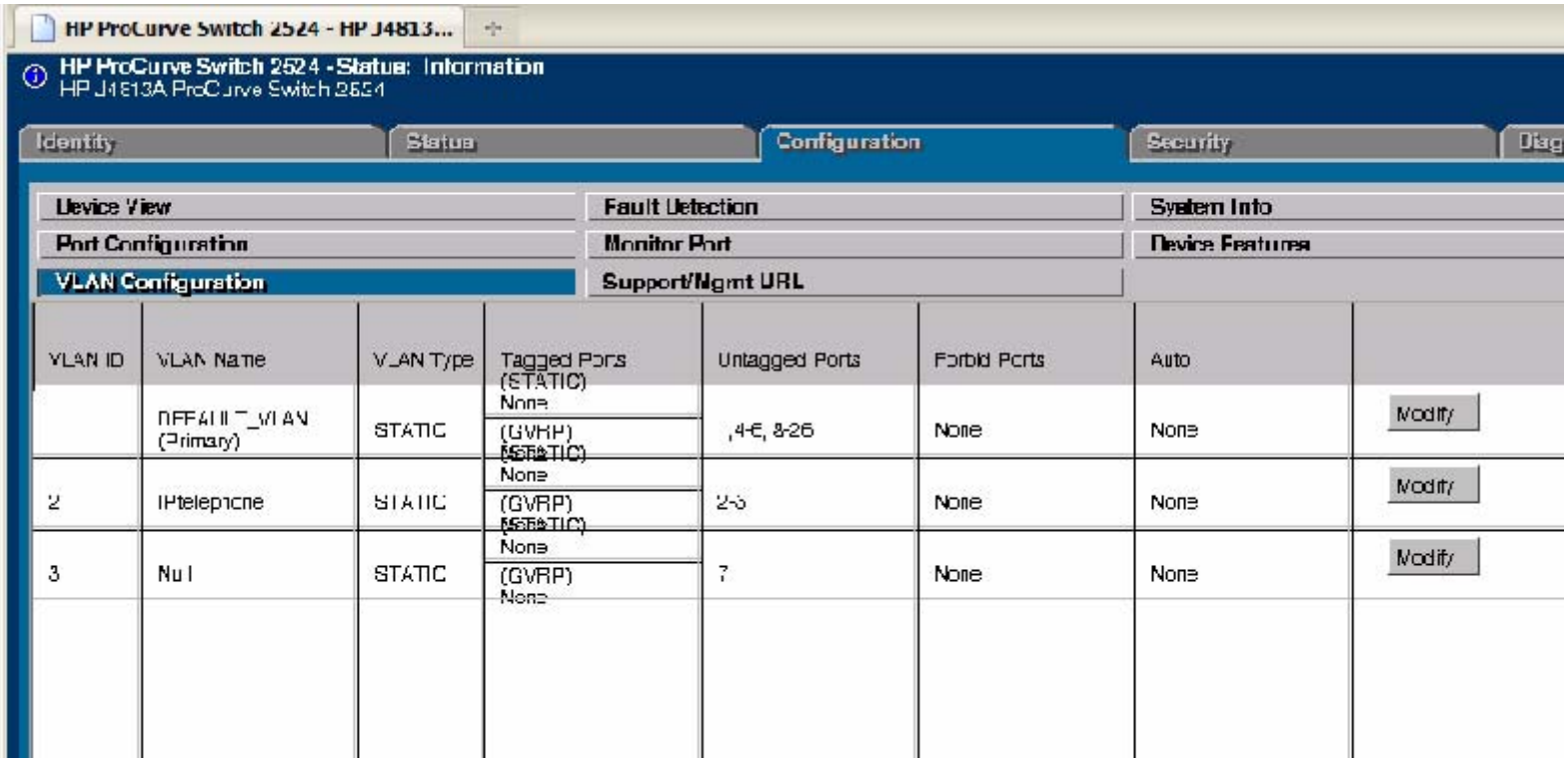


Figure 20: VLAN configuration

Device view

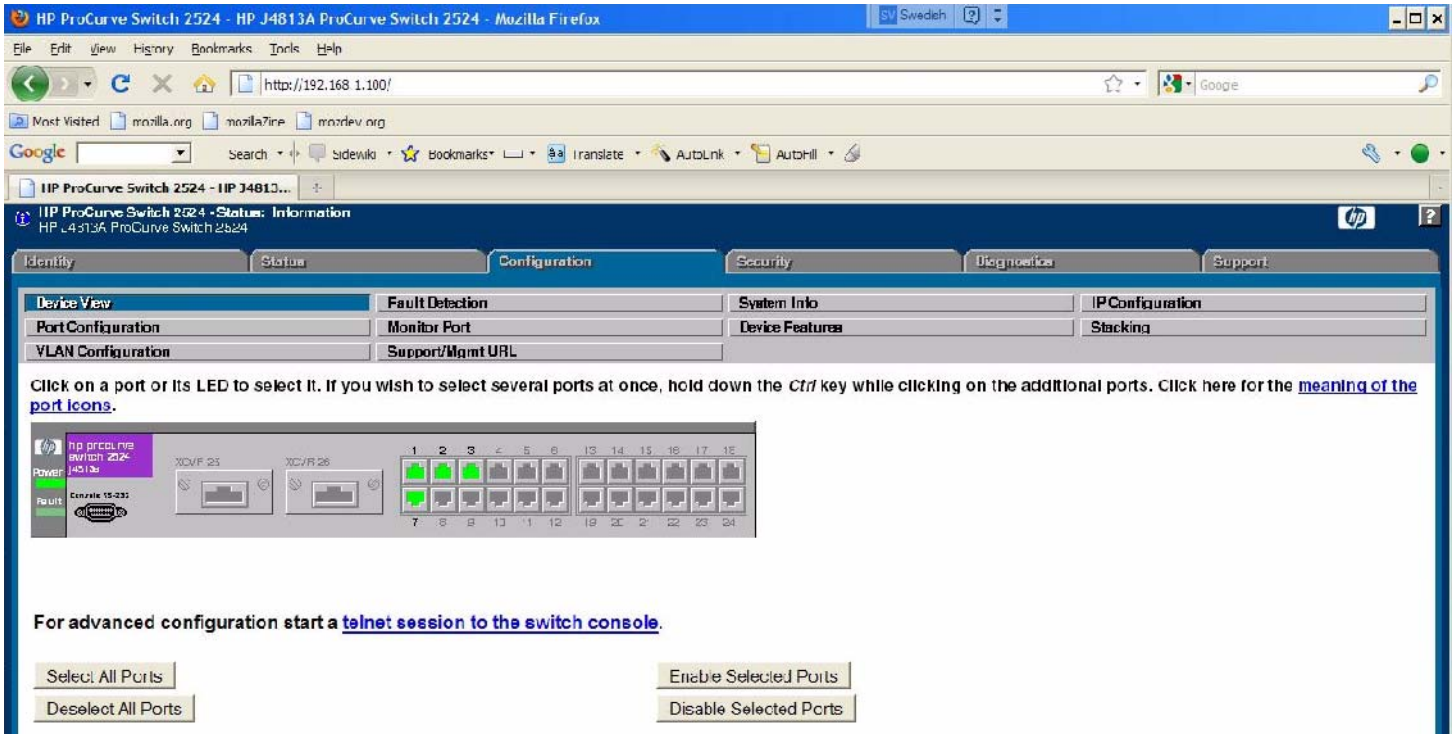
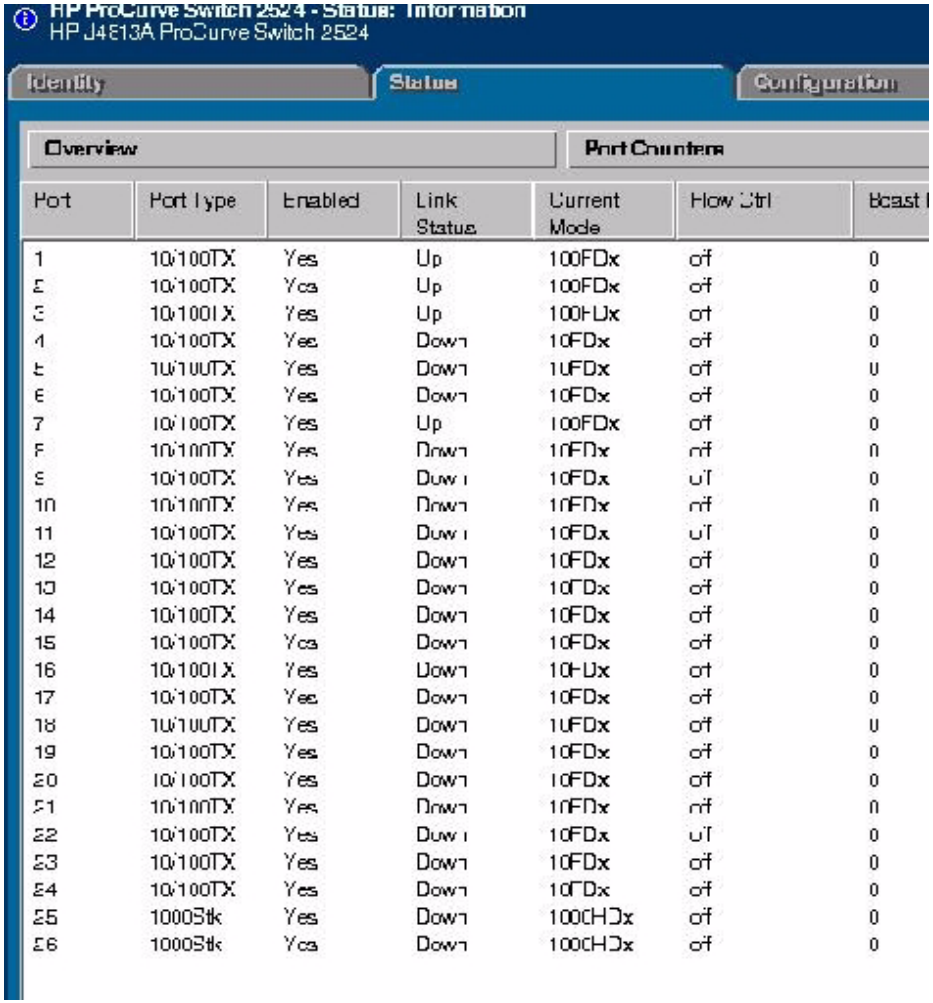


Figure 21: Device view

Port status



Port	Port Type	Enabled	Link Status	Current Mode	Flow Ctrl	Bcast
1	10/100TX	Yes	Up	100FDx	off	0
2	10/100TX	Yes	Up	100FDx	off	0
3	10/100TX	Yes	Up	100FDx	off	0
4	10/100TX	Yes	Down	10FDx	off	0
5	10/100TX	Yes	Down	10FDx	off	0
6	10/100TX	Yes	Down	10FDx	off	0
7	10/100TX	Yes	Up	100FDx	off	0
8	10/100TX	Yes	Down	10FDx	off	0
9	10/100TX	Yes	Down	10FDx	off	0
10	10/100TX	Yes	Down	10FDx	off	0
11	10/100TX	Yes	Down	10FDx	off	0
12	10/100TX	Yes	Down	10FDx	off	0
13	10/100TX	Yes	Down	10FDx	off	0
14	10/100TX	Yes	Down	10FDx	off	0
15	10/100TX	Yes	Down	10FDx	off	0
16	10/100TX	Yes	Down	10FDx	off	0
17	10/100TX	Yes	Down	10FDx	off	0
18	10/100TX	Yes	Down	10FDx	off	0
19	10/100TX	Yes	Down	10FDx	off	0
20	10/100TX	Yes	Down	10FDx	off	0
21	10/100TX	Yes	Down	10FDx	off	0
22	10/100TX	Yes	Down	10FDx	off	0
23	10/100TX	Yes	Down	10FDx	off	0
24	10/100TX	Yes	Down	10FDx	off	0
25	1000Stk	Yes	Down	100FHDx	off	0
26	1000Stk	Yes	Down	100FHDx	off	0

Figure 22: Port status

Set up monitor port

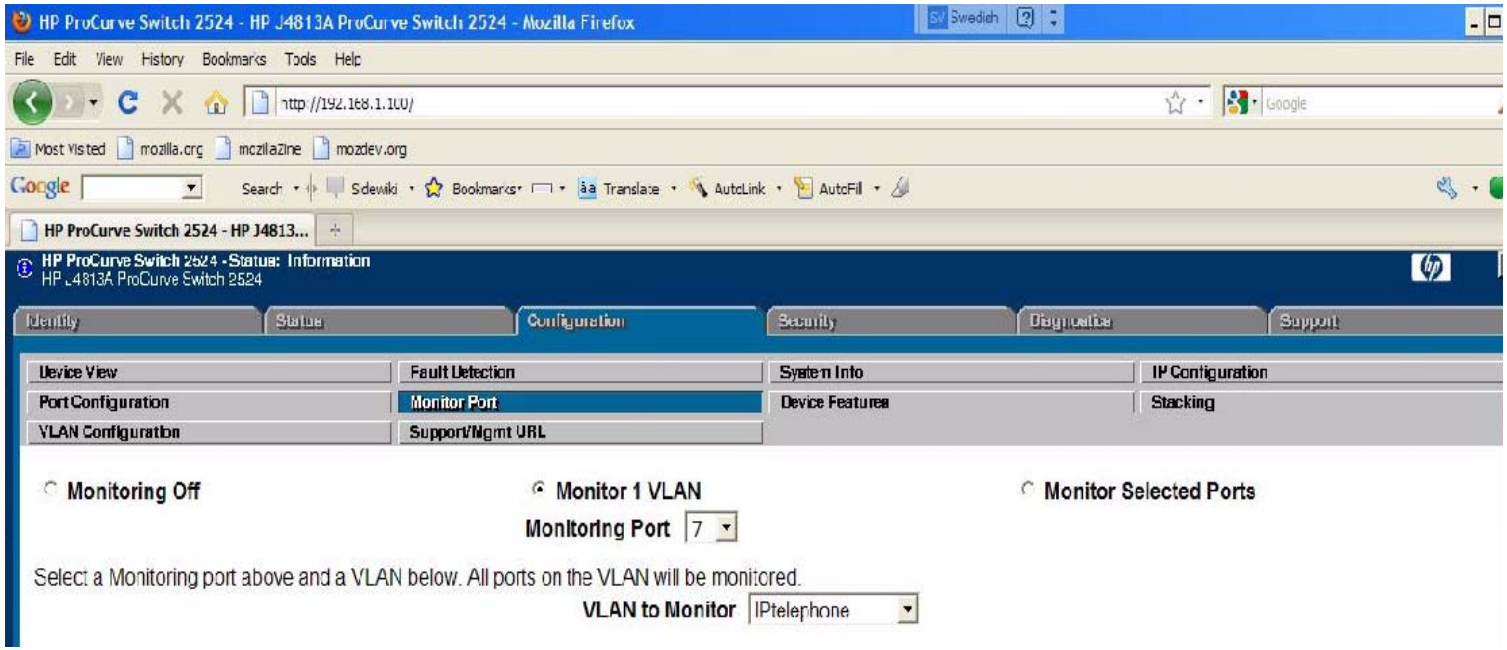
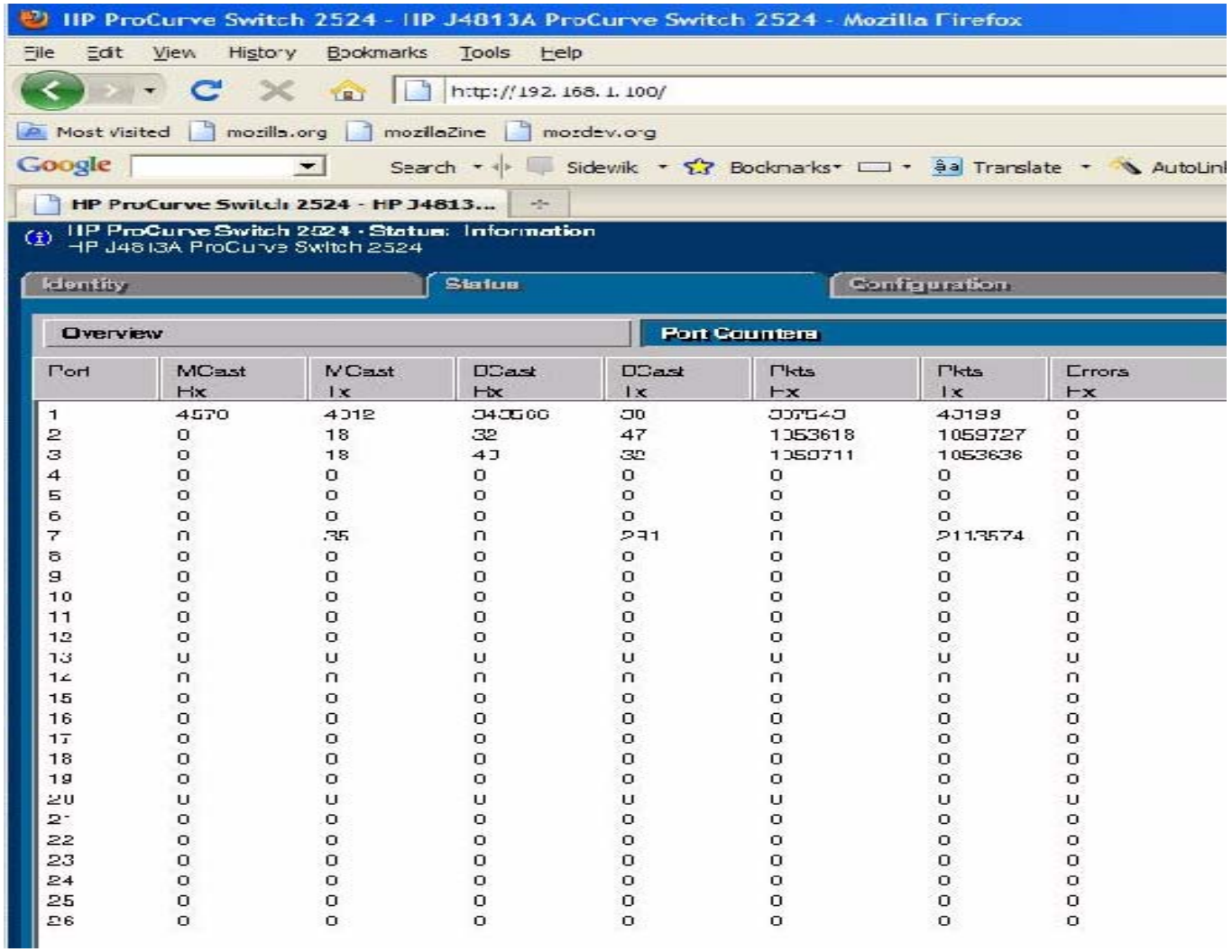


Figure 23: Set port 7 as the monitor port for the VLAN IPTelephone

Port counters



Port	MCast Rx	MCast Tx	BCast Rx	BCast Tx	Pkts Rx	Pkts Tx	Errors Rx
1	4570	4012	343560	30	337543	40199	0
2	0	18	32	47	1053618	1059727	0
3	0	18	40	32	1050711	1053636	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	35	0	231	0	2113574	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0

Figure 24: Port counters after two days

Tilgin AB Vood 322

The ATA that was used for these examples was made by Tilgin AB (formerly i3 Micro)[189]

Source code for some of the software is available under GPL or LGPL from:

ftp://ftp.opensource.tilgin.com/VOOD

Vood 322 additional details

Uses a TI TNETV 1060 chip. This combines a MIPS32™ 32-bit RISC processor with a TI TMS320C55x™ digital signal processor. For details on this chip see [190].

There are two FXS telephone interfaces (to connect analog telephones), 1 Ethernet uplink, and 1 ethernet port (the device can be a bridge or router), it support G.711, G.723, and G.729 CODECs, T.38 fax, and up to 12 different SIP accounts.

Note that Telia does **disables** access to many of the features of the device and does not provide a password so you can **not** administer the device yourself - otherwise you might enable some of the features (such as taking voice messages and forwarding them to you as e-mail attachments).

Getting and IP address and configuration

```
⊞ Frame 4 (590 bytes on wire, 590 bytes captured)
⊞ Ethernet II, Src: Tilgin_43:9b:47 (00:02:61:43:9b:47), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4beae090
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Tilgin_43:9b:47 (00:02:61:43:9b:47)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
  ⊞ Option: (t=61,l=7) Client identifier
  ⊞ Option: (t=60,l=18) Vendor class identifier = "tel-01-B-Tilgin322"
  ⊞ Option: (t=55,l=7) Parameter Request List
    End Option
    Padding
```

Figure 25: DHCP Discover

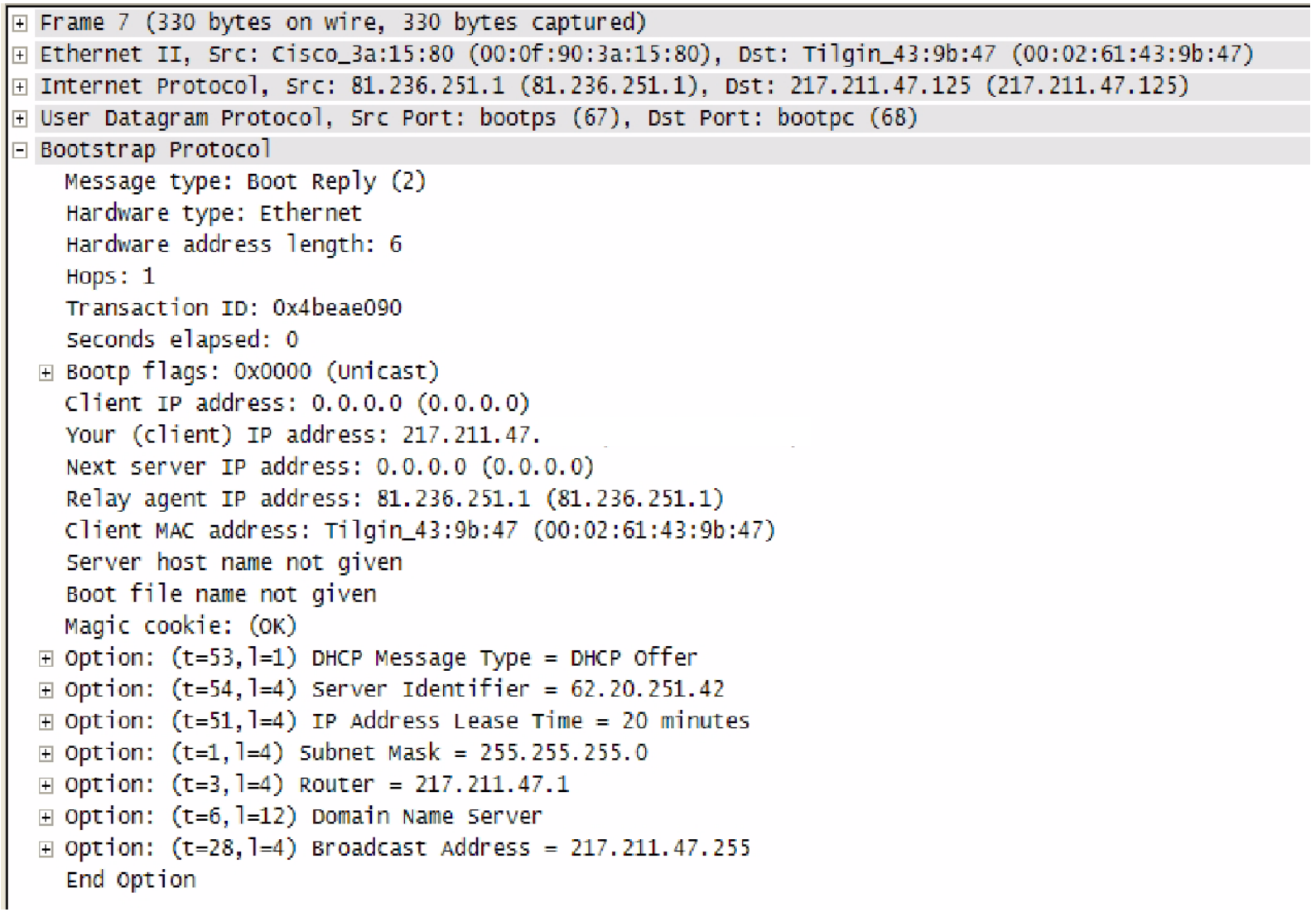


Figure 26: DHCP Offer (the local building router is a Cisco with MAC address: 00:0f:90:3a:15:80)

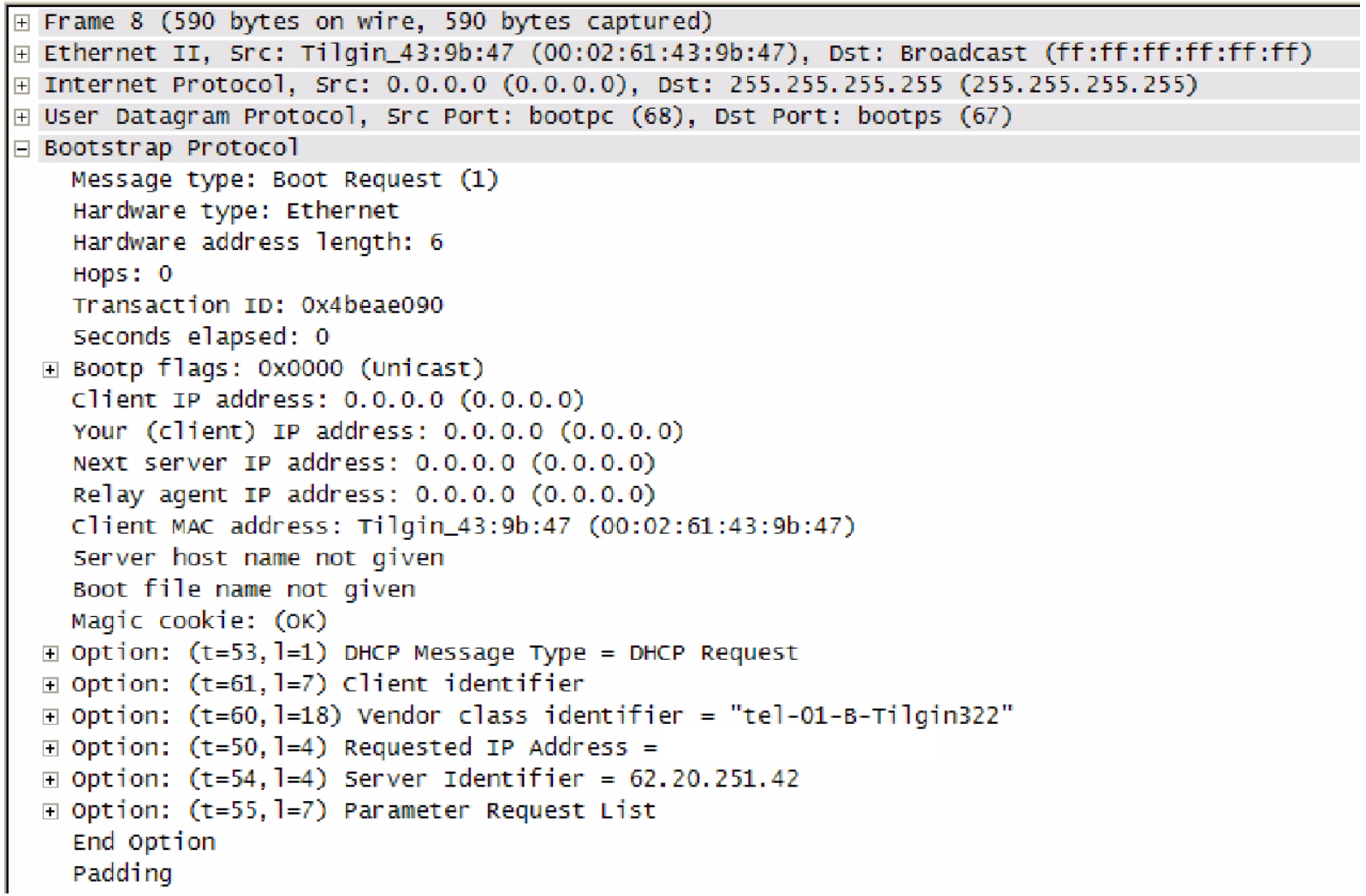


Figure 27: DHCP Request

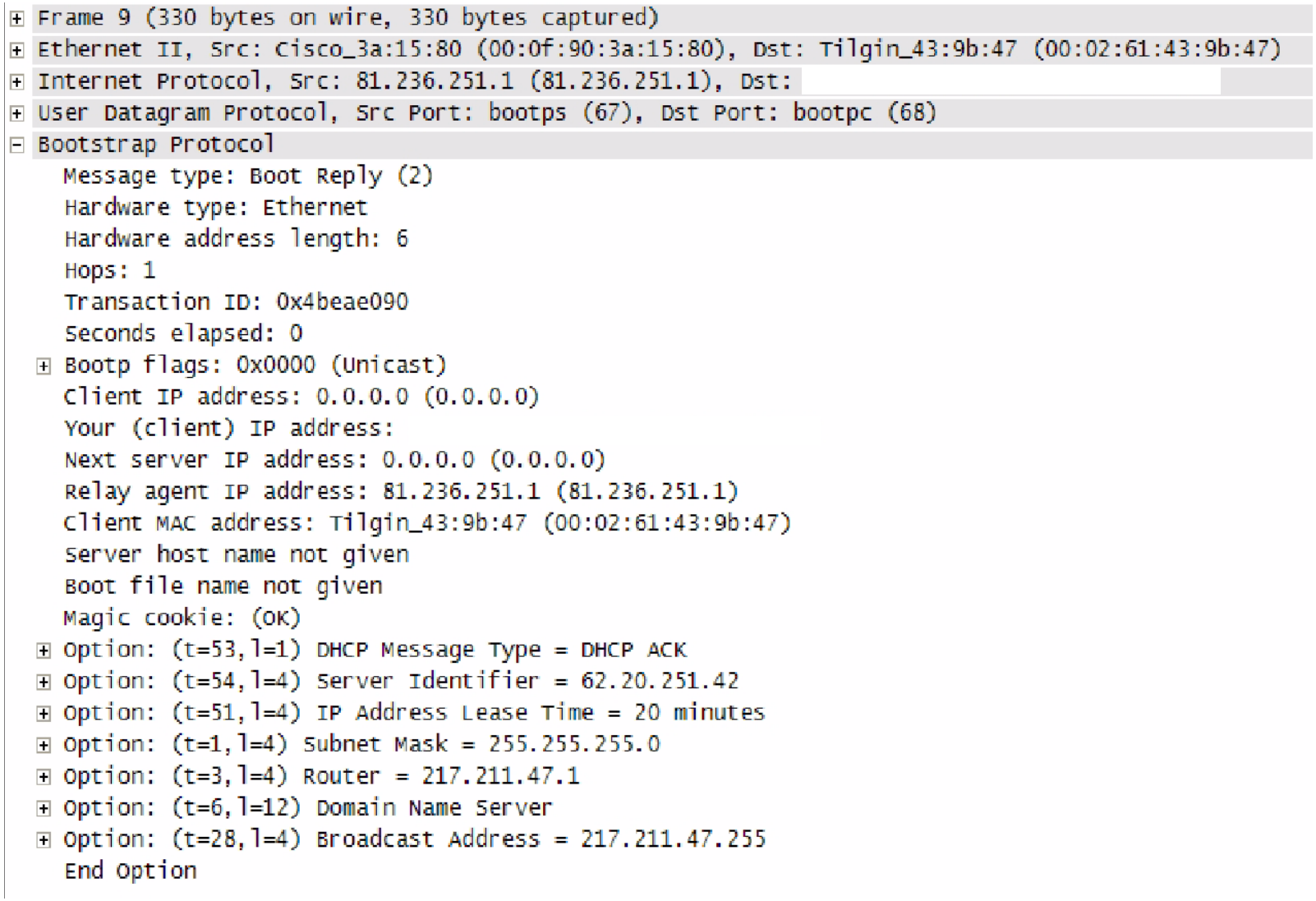


Figure 28: DHCP ACK

Addresses known at this point

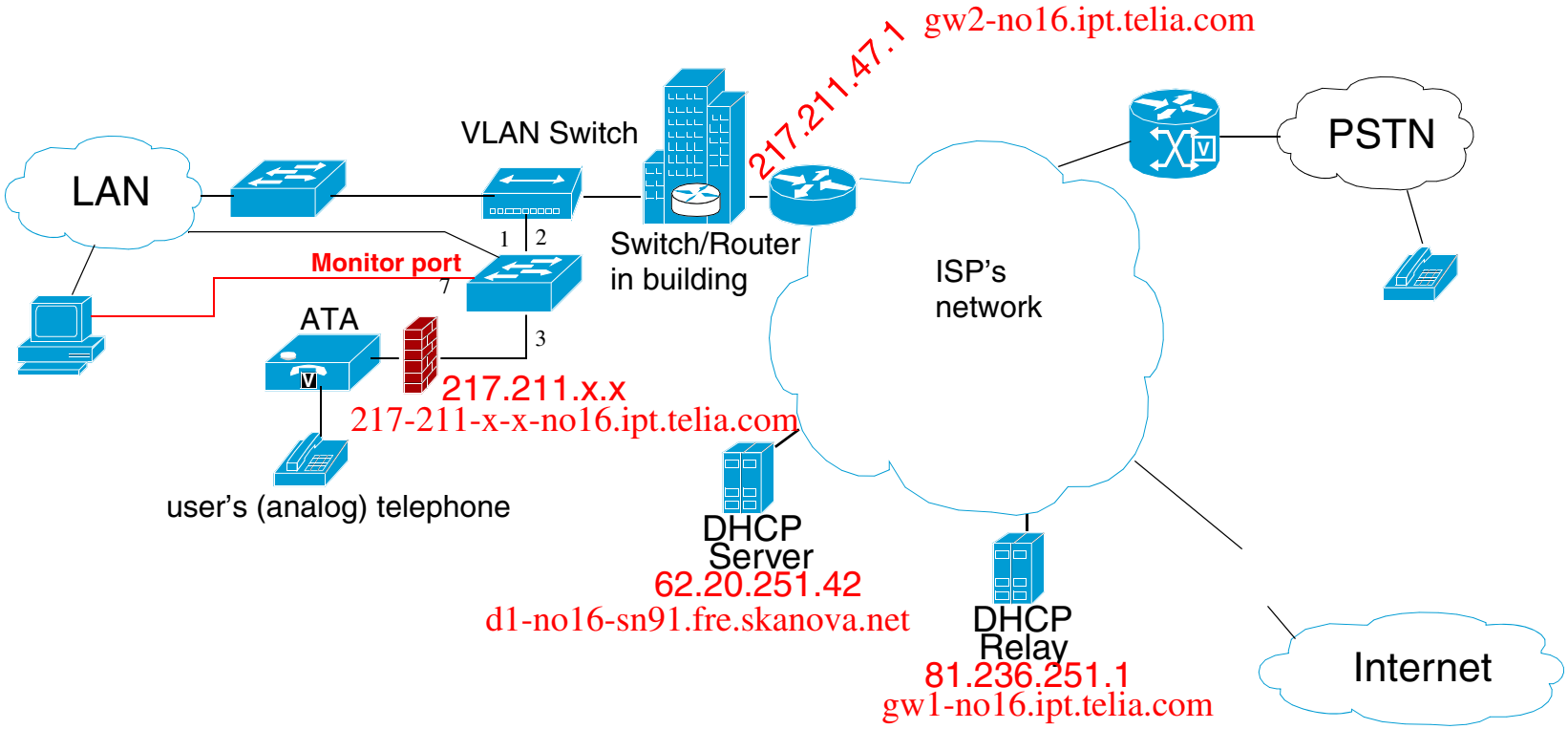


Figure 29: Learned the IP address of the ATA and also learned about additional entities: DHCP relay, DHCP server, default router

AS3301 includes: 217.208.0.0/13, 62.20.0.0/16, and 81.224.0.0/12

Incoming SIP INVITE

```
⊞ Ethernet II, Src: Cisco_3a:15:80 (00:0f:90:3a:15:80), Dst: Tilgin_43:9b:47 (00:02:61:43:9b:47)
⊞ Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211.
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊞ Request-Line: INVITE sip:+468313578@217.211.47.125:5060;transport=udp SIP/2.0
  ⊟ Message Header
    ⊞ v:SIP/2.0/UDP 90.226.251.75:5060;branch=z9hG4bK584ae9165f474239fa5a545dbe6eae45;lskpmc=P26
      Record-Route:<sip:90.226.251.75;routing_id=pcscf_b_side;lskpmc=P26;lr>
    ⊞ t:<sip:+468313578@ims.telia.com:5090>
    ⊞ f:"Anonymous"<sip:Anonymous@anonymous.invalid>;tag=snl_0015828889_NSN_CLIENT
      i:NSNSIP-862ee30a-862fe30a-2-21-1274283034-429883-1274712917
    ⊞ CSeq:1235 INVITE
    ⊞ m:<sip:pcscf1-hy-gm.ims.telia.com;transport=udp>
      Accept-Language:en;q=0.0
      Allow:REGISTER,INVITE,ACK,BYE,CANCEL,NOTIFY,REFER,UPDATE,PRACK
      k:timer
      Session-Expires:1800;refresher=uac
      Min-SE:1800
      Date:Wed, 19 May 2010 15:30:34 GMT
      Max-Forwards: 65
      c:application/sdp
      Content-Length: 135
      k:100rel
      P-Called-Party-ID:<sip:+468      @ims.telia.com>
  ⊟ Message Body
```

Figure 30: SIP INVITE

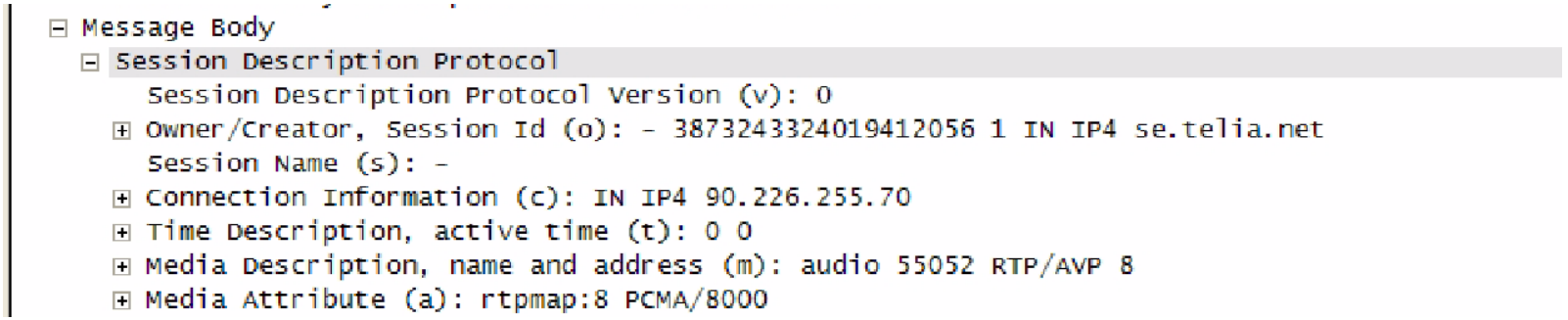


Figure 31: Message body of the INVITE

VoIP Gateway's address

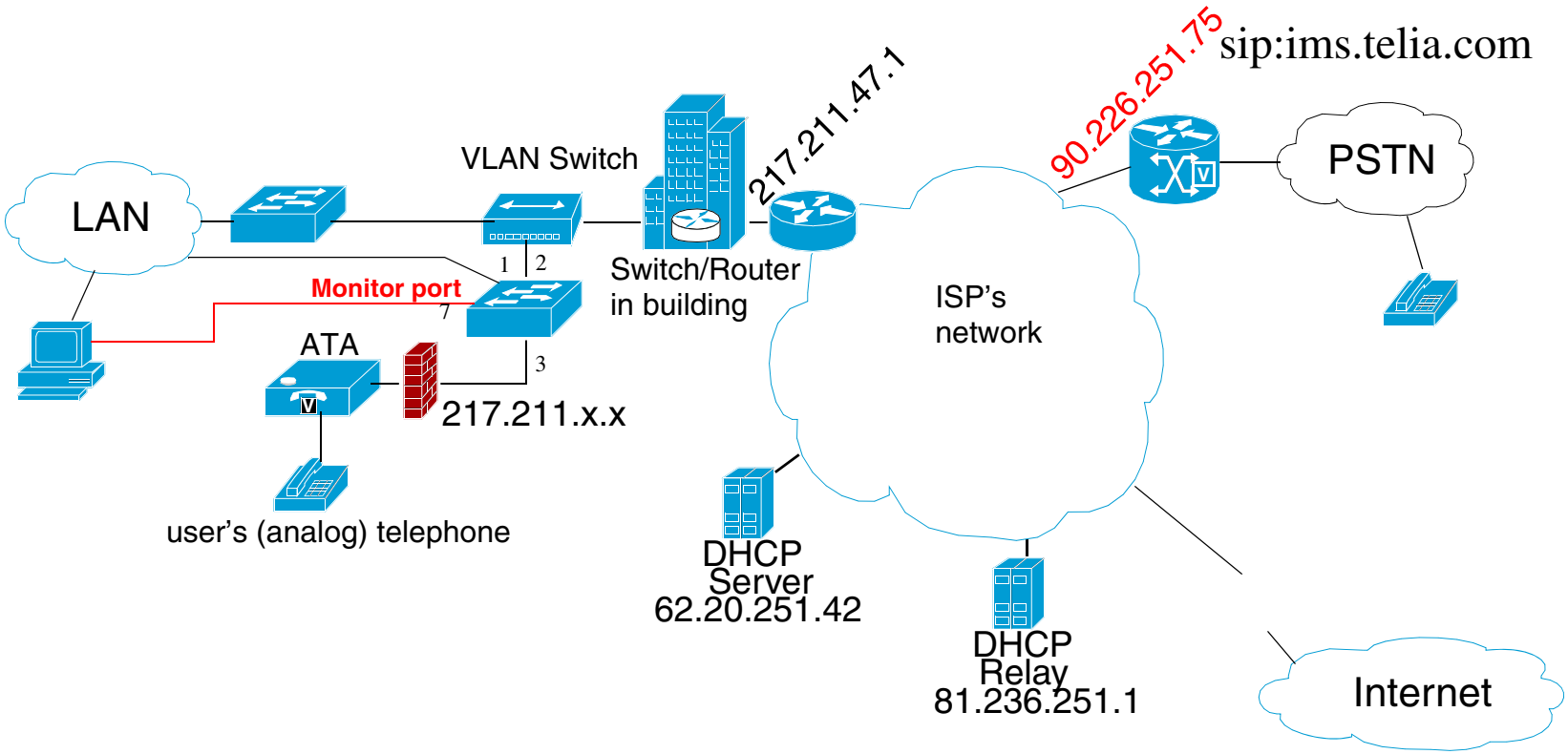


Figure 32: Learned the IP address of the SIP Registrar and Proxy (90.226.251.75)

180 Ringing

```
Frame 14 (677 bytes on wire, 677 bytes captured)
Ethernet II, Src: Tilgin_43:9b:47 (00:02:61:43:9b:47), Dst: Cisco_3a:15:80 (00:0f:90:3a:15:80)
Internet Protocol, Src: 217.211.                    , Dst: 90.226.251.75 (90.226.251.75)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
⊞ Status-Line: SIP/2.0 180 Ringing
⊟ Message Header
  ⊞ Via: SIP/2.0/UDP 90.226.251.75:5060;branch=z9hG4bK584ae9165f474239fa5a545dbe6eae45;lskpmc=P26
    Record-Route: <sip:90.226.251.75;routing_id=pcscf_b_side;lskpmc=P26;lr>
  ⊞ To: <sip:+468      @ims.telia.com>;tag=1274283034520173011
  ⊞ From: "Anonymous" <sip:Anonymous@anonymous.invalid>;tag=snl_0015828889_NSN_CLIENT
    Call-ID: NSNSIP-862ee30a-862fe30a-2-21-1274283034-429883-1274712917
  ⊞ CSeq: 1235 INVITE
    RSeq: 1
  ⊞ Contact: <sip:+468      @217.211.      :5060;transport=udp>
    Server: Telefonadapter - Telia Bredbandstelefoni
    X-NAT: nothing
    X-Serialnumber: V30100000000-0010493387
    Require: 100rel
    Content-Length: 0
```

Figure 33: 180 Ringing status message - the operator learns the serial number of the ATA

PRACK

```
⊞ Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211.
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Request-Line: PRACK sip:+468      @217.211.      :5060;transport=udp SIP/2.0
      Method: PRACK
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ v:SIP/2.0/UDP 90.226.251.75:5060;branch=z9hG4bK98b4bde1a54ce7c6c3a4d224a426a30a;lskpmc=P26
        Transport: UDP
        Sent-by Address: 90.226.251.75
        Sent-by port: 5060
        Branch: z9hG4bK98b4bde1a54ce7c6c3a4d224a426a30a
        lskpmc=P26
      Record-Route:<sip:90.226.251.75;routing_id=pcscf_b_side;lskpmc=P26;lr>
    ⊟ t:<sip:+468      @ims.telia.com:5090>;tag=1274283034520173011
        SIP to address: sip:+468      @ims.telia.com:5090
        SIP tag: 1274283034520173011
    ⊟ f:"Anonymous"<sip:Anonymous@anonymous.invalid>;tag=snl_0015828889_NSN_CLIENT
        SIP Display info: "Anonymous"
        SIP from address: sip:Anonymous@anonymous.invalid
        SIP tag: snl_0015828889_NSN_CLIENT
      i:NSNSIP-862ee30a-862fe30a-2-21-1274283034-429883-1274712917
    ⊟ CSeq:1236 PRACK
        Sequence Number: 1236
        Method: PRACK
    ⊟ RAck:1 1235 INVITE
        RSeq Sequence Number: 1
        CSeq Sequence Number: 1235
        CSeq Method: INVITE
      Max-Forwards: 66
      Content-Length: 0
```

200 OK

```
Internet Protocol, Src: 217.211.                    , Dst: 90.226.251.75 (90.226.251.75)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
⊟ Status-Line: SIP/2.0 200 OK
    Status-Code: 200
    [Resent Packet: False]
⊟ Message Header
  ⊟ Via: SIP/2.0/UDP 90.226.251.75:5060;branch=z9hG4bK98b4bde1a54ce7c6c3a4d224a426a30a;lskpmc=P26
      Transport: UDP
      Sent-by Address: 90.226.251.75
      Sent-by port: 5060
      Branch: z9hG4bK98b4bde1a54ce7c6c3a4d224a426a30a
      lskpmc=P26
    Record-Route: <sip:90.226.251.75;routing_id=pcscf_b_side;lskpmc=P26;lr>
  ⊟ To: <sip:+468      @ims.telia.com>;tag=1274283034520173011
      SIP to address: sip:+468      @ims.telia.com
      SIP tag: 1274283034520173011
  ⊟ From: "Anonymous" <sip:Anonymous@anonymous.invalid>;tag=snl_0015828889_NSN_CLIENT
      SIP Display info: "Anonymous"
      SIP from address: sip:Anonymous@anonymous.invalid
      SIP tag: snl_0015828889_NSN_CLIENT
    Call-ID: NSNSIP-862ee30a-862fe30a-2-21-1274283034-429883-1274712917
  ⊟ CSeq: 1236 PRACK
      Sequence Number: 1236
      Method: PRACK
  ⊟ Contact: <sip:+468      @217.211.      :5060;transport=udp>
    ⊞ Contact Binding: <sip:+468313578@217.211.      :5060;transport=udp>
    Supported: replaces, 100rel
    Server: Telefonadapter - Telia Bredbandstelefoni
    X-NAT: nothing
    X-Serialnumber: V30100000000-0010493387
    Content-Length: 0
```

CANCEL

```
⊞ Ethernet II, Src: Cisco_3a:15:80 (00:0f:90:3a:15:80), Dst: Tilgin_43:9b:47 (00:02:61:43:9b:47)
⊞ Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211.
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Request-Line: CANCEL sip:+468      @217.211.      :5060;transport=udp SIP/2.0
      Method: CANCEL
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ v:SIP/2.0/UDP 90.226.251.75:5060;branch=z9hG4bK584ae9165f474239fa5a545dbe6eae45;lskpmc=P26
        Transport: UDP
        Sent-by Address: 90.226.251.75
        Sent-by port: 5060
        Branch: z9hG4bK584ae9165f474239fa5a545dbe6eae45
        lskpmc=P26
    ⊟ t:<sip:+468      @ims.telia.com:5090>
        SIP to address: sip:+468      @ims.telia.com:5090
    ⊟ f:"Anonymous"<sip:Anonymous@anonymous.invalid>;tag=snl_0015828889_NSN_CLIENT
        SIP Display info: "Anonymous"
        SIP from address: sip:Anonymous@anonymous.invalid
        SIP tag: snl_0015828889_NSN_CLIENT
      i:NSNSIP-862ee30a-862fe30a-2-21-1274283034-429883-1274712917
    ⊟ CSeq:1235 CANCEL
        Sequence Number: 1235
        Method: CANCEL
      Max-Forwards: 65
    ⊟ Reason:Q.850;cause=31
        Reason Protocols: Q.850
        Cause: 31(0x1f)[Normal unspecified]
      Content-Length: 0
```

487 Request Terminated

```
Ethernet II, Src: Tilgin_43:9b:47 (00:02:61:43:9b:47), Dst: Cisco_3a:15:80 (00:0f:90:3a:15:80)
Internet Protocol, Src: 217.211.                    , Dst: 90.226.251.75 (90.226.251.75)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
  Status-Line: SIP/2.0 487 Request Terminated
    Status-Code: 487
    [Resent Packet: False]
  Message Header
    Via: SIP/2.0/UDP 90.226.251.75:5060;branch=z9hG4bK584ae9165f474239fa5a545dbe6eae45;lskpmc=P26
      Transport: UDP
      Sent-by Address: 90.226.251.75
      Sent-by port: 5060
      Branch: z9hG4bK584ae9165f474239fa5a545dbe6eae45
      lskpmc=P26
    Record-Route: <sip:90.226.251.75;routing_id=pcscf_b_side;lskpmc=P26;lr>
    To: <sip:+468      @ims.telia.com>;tag=1274283042430173012
      SIP to address: sip:+468      @ims.telia.com
      SIP tag: 1274283042430173012
    From: "Anonymous" <sip:Anonymous@anonymous.invalid>;tag=snl_0015828889_NSN_CLIENT
      SIP Display info: "Anonymous"
      SIP from address: sip:Anonymous@anonymous.invalid
      SIP tag: snl_0015828889_NSN_CLIENT
    Call-ID: NSNSIP-862ee30a-862fe30a-2-21-1274283034-429883-1274712917
    CSeq: 1235 INVITE
      Sequence Number: 1235
      Method: INVITE
    Server: Telefonadapter - Telia Bredbandstelefoni
    X-NAT: nothing
    X-Serialnumber: V30100000000-0010493387
    Content-Length: 0
```

ACK

```
⊞ Ethernet II, Src: Cisco_3a:15:80 (00:0f:90:3a:15:80), Dst: Tilgin_43:9b:47 (00:02:61:43:9b:47)
⊞ Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211.
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Request-Line: ACK sip:+468      @217.211.      :5060;transport=udp SIP/2.0
      Method: ACK
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ v:SIP/2.0/UDP 90.226.251.75:5060;branch=z9hG4bK584ae9165f474239fa5a545dbe6eae45;lskpmc=P26
        Transport: UDP
        Sent-by Address: 90.226.251.75
        Sent-by port: 5060
        Branch: z9hG4bK584ae9165f474239fa5a545dbe6eae45
        lskpmc=P26
    ⊟ t:<sip:+468      @ims.telia.com:5090>;tag=1274283042430173012
        SIP to address: sip:+468313578@ims.telia.com:5090
        SIP tag: 1274283042430173012
    ⊟ f:"Anonymous"<sip:Anonymous@anonymous.invalid>;tag=snl_0015828889_NSN_CLIENT
        SIP Display info: "Anonymous"
        SIP from address: sip:Anonymous@anonymous.invalid
        SIP tag: snl_0015828889_NSN_CLIENT
      i:NSNSIP-862ee30a-862fe30a-2-21-1274283034-429883-1274712917
    ⊟ CSeq:1235 ACK
        Sequence Number: 1235
        Method: ACK
      Max-Forwards: 65
      Content-Length: 0
```

200 OK

```
⊞ Internet Protocol, Src: 217.211.                    , Dst: 90.226.251.75 (90.226.251.75)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Status-Line: SIP/2.0 200 OK
      Status-Code: 200
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ Via: SIP/2.0/UDP 90.226.251.75:5060;branch=z9hG4bK584ae9165f474239fa5a545dbe6eae45;lskpmc=P26
        Transport: UDP
        Sent-by Address: 90.226.251.75
        Sent-by port: 5060
        Branch: z9hG4bK584ae9165f474239fa5a545dbe6eae45
        lskpmc=P26
    ⊟ To: <sip:+468      @ims.telia.com>;tag=1274283042440173013
        SIP to address: sip:+468      @ims.telia.com
        SIP tag: 1274283042440173013
    ⊟ From: "Anonymous" <sip:Anonymous@anonymous.invalid>;tag=snl_0015828889_NSN_CLIENT
        SIP Display info: "Anonymous"
        SIP from address: sip:Anonymous@anonymous.invalid
        SIP tag: snl_0015828889_NSN_CLIENT
      Call-ID: NSNSIP-862ee30a-862fe30a-2-21-1274283034-429883-1274712917
    ⊟ CSeq: 1235 CANCEL
        Sequence Number: 1235
        Method: CANCEL
      Supported: replaces, 100rel
      Server: Telefonadapter - Telia Bredbandstelefoni
      X-NAT: nothing
      X-Serialnumber: V30100000000-0010493387
      Content-Length: 0
```

Outgoing SIP INVITE

```
⊞ Internet Protocol, Src: 217.211.                          , Dst: 90.226.251.75 (90.226.251.75)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Request-Line: INVITE sip:001          @ims.telia.com;transport=udp SIP/2.0
      Method: INVITE
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ Via: SIP/2.0/UDP 217.211.       :5060;branch=z9hG4bK-1274283219410173016
        Transport: UDP
        Sent-by Address: 217.211.
        Sent-by port: 5060
        Branch: z9hG4bK-1274283219410173016
      Max-Forwards: 70
    ⊟ To: <sip:001          @ims.telia.com;transport=udp>
        SIP to address: sip:001          @ims.telia.com
    ⊟ From: +468       <sip:+468      @ims.telia.com>;tag=1274283219410173014
        SIP Display info: +468
        SIP from address: sip:+468      @ims.telia.com
        SIP tag: 1274283219410173014
      Call-ID: C-1274283219410173015@217.211.
    ⊟ CSeq: 10 INVITE
        Sequence Number: 10
        Method: INVITE
    ⊟ Contact: <sip:+468      @217.211.      :5060;transport=udp>
      ⊞ Contact Binding: <sip:+468      @217.211.4      :5060;transport=udp>
      Supported: replaces, 100rel
      User-Agent: Telefonadapter - Telia Bredbandstelefoni
      X-NAT: nothing
      X-Serialnumber: V30100000000-0010493387
      Allow: INVITE, UPDATE, ACK, PRACK, BYE, CANCEL, OPTIONS, INFO, REFER, NOTIFY, SUBSCRIBE
      Content-Length: 256
      Content-Type: application/sdp
```

SDP for this Outgoing INVITE

```
⊟ Message Body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): - 1274283219 1274283219 IN IP4 217.211.
      Session Name (s): -
    ⊞ Connection Information (c): IN IP4 217.211.
    ⊞ Time Description, active time (t): 0 0
    ⊞ Media Description, name and address (m): audio 8522 RTP/AVP 8 0 101
    ⊞ Media Attribute (a): rtpmap:8 PCMA/8000
    ⊞ Media Attribute (a): rtpmap:0 PCMU/8000
    ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
    ⊞ Media Attribute (a): fmtp:101 0-15,32,33,34,35,36
    ⊞ Media Attribute (a): ptime:20
      Media Attribute (a): sendrecv
```

100 Trying

```
⊞ Frame 25 (316 bytes on wire, 316 bytes captured)
⊞ Ethernet II, Src: Cisco_3a:15:80 (00:0f:90:3a:15:80), Dst: Tilgin_43:9b:47 (00:02:61:43:9b:47)
⊞ Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211.
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Status-Line: SIP/2.0 100 Trying
      Status-Code: 100
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ v:SIP/2.0/UDP 217.211        :5060;branch=z9hG4bK-1274283219410173016
        Transport: UDP
        Sent-by Address: 217.211.
        Sent-by port: 5060
        Branch: z9hG4bK-1274283219410173016
    ⊟ t:<sip:0017184296635@ims.telia.com;transport=udp>
        SIP to address: sip:001          @ims.telia.com
    ⊟ f:"+468313578"<sip:+468313578@ims.telia.com>;tag=1274283219410173014
        SIP Display info: "+468       "
        SIP from address: sip:+468      @ims.telia.com
        SIP tag: 1274283219410173014
      i:C-1274283219410173015@217.211.
    ⊟ CSeq:10 INVITE
        Sequence Number: 10
        Method: INVITE
      Content-Length: 0
```

407 Authentication Required

```
⊞ Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211.
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Status-Line: SIP/2.0 407 Proxy Authentication Required
      Status-Code: 407
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ v:SIP/2.0/UDP 217.211.47.125:5060;branch=z9hG4bK-127428321941017 3016
        Transport: UDP
        Sent-by Address: 217.211.
        Sent-by port: 5060
        Branch: z9hG4bK-127428321941017 3016
    ⊟ t:<sip:0017184296635@ims.telia.com;transport=udp>;tag=818385135
        SIP to address: sip:0017184296635@ims.telia.com
        SIP tag: 818385135
    ⊟ f:"+468313578"<sip:+46       @ims.telia.com>;tag=127428321941017 3014
        SIP Display info: "+46       "
        SIP from address: sip:+468      @ims.telia.com
        SIP tag: 127428321941017 3014
      i:C-127428321941017 3015@217.211.
    ⊟ CSeq:10 INVITE
        Sequence Number: 10
        Method: INVITE
    ⊟ Proxy-Authenticate:Digest realm="ims.telia.com",nonce="43cf5bdd4bf404d3-f22b68ebc133160b7ad283e5a8bb3df5",qop="auth"
        Authentication Scheme: Digest
        Realm: "ims.telia.com"
        Nonce Value: "43cf5bdd4bf404d3-f22b68ebc133160b7ad283e5a8bb3df5"
        QOP: "auth"
      Content-Length: 0
```

ACK

```
⊞ Internet Protocol, Src: 217.211.                          , Dst: 90.226.251.75 (90.226.251.75)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Request-Line: ACK sip:001          @ims.telia.com;transport=udp SIP/2.0
      Method: ACK
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ Via: SIP/2.0/UDP 217.211.       :5060;branch=z9hG4bK-1274283219410173016
        Transport: UDP
        Sent-by Address: 217.211.
        Sent-by port: 5060
        Branch: z9hG4bK-1274283219410173016
      Max-Forwards: 70
    ⊟ To: <sip:001          @ims.telia.com;transport=udp>;tag=818385135
        SIP to address: sip:001          @ims.telia.com
        SIP tag: 818385135
    ⊟ From: +468       <sip:+468      @ims.telia.com>;tag=1274283219410173014
        SIP Display info: +468
        SIP from address: sip:+468      @ims.telia.com
        SIP tag: 1274283219410173014
      Call-ID: C-1274283219410173015@217.211.
    ⊟ CSeq: 10 ACK
        Sequence Number: 10
        Method: ACK
      User-Agent: Telefonadapter - Telia Bredbandstelefoni
      X-NAT: nothing
      X-Serialnumber: V30100000000-0010493387
      Content-Length: 0
```

Second SIP INVITE

```
⊞ Internet Protocol, Src: 217.211.                          , Dst: 90.226.251.75 (90.226.251.75)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Request-Line: INVITE sip:001          @ims.telia.com;transport=udp SIP/2.0
      Method: INVITE
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ Via: SIP/2.0/UDP 217.211        :5060;branch=z9hG4bK-1274283219470173017
        Transport: UDP
        Sent-by Address: 217.211.
        Sent-by port: 5060
        Branch: z9hG4bK-1274283219470173017
      Max-Forwards: 70
    ⊟ To: <sip:001          @ims.telia.com;transport=udp>
        SIP to address: sip:001          @ims.telia.com
    ⊟ From: +468313578 <sip:+468      @ims.telia.com>;tag=1274283219410173014
        SIP Display info: +468
        SIP from address: sip:+468      @ims.telia.com
        SIP tag: 1274283219410173014
      Call-ID: C-12742832194101730l5@217.211.
    ⊟ CSeq: 11 INVITE
        Sequence Number: 11
        Method: INVITE
    ⊟ Contact: <sip:+468      @217.211.       :5060;transport=udp>
      ⊞ Contact Binding: <sip:+468      @217.211        :5060;transport=udp>
      Supported: replaces, 100rel
      User-Agent: Telefonadapter - Telia Bredbandstelefoni
      X-NAT: nothing
      X-Serialnumber: V30100000000-0010493387
      Allow: INVITE, UPDATE, ACK, PRACK, BYE, CANCEL, OPTIONS, INFO, REFER, NOTIFY, SUBSCRIBE
```

Authentication and SDP

```
⊟ Proxy-Authorization: Digest username="+468      @ims.telia.com",realm="ims.telia.com",nonce="43cf5bdd4bf404d3-f22b68ebc133160b7ad283e5a8bb3df5",
    Authentication Scheme: Digest
    Username: "+468      @ims.telia.com"
    Realm: "ims.telia.com"
    Nonce Value: "43cf5bdd4bf404d3-f22b68ebc133160b7ad283e5a8bb3df5"
    Authentication URI: "sip:001          @ims.telia.com;transport=udp"
    QOP: auth
    Nonce Count: 00000001
    CNonce Value: "b311f4a1"
    Digest Authentication Response: "b9254dce90d2df3382aa472190daddd9"
  Content-Length: 256
  Content-Type: application/sdp
⊟ Message Body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): - 1274283219 1274283219 IN IP4 217.211.
      Session Name (s): -
    ⊞ Connection Information (c): IN IP4 217.211.
    ⊞ Time Description, active time (t): 0 0
    ⊞ Media Description, name and address (m): audio 8522 RTP/AVP 8 0 101
    ⊞ Media Attribute (a): rtpmap:8 PCMA/8000
    ⊞ Media Attribute (a): rtpmap:0 PCMU/8000
    ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
    ⊞ Media Attribute (a): fmtp:101 0-15,32,33,34,35,36
    ⊞ Media Attribute (a): ptime:20
      Media Attribute (a): sendrecv
```

100 Trying (again)

```
⊞ Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211.
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Status-Line: SIP/2.0 100 Trying
      Status-Code: 100
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ v:SIP/2.0/UDP 217.211.       :5060;branch=z9hG4bK-1274283219470173017
        Transport: UDP
        Sent-by Address: 217.211.
        Sent-by port: 5060
        Branch: z9hG4bK-1274283219470173017
    ⊟ t:<sip:001          @ims.telia.com;transport=udp>
        SIP to address: sip:001          @ims.telia.com
    ⊟ f:"+468313578"<sip:+468       @ims.telia.com>;tag=1274283219410173014
        SIP Display info: "+468       '
        SIP from address: sip:+468      @ims.telia.com
        SIP tag: 1274283219410173014
      i:C-1274283219410173015@217.211.
    ⊟ CSeq:11 INVITE
        Sequence Number: 11
        Method: INVITE
      Content-Length: 0
```

First RTP packet from operator

```
⊞ Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211.
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Status-Line: SIP/2.0 100 Trying
      Status-Code: 100
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ v:SIP/2.0/UDP 217.211.       :5060;branch=z9hG4bK-127428321947017 3017
        Transport: UDP
        Sent-by Address: 217.211.
        Sent-by port: 5060
        Branch: z9hG4bK-127428321947017 3017
    ⊟ t:<sip:001          @ims.telia.com;transport=udp>
        SIP to address: sip:001          @ims.telia.com
    ⊟ f:"+468      "<sip:+468      @ims.telia.com>;tag=127428321941017 3014
        SIP Display info: "+468
        SIP from address: sip:+468      @ims.telia.com
        SIP tag: 127428321941017 3014
      i:c-127428321941017 3015@217.211.
    ⊟ CSeq:11 INVITE
        Sequence Number: 11
        Method: INVITE
      Content-Length: 0
```

180 Ringing

```
⊞ Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211.
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Status-Line: SIP/2.0 180 Ringing
      Status-Code: 180
      [Resent Packet: False]
  ⊟ Message Header
      i:C-1274283219410173015@217.211.
    ⊟ CSeq:11 INVITE
        Sequence Number: 11
        Method: INVITE
    ⊟ f:"+468      "<sip:+468      @ims.telia.com>;tag=1274283219410173014
        SIP Display info: "+468      "
        SIP from address: sip:+468      @ims.telia.com
        SIP tag: 1274283219410173014
    ⊟ t:<sip:001          @ims.telia.com;transport=udp>;tag=snl_0015830550
        SIP to address: sip:001          @ims.telia.com
        SIP tag: snl_0015830550
      Record-Route:<sip:90.226.251.75;routing_id=pcscf_a_side;lskpmc=P26;lr>
    ⊟ v:SIP/2.0/UDP 217.211.47.125:5060;branch=z9hG4bK-1274283219470173017
        Transport: UDP
        Sent-by Address: 217.211.
        Sent-by port: 5060
        Branch: z9hG4bK-1274283219470173017
    ⊟ m:<sip:pcscf1-hy-gm.ims.telia.com;transport=udp>
      ⊞ Contact Binding: <sip:pcscf1-hy-gm.ims.telia.com;transport=udp>
      Allow:REGISTER,INVITE,ACK,BYE,CANCEL,NOTIFY,REFER,UPDATE,PRACK
      Require:100rel
      RSeq: 1
```

180 Ringing SDP

```
⊟ m:<sip:pcscf1-hy-gm.ims.telia.com;transport=udp>
  ⊞ Contact Binding: <sip:pcscf1-hy-gm.ims.telia.com;transport=udp>
  Allow:REGISTER,INVITE,ACK,BYE,CANCEL,NOTIFY,REFER,UPDATE,PRACK
  Require:100rel
  RSeq: 1
  Date:Wed, 19 May 2010 15:33:42 GMT
  c:application/sdp
  Content-Length: 148
  u:CCNR
  P-Com.Siemens.Calling-Party-ID:<sip:+468      @ims.telia.com>
⊟ Message Body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): - 3873119333275827371 1 IN IP4 se.telia.net
      Session Name (s): -
    ⊞ Connection Information (c): IN IP4 90.226.255.198
    ⊞ Time Description, active time (t): 0 0
      Session Attribute (a): sendrecv
    ⊞ Media Description, name and address (m): audio 41904 RTP/AVP 8
    ⊞ Media Attribute (a): rtpmap:8 PCMA/8000
```

First outgoing RTP packet from ATA

26	0.028008	90.226.251.75		SIP	Status: 407 Proxy Authentication Required
27	0.017635		90.226.251.75	SIP	Request: ACK sip:001 @ims.telia.com;transport=udp
28	0.000485		90.226.251.75	SIP/SDP	Request: INVITE sip:001 @ims.telia.com;transport=udp, with session description
29	0.014385	90.226.251.75		SIP	Status: 100 Trying
30	3.012548	90.226.255.198		RTP	PT=ITU-T G.711 PCMA, SSRC=0x6674FDAE, Seq=139, Time=61667
31	0.002996	90.226.251.75		SIP/SDP	Status: 180 Ringing, with session description
32	0.010633		90.226.255.198	RTP	PT=ITU-T G.711 PCMA, SSRC=0xF99F2232, Seq=12021, Time=115504431
33	0.006376	90.226.255.198		RTP	PT=ITU-T G.711 PCMA, SSRC=0x6674FDAE, Seq=140, Time=61827
34	0.011737		90.226.251.75	SIP	Request: PRACK sip:pcscf1-hy-gm.ims.telia.com;transport=udp
35	0.001864		90.226.255.198	RTP	PT=ITU-T G.711 PCMA, SSRC=0xF99F2232, Seq=65062, Time=1668160239
36	0.006404	90.226.255.198		RTP	PT=ITU-T G.711 PCMA, SSRC=0x6674FDAE, Seq=141, Time=61987

```
⊞ Frame 32 (214 bytes on wire, 214 bytes captured)
⊞ Ethernet II, Src: Tilgin_43:9b:47 (00:02:61:43:9b:47), Dst: Cisco_3a:15:80 (00:0f:90:3a:15:80)
⊞ Internet Protocol, Src: 217.211.                    , Dst: 90.226.255.198 (90.226.255.198)
⊞ User Datagram Protocol, Src Port: 8522 (8522), Dst Port: 41904 (41904)
⊟ Real-Time Transport Protocol
  ⊞ [Stream setup by SDP (frame 31)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: ITU-T G.711 PCMA (8)
    Sequence number: 12021
    [Extended sequence number: 77557]
    Timestamp: 115504431
    Synchronization Source identifier: 0xf99f2232 (4187955762)
    Payload: 545454555455555D555D5545454545455D4D4D4D4D7D6D6...
```

Second packet from operator

```
⊞ Internet Protocol, Src: 90.226.255.198 (90.226.255.198), Dst: 217.211.
⊞ User Datagram Protocol, Src Port: 41904 (41904), Dst Port: 8522 (8522)
⊟ Real-Time Transport Protocol
  ⊞ [Stream setup by SDP (frame 28)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: ITU-T G.711 PCMA (8)
    Sequence number: 140
    [Extended sequence number: 65676]
    Timestamp: 61827
    Synchronization Source identifier: 0x6674fdae (1718943150)
    Payload: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF...
```

Outgoing PRACK

```
⊞ Internet Protocol, Src: 217.211.                    , Dst: 90.226.251.75 (90.226.251.75)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Request-Line: PRACK sip:pcscf1-hy-gm.ims.telia.com;transport=udp SIP/2.0
      Method: PRACK
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ Via: SIP/2.0/UDP 217.211.      :5060;branch=z9hG4bK-1274283222530173018
        Transport: UDP
        Sent-by Address: 217.211.
        Sent-by port: 5060
        Branch: z9hG4bK-1274283222530173018
      Max-Forwards: 70
      Route: <sip:90.226.251.75;routing_id=pcscf_a_side;lskpmc=P26;lr>
    ⊟ To: <sip:001          @ims.telia.com;transport=udp>;tag=snl_0015830550
        SIP to address: sip:001          @ims.telia.com
        SIP tag: snl_0015830550
    ⊟ From: +468313578 <sip:+468      @ims.telia.com>;tag=1274283219410173014
        SIP Display info: +468
        SIP from address: sip:+468      @ims.telia.com
        SIP tag: 1274283219410173014
      Call-ID: C-1274283219410173015@217.211.
    ⊟ CSeq: 12 PRACK
        Sequence Number: 12
        Method: PRACK
    ⊟ RAck: 1 11 INVITE
        RSeq Sequence Number: 1
        CSeq Sequence Number: 11
        CSeq Method: INVITE
```

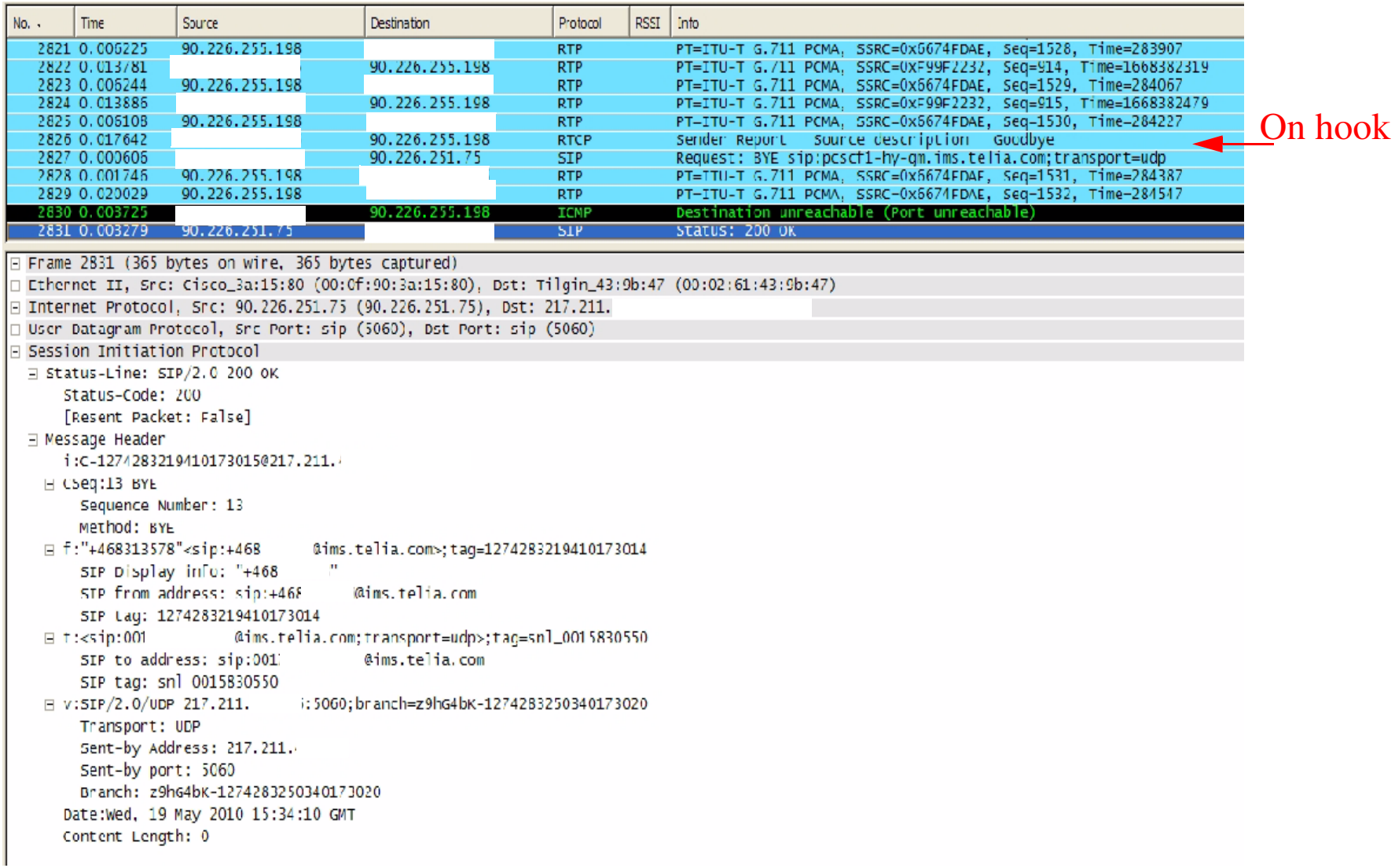
Authorization for outgoing PRACK

```
⊟ Contact: <sip:+468      @217.211.      :5060;transport=udp>
  ⊞ Contact Binding: <sip:+468      @217.211.      :5060;transport=udp>
  Supported: replaces, 100rel
  User-Agent: Telefonadapter - Telia Bredbandstelefoni
  X-NAT: nothing
  X-Serialnumber: V30100000000-0010493387
⊟ Proxy-Authorization: Digest username="+468      @ims.telia.com",realm="ims.telia.com",nonce="43
    Authentication Scheme: Digest
    Username: "+468      @ims.telia.com"
    Realm: "ims.telia.com"
    Nonce Value: "43cf5bdd4bf404d3-f22b68ebc133160b7ad283e5a8bb3df5"
    Authentication URI: "sip:001          @ims.telia.com;transport=udp"
    QOP: auth
    Nonce Count: 00000002
    CNonce Value: "b311f4a1"
```

200 OK

```
+ Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211.
+ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
- Session Initiation Protocol
  - Status-Line: SIP/2.0 200 OK
      Status-Code: 200
      [Resent Packet: False]
  - Message Header
      i:c-1274283219410173015@217.211.
    - CSeq:12 PRACK
        Sequence Number: 12
        Method: PRACK
    - f:"+468      "<sip:+468      @ims.telia.com>;tag=1274283219410173014
        SIP Display info: "+468      "
        SIP from address: sip:+468      @ims.telia.com
        SIP tag: 1274283219410173014
    - t:<sip:001          @ims.telia.com;transport=udp>;tag=snl_0015830550
        SIP to address: sip:0017184296635@ims.telia.com
        SIP tag: snl_0015830550
      Record-Route:<sip:90.226.251.75;routing_id=pcscf_a_side;lskpmc=P26;lr>
    - v:SIP/2.0/UDP 217.211.      :5060;branch=z9hG4bK-1274283222530173018
        Transport: UDP
        Sent-by Address: 217.211.
        Sent-by port: 5060
        Branch: z9hG4bK-1274283222530173018
    - m:<sip:pcscf1-hy-gm.ims.telia.com;transport=udp>
      - Contact Binding: <sip:pcscf1-hy-gm.ims.telia.com;transport=udp>
        - URI: <sip:pcscf1-hy-gm.ims.telia.com;transport=udp>
            SIP contact address: sip:pcscf1-hy-gm.ims.telia.com
      Content-Length: 0
```

End of outgoing call



No.	Time	Source	Destination	Protocol	RSSI	Info
2821	0.006225	90.226.255.198		RTP		PT=ITU-T G.711 PCMA, SSRC=0x6674FDAE, Seq=1528, Time=283907
2822	0.013781		90.226.255.198	RTP		PT=ITU-T G.711 PCMA, SSRC=0xF99F2232, Seq=914, Time=1668382319
2823	0.006244	90.226.255.198		RTP		PT=ITU-T G.711 PCMA, SSRC=0x6674FDAE, Seq=1529, Time=284067
2824	0.013886		90.226.255.198	RTP		PT=ITU-T G.711 PCMA, SSRC=0xF99F2232, Seq=915, Time=1668382479
2825	0.006108	90.226.255.198		RTP		PT=ITU-T G.711 PCMA, SSRC=0x6674FDAE, Seq=1530, Time=284227
2826	0.017642		90.226.255.198	RTCP		Sender Report Source description Goodbye
2827	0.000606		90.226.251.75	SIP		Request: BYE sip:pcscf1-hy-gm.ims.telia.com;transport=udp
2828	0.001746	90.226.255.198		RTP		PT=ITU-T G.711 PCMA, SSRC=0x6674FDAE, Seq=1531, Time=284387
2829	0.020029	90.226.255.198		RTP		PT=ITU-T G.711 PCMA, SSRC=0x6674FDAE, Seq=1532, Time=284547
2830	0.003725		90.226.255.198	ICMP		Destination unreachable (Port unreachable)
2831	0.003279	90.226.251.75		SIP		Status: 200 OK

On hook

```
Frame 2831 (365 bytes on wire, 365 bytes captured)
Ethernet II, Src: Cisco_3a:15:80 (00:0f:90:3a:15:80), Dst: Tilgin_43:9b:47 (00:02:61:43:9b:47)
Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211.
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
  Status-Line: SIP/2.0 200 OK
    Status-Code: 200
    [Resent Packet: False]
  Message Header
    i:C-1274283219410173015@217.211.
    CSeq:13 BYE
      Sequence Number: 13
      Method: BYE
    f:"+468313578"<sip:+468      @ims.telia.com>;tag=1274283219410173014
      SIP Display info: "+468      "
      SIP from address: sip:+468      @ims.telia.com
      SIP tag: 1274283219410173014
    t:<sip:001          @ims.telia.com;transport=udp>;tag=snl_0015830550
      SIP to address: sip:001          @ims.telia.com
      SIP tag: snl_0015830550
    v:SIP/2.0/UDP 217.211.      :5060;branch=z9hG4bK-1274283250340173020
      Transport: UDP
      Sent-by Address: 217.211.
      Sent-by port: 5060
      Branch: z9hG4bK-1274283250340173020
    Date:Wed, 19 May 2010 15:34:10 GMT
    Content Length: 0
```

RTP Sender Report Goodbye

```
⊞ Internet Protocol, Src: 217.211.                    , Dst: 90.226.255.198 (90.226.255.198)
⊞ User Datagram Protocol, Src Port: 8523 (8523), Dst Port: 41905 (41905)
⊞ Real-time Transport Control Protocol (Sender Report)
⊞ Real-time Transport Control Protocol (Source description)
⊟ Real-time Transport Control Protocol (Goodbye)
  ⊞ [Stream setup by SDP (frame 31)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 0001 = Source count: 1
    Packet type: Goodbye (203)
    Length: 1 (8 bytes)
    Identifier: 0xf99f2232 (4187955762)
  [RTCP frame length check: OK - 92 bytes]
```

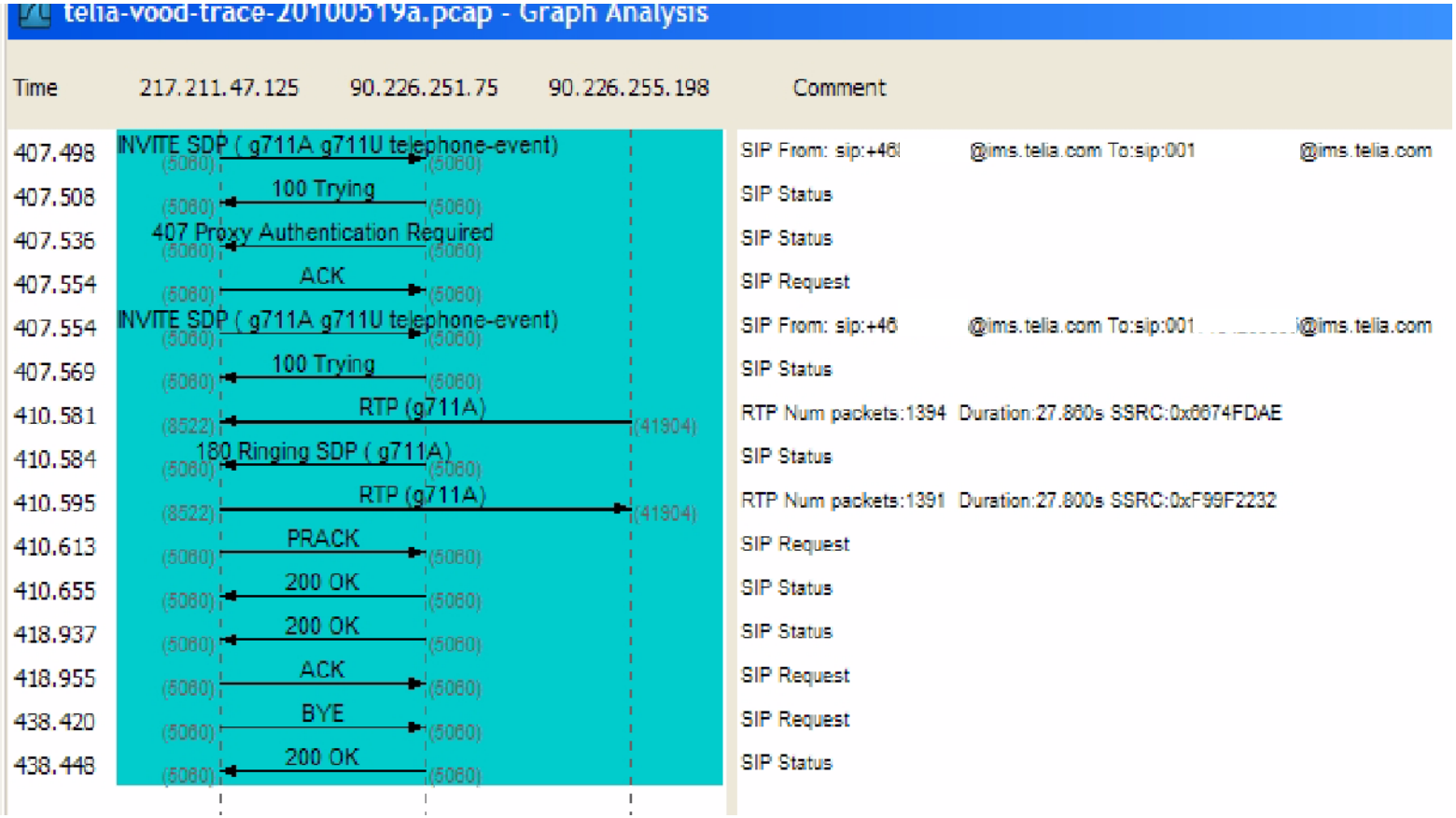
SIP Bye

```
⊞ Internet Protocol, Src: 217.211.                    , Dst: 90.226.251.75 (90.226.251.75)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊟ Request-Line: BYE sip:pcscf1-hy-gm.ims.telia.com;transport=udp SIP/2.0
      Method: BYE
      [Resent Packet: False]
  ⊟ Message Header
    ⊟ Via: SIP/2.0/UDP 217.211.       :5060;branch=z9hG4bK-1274283250340173020
        Transport: UDP
        Sent-by Address: 217.211.
        Sent-by port: 5060
        Branch: z9hG4bK-1274283250340173020
      Max-Forwards: 70
      Route: <sip:90.226.251.75;routing_id=pcscf_a_side;lskpmc=P26;lr>
    ⊟ To: <sip:001          @ims.telia.com;transport=udp>;tag=snl_0015830550
        SIP to address: sip:001          @ims.telia.com
        SIP tag: snl_0015830550
    ⊟ From: +468313578 <sip:+468       @ims.telia.com>;tag=1274283219410173014
        SIP Display info: +468
        SIP from address: sip:+468      @ims.telia.com
        SIP tag: 1274283219410173014
      Call-ID: C-1274283219410173015@217.211.
    ⊟ CSeq: 13 BYE
        Sequence Number: 13
        Method: BYE
```

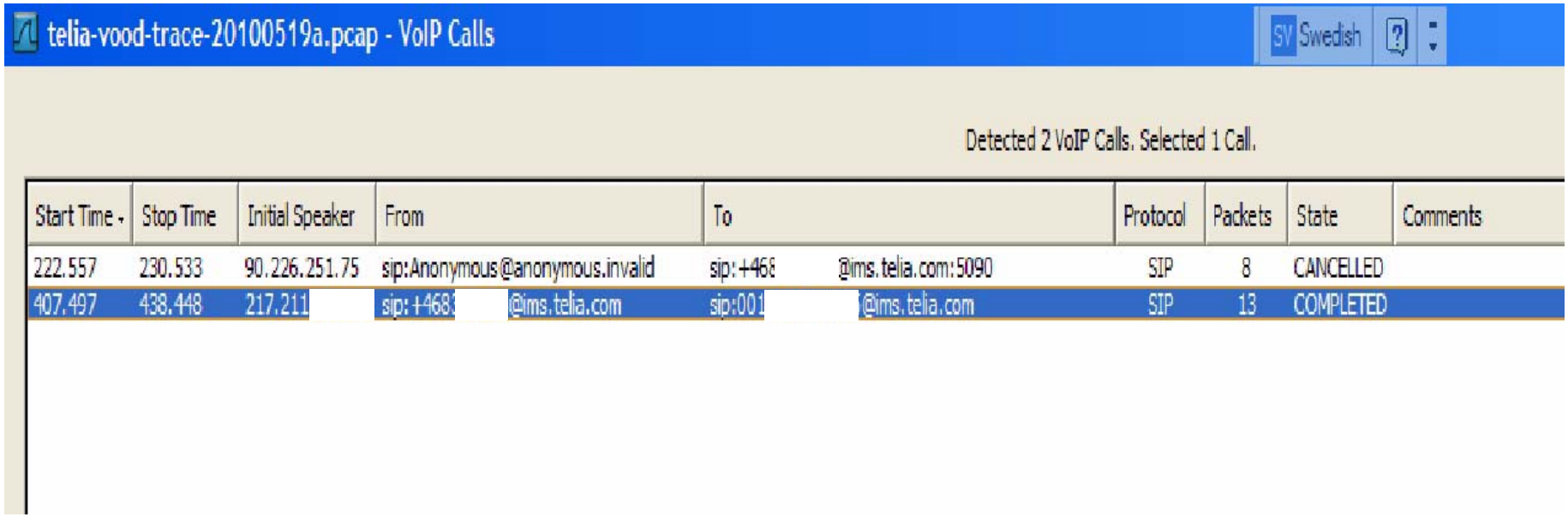
The Contact and Authentication for SIP BYE

```
CSeq: 13 BYE
  Sequence Number: 13
  Method: BYE
Contact: <sip:+468      @217.211.      :5060;transport=udp>
  Contact Binding: <sip:+468      @217.211.      :5060;transport=udp>
    URI: <sip:+468_____@217.211.      :5060;transport=udp>
      SIP contact address: sip:+468      @217.211.      :5060
  Supported: replaces, 100rel
  User-Agent: Telefonadapter - Telia Bredbandstelefoni
  X-NAT: nothing
  X-Serialnumber: V30100000000-0010493387
Proxy-Authorization: Digest username="+468      @ims.telia.com",realm="ims.telia.
  Authentication Scheme: Digest
  Username: "+468_____@ims.telia.com"
  Realm: "ims.telia.com"
  Nonce Value: "43cf5bdd4bf404d3-f22b68ebc133160b7ad283e5a8bb3df5"
  Authentication URI: "sip:0017184296635@ims.telia.com;transport=udp"
  QOP: auth
  Nonce Count: 00000003
  CNonce Value: "b311f4a1"
  Digest Authentication Response: "d43bca6a38700f9a40b2c928983e709c"
Content-Length: 0
```

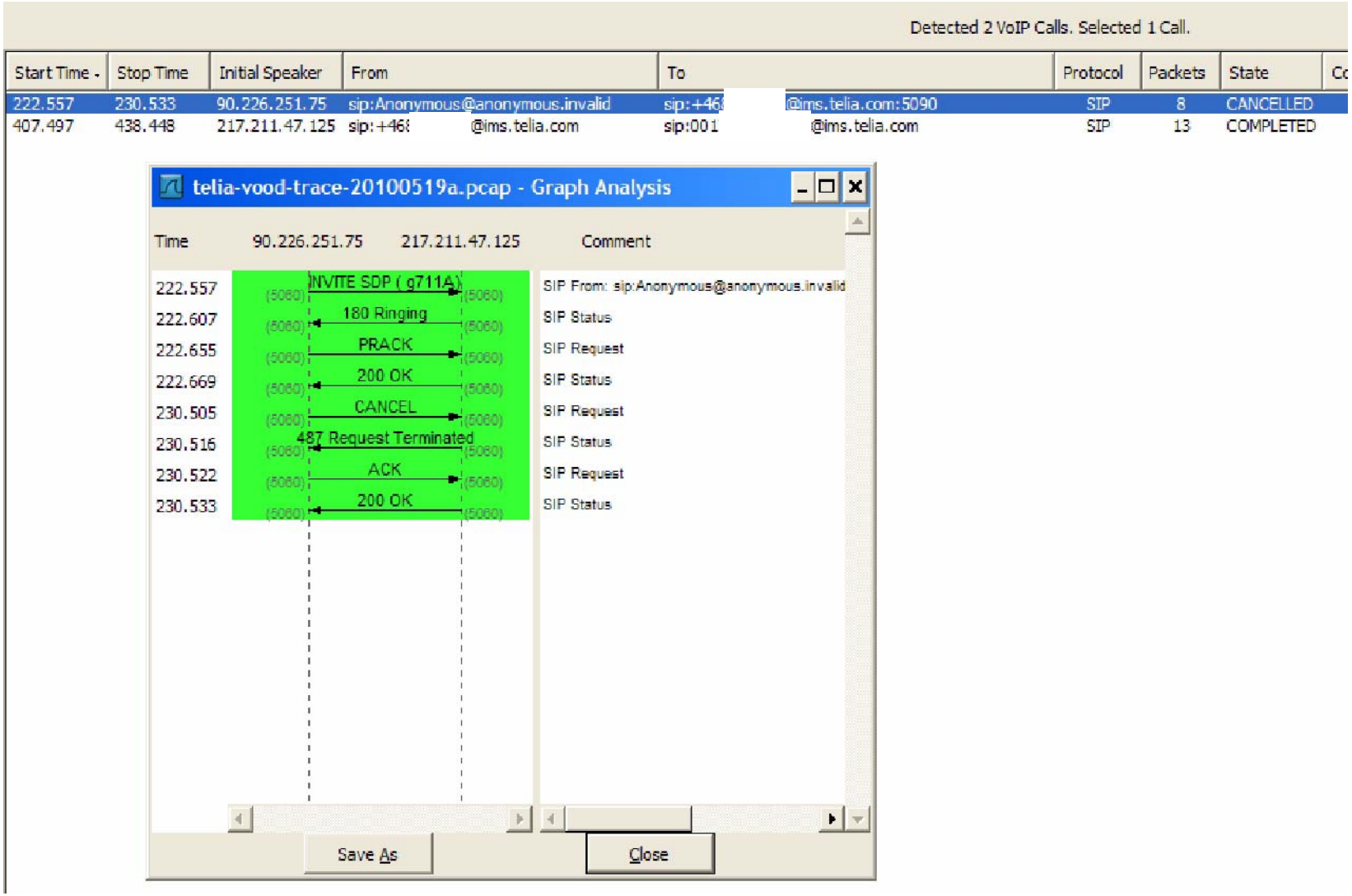
Outgoing call graph



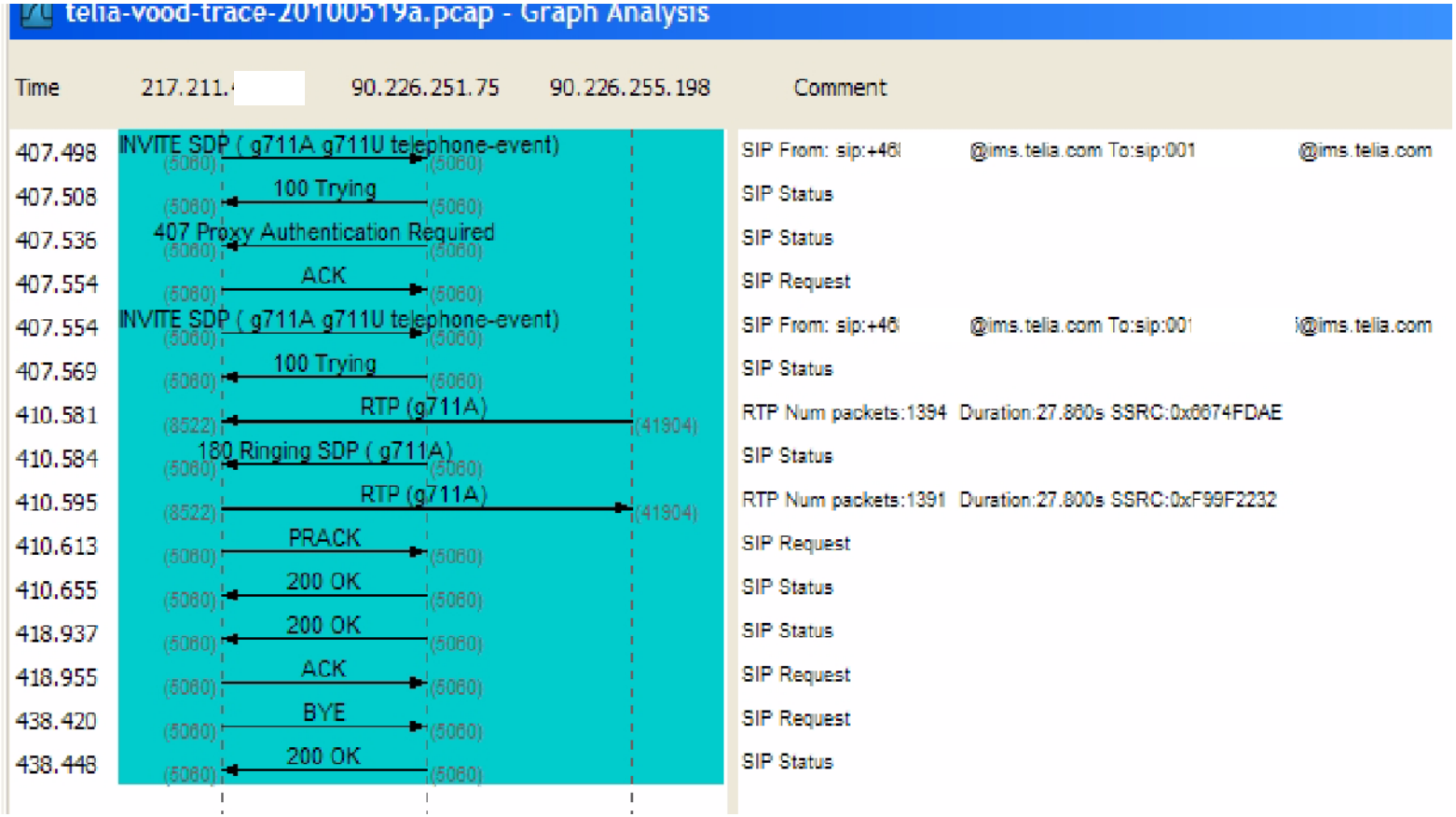
Wireshark Analysis-Two calls



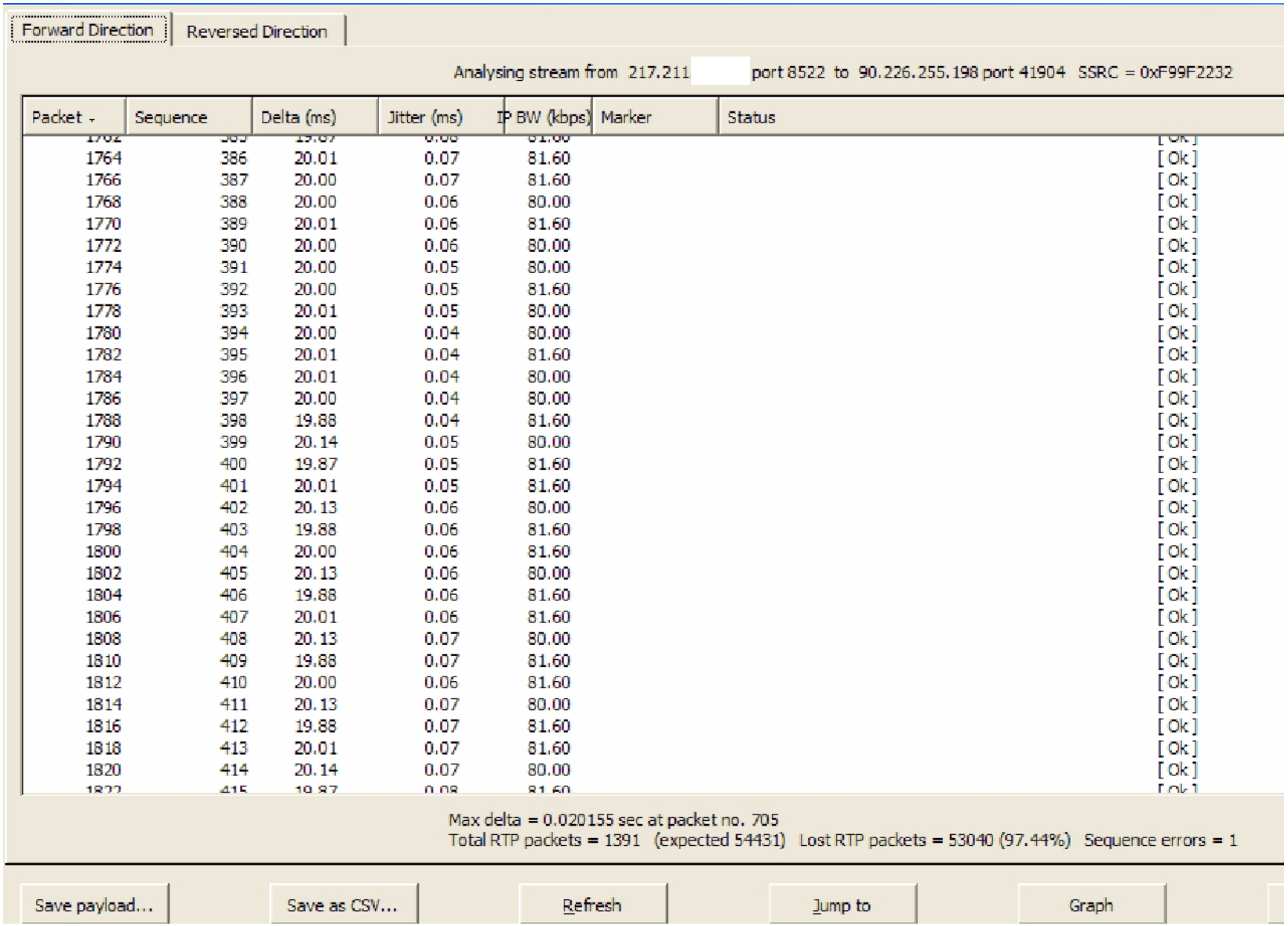
First Call


Detected 2 VoIP Calls. Selected 1 Call.
Start Time
Stop Time
Initial Speaker
From
To
Protocol
Packets
State
222.557
230.533
90.226.251.75
sip:Anonymous@anonymous.invalid
@ims.telia.com:5090
SIP
8
CANCELLED
407.497
438.448
217.211.47.125
@ims.telia.com
sip:001
@ims.telia.com
SIP
13
COMPLETED
telia-vood-trace-20100519a.pcap - Graph Analysis
Time
90.226.251.75
217.211.47.125
Comment
222.557
INVITE SDP (g711A)
SIP From: sip:Anonymous@anonymous.invalid
222.607
180 Ringing
SIP Status
222.655
PRACK
SIP Request
222.669
200 OK
SIP Status
230.505
CANCEL
SIP Request
230.516
487 Request Terminated
SIP Status
230.522
ACK
SIP Request
230.533
200 OK
SIP Status
Save As
Close

Second Call


telia-vood-trace-20100519a.pcap - Graph Analysis
Time
217.211.
90.226.251.75
90.226.255.198
Comment
407.498
INVITE SDP (g711A g711U telephone-event)
SIP From: sip:+46 @ims.telia.com To:sip:001 @ims.telia.com
407.508
100 Trying
SIP Status
407.536
407 Proxy Authentication Required
SIP Status
407.554
ACK
SIP Request
407.554
INVITE SDP (g711A g711U telephone-event)
SIP From: sip:+46 @ims.telia.com To:sip:001 @ims.telia.com
407.569
100 Trying
SIP Status
410.581
RTP (g711A)
RTP Num packets:1394 Duration:27.860s SSRC:0x0674FDAE
410.584
180 Ringing SDP (g711A)
SIP Status
410.595
RTP (g711A)
RTP Num packets:1391 Duration:27.800s SSRC:0xF99F2232
410.613
PRACK
SIP Request
410.655
200 OK
SIP Status
418.937
200 OK
SIP Status
418.955
ACK
SIP Request
438.420
BYE
SIP Request
438.448
200 OK
SIP Status

RTP statistics (some examples)



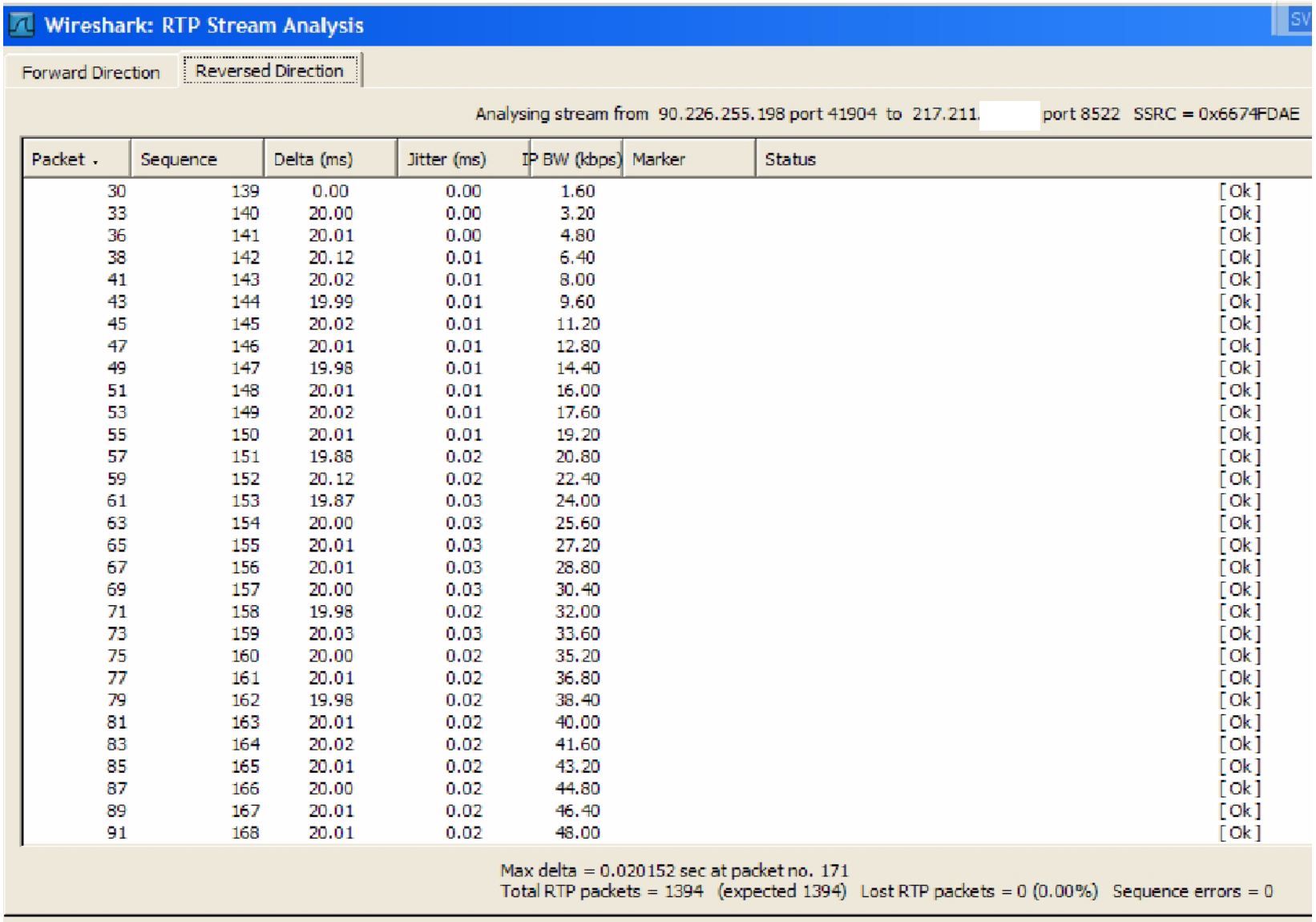
Forward Direction | Reversed Direction

Analysing stream from 217.211 port 8522 to 90.226.255.198 port 41904 SSRC = 0xF99F2232

Packet	Sequence	Delta (ms)	Jitter (ms)	IP BW (kbps)	Marker	Status
1764	386	20.01	0.07	81.60		[Ok]
1766	387	20.00	0.07	81.60		[Ok]
1768	388	20.00	0.06	80.00		[Ok]
1770	389	20.01	0.06	81.60		[Ok]
1772	390	20.00	0.06	80.00		[Ok]
1774	391	20.00	0.05	80.00		[Ok]
1776	392	20.00	0.05	81.60		[Ok]
1778	393	20.01	0.05	80.00		[Ok]
1780	394	20.00	0.04	80.00		[Ok]
1782	395	20.01	0.04	81.60		[Ok]
1784	396	20.01	0.04	80.00		[Ok]
1786	397	20.00	0.04	80.00		[Ok]
1788	398	19.88	0.04	81.60		[Ok]
1790	399	20.14	0.05	80.00		[Ok]
1792	400	19.87	0.05	81.60		[Ok]
1794	401	20.01	0.05	81.60		[Ok]
1796	402	20.13	0.06	80.00		[Ok]
1798	403	19.88	0.06	81.60		[Ok]
1800	404	20.00	0.06	81.60		[Ok]
1802	405	20.13	0.06	80.00		[Ok]
1804	406	19.88	0.06	81.60		[Ok]
1806	407	20.01	0.06	81.60		[Ok]
1808	408	20.13	0.07	80.00		[Ok]
1810	409	19.88	0.07	81.60		[Ok]
1812	410	20.00	0.06	81.60		[Ok]
1814	411	20.13	0.07	80.00		[Ok]
1816	412	19.88	0.07	81.60		[Ok]
1818	413	20.01	0.07	81.60		[Ok]
1820	414	20.14	0.07	80.00		[Ok]

Max delta = 0.020155 sec at packet no. 705
Total RTP packets = 1391 (expected 54431) Lost RTP packets = 53040 (97.44%) Sequence errors = 1

Save payload... | Save as CSV... | Refresh | Jump to | Graph


Wireshark: RTP Stream Analysis
Forward Direction
Reversed Direction
Analysing stream from 90.226.255.198 port 41904 to 217.211. port 8522 SSRC = 0x6674FDAE
Packet
Sequence
Delta (ms)
Jitter (ms)
IP BW (kbps)
Marker
Status
30 139 0.00 0.00 1.60 [Ok]
33 140 20.00 0.00 3.20 [Ok]
36 141 20.01 0.00 4.80 [Ok]
38 142 20.12 0.01 6.40 [Ok]
41 143 20.02 0.01 8.00 [Ok]
43 144 19.99 0.01 9.60 [Ok]
45 145 20.02 0.01 11.20 [Ok]
47 146 20.01 0.01 12.80 [Ok]
49 147 19.98 0.01 14.40 [Ok]
51 148 20.01 0.01 16.00 [Ok]
53 149 20.02 0.01 17.60 [Ok]
55 150 20.01 0.01 19.20 [Ok]
57 151 19.88 0.02 20.80 [Ok]
59 152 20.12 0.02 22.40 [Ok]
61 153 19.87 0.03 24.00 [Ok]
63 154 20.00 0.03 25.60 [Ok]
65 155 20.01 0.03 27.20 [Ok]
67 156 20.01 0.03 28.80 [Ok]
69 157 20.00 0.03 30.40 [Ok]
71 158 19.98 0.02 32.00 [Ok]
73 159 20.03 0.03 33.60 [Ok]
75 160 20.00 0.02 35.20 [Ok]
77 161 20.01 0.02 36.80 [Ok]
79 162 19.98 0.02 38.40 [Ok]
81 163 20.01 0.02 40.00 [Ok]
83 164 20.02 0.02 41.60 [Ok]
85 165 20.01 0.02 43.20 [Ok]
87 166 20.00 0.02 44.80 [Ok]
89 167 20.01 0.02 46.40 [Ok]
91 168 20.01 0.02 48.00 [Ok]
Max delta = 0.020152 sec at packet no. 171
Total RTP packets = 1394 (expected 1394) Lost RTP packets = 0 (0.00%) Sequence errors = 0

RTCP

During a call with 1619 RTCP Reports, these reports were sent by the ATA roughly every 5 seconds:

4.999864	**Median (seconds)**
4.999363	Min (seconds)
5.01011	Max (seconds)

DHCP lease renewal

The IP address lease was for 20 minutes.

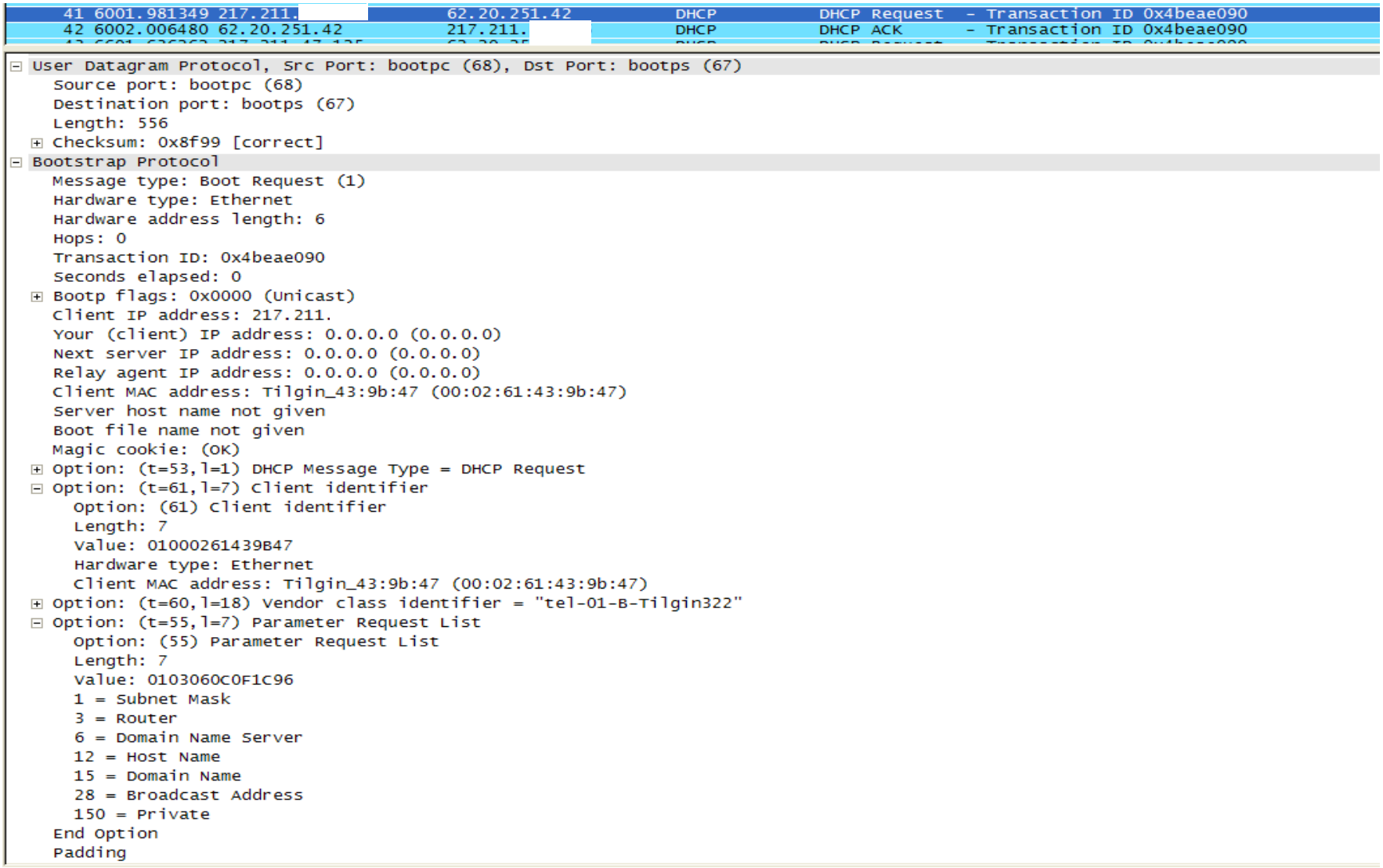
In one trace file 28 DHCP Requests occurred roughly every 600s:

599.6613 median
599.6257 min
600.6922 max

The DHCP ACK came roughly 0.02 s later:

0.024378 median
0.022617 min
0.275309 max

DHCP request details

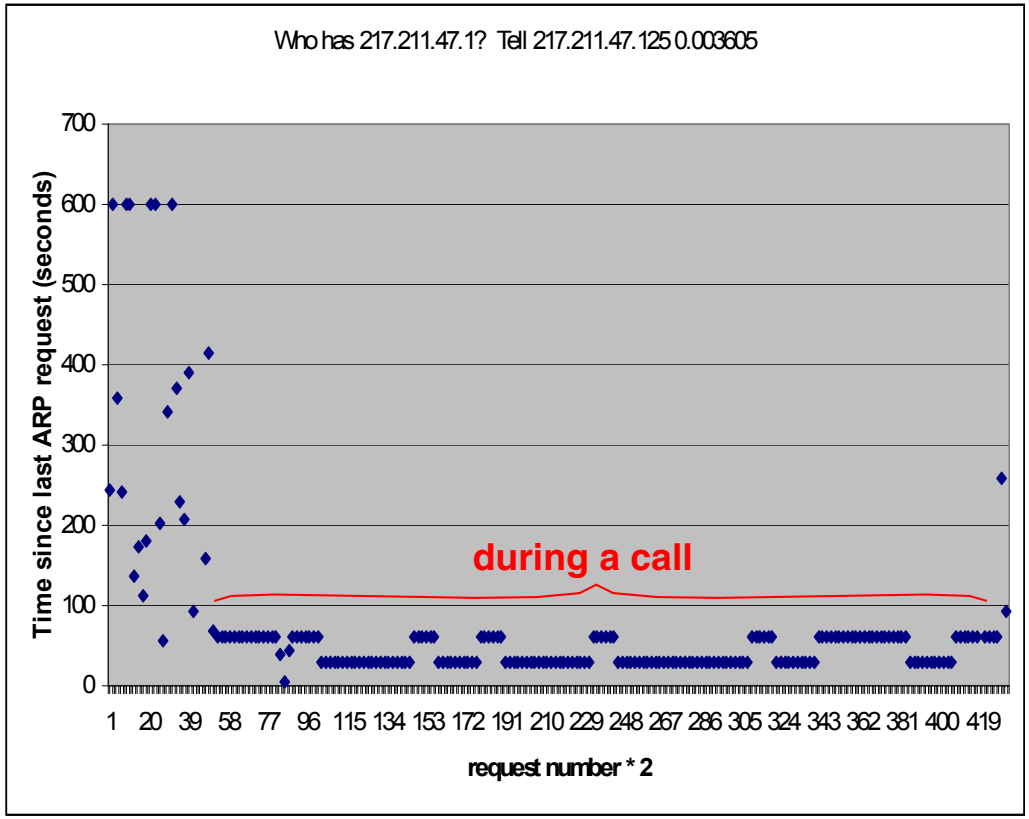


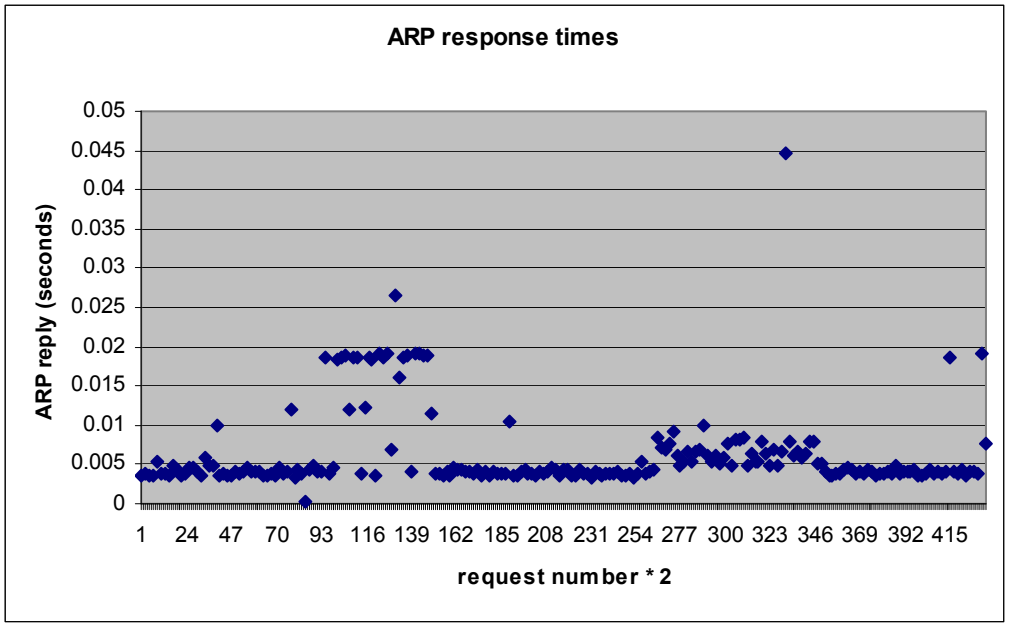
```
    41 6001.981349 217.211.          62.20.251.42          DHCP     DHCP Request  - Transaction ID 0x4beae090
    42 6002.006480 62.20.251.42      217.211.              DHCP     DHCP ACK      - Transaction ID 0x4beae090

⊟ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
    Length: 556
  ⊞ Checksum: 0x8f99 [correct]
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4beae090
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 217.211.
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Tilgin_43:9b:47 (00:02:61:43:9b:47)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP Request
  ⊟ Option: (t=61,l=7) Client identifier
      Option: (61) Client identifier
      Length: 7
      Value: 01000261439B47
      Hardware type: Ethernet
      Client MAC address: Tilgin_43:9b:47 (00:02:61:43:9b:47)
  ⊞ Option: (t=60,l=18) Vendor class identifier = "tel-01-B-Tilgin322"
  ⊟ Option: (t=55,l=7) Parameter Request List
      Option: (55) Parameter Request List
      Length: 7
      Value: 0103060C0F1C96
      1 = Subnet Mask
      3 = Router
      6 = Domain Name Server
      12 = Host Name
      15 = Domain Name
      28 = Broadcast Address
      150 = Private
    End Option
    Padding
```

DHCP ACK details

```
    41 6001.981349 217.211.          62.20.251.42          DHCP     DHCP Request  - Transaction ID 0x4beae090
    42 6002.006480 62.20.251.42      217.211.              DHCP     DHCP ACK      - Transaction ID 0x4beae090

⊞ Frame 42 (330 bytes on wire, 330 bytes captured)
⊞ Ethernet II, Src: Cisco_3a:15:80 (00:0f:90:3a:15:80), Dst: Tilgin_43:9b:47 (00:02:61:43:9b:47)
⊞ Internet Protocol, Src: 62.20.251.42 (62.20.251.42), Dst: 217.211.
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4beae090
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 217.211.
    Your (client) IP address: 217.211.
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Tilgin_43:9b:47 (00:02:61:43:9b:47)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ⊞ Option: (t=53,l=1) DHCP Message Type = DHCP ACK
  ⊞ Option: (t=54,l=4) Server Identifier = 62.20.251.42
  ⊞ Option: (t=51,l=4) IP Address Lease Time = 20 minutes
  ⊞ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ⊞ Option: (t=3,l=4) Router = 217.211.47.1
  ⊟ Option: (t=6,l=12) Domain Name Server
      Option: (6) Domain Name Server
      Length: 12
      Value: C343C70FC343C710C343C711
      IP Address: 195.67.199.15
      IP Address: 195.67.199.16
      IP Address: 195.67.199.17
  ⊞ Option: (t=28,l=4) Broadcast Address = 217.211.
    End Option
```

ARP


Who has 217.211.47.1? Tell 217.211.47.125 0.003605
Time since last ARP request (seconds)
700
600
500
400
300
200
100
0
during a call
1 20 39 58 77 96 115 134 153 172 191 210 229 248 267 286 305 324 343 362 381 400 419
request number * 2


ARP response times
ARP reply (seconds)
0.05
0.045
0.04
0.035
0.03
0.025
0.02
0.015
0.01
0.005
0
1 24 47 70 93 116 139 162 185 208 231 254 277 300 323 346 369 392 415
request number * 2

NTP

The ATA makes an NTP client request roughly every1749.96 seconds. The NTP sever (at 81.228.11.66) answers with a response in roughly 0.5 millisecond - some statistics are shown for this below (with the unit of time being seconds):

0.000598 median
0.000473 min
0.001377 max

NTP client request details

No.	Time	Source	Destination	Protocol	RSSI	Info
48	7365.529711	217.211	81.228.11.66	NTP		NTP client
49	7365.530312	81.228.11.66	217.211.	NTP		NTP server

```
+ Frame 48 (90 bytes on wire, 90 bytes captured)
+ Ethernet II, Src: Tilgin_43:9b:47 (00:02:61:43:9b:47), Dst: Cisco_3a:15:80 (00:0f:90:3a:15:80)
+ Internet Protocol, Src: 217.211.                    , Dst: 81.228.11.66 (81.228.11.66)
+ User Datagram Protocol, Src Port: vcrp (3073), Dst Port: ntp (123)
- Network Time Protocol
  - Flags: 0x1b
      00.. .... = Leap Indicator: no warning (0)
      ..01 1... = Version number: NTP Version 3 (3)
      .... .011 = Mode: client (3)
    Peer Clock Stratum: secondary reference (15)
    Peer Polling Interval: 8 (256 sec)
    Peer Clock Precision: 1.000000 sec
    Root Delay:    0.0000 sec
    Root Dispersion:    0.0000 sec
    Reference Clock ID: 0.0.0.0
    Reference Clock Update Time: NULL
    Originate Time Stamp: NULL
    Receive Time Stamp: NULL
    Transmit Time Stamp: May 19, 2010 18:41:57.8969 UTC
```

NTP server response details

```
+ User Datagram Protocol, Src Port: ntp (123), Dst Port: vcrp (3073)
- Network Time Protocol
  - Flags: 0x1c
      00.. .... = Leap Indicator: no warning (0)
      ..01 1... = Version number: NTP Version 3 (3)
      .... .100 = Mode: server (4)
    Peer Clock Stratum: secondary reference (2)
    Peer Polling Interval: 8 (256 sec)
    Peer Clock Precision: 0.000001 sec
    Root Delay:    0.0008 sec
    Root Dispersion:    0.0434 sec
    Reference Clock ID: 192.36.144.22
    Reference Clock Update Time: May 19, 2010 18:28:55.0761 UTC
    Originate Time Stamp: May 19, 2010 18:41:57.8969 UTC
    Receive Time Stamp: May 19, 2010 18:41:57.8531 UTC
    Transmit Time Stamp: May 19, 2010 18:41:57.8531 UTC
```

ATA is ahead of the NTP server

Registration of ATA

82	6130.697038	217.211	90.226.251.75	SIP	Request: REGISTER sip:ims.telia.com;transport=udp
83	6130.719173	90.226.251.75	217.211.	SIP	Status: 401 Unauthorized (0 bindings)
84	6130.732297	217.211.	90.226.251.75	SIP	Request: REGISTER sip:ims.telia.com;transport=udp
85	6130.766184	90.226.251.75	217.211.	SIP	Status: 200 OK (1 bindings)

Figure 34: Registration in four messages

REGISTER

```
⊞ Internet Protocol, Src: 217.211.[illegible], Dst: 90.226.251.75 (90.226.251.75)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:ims.telia.com;transport=udp SIP/2.0
  ⊟ Message Header
    ⊞ Via: SIP/2.0/UDP 217.211.[illegible]:5060;branch=z9hG4bK-1274567500134004126
      Max-Forwards: 70
    ⊞ To: +468313578 <sip:+468[illegible]@ims.telia.com;transport=udp>
    ⊞ From: +468313578 <sip:+468[illegible]@ims.telia.com;transport=udp>;tag=1274567500134004125
      Call-ID: RA-1274065284881840001@217.211.[illegible]
    ⊞ CSeq: 311 REGISTER
    ⊞ Contact: +468313578 <sip:+468[illegible]@217.211.[illegible]:5060;transport=udp>;q=1.000;description="ADAPTER"
      Expires: 3600
      Supported: replaces, 100rel
      User-Agent: Telefonadapter - Telia Bredbandstelefoni
      X-NAT: nothing
      X-Serialnumber: V30100000000-0010493387
      Content-Length: 0
```

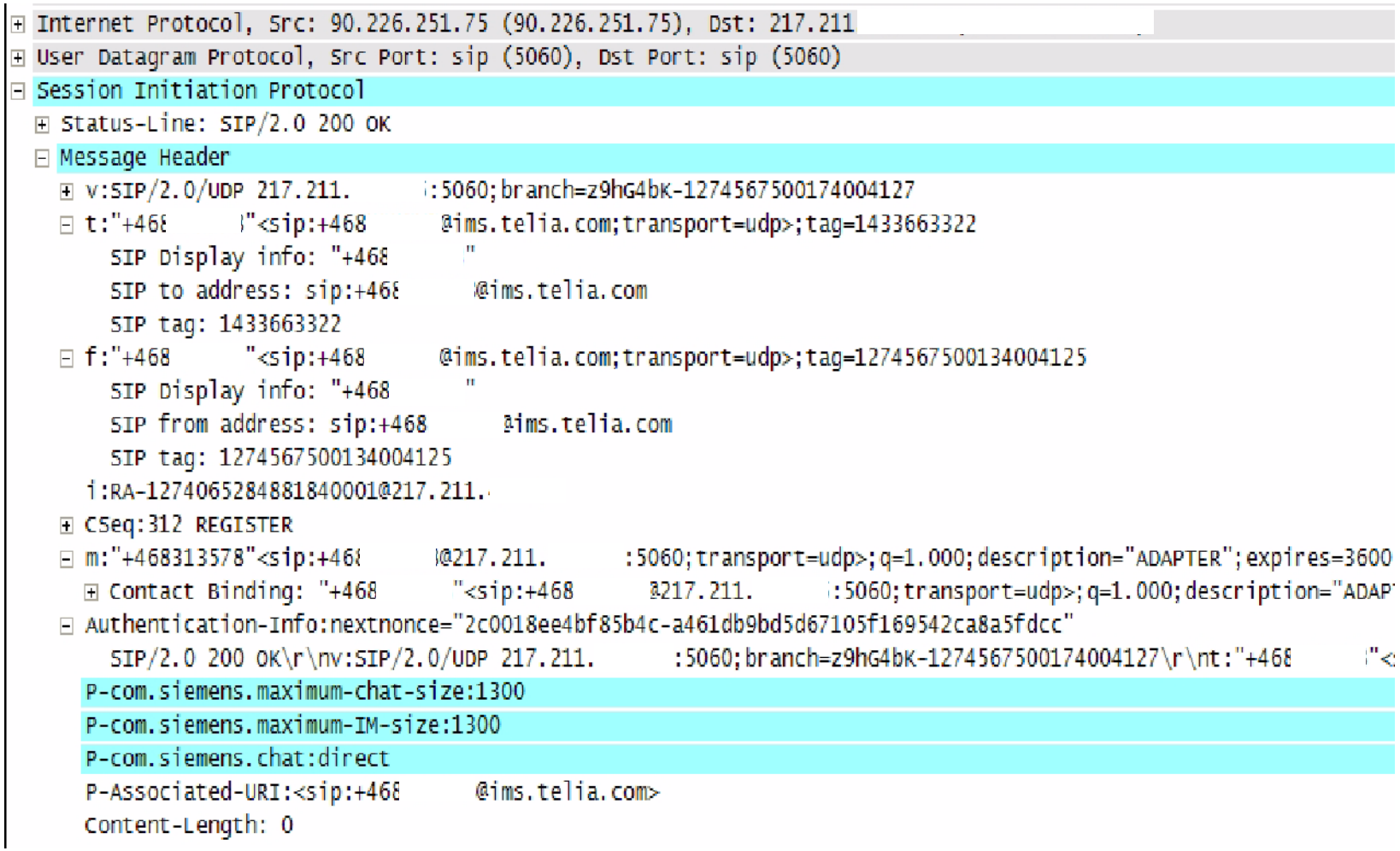
401 Unauthorized

```
⊞ Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211.
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊞ Status-Line: SIP/2.0 401 Unauthorized
  ⊟ Message Header
    ⊞ v:SIP/2.0/UDP 217.211.      :5060;branch=z9hG4bK-1274567500134004126
    ⊞ t:"+468313578"<sip:+46      @ims.telia.com;transport=udp>;tag=780521824
    ⊞ f:"+468313578"<sip:+46      @ims.telia.com;transport=udp>;tag=1274567500134004125
      i:RA-1274065284881840001@217.211.
    ⊞ CSeq:311 REGISTER
    ⊟ WWW-Authenticate:Digest realm="ims.telia.com",nonce="2bff17c84bf85b4c-4d87647069d161026214cc82db60b6e3",qop="auth"
        Authentication Scheme: Digest
        Realm: "ims.telia.com"
        Nonce Value: "2bff17c84bf85b4c-4d87647069d161026214cc82db60b6e3"
        QOP: "auth"
      Content-Length: 0
```

REGISTER with authorization

```
⊞ Internet Protocol, Src: 217.211.                    , Dst: 90.226.251.75 (90.226.251.75)
⊞ User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
⊟ Session Initiation Protocol
  ⊞ Request-Line: REGISTER sip:ims.telia.com;transport=udp SIP/2.0
  ⊟ Message Header
    ⊞ Via: SIP/2.0/UDP 217.211.      :5060;branch=z9hG4bK-127456750017400412 7
      Max-Forwards: 70
    ⊟ To: +468313578 <sip:+468      @ims.telia.com;transport=udp>
        SIP Display info: +468
        SIP to address: sip:+46      @ims.telia.com
    ⊟ From: +468313578 <sip:+46      @ims.telia.com;transport=udp>;tag=127456750013400412 5
        SIP Display info: +468
        SIP from address: sip:+46      @ims.telia.com
        SIP tag: 127456750013400412 5
      Call-ID: RA-127406528488184000 1@217.211.
    ⊞ CSeq: 312 REGISTER
    ⊟ Contact: +468313578 <sip:+46      @217.211.      :5060;transport=udp>;q=1.000;description="ADAPTER"
      ⊞ Contact Binding: +468313578 <sip:+468      @217.211.      :5060;transport=udp>;q=1.000;description="ADAPTER"
      Expires: 3600
      Supported: replaces, 100rel
      User-Agent: Telefonadapter - Telia Bredbandstelefoni
      X-NAT: nothing
      X-Serialnumber: V30100000000-0010493387
    ⊟ Authorization: Digest username="+468      @ims.telia.com",realm="ims.telia.com",nonce="2bff17c84bf85b4c-4d876470
        Authentication Scheme: Digest
        Username: "+468      @ims.telia.com"
        Realm: "ims.telia.com"
        Nonce Value: "2bff17c84bf85b4c-4d87647069d161026214cc82db60b6e3"
        Authentication URI: "sip:ims.telia.com;transport=udp"
        QOP: auth
        Nonce Count: 00000001
        CNonce Value: "b311f4a0"
        Digest Authentication Response: "ed96ef45174250c0f18853b7616bbecf"
      Content-Length: 0
```

200 OK


Internet Protocol, Src: 90.226.251.75 (90.226.251.75), Dst: 217.211
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol
Status-Line: SIP/2.0 200 OK
Message Header
v:SIP/2.0/UDP 217.211. :5060;branch=z9hG4bK-1274567500174004127
t:"+468 "<sip:+468 @ims.telia.com;transport=udp>;tag=1433663322
SIP Display info: "+468 "
SIP to address: sip:+468 @ims.telia.com
SIP tag: 1433663322
f:"+468 "<sip:+468 @ims.telia.com;transport=udp>;tag=1274567500134004125
SIP Display info: "+468 "
SIP from address: sip:+468 @ims.telia.com
SIP tag: 1274567500134004125
i:RA-1274065284881840001@217.211.
CSeq:312 REGISTER
m:"+468313578"<sip:+46 @217.211. :5060;transport=udp>;q=1.000;description="ADAPTER";expires=3600
Contact Binding: "+468 "<sip:+468 @217.211. :5060;transport=udp>;q=1.000;description="ADAP
Authentication-Info:nextnonce="2c0018ee4bf85b4c-a461db9bd5d67105f169542ca8a5fdcc"
SIP/2.0 200 OK\r\nv:SIP/2.0/UDP 217.211. :5060;branch=z9hG4bK-1274567500174004127\r\nt:"+468
P-com.siemens.maximum-chat-size:1300
P-com.siemens.maximum-IM-size:1300
P-com.siemens.chat:direct
P-Associated-URI:<sip:+468 @ims.telia.com>
Content-Length: 0

Provisioning

196	14133.73184	217.211	62.71.2.165	HTTP	GET /BcxManager/V30100000000-0010493387.list HTTP/1.0
198	14133.76225	62.71.2.165	217.211.	HTTP	HTTP/1.1 200 OK (application/octet-stream)
206	14135.13891	217.211.	62.71.2.165	HTTP	GET /BcxManager/V30100000000-0010493387.conf HTTP/1.0
219	14135.18830	62.71.2.165	217.211.	HTTP	HTTP/1.1 200 OK (application/octet-stream)
228	14135.29019	217.211.	62.71.2.165	HTTP	GET /BcxManager/V30100000000-0010493387.ack?SW_VER=322_AS0500-03_05_11_02&RESULT=OK&MSG=
230	14135.31696	62.71.2.165	217.211.	HTTP	HTTP/1.1 200 OK

Figure 35: ATA contacts the provisioning server at 62.71.2.165

62.71.2.128 - 62.71.2.191 is allocated to TeliaSonera Finland Oy, and Sonera Carrier Networks Oy. This is in AS 5515.

First GET

First get /BoxManager/V30100000000-00104933B7.list

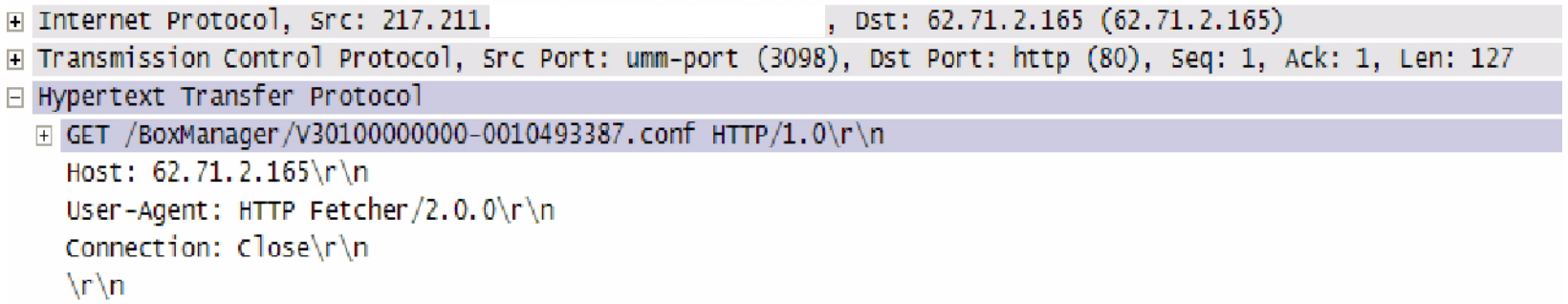
```
⊞ Internet Protocol, Src: 217.211.                    , Dst: 62.71.2.165 (62.71.2.165)
⊞ Transmission Control Protocol, Src Port: 3097 (3097), Dst Port: http (80), Seq: 1, Ack: 1, Len: 127
⊟ Hypertext Transfer Protocol
  ⊞ GET /BoxManager/V30100000000-0010493387.list HTTP/1.0\r\n
    Host: 62.71.2.165\r\n
    User-Agent: HTTP Fetcher/2.0.0\r\n
    Connection: Close\r\n
    \r\n
```

200 OK

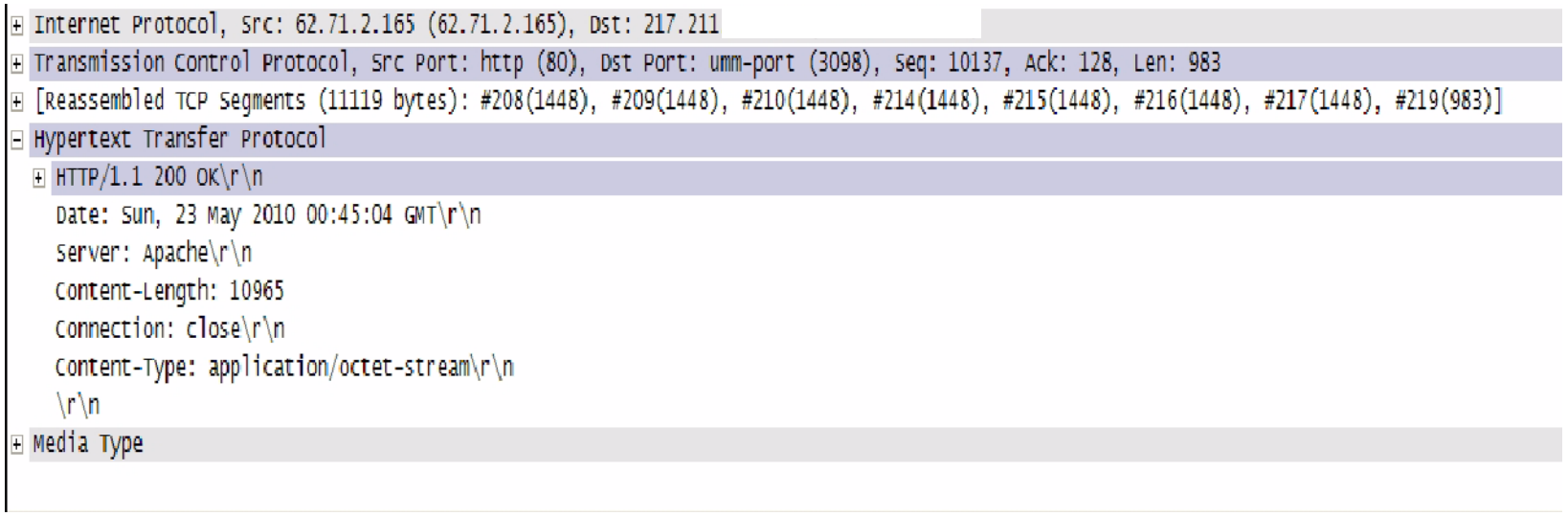
```
⊞ Internet Protocol, Src: 62.71.2.165 (62.71.2.165), Dst: 217.211.
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 3097 (3097), Seq: 1, Ack: 128, Len: 544
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Date: Sun, 23 May 2010 00:45:03 GMT\r\n
    Server: Apache\r\n
    Content-Length: 392
    Connection: close\r\n
    Content-Type: application/octet-stream\r\n
    \r\n
⊞ Media Type
```

Second GET

GET /BoxManager/V30100000000-00104933B7.conf

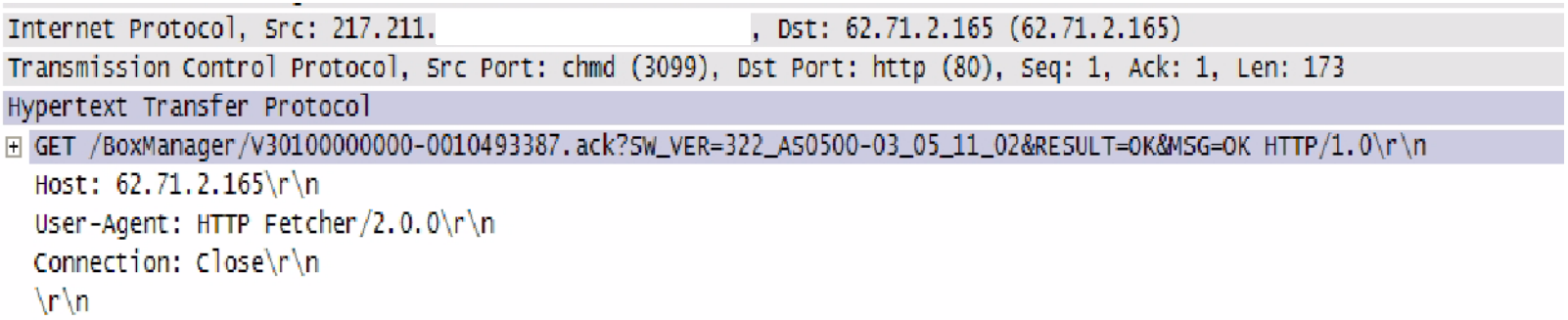


200 OK

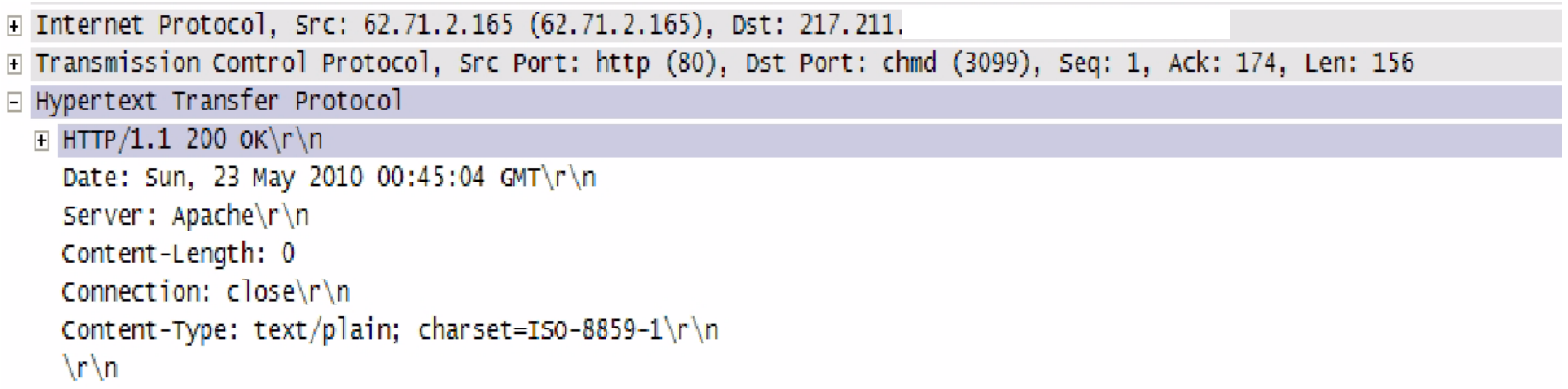

Internet Protocol, Src: 62.71.2.165 (62.71.2.165), Dst: 217.211
Transmission Control Protocol, Src Port: http (80), Dst Port: umm-port (3098), Seq: 10137, Ack: 128, Len: 983
[Reassembled TCP Segments (11119 bytes): #208(1448), #209(1448), #210(1448), #214(1448), #215(1448), #216(1448), #217(1448), #219(983)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sun, 23 May 2010 00:45:04 GMT\r\n
Server: Apache\r\n
Content-Length: 10965
Connection: close\r\n
Content-Type: application/octet-stream\r\n
\r\n
Media Type

Third GET

GET /BoxManager/V30100000000-00104933B7.ack?SW_VER=322_AS0500-03_05_11_02&RESULT=OK HTTP/1.0\r\n



200 OK


Internet Protocol, Src: 62.71.2.165 (62.71.2.165), Dst: 217.211.
Transmission Control Protocol, Src Port: http (80), Dst Port: chmd (3099), Seq: 1, Ack: 174, Len: 156
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sun, 23 May 2010 00:45:04 GMT\r\n
Server: Apache\r\n
Content-Length: 0
Connection: close\r\n
Content-Type: text/plain; charset=ISO-8859-1\r\n
\r\n

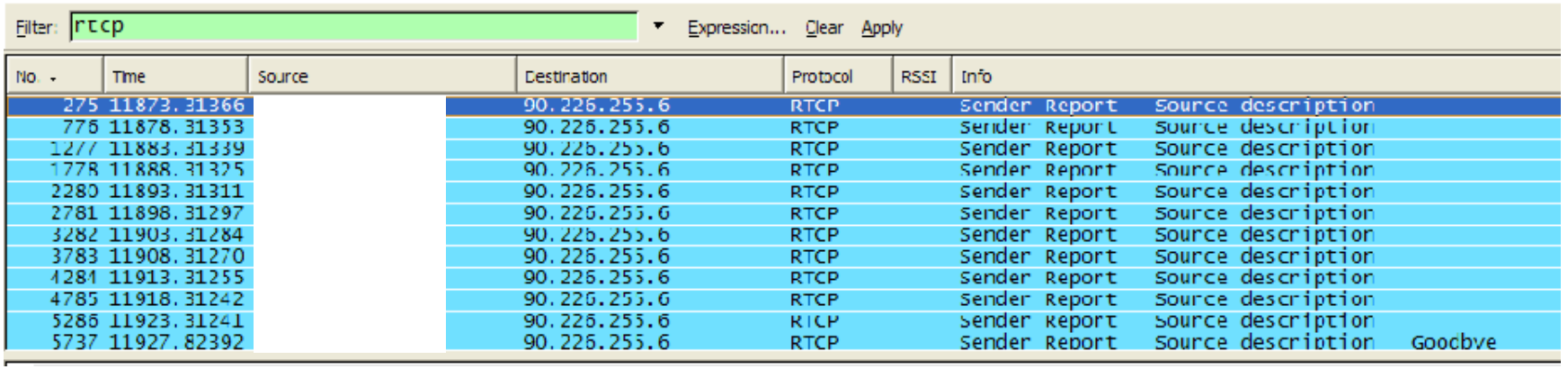
RTP packet details

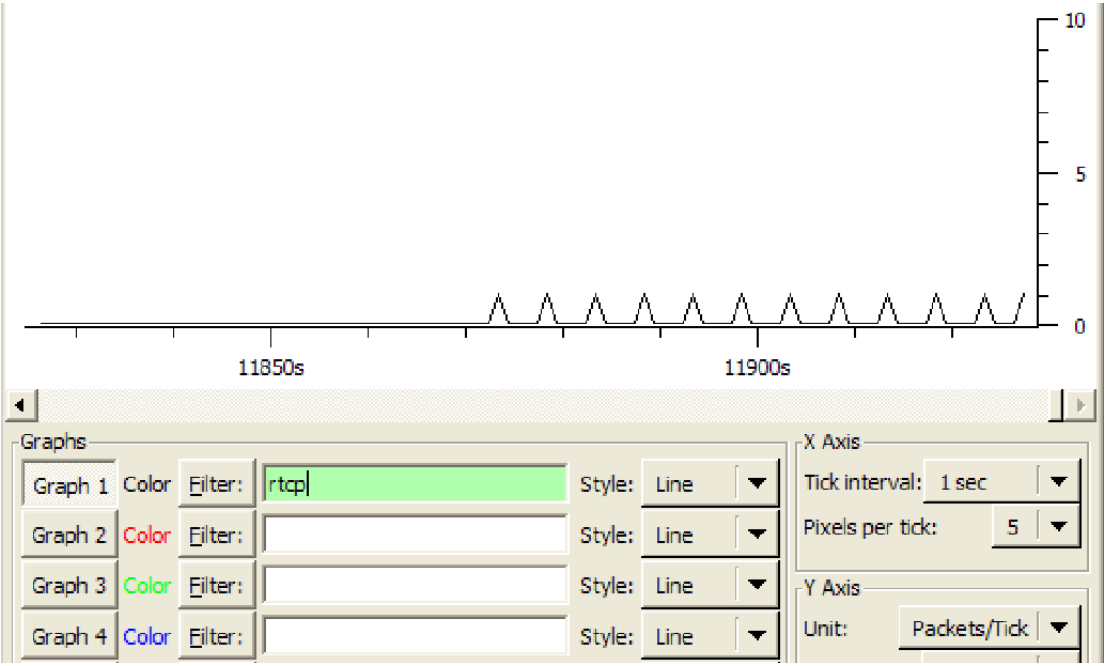
No.	Time	Source	Destination	Protocol	RSSI	Info
85	11871.42474	90.226.255.6		RTP		PT=ITU-T G.711 PCMA, SSRC=0x1D1814C9, Seq=118, Time=28342
87	11871.44475	90.226.255.6		RTP		PT=ITU-T G.711 PCMA, SSRC=0x1D1814C9, Seq=119, Time=28502
89	11871.46473	90.226.255.6		RTP		PT=ITU-T G.711 PCMA, SSRC=0x1D1814C9, Seq=120, Time=28662
90	11871.48451		90.226.255.6	RTP		PT=ITU-T G.711 PCMA, SSRC=0x4857EB24, Seq=707, Time=525663851
91	11871.48473	90.226.255.6		RTP		PT=ITU-T G.711 PCMA, SSRC=0x1D1814C9, Seq=121, Time=28822
92	11871.50438		90.226.255.6	RTP		PT=ITU-T G.711 PCMA, SSRC=0x4857EB24, Seq=708, Time=525664011
93	11871.50474	90.226.255.6		RTP		PT=ITU-T G.711 PCMA, SSRC=0x1D1814C9, Seq=122, Time=28982
95	11871.52451		90.226.255.6	RTP		PT=ITU-T G.711 PCMA, SSRC=0x4857EB24, Seq=709, Time=525664171
96	11871.52475	90.226.255.6		RTP		PT=ITU-T G.711 PCMA, SSRC=0x1D1814C9, Seq=123, Time=29142
97	11871.54440		90.226.255.6	RTP		PT=ITU-T G.711 PCMA, SSRC=0x4857EB24, Seq=710, Time=525664331
98	11871.54475	90.226.255.6		RTP		PT=ITU-T G.711 PCMA, SSRC=0x1D1814C9, Seq=124, Time=29302
99	11871.56440		90.226.255.6	RTP		PT=ITU-T G.711 PCMA, SSRC=0x4857EB24, Seq=711, Time=525664491

```
⊞ Frame 85 (214 bytes on wire, 214 bytes captured)
⊞ Ethernet II, Src: Cisco_3a:15:80 (00:0f:90:3a:15:80), Dst: Tilgin_43:9b:47 (00:02:61:43:9b:47)
⊞ Internet Protocol, Src: 90.226.255.6 (90.226.255.6), Dst: 217.211.
⊟ User Datagram Protocol, Src Port: 41164 (41164), Dst Port: 8526 (8526)
    Source port: 41164 (41164)
    Destination port: 8526 (8526)
    Length: 180
  ⊞ Checksum: 0x45b4 [correct]
⊟ Real-Time Transport Protocol
  ⊞ [Stream setup by SDP (frame 83)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: ITU-T G.711 PCMA (8)
    Sequence number: 118
    [Extended sequence number: 65654]
    Timestamp: 28342
    Synchronization Source identifier: 0x1d1814c9 (488117449)
    Payload: 071E685DEC9C8586878592E04E14190706071B167FFE9698...
```

RTCP traffic more details

As noted earlier, RTCP sender reports sent every 5 seconds: :





An example RTCP Sender report (first in this call)

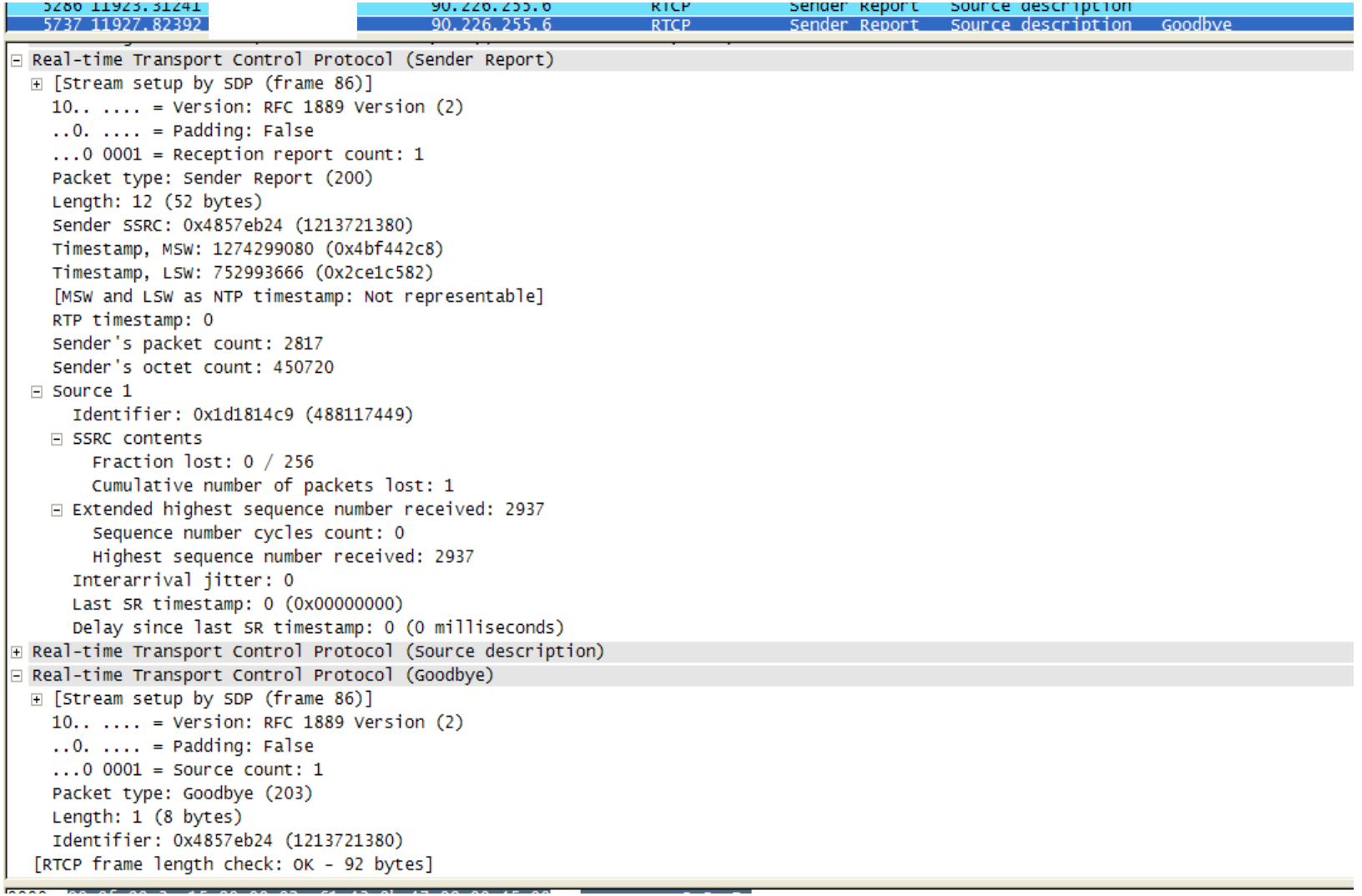
```
Real-time Transport Control Protocol (Sender Report)
  [Stream setup by SDP (frame 86)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 0001 = Reception report count: 1
    Packet type: Sender Report (200)
    Length: 12 (52 bytes)
    Sender SSRC: 0x4857eb24 (1213721380)
    Timestamp, MSW: 1274299025 (0x4bf44291)
    Timestamp, LSW: 2857527641 (0xaa526959)
    [MSW and LSW as NTP timestamp: Not representable]
    RTP timestamp: 525678803
    Sender's packet count: 92
    Sender's octet count: 14720
  Source 1
      Identifier: 0x1d1814c9 (488117449)
    SSRC contents
        Fraction lost: 0 / 256
        Cumulative number of packets lost: 0
    Extended highest sequence number received: 212
        Sequence number cycles count: 0
        Highest sequence number received: 212
      Interarrival jitter: 0
      Last SR timestamp: 0 (0x00000000)
      Delay since last SR timestamp: 0 (0 milliseconds)
```

An example RTCP Sender report (second in the same call)

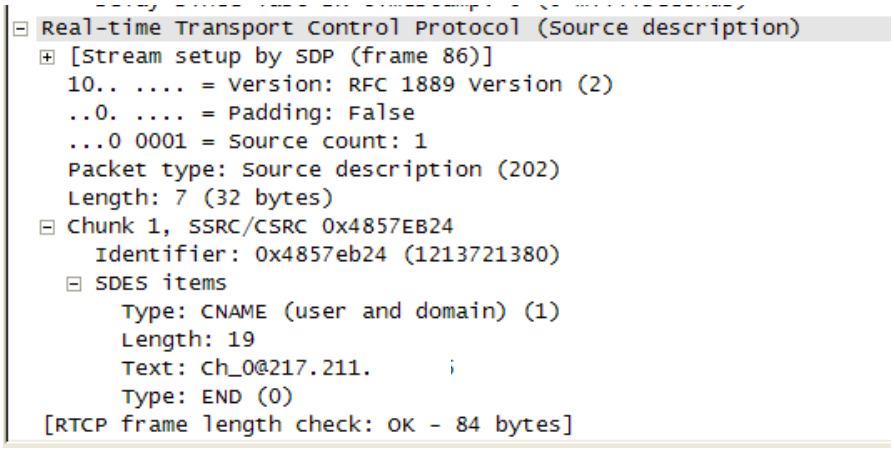
No.	Time	Source	Destination	Protocol	RSSI	Info
275	11873.31366		90.226.255.6	RTCP		Sender Report Source description
776	11878.31353		90.226.255.6	RTCP		Sender Report Source description
1277	11883.31339		90.226.255.6	RTCP		Sender Report Source description

```
Frame 776 (126 bytes on wire, 126 bytes captured)
Ethernet II, Src: Tilgin_43:9b:47 (00:02:61:43:9b:47), Dst: Cisco_3a:15:80 (00:0f:90:3a:15:80)
Internet Protocol, Src: 217.211.                    , Dst: 90.226.255.6 (90.226.255.6)
User Datagram Protocol, Src Port: 8527 (8527), Dst Port: 41165 (41165)
Real-time Transport Control Protocol (Sender Report)
  [Stream setup by SDP (frame 86)]
  10.. .... = Version: RFC 1889 Version (2)
  ..0. .... = Padding: False
  ...0 0001 = Reception report count: 1
  Packet type: Sender Report (200)
  Length: 12 (52 bytes)
  Sender SSRC: 0x4857eb24 (1213721380)
  Timestamp, MSW: 1274299030 (0x4bf44296)
  Timestamp, LSW: 2857527641 (0xaa526959)
  [MSW and LSW as NTP timestamp: Not representable]
  RTP timestamp: 525718803
  Sender's packet count: 342
  Sender's octet count: 54720
  Source 1
    Identifier: 0x1d1814c9 (488117449)
    SSRC contents
      Fraction lost: 0 / 256
      Cumulative number of packets lost: 0
    Extended highest sequence number received: 462
      Sequence number cycles count: 0
      Highest sequence number received: 462
    Interarrival jitter: 0
    Last SR timestamp: 0 (0x00000000)
    Delay since last SR timestamp: 0 (0 milliseconds)
Real-time Transport Control Protocol (Source description)
[RTCP frame length check: OK - 84 bytes]
```

Details of the RTCP Goodbye:



A source description within the Sender Report:



Note that the CNAME is Ch_0@217.211.x.x - a single audio channel at the IP address of the ATA.

Interestingly there is never a RTCP sender report from operator's gateway.

VoIP Media Gateway's address and NTP server's address

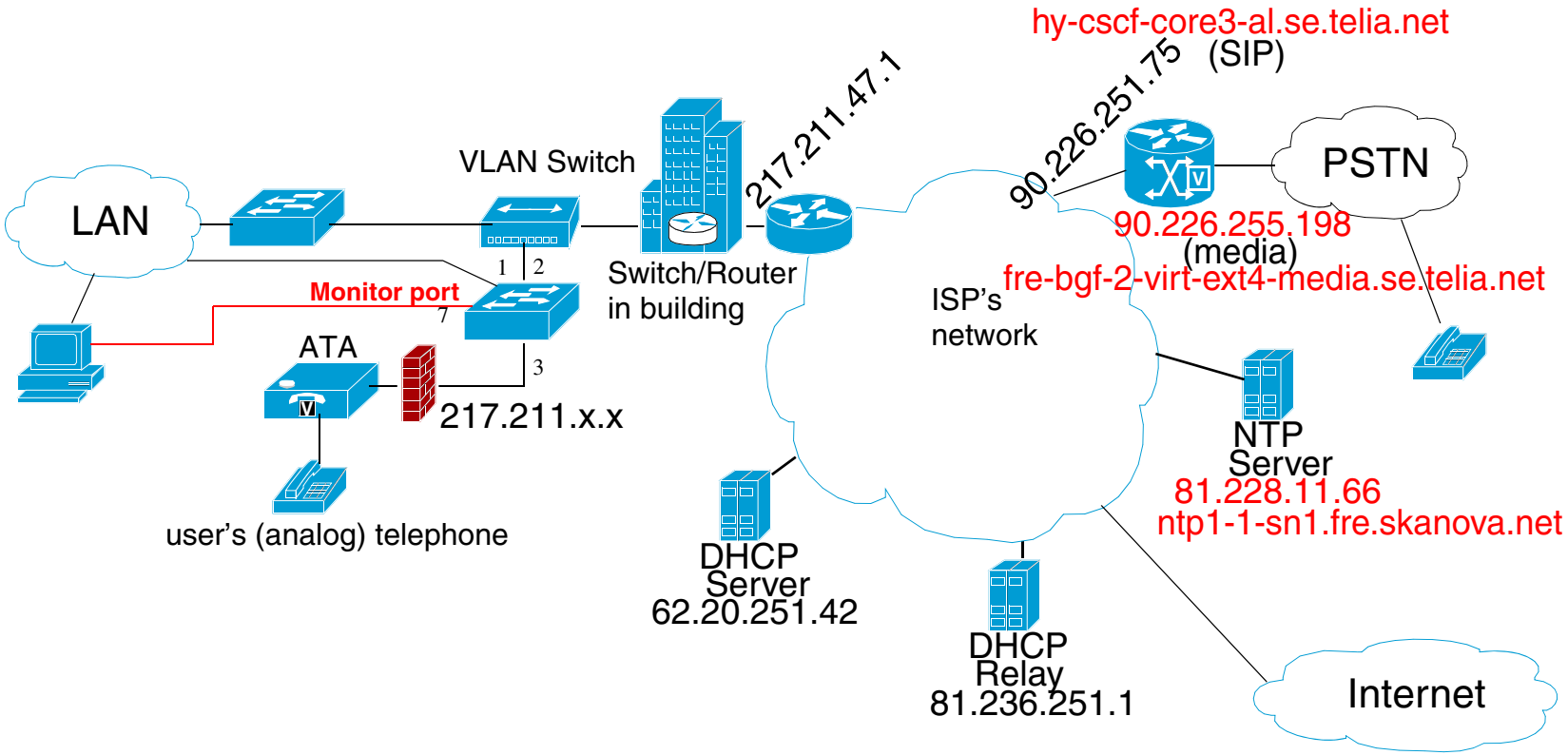
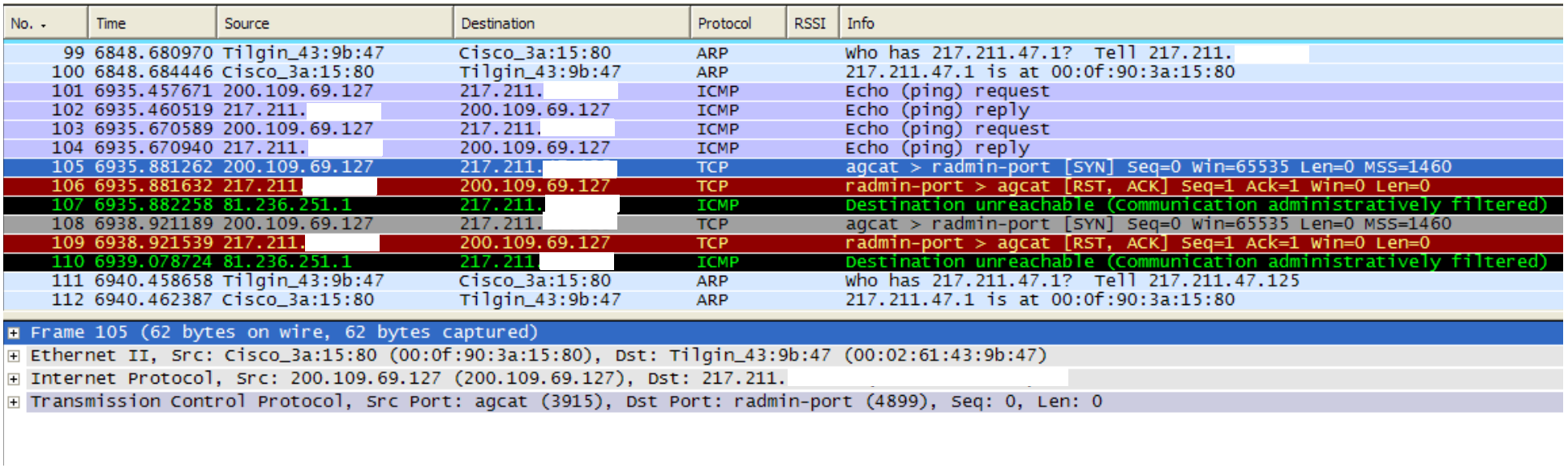


Figure 36: Learned the IP addresses of the Media gateway & NTP server

90.224.0.0 - 90.228.255.255 is assigned to TELIANET, Telia Network Services and is in AS3301.

Probing and possibly attack traffic

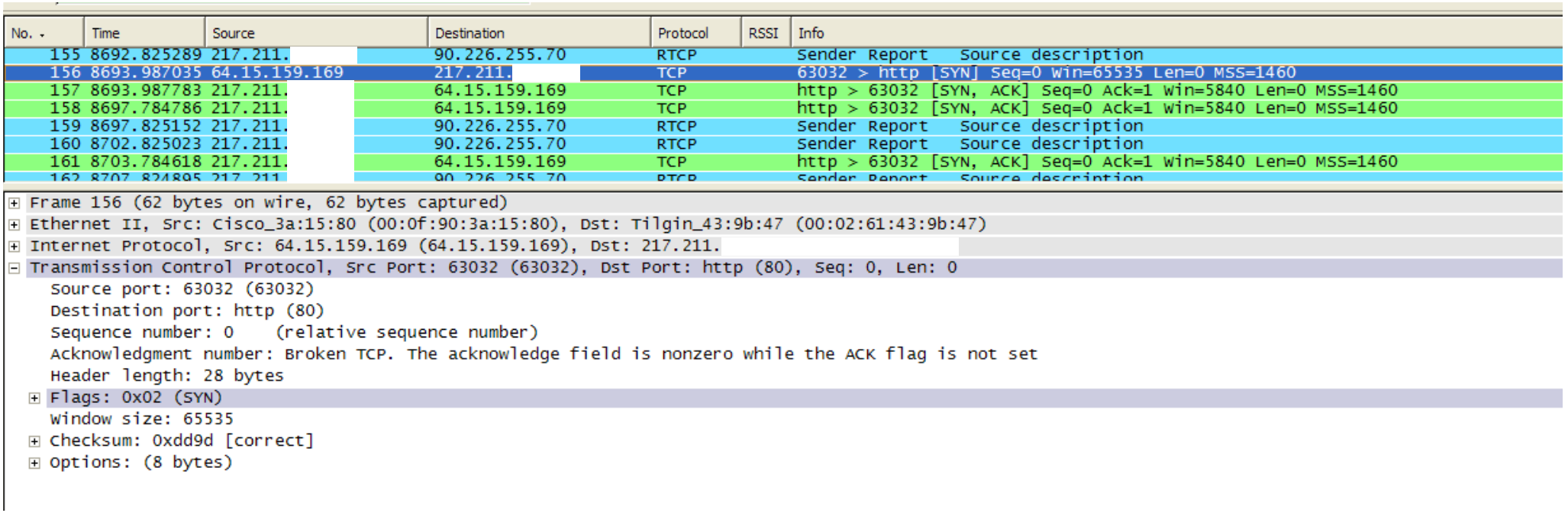


No.	Time	Source	Destination	Protocol	RSSI	Info
99	6848.680970	Tilgin_43:9b:47	Cisco_3a:15:80	ARP		Who has 217.211.47.1? Tell 217.211.
100	6848.684446	Cisco_3a:15:80	Tilgin_43:9b:47	ARP		217.211.47.1 is at 00:0f:90:3a:15:80
101	6935.457671	200.109.69.127	217.211.	ICMP		Echo (ping) request
102	6935.460519	217.211.	200.109.69.127	ICMP		Echo (ping) reply
103	6935.670589	200.109.69.127	217.211.	ICMP		Echo (ping) request
104	6935.670940	217.211.	200.109.69.127	ICMP		Echo (ping) reply
105	6935.881262	200.109.69.127	217.211.	TCP		agcat > radmin-port [SYN] Seq=0 Win=65535 Len=0 MSS=1460
106	6935.881632	217.211	200.109.69.127	TCP		radmin-port > agcat [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	6935.882258	81.236.251.1	217.211.	ICMP		Destination unreachable (Communication administratively filtered)
108	6938.921189	200.109.69.127	217.211.	TCP		agcat > radmin-port [SYN] Seq=0 Win=65535 Len=0 MSS=1460
109	6938.921539	217.211.	200.109.69.127	TCP		radmin-port > agcat [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
110	6939.078724	81.236.251.1	217.211	ICMP		Destination unreachable (Communication administratively filtered)
111	6940.458658	Tilgin_43:9b:47	Cisco_3a:15:80	ARP		Who has 217.211.47.1? Tell 217.211.47.125
112	6940.462387	Cisco_3a:15:80	Tilgin_43:9b:47	ARP		217.211.47.1 is at 00:0f:90:3a:15:80

```
⊞ Frame 105 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: Cisco_3a:15:80 (00:0f:90:3a:15:80), Dst: Tilgin_43:9b:47 (00:02:61:43:9b:47)
⊞ Internet Protocol, Src: 200.109.69.127 (200.109.69.127), Dst: 217.211.
⊞ Transmission Control Protocol, Src Port: agcat (3915), Dst Port: radmin-port (4899), Seq: 0, Len: 0
```

In this example, a computer at IP address 200.109.69.127 (a dynamically allocated address in the DSL pool of cantv.net) send a ping request and gets an acknowledgement, then repeats this process -again getting an acknowledgement; then it sends a TCP SYN to TCP port 4899 (radmin-port) to which the ATA replies with an ACK and RST (reset) - after which the operator's DHCP Relay replies with a ICMP destination unreachable (Communication administratively filtered) message.

An attempt to connect to the HTTP server port of the ATA



No.	Time	Source	Destination	Protocol	RSSI	Info
155	8692.825289	217.211.	90.226.255.70	RTCP		Sender Report Source description
156	8693.987035	64.15.159.169	217.211.	TCP		63032 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
157	8693.987783	217.211.	64.15.159.169	TCP		http > 63032 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
158	8697.784786	217.211.	64.15.159.169	TCP		http > 63032 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
159	8697.825152	217.211.	90.226.255.70	RTCP		Sender Report Source description
160	8702.825023	217.211.	90.226.255.70	RTCP		Sender Report Source description
161	8703.784618	217.211.	64.15.159.169	TCP		http > 63032 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
162	8707.824895	217.211.	90.226.255.70	RTCP		Sender Report Source description

```
⊞ Frame 156 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: Cisco_3a:15:80 (00:0f:90:3a:15:80), Dst: Tilgin_43:9b:47 (00:02:61:43:9b:47)
⊞ Internet Protocol, Src: 64.15.159.169 (64.15.159.169), Dst: 217.211.
⊟ Transmission Control Protocol, Src Port: 63032 (63032), Dst Port: http (80), Seq: 0, Len: 0
    Source port: 63032 (63032)
    Destination port: http (80)
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: Broken TCP. The acknowledge field is nonzero while the ACK flag is not set
    Header length: 28 bytes
  ⊞ Flags: 0x02 (SYN)
    Window size: 65535
  ⊞ Checksum: 0xdd9d [correct]
  ⊞ Options: (8 bytes)
```

In this case a machine at 64.15.159.169 attempts to connect to the ATA's HTTP server TCP port. Note that unlike the previous exampe, there is **not** an ICMP message sent in this case.

References and Further Reading

SIP Example

[189]Tilgin AB, web page, last accessed 2010.08.05, http://www.tilgin.com/

[190]TNETV1060 Communications Processor for VoIP Gateway Applications Data Manual, Texas Instruments, Literature Number SPRS255, June 2004, 139 pages http://focus.ti.com/pdfs/vf/bband/tnetv1060_datasheet.pdf

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1
Module 10: SIP Service Creation

KTH Information and
Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:31

SIP Service Creation

It is the increased opportunities for the exchange of signaling information via SIP which enables many new features and services.

Services implemented by x

Where x is:

- proxy server,
- called user agent,
- calling user agent, or
- Back-to-Back User Agent (B2BUA)

See examples of call-forward, no-answer service in chapter 6 of Sinnreich and Johnston[2].

Services implemented by Extensions

i.e., new methods and headers

See the activities of the IETF SIP, SIPPING, and SIMPLE working groups

Proxy servers - simply treat unknown methods as an `OPTION` request, unless there is a `Proxy-Require` header.

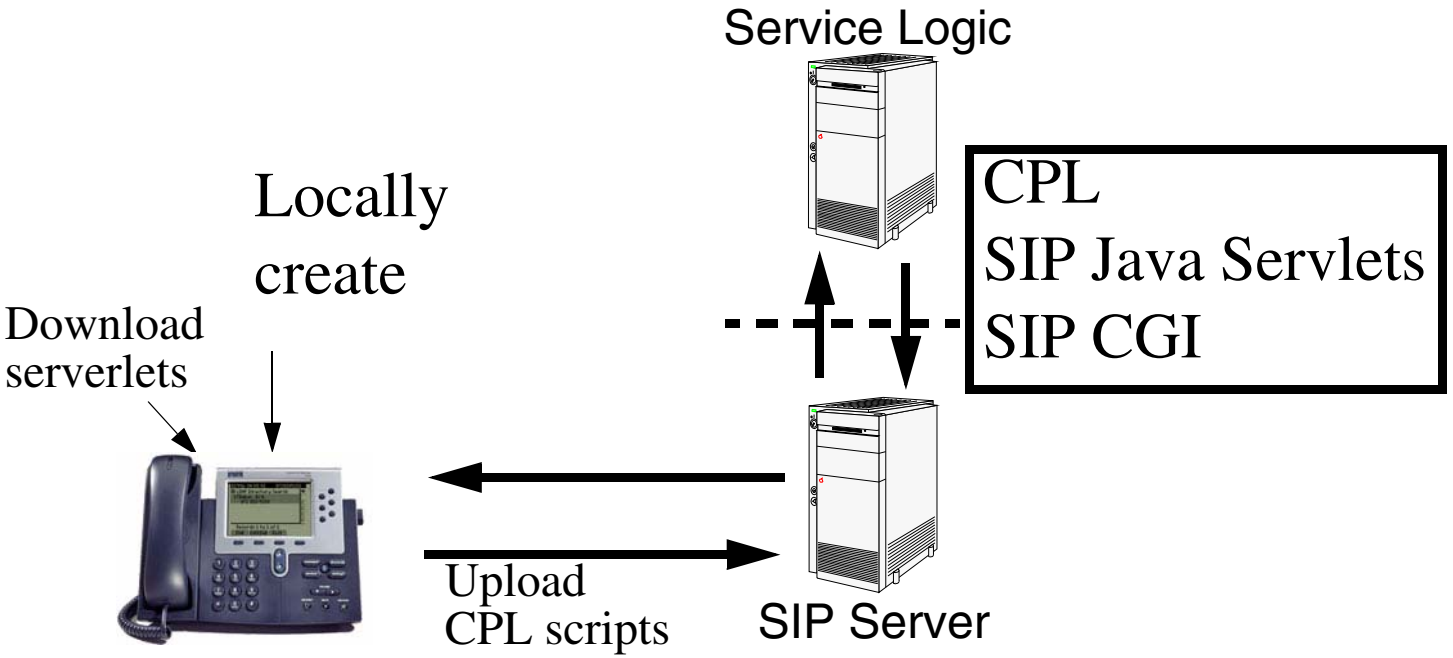
User agents return:

`405 Method Not Allowed`	if the method is recognized, but not supported
`500 Bad Request`	if it does not recognize the method
`420 Bad Extension`	if the UAS does not support the requested feature

- All SIP extensions which use the `Require` or `Supported` header[1] **must** be documented as an RFC - to prevent interoperability problems
- All standardized SIP extensions **must** document how the extension interacts with elements that **don't understand** this extension

1. See **Other header fields** on page 182

SIP Service Logic



- Call Processing Language (CPL)
- SIP Common Gateway Interface (CGI)
- SIP Java Servlets

Call Processing Language (CPL)

RFC 2824: Call Processing Language (CPL) [191] and [192]

An XML-based scripting language for describing and controlling call services.

CPL is a very simple language without variables, loops, or the ability to run external programs! {Hence non-trusted end users can upload services to their SIP server} However, it has **primitives for making decisions** and **acting based on call properties** (e.g., time of day, caller, called party, …).

There is a Document Type Definition (DTD) "cpl.dtd" and strict parsing[1] is done based on this DTD.

See also Chapter 13 of *Practical VoIP: Using VOCAL*[1], this includes an example of developing a feature in CPL

See also the dynamic loading of CPL in [195].

1. Thus **any** discrepancies between the script and the scheme are errors.

SIP Common Gateway Interface (CGI)

RFC 3050: Common Gateway Interface for SIP [193]

Similar to HTML CGI, a SIP CGI script resides on the server and passes message parameters via environment variables to a separate process. This process sends instructions back to the server through its standard output file descriptor.

Scripts can be written in Perl, Tcl, C, C++, Java, …

Of course these scripts (being based on general purpose programming languages) do **not** have the limitations of CPL and hence **only trusted users** can be allowed to provide such scripts.

CGI scripts have access to both the request headers and the body and can therefore do general computations based on all this information.

SIP Java Servlets

Extends functionality of SIP client by passing messages to the SIP servelets.

Servlets are similar to the CGI concept, but instead of using a separate **process**, the messages are passed to a class that runs within a Java Virtual Machine (JVM) *inside the server*.

Servlets are portable between servers and operating systems, due to the portability of the Java code.

For details see: K. Peterbauer, J. Stadler, et al., "SIP Servlet API Extensions", February 2001, (an expired internet draft)

http://www.cs.columbia.edu/sip/drafts/draft-peterbauer-sip-servlet-ext-00.txt

SIP Servlets were defined in A. Kristensen and A. Byttner, "The SIP Servlet API", IETF Draft, September 1999,

http://www.cs.columbia.edu/sip/drafts/draft-kristensen-sip-servlet-00.txt

- Unfortunately this draft expired and was not carried forward, but is referenced (and large parts included) in subsequent work. See also [194].
- Today SIP Java Servlets are specified in JSR 116 and JSR 289[196].

JAIN APIs

Providing a level of abstraction for service creation across circuit switched and packet networks, i.e., bridging IP and IN protocols. Goal is provisioning of telecom services by:

- Service Portability: - Write Once, Run Anywhere. (via Java portability)
- Network Convergence: (Integrated Networks) - Any Network
- Service Provider Access - By Anyone!
  - to allow services direct access to network resources and devices

SIP APIs - especially those within the JAIN™ initiative (Java Application Interfaces for Communications & Java Application Containers for Communications) (http://java.sun.com/products/jain/index.jsp) :

- JAIN SIP (JSR-000032) - a low level API that maps directly to RFC 2543 - http://jcp.org/en/jsr/detail?id=32

- JAIN SIP Lite (JSR-000125)- a high-level API, to allow application developers to create applications that have SIP as their underlying protocol **without** needing extensive knowledge of SIP - http://jcp.org/en/jsr/detail?id=125
- SDP API (JSR-000141) - to enable users to manipulate SDP messages http://jcp.org/en/jsr/detail?id=141
- JAIN SIP Servlet API (JSR-000116) - http://jcp.org/en/jsr/detail?id=116
- SIMPLE related APIs
  - JAIN SIMPLE Instant Messaging (JSR-000165) - to exchange messages between SIMPLE clients http://jcp.org/en/jsr/detail?id=165
  - JAIN Instant Messaging (JSR-000187) - to control, manage and manipulate instant messages between clients through the use of presence servers http://jcp.org/en/jsr/detail?id=187
  - JAIN SIMPLE Presence (JSR-000164) - to manipulate presence information between a SIMPLE client (watcher) and a presence server (presence agent) http://jcp.org/en/jsr/detail?id=164
  - JAIN Presence and Availability Management (PAM) API (JSR-000123) - http://jcp.org/en/jsr/detail?id=123
  - JAIN Presence (JSR-000186) - to control, manage and manipulate Presence information between Presence clients and servers http://jcp.org/en/jsr/detail?id=186
- JAIN Service Provider APIs (SPA) - Java implementation of Parlay APIs

  - JAIN SPA Common API (JSR-000145) common across the JAIN SPA JSRs *http://jcp.org/en/jsr/detail?id=145*
  - JAIN SPA Integrity Management and Event Notification API (JSR-000119) *http://jcp.org/en/jsr/detail?id=119*
- Regarding Location
  - JAIN User Location and Status API (JSR-000098) - *http://jcp.org/en/jsr/detail?id=98*
  - JAIN User Location and Status (ULS) (JSR-000194) - to interrogate the location and status of a user's mobile device *http://jcp.org/en/jsr/detail?id=194*
- JAIN OAM API Specification v2.0 (JSR-000132) - *http://jcp.org/en/jsr/detail?id=132*
- JAIN ENUM API Specification (JSR-000161) - API to query and provision E.164 telephone numbers and their service-specific Uniform Resource Identifiers (URI) *http://jcp.org/en/jsr/detail?id=161*
- JAIN 3G MAP Specification (JSR-000137) - to enable mobile applications in the 3G domain to talk to each other *http://jcp.org/en/jsr/detail?id=137*

The full list of JAIN related specification can be found at:

http://java.sun.com/products/jain/api_specs.html

US National Institute of Standards and Technology - SIP and Jain

- NIST-SIP 1.2
- JAIN-SIP Proxy
- JAIN-SIP Instant Messaging Client
- JsPhone - a JAIN-SIP Video Phone
- NIST-SIP traces viewer
- JAIN-SIP gateway
- JAIN-SIP Third Party Call Controller

Parlay

Parlay Group formed (1998, ended ~2007) to specify and promote open APIs that "intimately link IT applications with the capabilities of the communications world".

Goal: to allow applications to access the functionality of the telecommunication network in a **secure** way.

Parlay APIs:

- Service interfaces - provide access to network capabilities and information
- Framework interfaces provide the underlying supporting necessary for the service interfaces to be secure and manageable.

The APIs are defined in Universal Modeling Language (UML).

For further info see [200] and 3GPP's Open Services Architecture.

SIP Request-URIs for Service Control

B. Campbell and R. Sparks, "Control of Service Context using SIP Request-URI", IETF RFC 3087, April 2001 [201] - proposes a mechanism to communicate context information[1] to an application (via the use of a distinctive Request-URI).

Using different URIs to provide both state information and the information about what lead to this state transition (for example, you were forwarded to the voicemail system because the user did not answer vs. being forwarded to the voicemail system because the user is busy with another call).

1. Call state information, such as the calling party, called party, reason for forward, etc.

Reason Header

Since it is (often) useful to know why a Session Initiation Protocol (SIP) request was issued, the Reason header was introduced. It encapsulates a final status code in a provisional response.

This functionality was needed to resolve the "Heterogeneous Error Response Forking Problem" (HERFP).

For details see [202].

Voice eXtensible Markup Language (VoiceXML^{3TM})

VoiceXML designed for creating audio dialogs (i.e., audio **in** and **out**) that feature: synthesized speech, digitized audio, recognition of spoken and DTMF key input, recording of spoken input, telephony, and mixed-initiative conversations.

Goal: To bring the advantages of web-based development and content delivery to interactive voice response applications.

For details see: *http://www.w3.org/TR/voicexml* [203]

Open VXI VoiceXML Interpreter (*http://sourceforge.com/projects/openvxi*) - an open source library to interpret VoiceXML.

VoiceXML is designed to go beyond Interactive Voice Response (IVR) systems.

CallControl XML (CCXML)

W3C's Voice Browser Working Group's CCXML [204] provides a standardized means of call control encoded in XML. Thus using CCXML you can set up, modify, and tear down calls.

R.J. Auburn, Chief Technology Officer, Voxeo Corporation and Editor and Chair, W3C CCXML working group has written a good introduction to CCXML [205].

Unlike VoiceXML, CCXML does not do any media process, but only does call control.

You can easily write CCXML that can answer a call from a given caller ID, but reject others. When the call is answered, it can be connected to an instance of a VoiceXML server. The VoiceXML server can collect information from the caller and then the call could be redirected to a human user agent - who could of course have all of the information relevant to this call brought up on their display based on processing of the collected information (this later is often called "Computer Telephony Integration (CTI)").

CCXML implementations

- Voxeo's Prophecy IVR platform [206]
- Oktopous™ ccXML Platform Integration Kit [207]
- Oktopous™, ccXML Open Source PIK [208]
- CCXML4J - a CCXML interpreter in Java [209]

Combining VoiceXML with CCXML

D. Amyot and R. Simoes describe the lessons they learned when implementing a Personal Assistant in ‘Combining VoiceXML with CCXML: A Comparative Study’ [210]

Projects: GlassFish and SailFin

SailFin - IMS Application Server supporting JSR 289 SIP servlets technology

For details see: SailFin[211] website, http://sailfin.java.net/

For an application built using this technology see [212].

There is an example of a Click to Dial service in Glassfish at:

https://wikis.oracle.com/display/GlassFish/SipClickToDialExample2

References and Further Reading

SIP Service Creation

[191] J. Lennox and H. Schulzrinne, “Call Processing Language Framework and Requirements”, IETF RFC 2824, May 2000.

[192]J. Lennox, X. Wu, and H. Schulzrinne, “Call Processing Language (CPL): A Language for User Control of Internet Telephony Services”, IETF RFC 3880, October 2004 http://www.ietf.org/rfc/rfc3880.txt

[193]J. Lennox, H. Schulzrinne, and J. Rosenberg, “Common Gateway Interface for SIP”, IETF RFC 3050, January 2001.

[194]Anders Byttner, “SIP Caller Preferences”, M.Sc. thesis, Department of Teleinformatics, Royal Institute of Technology, March 2000.

[195]Younes Oukhay, Context Aware Services, M.Sc. Thesis, Department of Communication Systems, Royal Institute of Technology (KTH), COS/CCS 2006-3, January 25, 2006

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/060125-Younes_Oukhay-with-cover.pdf

[196]Java Specification Requests (JSR 289): SIP Servlet v1.1
http://www.jcp.org/en/jsr/detail?id=289

JAIN

[197] JAIN website: http://java.sun.com/products/jain

[198] Java Community Process website: http://jcp.org/

[199]JAIN SIP 1.0 API specification

Parley

[200]Magnus Almkvist and Marcus Wahren, “Preserving Integrity in Telecommunication Networks opened by the Parlay Service Interface”, M.S. Thesis, Dept. of Microelectronics and Information Technology, Royal Institute of Technology, Sept. 2002

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/020930-Magnus-Almkvist-and-Marcus-Wahren.pdf

SIP Request URI

[201]B. Campbell and R. Sparks, “Control of Service Context using SIP Request-URI”, IETF RFC 3087, April 2001 http://www.ietf.org/rfc/rfc3087.txt

Reason Header

[202]H. Schulzrinne, D. Oran, and G. Camarillo, "The Reason Header Field for the Session Initiation Protocol (SIP)", IETF RFC 3326, December 2002 *ftp://ftp.rfc-editor.org/in-notes/rfc3326.txt*

VoiceXML

[203]Linda Boyer, Peter Danielsen, Jim Ferrans, Gerald Karam, David Ladd, Bruce Lucas, and Kenneth Rehor, "Voice eXtensible Markup Language (VoiceXML™)" version 1.0, W3C Note, 5 May 2000 *http://www.w3.org/TR/2000/NOTE-voicexml-20000505*

CCXML

[204]R.J. Auburn (Editor in Chief), Paolo Baggia and Mark Scott (Editors), Voice Browser Call Control: CCXML Version 1.0, W3C Candidate Recommendation 1, April 2010 *http://www.w3.org/TR/2010/CR-ccxml-20100401/*

[205]R.J. Auburn, Introduction to CCXML, web page, Voxeo Corporation, last accessed 20 August 2010 *http://www.voxeo.com/library/ccxml.jsp*

[206]Voxeo, IVR > Prophecy IVR Platform Software, webpage, Voxeo Corporation, last accessed 20 August 2010

http://www.voxeo.com/products/voicexml-ivr-platform.jsp

[207]Phonologies, Oktopous™, ccXML Platform Integration Kit, webpage, Phonologies (India) Private Limited, last accessed 20 August 2010

http://www.phonologies.com/oktopous.php

[208]Phonologies, Oktopous™, ccXML Open Source PIK v1.1, webpage, Phonologies (India) Private, Limited, last accessed 20 August 2010

http://www.phonologies.com/okto_os.php

[209]werner_di, CCXML4J, webpage, SourceForge, last accessed 20 August 2010 http://sourceforge.net/projects/ccxml4j/

[210]D. Amyot and R. Simoes, 'Combining VoiceXML with CCXML: A Comparative Study', presented at the 4th IEEE Consumer Communications and Networking Conference, 2007. CCNC 2007., 2007, pp. 342–346 [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4199162 .

SailFin

[211]GlassFish >> SailFin, website, last accessed 20 August 2009

https://sailfin.dev.java.net/

[212]Dan Peterström, IP Multimedia for Municipalities: The supporting architecture,TRITA-ICT-EX-2009:103, August 2009

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/090818-Dan_Peterstrom-with-cover.pdf

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1
Module 11: User Preferences

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:32

User Preferences

- Caller preference
  - allows caller to specify how a call should be handled
  - to specify media types: audio, video, whiteboard, …
  - to specify languages (of the callee -- consider for example a help desk call where you want to get help in *your* choice of language)
  - do you want to reach the callee at home or only at work?, via a landline or on their mobile phone? …
  - examples: should the call be **forked** or recurse, do you want to use a proxy or redirect, do you want to `CANCEL` 200 messages or not,
- Called party (i.e., Callee) preference
  - accepting or rejecting calls: based on time of day, day of week, location of called party, from unlisted numbers, …

Caller/callee different

- Callee is **passive**, caller is **active**
  - Thus callee's preferences must be defined ahead of time (for example by CPL)
  - However, caller's preferences can be in request
- Services (usually) run on callee server
- A given caller might contact any of a large number of number of servers (each of which will have to decide how to process this caller's request)

Conclusion: Include **caller** preferences in request

Contact parameters

Values are either pre-set or indicated when a user REGISTER's:

Parameter	Value	example(s)	Explaination of example(s)
class	personal business	class=personal	Call should go the "home" not the office.
duplex	full half send-only receive-only	duplex=full	should be a full duplex call
feature	voicemail attendant	feature=voicemail	Caller wants to be connected to voicemail server
language	language tag	language="en,de,se,!fi"	Connect caller to someone who speaks English, German, Swedish, not Finnish
media	MIME types	media="text/html"	use HTML as the media type
mobility	fixed mobile	mobility=fixed	connect to the callee's fixed rather than mobile terminal
priority	urgent emergency non-urgent	priority=urgent	call is urgent (as seen by the caller).
service	fax | IP | ISDN | PSTN | text	service=IP	use IP rather than fax/ISDN/PSTN/…

Contact header example

```
Contact: maguire <sip:maguire@it.kth.se> ;language="en,de,se,!es"
     ;media="audio,video,application/chat“
     ;duplex="full"
     ;priority="urgent"
```

Accept/Reject-Contact header(s)

SIP request contains Accept-Contact and Reject-Contact headers

`Reject-Contact` indicates URI's not acceptable

`Accept-Contact` indicates ordered list of acceptable URI's

Indication by means of rules

- set intersection and non-intersection of parameters
- string match of URIs

Example:

```
Accept-Contact: sip:sales@acme.com ;q=0,
    ;media="!video" ;q=0.1,
    ;mobility="fixed"  ;q=0.6,
    ;mobility="!fixed" ;q=0.4
```

In the second example, the caller does **not** want to talk to sales@acme.com, but has a preference for video and somewhat prefers the user's fixed to non-fixed (i.e., mobile) terminal.

Callee (i.e., called party) Parameter processing

- Proxy obtains list of URI's and the parameters for each, for callee
- Those that match a rule in Reject-Contact are discarded
- Matching set of URI's determined
- q parameters merged
- Result split into sets of q-equivalency classes
- Parallel search of highest preference q-equivalence class

Request-Disposition

Defines services desired from proxy servers

Feature values	Meaning
proxy redirect	whether to proxy or redirect
cancel no-cancel	whether to return just the first 200-class response, or all 2xx responses
fork no-fork	whether to fork or not (i.e., proxy to only a single address)
recurse no-recurse	whether a proxy server upon receiving a 3xx-class response should recurse (i.e., send requests to the addresses listed in the response) or not (i.e., simply forward the list of addresses upstream towards the caller)
parallel sequential	For a forking proxy server, should it send the request to all known addresses at once (parallel), or go through them sequentially, i.e., contacting the next address only after receiving a non-2xx or non-6xx final response.
queue no-queue	If called party is temporarily unreachable, caller can indicate that it wants to enqueue rather than be rejected immediately. Pending call be terminated by a SIP CANCEL or BYE request.

Based on a list of keywords

- example: `Request-Disposition: fork, parallel`

SIP Service Examples

Some examples of SIP Services are listed below (from [214])

- Call Hold
- Consultation Hold
- Music On Hold
- Unattended Transfer
- Attended Transfer
- Call Forwarding Unconditional
- Call Forwarding - Busy
- Call Forwarding - No Answer
- 3-way Conference - Third Party is Added
- 3-way Conference - Third Party Joins
- Single Line Extension
- Find-Me
- Call Management (Incoming Call Screening)
- Call Management (Outgoing Call Screening)
- Call Park
- Call Pickup
- Automatic Redial

You should compare these to the list we saw earlier: **Features** on page 218

Privacy-Conscious Personalization

Bell Labs' has developed software designed to give cell phone users greater control over the disclosure of their location [216].

Preferences could depend on:

- who is requesting the location data,
- what time of day it is,
- or the callers' activities,
- … .

Requests for location are then filtered through these preferences, and are permitted or blocked accordingly.

Operators might provide users with a selection of "preference palettes" to start with, the user could then customize their preferences over time.

References and Further Reading

User Preferences

[213] J. Rosenberg, H. Schulzrinne , and P. Kyzivat, "Caller Preferences for the Session Initiation Protocol (SIP)", IETF RFC 3841, August 2004 http://www.ietf.org/rfc/rfc3841.txt

[214] A. Johnston, R. Sparks, C. Cunningham, S. Donovan, and K. Summers, "Session Initiation Protocol Service Examples", Internet Request for Comments, RFC Editor, RFC 5359 (Best Current Practice), ISSN 2070-1721, October 2008 http://www.rfc-editor.org/rfc/rfc5359.txt

[215] J. Lennox, X. Wu, and H. Schulzrinne, "Call Processing Language (CPL): A Language for User Control of Internet Telephony Services", RFC 3880, October 2004 http://www.ietf.org/rfc/rfc3880.txt

[216] Jeffrey Selingo, "Protecting the Cellphone User's Right to Hide", New York Times, 5 Feb. 2004, p. E5 http://www.nytimes.com/2004/02/05/technology/circuits/05next.html

[217] Zohair Chentouf, Ahmed Khoumsi, and Soumaya Cherkaoui, Conceptual foundations of user preference modeling, In *Network control and engineering for QoS*, security and mobility II, D. Gaïti, G. Pujolle, A. Al-Naamany, H. Bourdoucen, and L. Khriji (Eds.), Kluwer Academic Publishers, Norwell, MA, USA, 2003, ISBN 1-4020-7616-9, pages 238-250.

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 12: SIP Security, NATs, and Firewalls

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:32

maguire@kth.se

SIP Security

SIP Security - RFC 3261 [218], obsoleted by RFCs 3261, 3262, 3263, 3264, 3265

If you want to secure **both** the SIP and RTP traffic, then you should probably be using an IPSec VPN.

SIP's rich signalling means that the traffic reveals:

- caller and called parties IP addresses
- contact lists
- traffic patterns

For further details concerning how complex it is to protect such personal information see the dissertation by Alberto Escudero-Pascual, "Privacy in the next generation Internet, Data Protection in the context of European Union Data Protection Policy" [265].

For an example of a **call anonymizer service** -- using a back-to-back user agent (B2BUA), see figure 8.6 on page 121 of Sinnreich and Johnston.

SIP Digest Authentication

Built upon HTTP's challenge/response mechanism

Challenges:

- `401 Authentication Required` or
- `407 Proxy Authorization Required`

Header fields:

Digest	the schema name
username="A"	The user name as specified in the credentials
realm="sip:proxy.com"	realm - copied from the challenge realm indicates the domain for the authentication
nonce="e288df84f1cec4341ade6e5a359"	nonce - copied from the challenge a unique string - typically generated from a timestamp (and possibly a seed), then encrypted with the user's private key
opaque="63632f41"	opaque string which should be returned unchanged to be matched against the challenge (allows for a stateless system)
uri="sip:UserB@there.com"	URI from the `Request-URI`
response="1d19580cd833064324a787ecc"	message digest computed using user's credentials and the nonce

SIP and S/MIME

RFC 3261 describes the use of Secure MIME (S/MIME) message bodies:

- SIP header fields can be encrypted in an S/MIME message body
- see RFC 5751[221] (which has replaced RFC 2633 and RFC 3851)

Provides:

- Message integrity
  - Allows detection of any modification of message contents
- Message privacy
  - Private headers protected by S/MIME
- Identity
  - Certificates can be verified to validate identity

SDP & RTP security

As noted earlier SDP enables you to say that you will encrypt the media stream which is sent via RTP - such as DES in CBC Mode (DES-CBC)[1] or AES in f8-mode [228].

This is done via adding to the SDP for each media description:

k=encryption key

1. All encryption capable RTP clients must support this as their default algorithm. In addition, to prevent known plain text attacks, RTCP headers have a 32 bit random prefix.

User identity

J. Peterson and C. Jennings in RFC 4474 [222] define mechanims and practices to assure the identity of the end user that *originates a SIP request* (does **not** cover identity for *responses*).

Their identity mechanism derives from the following principle:

> If you can prove you are eligible to register in a domain under a particular address-of-record (AoR), then you are also proving that you are capable of receiving requests for that AoR
> ∴ when you place that AoR in the `From` header field of a SIP request other than a registration (e.g., `INVITE`), you are providing a 'return address' where you can legitimately be reached.

adapted from [222]

Introduces:
(a) *authentication service* (at either a **user agent** or a **proxy server**) and
(b) two new SIP headers, **Identity** & **Identity-Info** headers

Identity header example

from [222]

```
INVITE sip:bob@biloxi.example.org SIP/2.0
   Via: SIP/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bKnashds8
   To: Bob <sip:bob@biloxi.example.org>
   From: Alice <sip:alice@atlanta.example.com>;tag=1928301774
   Call-ID: a84b4c76e66710
   CSeq: 314159 INVITE
   Max-Forwards: 70
   Date: Thu, 21 Feb 2002 13:02:03 GMT
   Contact: <sip:alice@pc33.atlanta.example.com>
   Identity:
  "ZYNBbHC00VMZr2kZt6VmCvPonWJMGvQTBDqghoWeLxJfzB2a1pxAr3VgrB0SsSAa
  ifsRdiOPoQZYOy2wrVghuhcsMbHWUSFxI6p6q5TOQXHMmz6uEo3svJsSH49thyGn
      FVcnyaZ++yRlBYYQTLqWzJ+KVhPKbfU/pryhVn9Yc6U="
   Identity-Info: <https://atlanta.example.com/atlanta.cer>;alg=rsa-sha1
   Content-Type: application/sdp
   Content-Length: 147

   v=0
   o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com
   s=Session SDP
   c=IN IP4 pc33.atlanta.example.com
   t=0 0
   m=audio 49172 RTP/AVP 0
   a=rtpmap:0 PCMU/8000
```

Saying BYE *also* needs to be authenticated!

```
BYE sip:alice@pc33.atlanta.example.com SIP/2.0
   Via: SIP/2.0/TLS 192.0.2.4;branch=z9hG4bKnashds10
   Max-Forwards: 70
   From: Bob <sip:bob@biloxi.example.org>;tag=a6c85cf
   To: Alice <sip:alice@atlanta.example.com>;tag=1928301774
   Date: Thu, 21 Feb 2002 14:19:51 GMT
   Call-ID: a84b4c76e66710
   CSeq: 231 BYE
   Identity:
  "sv5CTo05KqpSmtHt3dcEiO/1CWTSZtnG3iV+1nmurLXV/HmtyNS7Ltrg9dlxkWzo
   eU7d7OV8HweTTDobV3itTmgPwCFjaEmMyEI3d7SyN21yNDo2ER/Ovgtw0Lu5csIp
      pPqOg1uXndzHbG7mR6Rl9BnUhHufVRbp51Mn3w0gfUs="
   Identity-Info: <https://biloxi.example.org/biloxi.cer>;alg=rsa-sha1
   Content-Length: 0
```

`alg=rsa-sha1` is a new part of the RFC that was not in the earlier internet draft.

Erik Eliasson's miniSIP[1]

miniSIP supports pluggable CODECs:

- each RTP packet says which codec was used
- SDP can specify multiple codecs each with different properties (including better than toll quality)
- tests used PCM ⇒ sending 50 packets of 160 byte RTP payload length (packet size is 176 bytes) per second (i.e. 64 Kbps), i.e., 20 ms between packets
- Configuration used in the test described next:
  - time to transmit/receive a packet ~55-60 μs
  - Laptop ASUS 1300B with Pentium III processor, 700 MHz
  - 112 MB RAM (no swapping)
  - Operating System: SuSE Linux 7.1 Personal Edition
  - Security Services: confidentiality and message authentication (with Replay Protection)
  - Cryptographic Algorithms: AES in Counter Mode for the confidentiality and HMAC SHA1 for the message authentication
  - Lengths: master key: 16 bytes; salting key: 14 bytes; authentication key: 16 bytes; encryption key: 16 bytes; block: 128 bytes

1. http://www.minisip.org/

Secure Real Time Protocol (SRTP)

Described in RFC 3711 [232], provides confidentiality, message authentication, and replay protection for RTP and RTCP traffic.

Sender behavior	Receiver behavior
	Read the SRTP packet from the socket.
Determine cryptographic context to use	Determine the cryptographic context to be used
Derive session keys from master key (via MIKEY)	Determine the session keys from master key (via MIKEY)
	If message authentication and replay protection are provided, check for possible replay and verify the authentication tag
Encrypt the RTP payload	Decrypt the Encrypted Portion of the packet
If message authentication required, compute authentication tag and append	If present, remove authentication tag
Send the SRTP packet to the socket	Pass the RTP packet up the stack

In 2003, Israel M. Abad Caballero, *Secure Mobile Voice over IP*, M.Sc. Thesis [223]

- AES CM (Rijndael) or Null Cipher for encryption (using libcrypto)
- HMAC or, Null authenticator for message authentication
- SRTP packet is 176 bytes (RTP + 4 for the authentication tag if message authentication is to be provided)
- Packet creation: RTP 3-5 µs; RTP+SRTP 76-80 µs (throughput 20Mbps)
  - ~1% of the time there are packets which take as long as 240 µs

Multimedia Internet KEYing (MIKEY) [236]as the key management protocol

In 2003, Johan Bilien, *Key Agreement for Secure Voice over IP*, M.Sc. Thesis [224]

Extends earlier thesis - Runs on a laptop or iPAQ under linux

Secure Call Setup [226]

Total delay (in ms)	Calling Delay	Answering Delay
No security	19.5	9.5
MIKEY, shared key	20.9	10.5
MIKEY, Diffie-Hellman	52.5 (UDP)	47.6 (UDP)
	58.9 TCP)	48.9 (TCP)

- name-servers (BIND 8.2 on Linux 2.4, 500 MHz Pentium 3 laptops)
- root name-server ns.lab manages the delegation of minisip.com and ssvl.kth.se to their respective name server
- two routers (1.1 GHz Celeron desktops) perform static routing, and each router also runs a SIP server, SIP Express Router (SER v0.8.11))
- Alice and Bob use minisip, running on 1.4 GHz Pentium 4 laptops,running Linux 2.4

In 2005, Joachim Orrblad in his thesis, “Alternatives to MIKEY/SRTP to secure VoIP”[225], examines the use of MIKEY together with IPSec.

Efficient Stream Loss-tolerant Authentication (TESLA)

SRTP TESLA [237] was designed to provide efficient data origin authentication for multicast and broadcast session.

This is needed since we do **not** want to create all possible pairwise authentications for the participants in a conference.

Elisabetta Carrara

For details of the reasoning behind SRTP and MIKEY, see Elisabetta Carrara's licentiate thesis: Security for IP Multimedia Applications over Heterogeneous Networks [238].

NATs and Firewalls

Because Network Address Translation (NAT) devices change addresses and sometimes port numbers and because addresses and port numbers are **inside** both SIP and SDP there can be a problem!

Fredrik Thernelius, "SIP, NAT, and Firewalls", looked at this in detail in his M.Sc. thesis [239]. See also the other documents at

http://www.cs.columbia.edu/sip/drafts_firewall.html

Note: CNAME's in RTCP may need to be updated by the Network Address Translation (NAT) to **hide** private network addresses.

To protocols being developed to help deal with NATs:

- Simple Traversal of User Datagram Protocol Through Network Address Translators (STUN)
- Globally Routable User Agent Universal (GRUU) Resource Indicator[246]
  - a URI which can be used by anyone on the Internet to route a call to a specific UA instance

See also pages 237-239 of *Practical VoIP: Using VOCAL* [1]; particularily the example of using a Cisco ATA (Analog Telephone Adaptor) behind a Linksys firewall (which configures the firewall to pass incoming traffic on port 5060, 4000, and 4001 to the Cisco ATA) - which also refers to http://www.dyndns.org/

Types of NAT

Source NAT	All callers look like they come from the same IP address
Destination NAT	Which internal address should traffic to a given port be forwarded to?

Four types of NATs [247] and

Type	Description
Full Cone	maps a specific internal IP address and port number to a given external IP address and port number This is the only type of NAT that allows an external host to contact an internal host (i.e., behind the NAT) **without** having previously received packets from this internal host.
Restricted Cone	external hosts must have the IP address of an internal host **prior** to communicating with this internal host
Port Restricted Cone	external hosts must have the IP address and port number of an internal host **prior** to communicating with this internal host
Symmetric	assigns unique internal IP address and port numbers based on the specific internal destination

Cone vs. Symmetric NAT

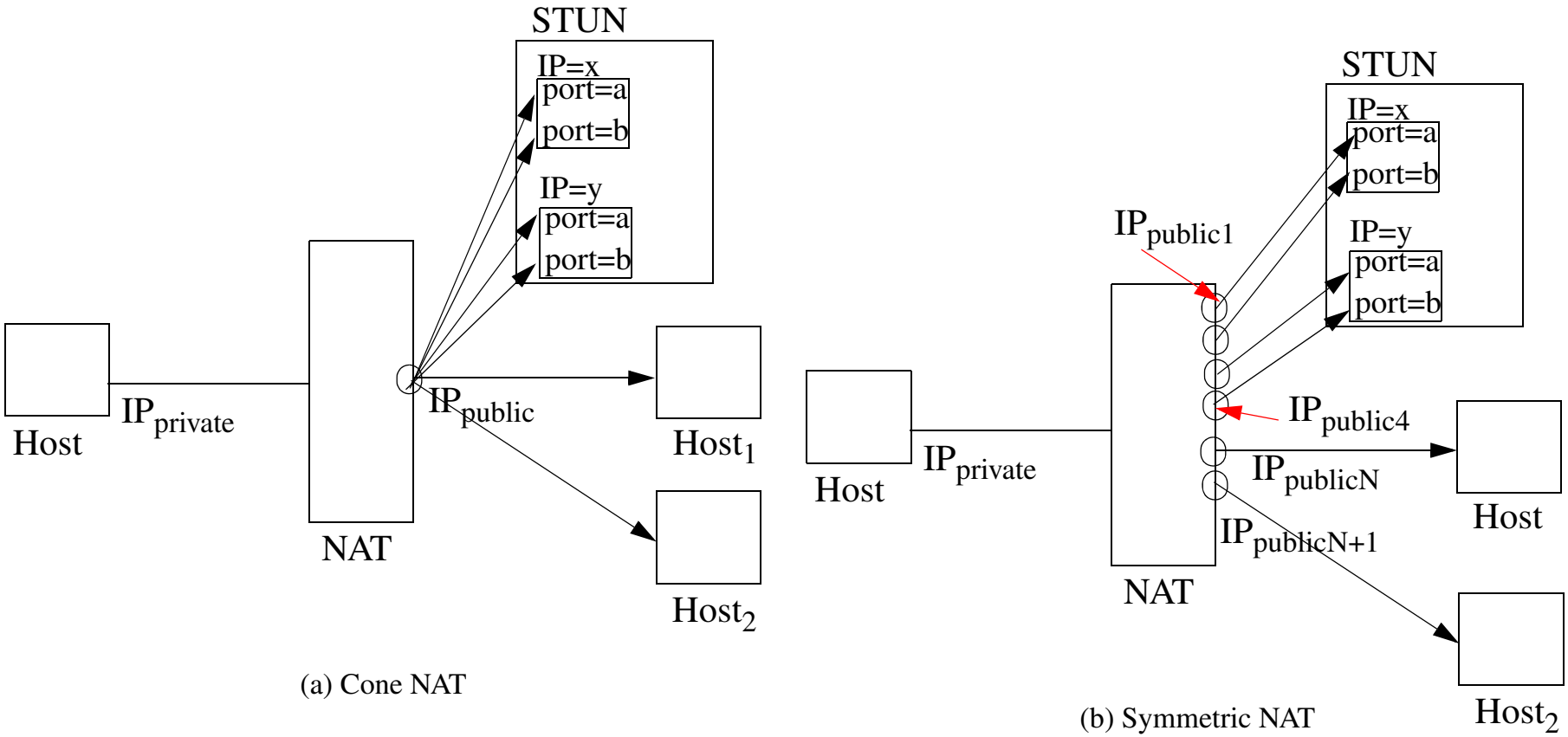


Figure 37: (a) Cone NAT vs. (b) Symmetric NAT - figure inspired by figures 1 and 2 of [251]

NAT traversal methods

- Symmetric media streams
- STUN protocol
  - also: Extended STUN for Symmetric NAT
- rport SIP extension
  - See RFC 3581[248] - defines a new parameter for the Via header field, called "rport", this “allows a client to request that the server send the response back to the source IP address and port from which the request originated.”
- OPTIONS request registration refresh
  - Causes the UA to send traffic out - thus refreshing the NAT bindings
- Outgoing INVITE transaction refresh
- Traversal using Relay NAT (TURN)
  - insert a server in the media and signalling path (to deal with Symmetric NATs)
- Application Layer Gateway (ALG)
  - Here the NAT knows about SIP and “does the right thing”
- Universal Plug and Play (UPnP)
  - Use UPnP to control the NAT to open a specific “pinhole” in the firewall
- Manual Configuration
  - manually configure a set of addresses and ports for SIP to use

- Tunnel
  - Tunnel the traffic - inside IPsec, HTTP (i.e., act like HTTP), …

A NAT support "**hairpinning**" if it can route packets coming **from** the private network addressed to a public IP address **back** into the private network. For example, a mobile user might actually be connected to the private network - thus packets to this user do not actually need to be sent out and then sent back into the private network!

STUN (Simple Traversal of UDP through NATs (Network Address Translation))

STUN, defined in RFC 3489 [244] (replaced by RFC 5389 [245]), assists devices behind a NAT firewall or router with their packet routing.

- enables a device to find out its public IP address and the type of NAT service its sitting behind
  - By querying a STUN server with a known public address, the STUN client learns the public IP and port address that were allocated by this client's) NAT.
- operates on TCP and UDP port 3478
- uses DNS SRV records to find STUN servers attached to a domain. The service name is _stun._udp or _stun._tcp
- Unfortunately, it is not (yet) widely supported by VOIP devices

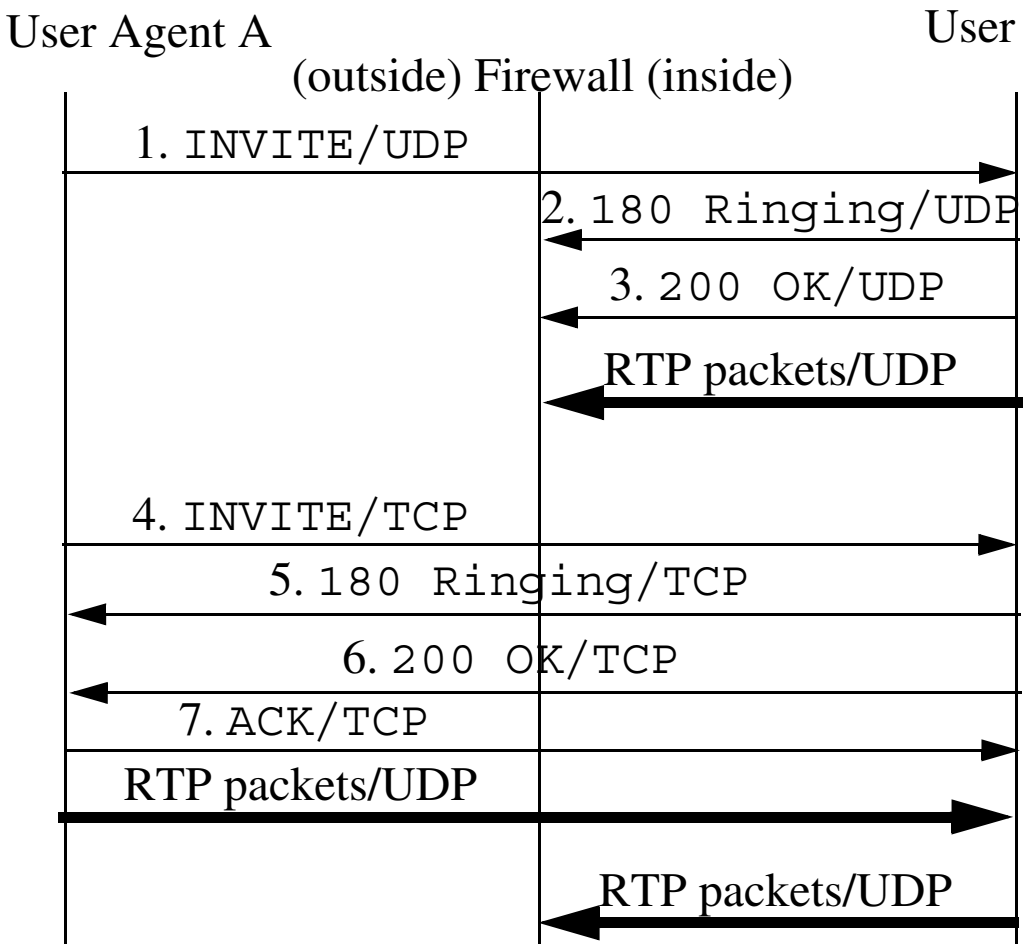
Note: The STUN RFC states: This protocol is not a cure-all for the problems associated with NAT.

Open source STUN servers - see http://www.voip-info.org/wiki/view/STUN .

STUN steps

1. Client queries a STUN server for a shared secret username and password
2. Server responds with a unique username/password combination for this client
3. Client sends a binding request using this username/password to the server via UDP
4. Server copies the source IP and port number into a binding response, and sends this response back to the client
5. Client compares the IP address and port number received from the server with its local IP address and port number. If they **do not** match, then the client is behind some type of NAT.
   - A full flowchart to find each of the potential situations is shown as Figure 14 “Flow Chart: Determining NAT type” in [247].

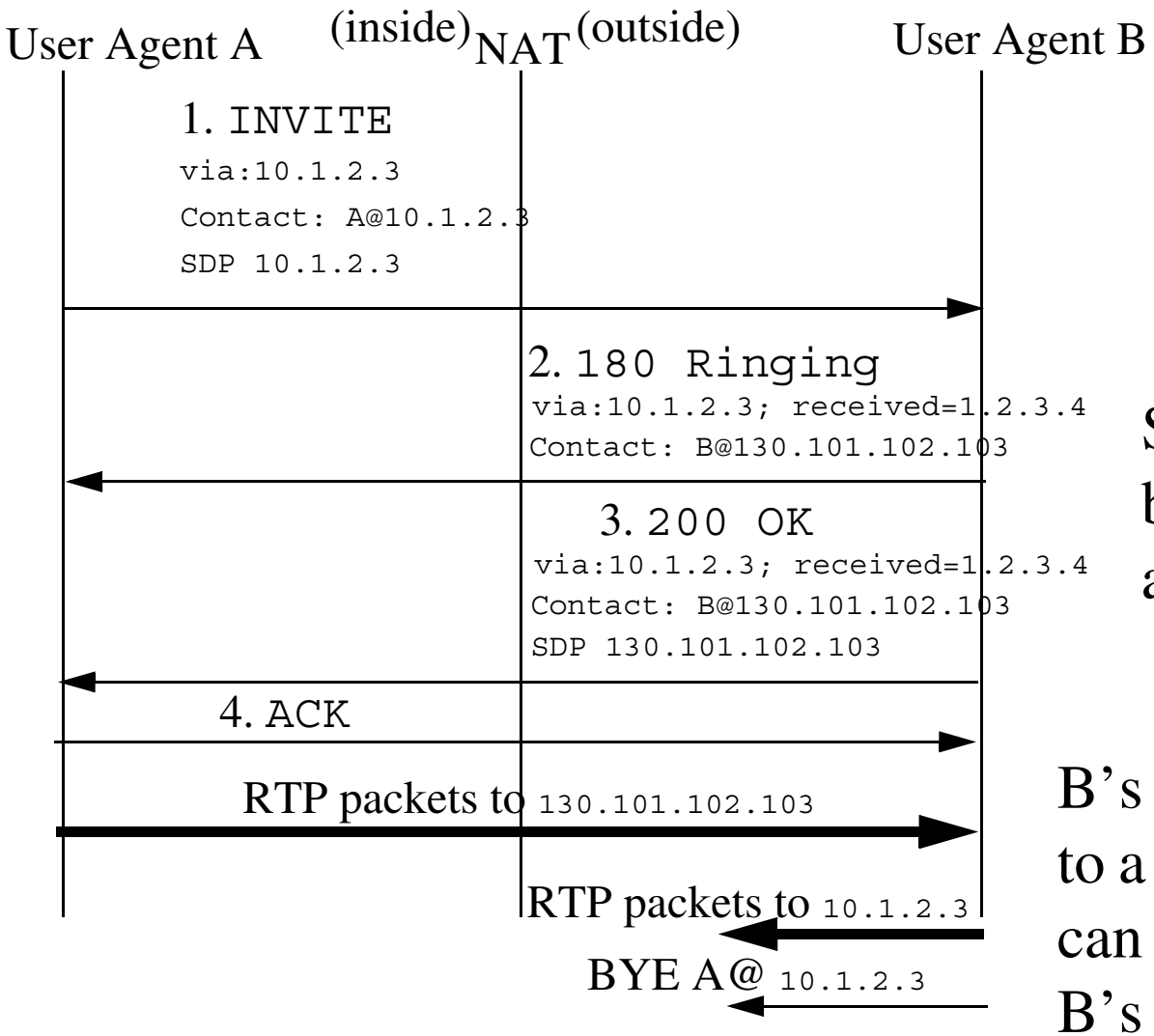
UDP and TCP Firewall Traversal problems



Using UDP all of B's responses and packets are filtered out by the firewall and there is no session!

Using TCP for SIP enables the session to be setup, but B's RTP packets are still filtered out by the firewall!

UDP and TCP NAT Traversal problems



SIP can negociate the NAT, but A's SDP contains a privat address

B's RTP packets are directed to a private address and hence can not be routed; similarily B's requests also fail

NAT and RTSP

NATs also affect RTSP, hence there are several efforts to address this:

- M. Westerlund and T. Zeng, The Evaluation of Different Network Addres Translator (NAT) Traversal Techniques for Media Controlled by Real-time Streaming Protocol (RTSP) [262]
- J. Goldberg, M. Westerlund, and T. Zeng, A Network Address Translator (NAT) Traversal mechanism for media controlled by Real-Time Streaming Protocol (RTSP) [263]

Other NAT traversal protocols

Traversal Using Relay Nat (TURN)

A. La Torre Yurkov's masters thesis: Implementation of Traversal Using Relay Nat for SIP based VoIP [252] describes TURN, its implementation, and performance.

TURN is specified in RFC 5766 [253].

ICE

Another protcol for NAT traversal is "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocol" as specified in RFC 5245 [254].

RFC 6544: TCP Candidates with Interactive Connectivity Establishment (ICE)[256]

RFC 6336 : IANA Registry for Interactive Connectivity Establishment (ICE) Options [257]

With several Internet-Drafts:

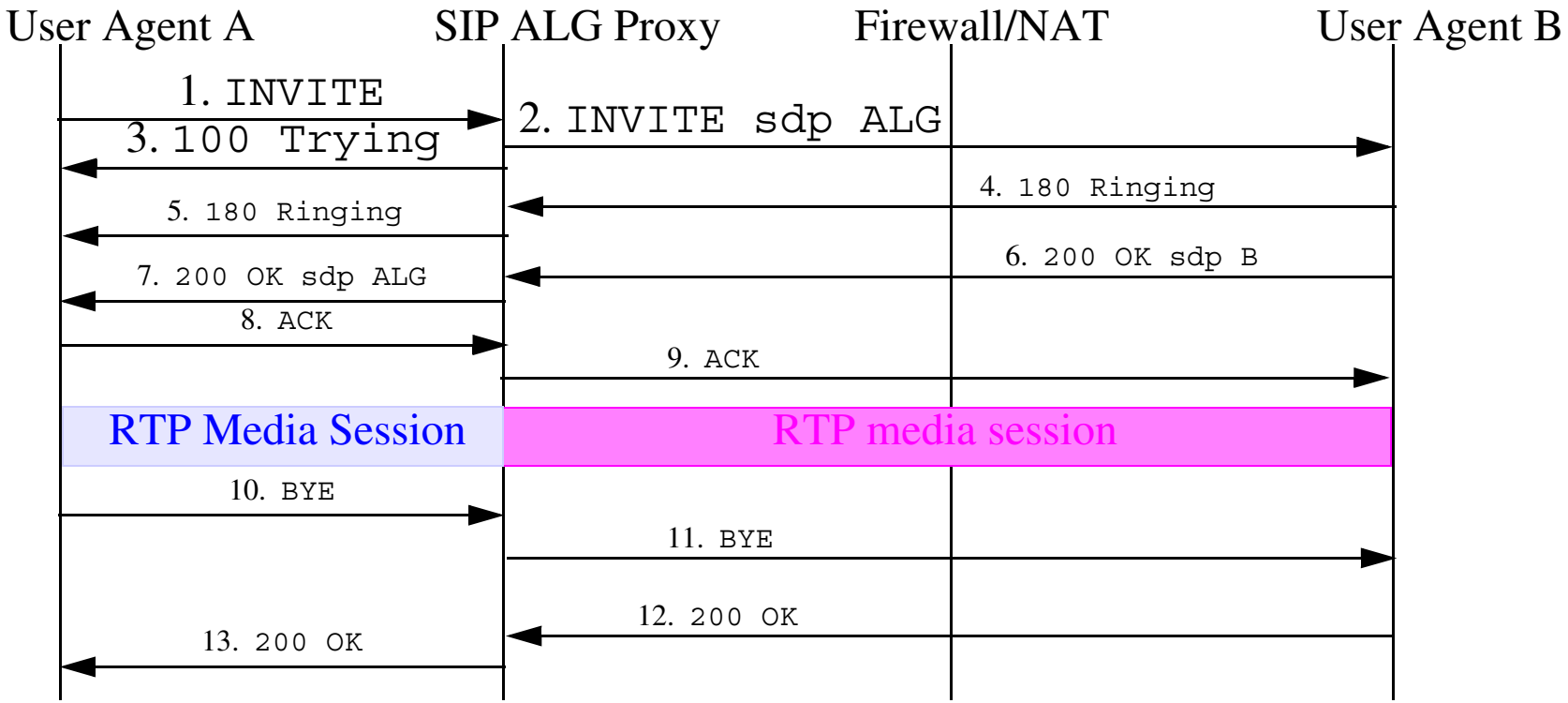
- M. Petit-Huguenin and A. Keranen, Using Interactive Connectivity Establishment (ICE) with Session Description Protocol (SDP) offer/answer and Session Initiation Protocol (SIP) [258]
- E. Ivov, H. Kaplan, and D. Wing, Latching: Hosted NAT Traversal (HNT) for Media in Real-Time Communication [259]
- T. Reddy, P. Patil, and D. Wing, Happy Eyeballs Extension for ICE [260]
- Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols [261]

HIP

Yet another NAT traversal protocol is "Basic Host Identity Protocol (HIP) Extensions for Traversal of Network Address Translators" as specified in RFC 5770 [255].

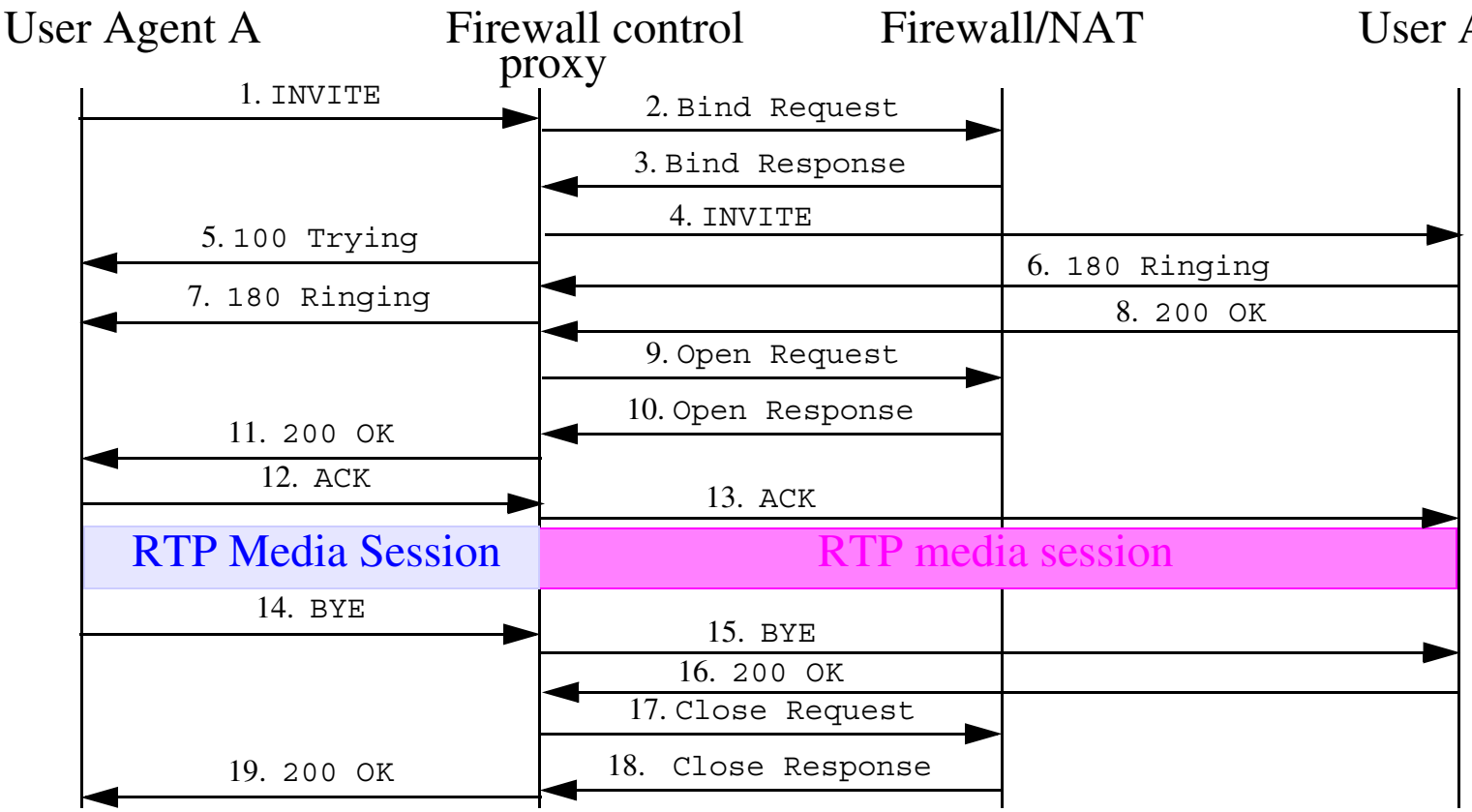
SIP Application Level Gateway (ALG) for Firewall Traversal

Use a proxy within the (possibly private) network:



Firewall permits SIP and RTP traffic to/from the Application Level Gateway (ALG) proxy. For some recent work in this area see [242].

Middlebox communications (MIDCOM)



The generic problem of enabling complex applications through the middleboxes is being addressed by the Middlebox communications (MIDCOM) Working Group, they do so via MIDCOM agents which perform ALG functions, logically external to a middlebox [241]. See also [264].

Application aware Middlebox

Newport Networks' Automatic Channel Mapping™ (ACM) [250]:

- SignallingProxy™ acts as a high-performance B2BUA (Back to Back User Agent
- MediaProxy™ provides a transit point for RTP and RTCP media streams between User Agents

Security flaws in Abstract Syntax Notation One (ASN.1)

Note that the vulnerability was discovered in June 2002!

The United Kingdom National Infrastructure Security Co-Ordination Centre revealed in Jan. 2004, “that it had discovered security flaws that affect the products of dozens of vendors. The flaws were found in software that support a variety of applications and technologies, including voice over IP, videoconferencing, text messaging, Session Initiation Protocol, devices and hardware, and critical networking equipment such as routers and firewalls.” …

“CIOs need to be aware that voice over IP creates exposure to vulnerabilities, says David Fraley, a principal analyst at Gartner Dataquest. "While there are very real and neat opportunities with VoIP, as convergence increases, the risks to attacks to these systems are going to increase," he says.

George V. Hulme, “H.323 Flaws Threaten Scores Of Products”, InformationWeek, January 15, 2004, http://update.internetweek.com/cgi-bin4/DM/y/eer70Blkgg0V30CKN80Av

Risks range from denial-of-service attacks to allowing access to malicious code. according to the

see *http://www.cert.org/advisories/CA-2004-01.html#vendors*

Communications and Privacy

- Encryption as the norm - even onetime pads are feasible
  - Since all speech and other media content will be in digital form, it will be trivial to provide encryption and authentication of all communication (if the participants want to)
  - traditional public telephony **less secure** than using: VPNs, SRTP, MIKEY, …
  - For WLANs: IEEE 802.11i security features along with 128-bit Advanced Encryption Standard (AES) encryption, …
- Identity hiding - Authentication when you mutually want to
- Mobile presence has to be done carefully
- Anonymous network access
- Location hiding & Privacy
  - Alberto Escudero-Pascual, http://www.it.kth.se/~aep
    - *Anonymous and Untraceable Communications - Location privacy in mobile internetworking*, Licentiate Thesis, June 2001
    - *Privacy in the Next generation Internet: Data Protection in the context of the European Union Policy*, Dissertation, Dec. 2002
- Location mis-direction $\Rightarrow$ End of Sovereignty
- Traffic pattern hiding
- Traffic hiding

See [266] to [270].

Swedish Electronic Communications Act

Swedish Electronic Communications Act (SFS 2003:389) (aka 'LEK ')[271] (modified in SFS 2012:128) provides the regulatory framework for electronic communications networks and services. "The Electronic Communications Act (SFS 2003:389) contains the basic principle that the use of numbering resources from a national plans is subject to a license obligation. The Post- and Telecom Agency (PTS) is given the authority to handle national numbering and addressing plans and provide licenses for these resources." Ylva Ehn, PTS, 23 of October 2006 #06-13999 http://www.pts.se/upload/Documents/EN/06_13999_remiss_eng_kortversion_forslag_foreskrift_tekniska_planer_okt06.pdf

It is based on EU directives and became effective on July 25th, 2003. It defines what/who an operator is and what their obligations are. (note: it replaces the earlier swedish definition of "teleoperator").

It is relevant to **publically available** telephone services in 3 major areas:

- emergency calls (Chapter 5, section 7)[271]
- number portability (Chapter 5, section 9)[271], and
- legal intercept (Chapter 6, section 19)[271]

See also the controversy surrounding the "FRA-lagen" - as per proposition 2006/07:63 – *En anpassad försvarsunderrättelseverksamhet*

Electronic communications service

According to the PTS, in order for a service to be an electronic communications service it must meet the following criteria:

- “the service is provided to another (external) party, on commercial grounds, and
- the service consists mainly in the conveyance of signals, and
- the service provider has the power to control the transmission”. [286]

Recording of Call Contents

The lawful "use of electronic recording equipment" - when can you make a recording of a call's contents (i.e., wiretapping and eavesdropping)?

The US Federal government (18 U.S.C. Sec 2511,) and many states have "one-party consent" statutes, i.e., if you are a party to the conversation you can record it. However, note that not all states permit this (some have an "all-party" rule)! Note that these rules often apply to in-person recordings, radio/telecommunication, … , all "electronic communications".

There are additional rules concerning Broadcasters - who must inform the person that the recording may be subsequently broadcase **before** the recording begins.

A summary of the rules for the US can be found at: http://www.rcfp.org/taping/index.html

In addition, there are also laws concerning "employee privacy" which may also be relevant.

For the IETF policy on wiretapping see RFC 2804 [285].

Privacy & Lawful Intercept (LI)

There is a proposal that Communications Assistance for Law Enforcement Act (CALEA) {47 U.S.C. § 1001 et seq. [272]} should be applied to VoIP services (and other data services) to "conduct lawful electronic surveillance":

U.S. Dept. of Justice, FBI and DEA, Joint Petition [to US FCC] for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, 10 March, 2004[273].

Types of surveillance [275]:

"pen register"	records call-identifying information for calls **originated** by a subject
"trap and trace"	records call-identifying information for calls **received** by a subject, and
"interception"	records the **conversations** of the subject, as well as call identifying information

There is a great variety of proposals for LI [284].

Reasonably Available Information

Operators are only required to provide information to law enforcement if it is reasonably available. For example, “call-identifying information is reasonably available to a carrier if it is present at an intercept access point and can be made available without the carrier being unduly burdened with network modifications”.

The EU statute is similar in identifying when information is technically feasible and economically feasible available.

Thus **Call Forwarding Information** might **not** always be reasonably available in a SIP environment - since the call forwarding could happen outside the control of a given operator.

Similarily **Dialed-Digit Extraction** might **not** be available in a SIP environment since the actual IP address of the source and destination might be inside encrypted SDP

EU privacy and Lawful Intercept (LI)

EU Directive 95/46/EC - Data Protection Directive,
EU Directive 97/66/EC - Telecommunications Data Protection, and
EU Directive 2002/58/EC - the e-Communications Directive

http://www.dataprivacy.ie/images/Directive%202002-58.pdf

A good summary of the EU situation can be found at [274].

ETSI is defining a standard LI architecture see [277] and [278]. For a list of the LI standards as collected by the Global LI Industry Forum, Inc. [280] see [281].

Intercept architecture

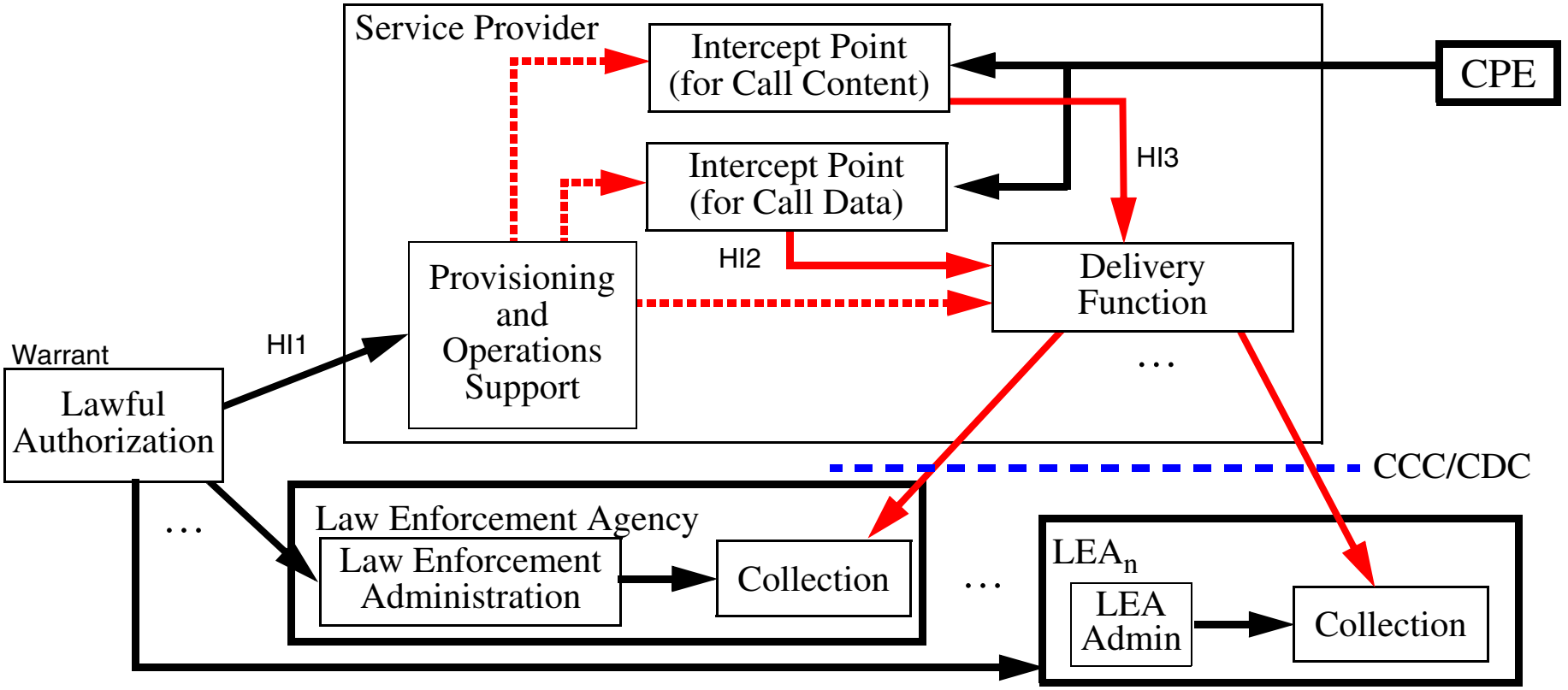


Figure 38: Interfaces in RED should be standard to allow interoperability; HI_n = Handover $Interface_n$

- The existance of Intercepts should be transparent to both the **subject** and **other** LEAs!
- The dotted links (probably SNMPv3) must be secured to prevent **Unauthorized Creation** and **Detection** of intercepts - while solid red links must be secured to protect intercept related information (IRI) [276]
- Intercept [Access] Point (IAP): router, PSTN gateway, SIP proxy, RADIUS server, …

Lawful Intercept - some additional problems

A survey of lawful intercept (for both analog telephony and VoIP) can be found in Romanidis Evripidis's thesis: Lawful Interception and Countermeasures: In the era of Internet Telephony [287]. He points out a problem for key escrow in that the law enforcement agency can fabricate evidence - once they have the key!

A key esrow system for minisip with countermeasures for fabrication of evidence (based on the idea proposed in the above thesis) as been implemented in:

- Md. Sakhawat Hossen, "A Session Initiation Protocol User Agent with Key Escrow: Providing authenticity for recordings of secure sessions", [288]
- Muhammad Sarwar Jahan Morshed, "Voice over IP and Lawful Intercept: God cop/Bad cop" [289]

Data Retention Directive

European Parliament and the Council of the European Union, Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [290].

Article 5: Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

(a) data necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony and mobile telephony:

..

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii) the user ID and telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

..

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

..

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a

communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

..

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

..

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;

(f) data necessary to identify the location of mobile communication equipment:

(1) the location label (Cell ID) at the start of the communication;

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Sweden was “late” implementing a national law in regard to this directive (hence the EU Commission took Sweden to the European Court of Justice). Note that: Austria, Greece, Ireland, The Netherlands, and Poland are also “late” to implement national laws regarding this directive.

SIP Recording

SIP recording is often necessary for regulatory or compliance reasons (for example, emergency call centers, banks & trading floors, …) and calls might be recorded for "quality control", supervision, business analysis, …
⇒ SIP-based Media Recording

The requirements are described in a recent Internet draft: "Requirements for SIP-based Media Recording (SIPREC)" [301] - this defines several use cases:

- Total call recording - all of every call is to be recorded
- Selective recording - only specific calls are recorded
- Dynamic recording (also known as Mid-session or Mid-call recording)
- Persistant recording - all calls recorded as a single recording session
- Real-time recording controls to enable some portions of the call
- IVR/Voice portal recording - recording media during interaction with an interactive voice response (IVR) application

- Enterprise mobility recording - recording sessions when a user is not within the enterprise, but is acting on behalf of the enterprise
- Geographically vs. centralized recording schemes
- Recording “complex” calls - for example maintaining a continguous recording despite the caller being transferred to another party
- High-availability and high reliability recording - being able to either reject a communication call setup or transfer the recording responsibility to another recording server, handle failover/transfer of recorder responsibility in the middle of a recording session, etc.
- Recording multi-media and multi-channel sessions
- Real-time media processing - to support real-time analysis of the voice (for example, automatically generating an alert based upon the speech content, stopping a session on a keyword, …)

SIP Recording Architecture

An architecture has been proposed, see the Internet draft: “An Architecture for Media Recording using the Session Initiation” [302]

In addition to defining some entities (recording session server, recording session client, and recording aware user agent), the architecture defines a communication session, a recording session, replicated media, and explicitly addresses the issue of **media recording metadata**.

This metadata is important in order to identify the participants in a session, the call state, and other parameters of the session.

SIP extentions for SIP recording

A set of SIP extentions have been defined to allow SIP entities to distinguish between a Recording Session and a Communication Session and so that a SIP UA can know if a session is being recorded - see Internet draft: “SIP Call Control - Recording Extensions” [303] - for the definitions of the new feature tags: src (session recording clients indicates this session is for the purposes of a recording session), srs (used by the session recording server), and recorded (to indicate that some or all of the media session is being recorded)

Will VoIP calls have to:

- Be stored for compliance reasons?
- Be stored for discovery reasons?
- Will they have to be indexed? (to make them accessible)
- UK is proposing that top level ISPs store all records of Internet communications (date, time, sender/ caller, receiver/callee, URL, cell ID, IP address(es), routing, duration, …) to make it convenient for the government to access them, because they do not want to have to pay each of the individual ISPs, and to limit the number of parties that they have to deal with. (See EU Data Retention Directive (EUDRD).)

Lawful intercept of VoIP communications

- Generally mandated by law and/or regulations to support law enforcement and national security
- Is it technically feasible?
- Who pays?

Romanidis Evripidis, Lawful Interception and countermeasures: in the era of internet telephony, Masters thesis, Royal Institute of Technology (KTH), School of Information and Communication Technology,Stockholm, Sweden, COS/CCS 2008-20, September 2008.

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/080922-Romanidis_Evripidis-with-cover.pdf

Consider the case of key escrow

The key used to encrypt the media or the signaling can be escrowed with another party (either inside the same organization or outside of it)

However, given a session key - content (the media in the call) could later be generated which the parties to the call would have a hard time denying (i.e., the content could be fabricated).

- Md. Sakhawat Hossen, A Session Initiation Protocol User Agent with Key Escrow:Providing authenticity for recordings of secure sessions, Masters thesis, KTH, ICT/COS, TRITA-ICT-EX-2010:1,January 2010

  http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/100118-Md._Sakhawat_Hossen-with-cover.pdf
- Muhammad Sarwar Jahan Morshed, Voice over IP and Lawful Intercept: God cop/Bad cop, Masters thesis, KTH, ICT/COS, TRITA-ICT-EX-2010:28, February 2010.

  http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/100221-Muhammad_Sarwar_Jahan_Morshed-with-cover.pdf
- Abdullah Azfar, Multiple Escrow Agents in VoIP, Masters thesis, KTH, ICT/COS, TRITA-ICT-EX-2010:109, June2010,

  http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/100607-Abdullah_Azfar-with-cover.pdf

MIKEY + SRTP

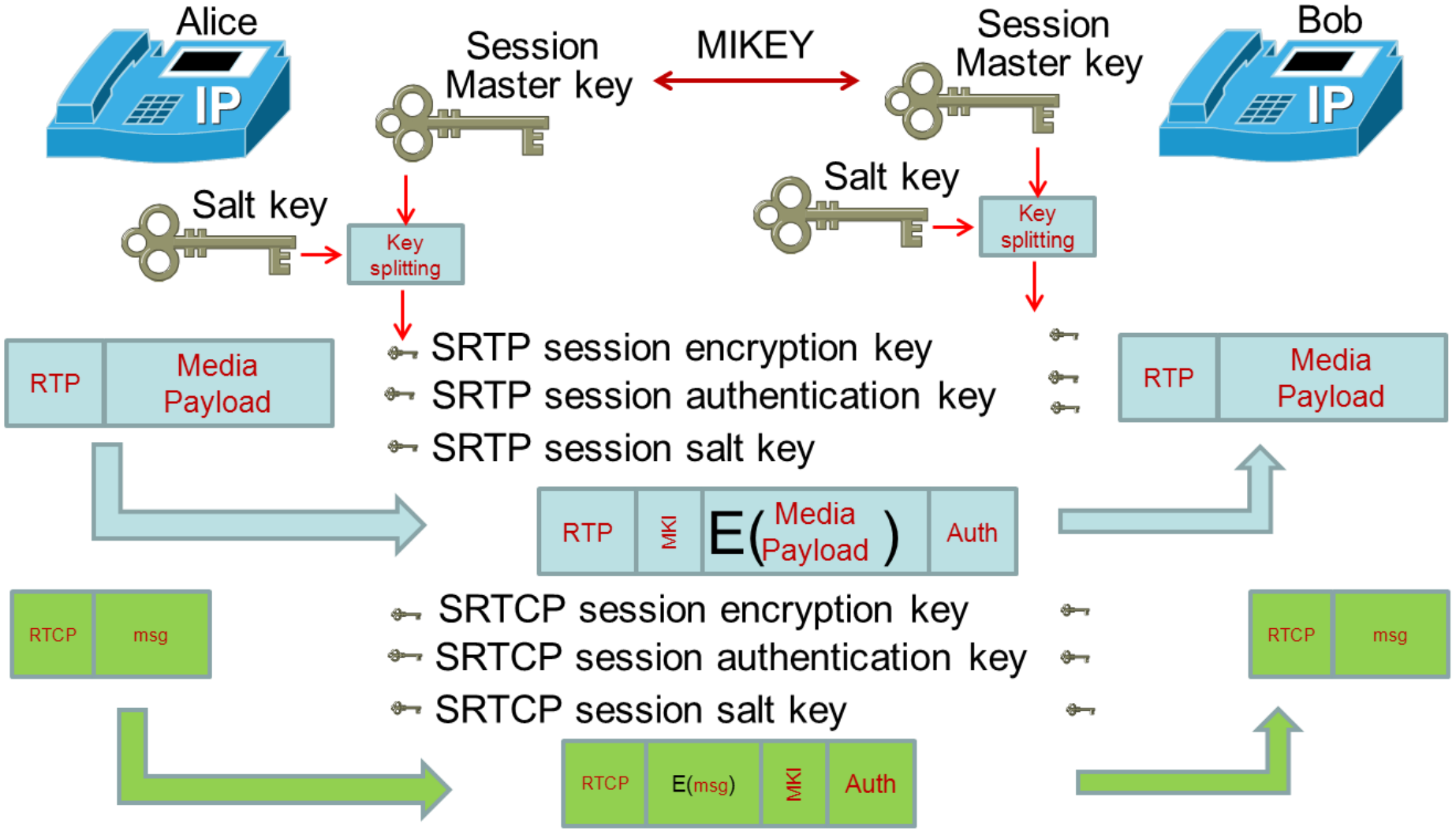


Figure 39: MIKEY+SRTP

Key Escrow

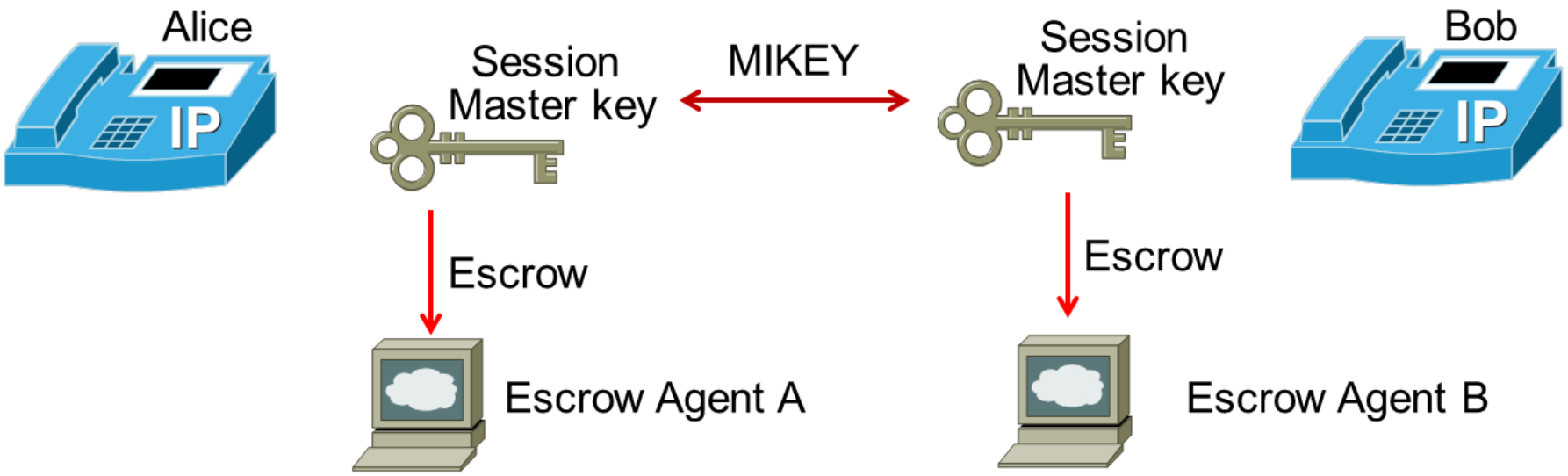


Figure 40: Key Escrow

- Alice and Bob can independently choose their escrow agent.
- Either might choose not to escrow their copy of the session master key – in which case they will not be able to recover the session from a stored copy of the encrypted session - but they might store an unencrypted session.
- If an escow agent fails or is unavailable, then the sesssion master key may be unavailable.

Lawful intercept with Key Escrow

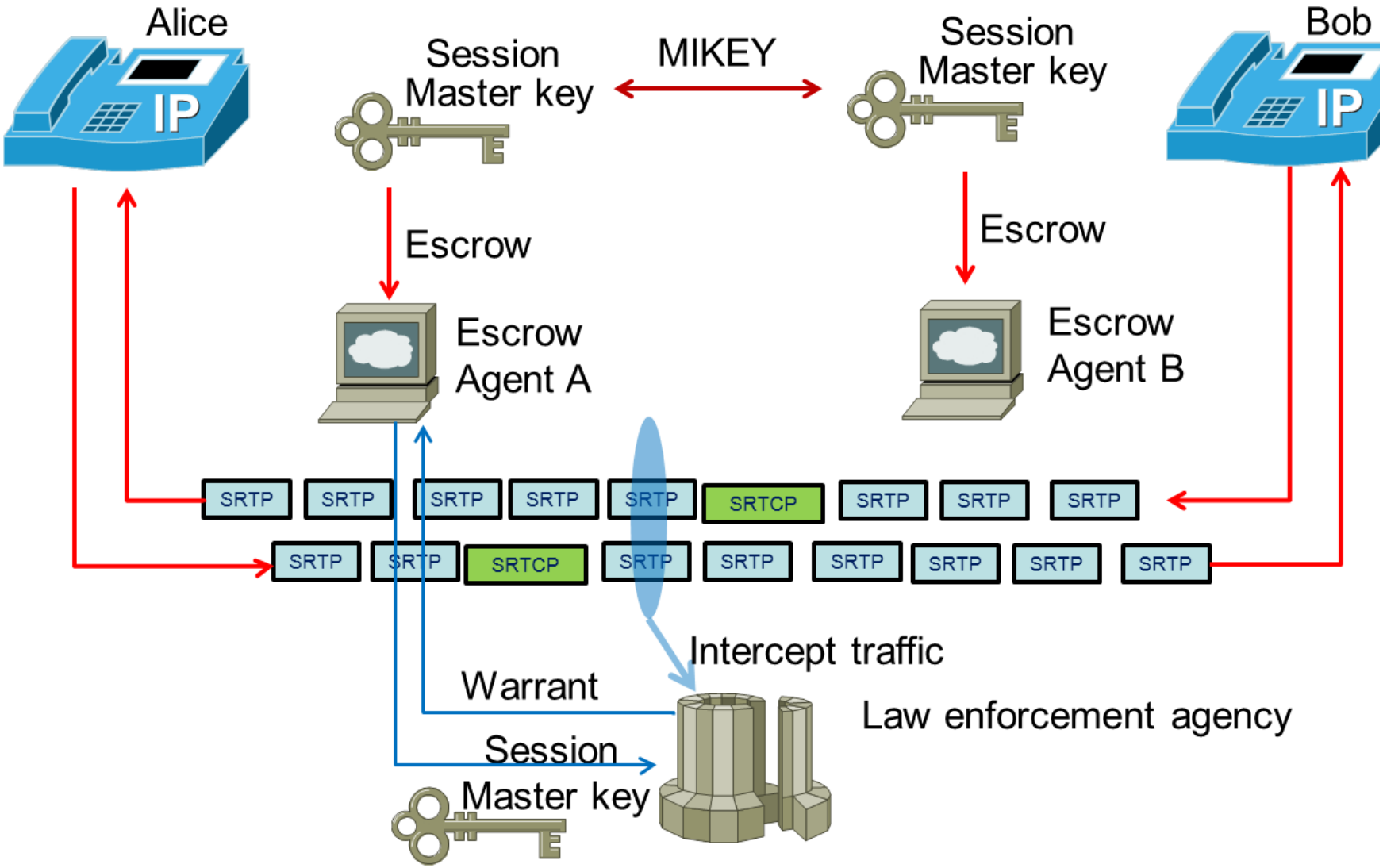


Figure 41: Lawful intercept with Key Escrow

Problems with Lawful Intercept with Key Escrow

Once any one gains access to the session master key they have access to al of the media streams and the control information (contained in the RTCP).

Given this session master key, a malicious party can fabricate contents of a media stream, create completely ficticous new media stream(s), fabricate control messages, etc.

Key Escrow

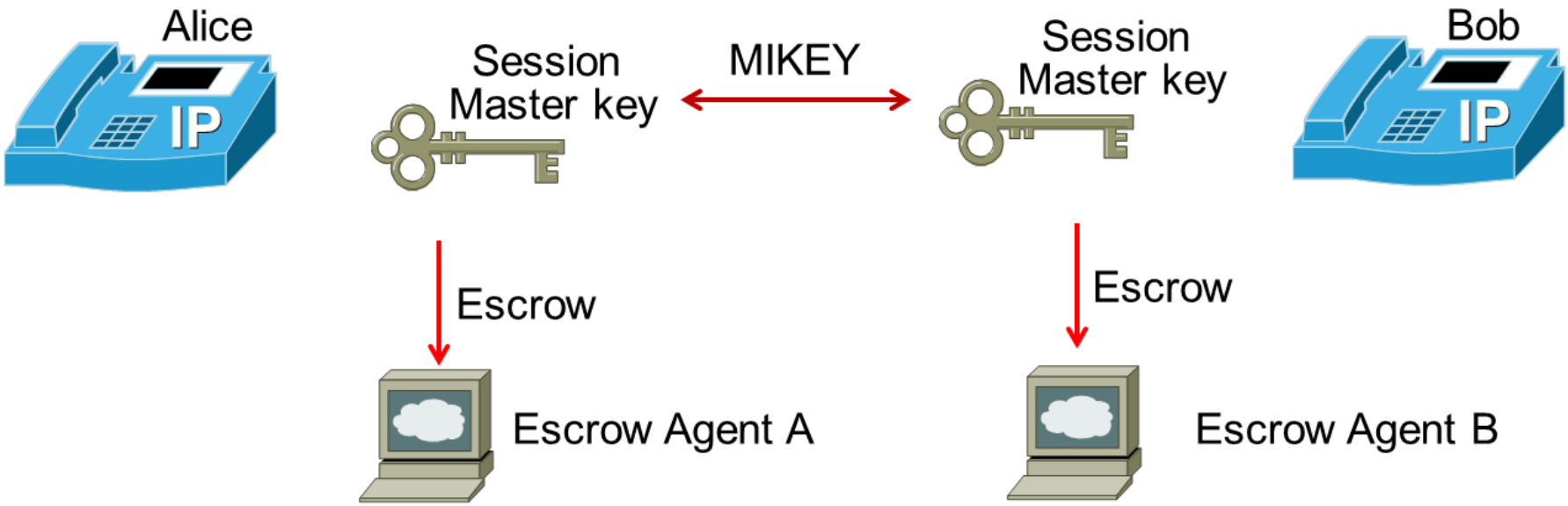


Figure 42: Key Escrow

Key Escrow two strings that when XORd regenerate the session master key

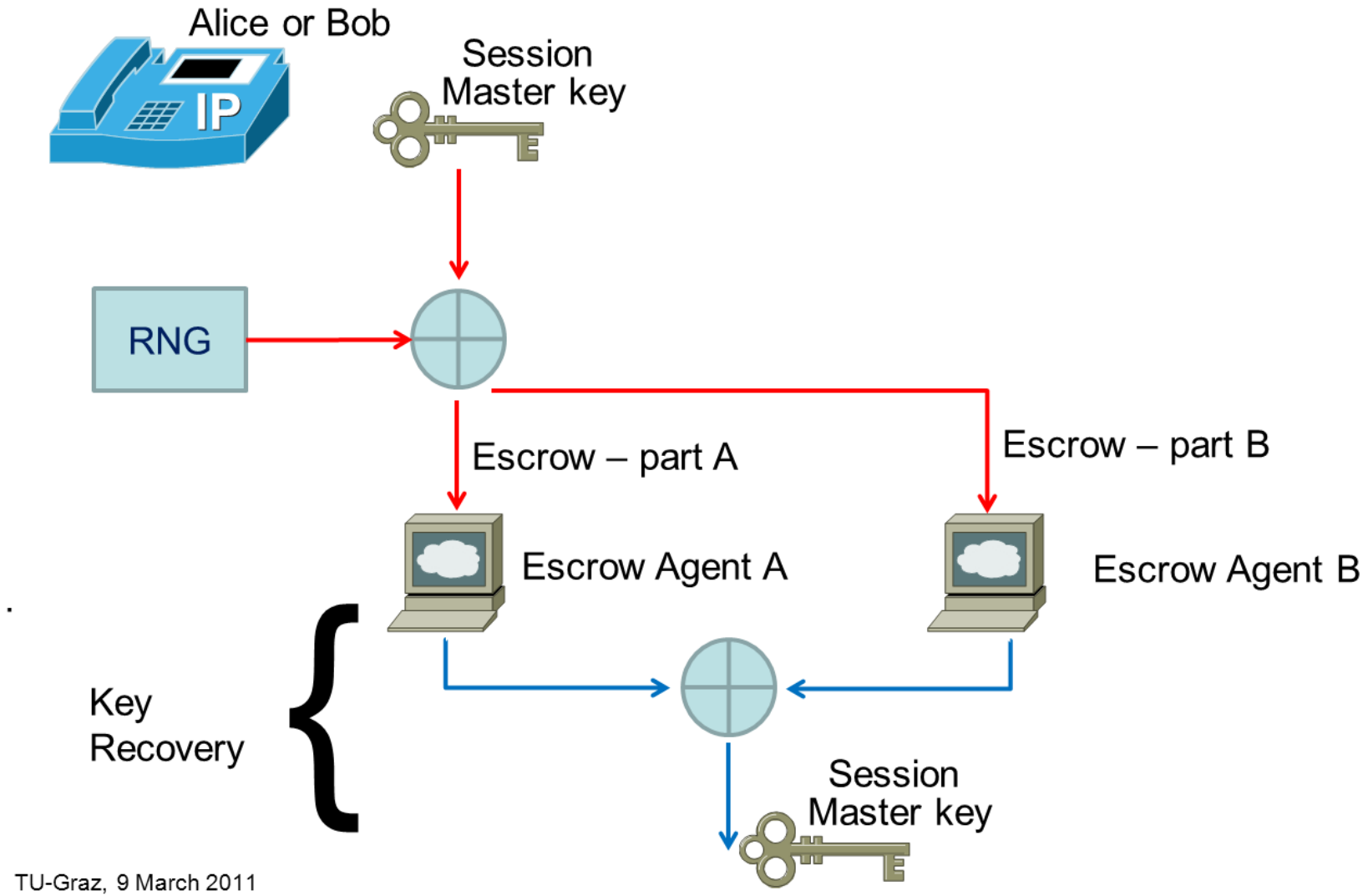


Figure 43: Key Escrow two strings that when XORd regenerate the session master key

Key Escrow n strings such that any m can be used to regenerate the session master key

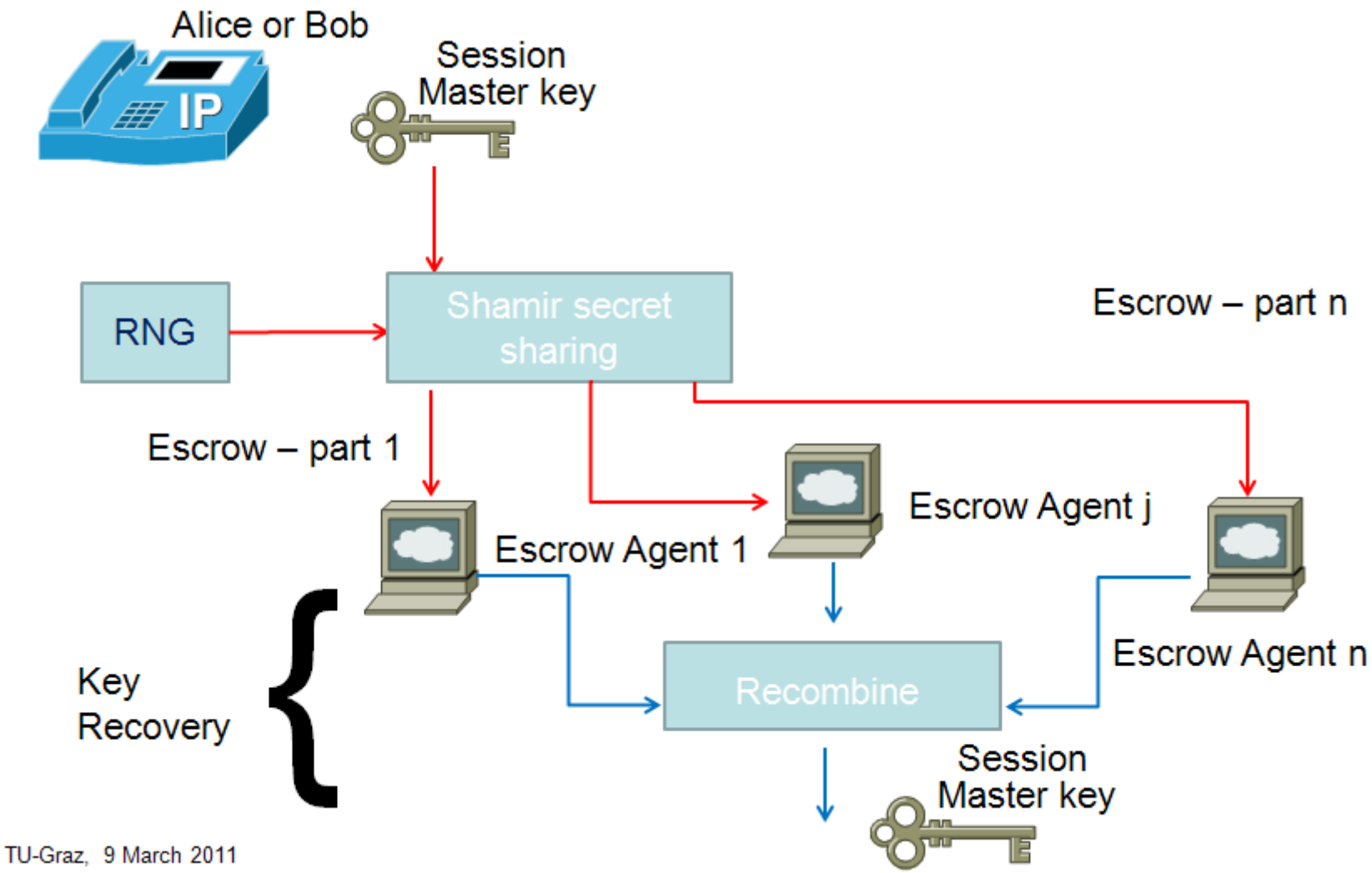


Figure 44: Key Escrow n strings such that any m can be used to regenerate the session master key

Evaluation of Key Escrow n of m

- A user agent need only wait for n of the m keys to be escrowed – the rest can be escrowed in the background at a later time.
- Key recovery can be done despite m-n escrow agents failing or being unavailable.
- Key recovery can be done as soon as n escrow agents have answered.
- Key Escrow two strings that when XORd regenerate the session master key

Avoiding fabrication of contents

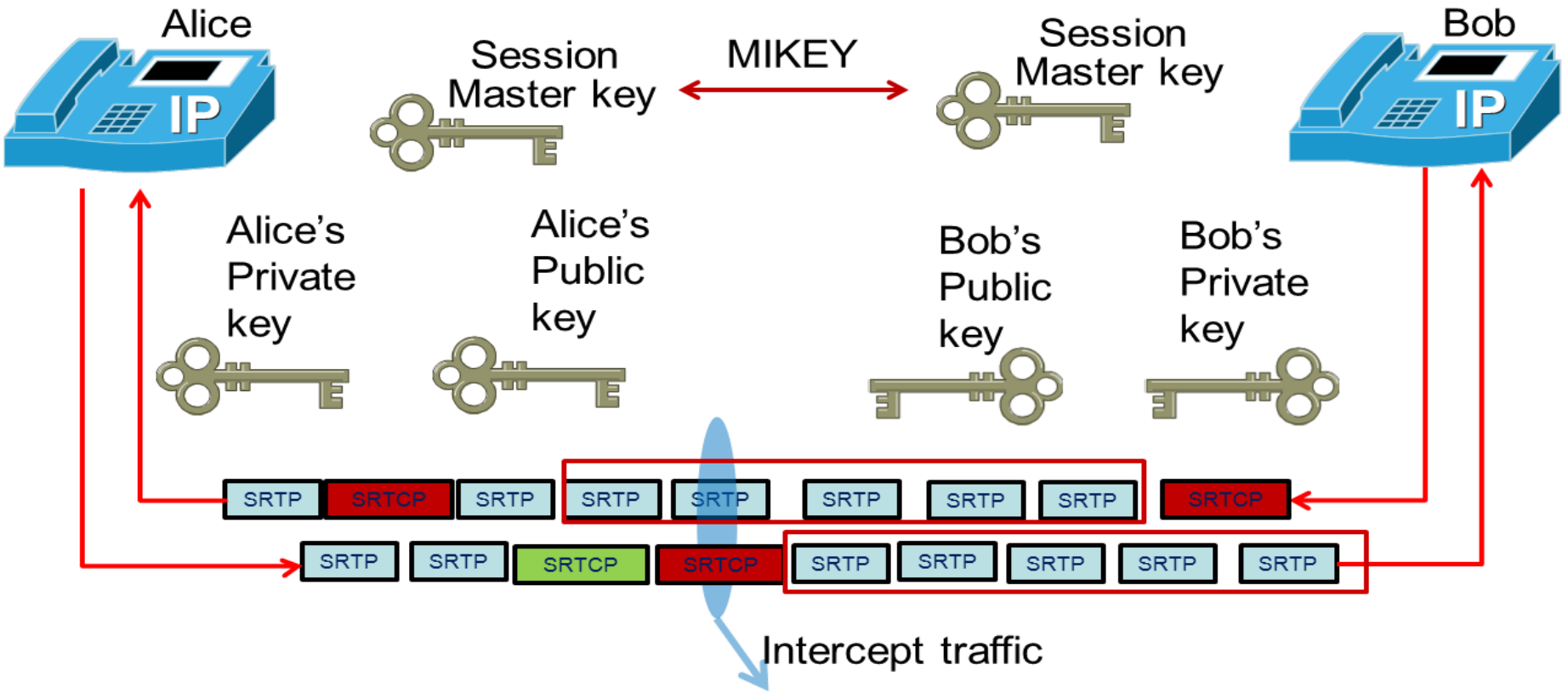


Figure 45: Avoiding fabrication of contents

- Add new RTCP packets containing signed hashes over blocks of (S)RTP packets or (S)RTCP packets. Sign with private key. Verify with public key!
- This signed hash need not immediately follow the block of packets it is computed over.

Avoiding fabrication of contents

Sign blocks of the encrypted call session

- The parties to the call can prove which content is or is not part of their call
- There is no need to make the signing key public, only the corresponding public key is needed – this could be published in a public place/record for later use.

This potentially leaks private key bits due to the large number of signatures! However, it is not clear what rate this leakage occurs at (especially with video conferencing).

MIKEY-TICKET

John Mattsson and Tian Tian proposed MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY), RFC 6043 [292] to get the MIKEY key from a trusted key management service.

Prajwol Kumar Nakarmi implemented and evaluated this in the context of a secure VoIP client (based on Sipdroid) in his Masters thesis “Evaluation of VoIP Security for Mobile Devices: In the context of IMS” [291]. 3GPP's Generic Bootstrapping Architecture (GBA) (TS 33.220 [293]) and GBA Digest (TR 33.914 [294]) were used for authentication bootstrapping.

- His GBA client written in C took only ~40 ms to bootstrap
- <500 ms of additional delay in the callsetup
- <500 µs of additional overhead for every 160 bytes of voice data

Voice over IP Security Alliance

The Voice over IP Security Alliance (http://www.voipsa.org/) was formed February 7, 2005

They have a moderated mailing list: VOIPSEC

Spam over Internet Telephony (SPIT)

There is rising concern that misconfigured voice gateways, … will lead to increased IP telephony SPAM.

One solution is using speaker recognition and then checking to see of this speaker is on:

- awhite list (automatic accept),
- a black list(automatic reject), or
- unknown (message could be recorded and the user listens to it later and then adds the user to their white or black lists).

See for example [282].

Issues of SIP and SPAM and solutions in addition to the above are discussed in [283].

VoIP Security: Attacks and Countermeasures

There are numerous types of attacks, for some details see [295],[296],[297].

Note that Denial of Service (DoS) is a major attack form against VoIP (as well as other IP based services) - this could be done by flooding a node or nodes with SIP messages, sending malformed packets ("fuzzing"), .

Some other types of attacks:

- BYE attack: Attacker sends a SIP BYE to terminate a session
- CANCEL attack: Attacker sends a SIP CANCEL to a proxy between the caller and callee, cancelling the session setup in progress
- Registration manipulation and call hijacking
- Media hijacking
- Directory enumeration (for example, to find targets)
- An attacker might also access a VoIP gateway to steal/abuse services.

For futher details of some of these (along with tools which implement them), see [298].

VoIP forensics

When a crime is thought to have occured it is important to preserve the evidence and analysis this data, for a suggest for a “VoIP Digital Evidence Forensics Standard Operating Procedures (DEFSOP)” see [299].

Artemisa: a VoIP/SIP-specific honeypot

Implements a user-agent back-end to detect malicious activity:

http://artemisa.sourceforge.net/

Rodrigo do Carmo, Mohamed Nassar, and Olivier Festor have written a conference paper: "Artemisa: an Open-Source Honeypot Back-End to Support Security in VoIP Domains" [300] about this system.

Call contents, Meta data, etc.

U. S. National Security Agency's PRISM (US-984XN) program

Slide deck: PRISM/US-984XN Overview or The SIGAD Used Most in NSA Reporting Overview. April 2013. Slides as publised in the Washington Post, 6 June, 29 June, and 10 July 2013

"NSA slides explain the PRISM data-collection program", Published: June 6, 2013, Updated July 10, 2013, Washington Post:

http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

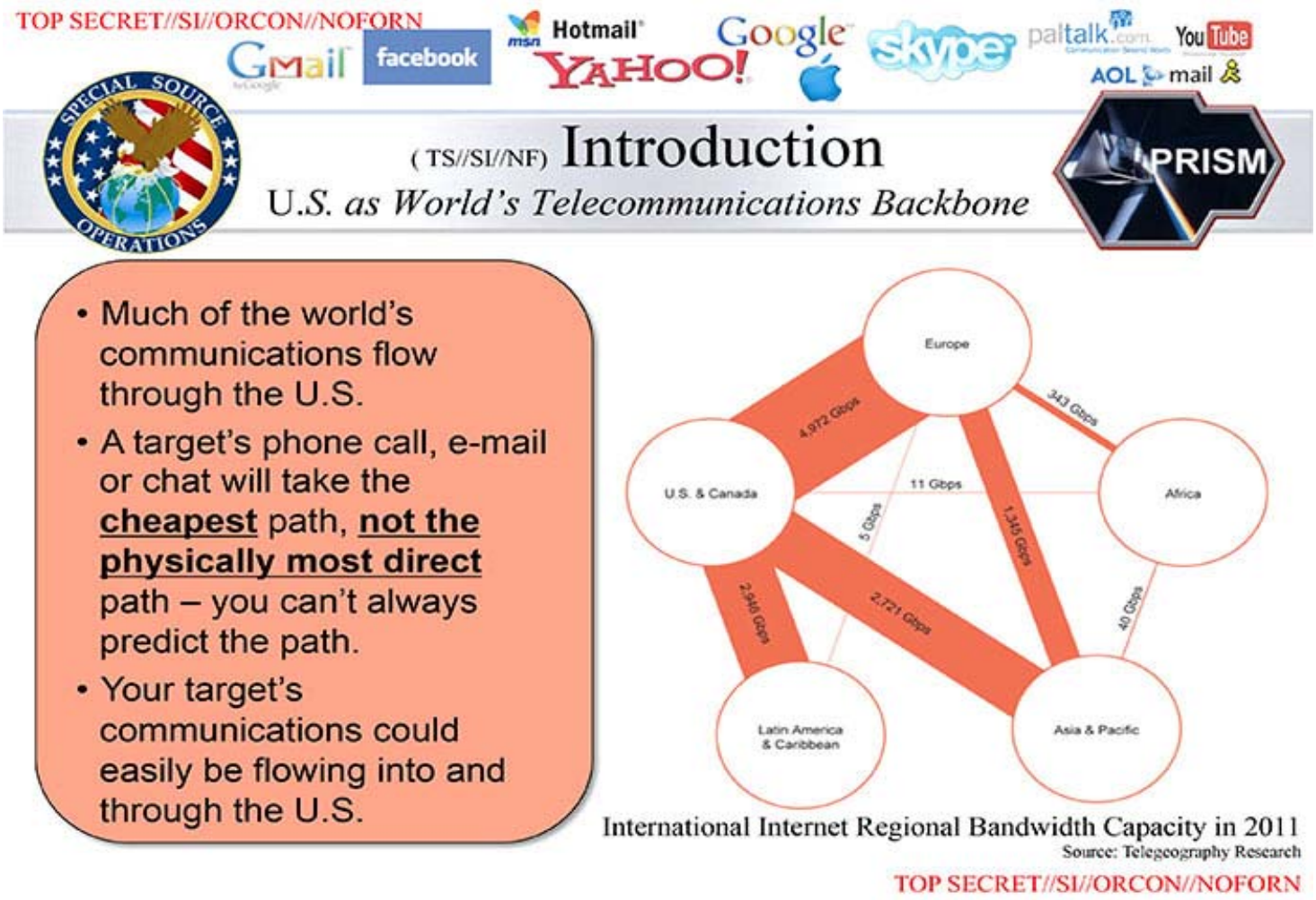


Figure 46: Slide 2 - published 6 June 2013

(see the related article Todd Lindeman, "A connected world", Washington Post, July 6, 2013 http://apps.washingtonpost.com/g/page/business/a-connected-world/305/)

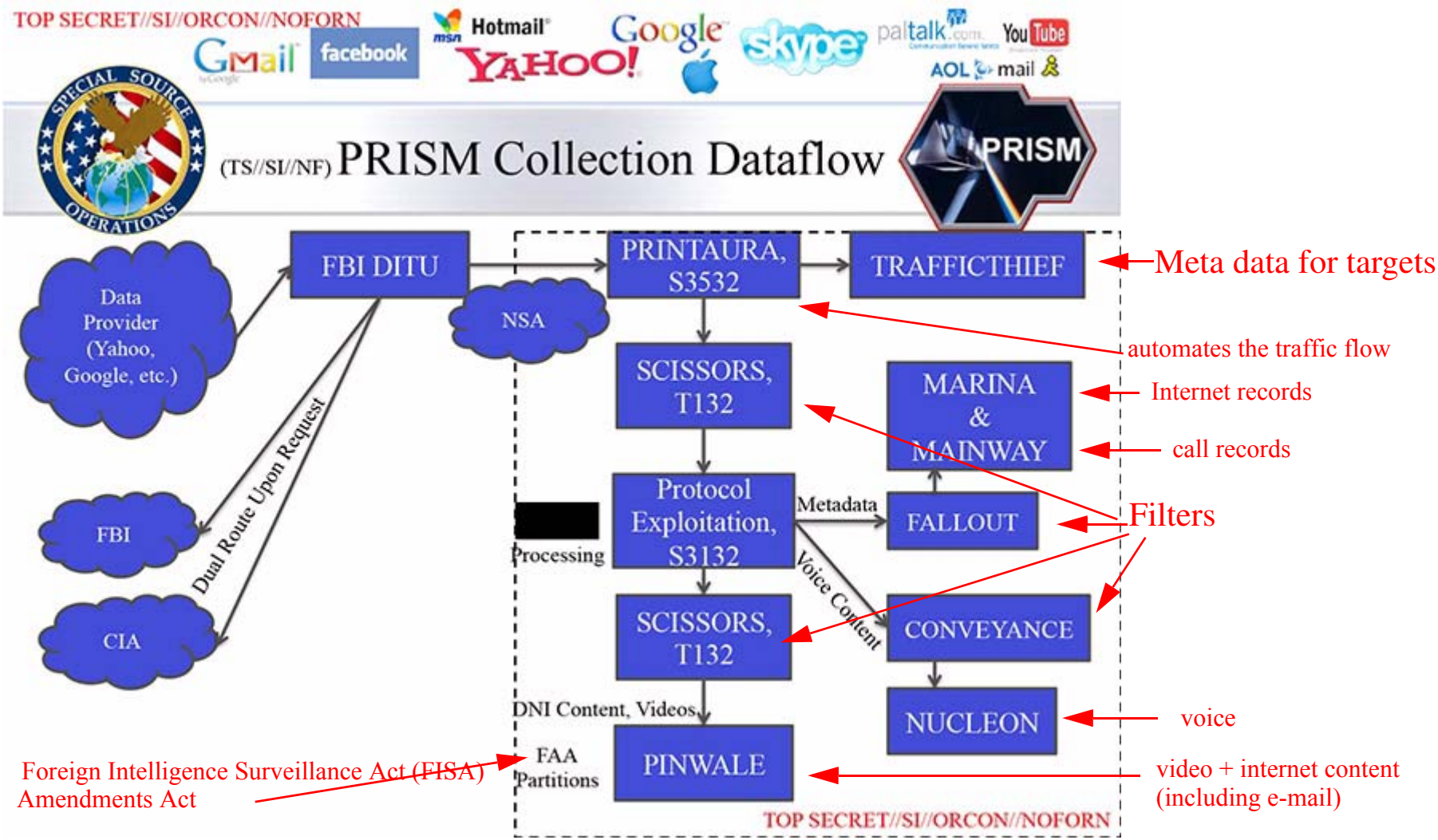


Figure 47: Slide 7- published 29 June 2013

Scope of data collection

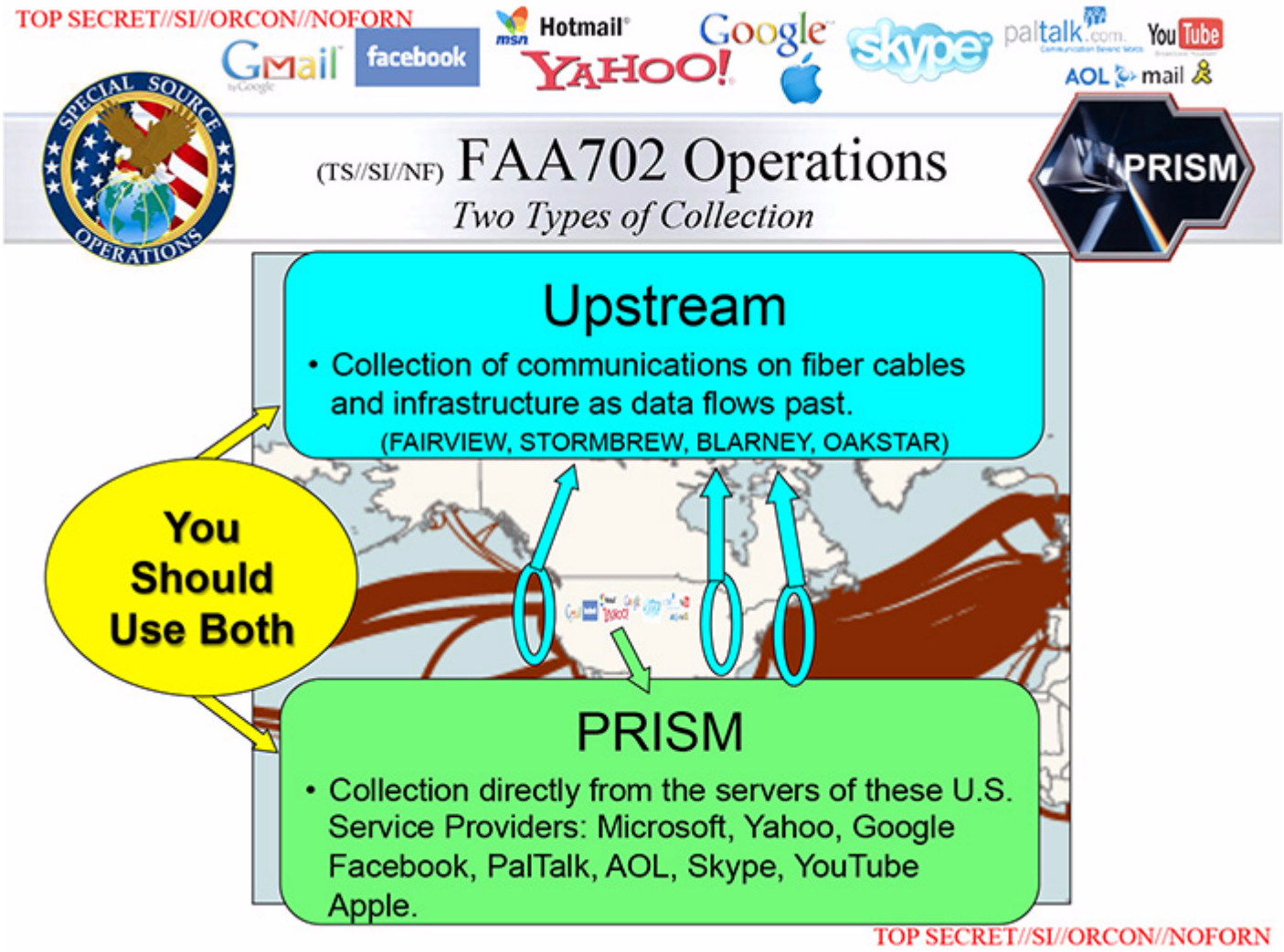


Figure 48: Upstream - published 10 July 2013

References and Further Reading

SIP Security

[218]J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol", IETF RFC 3261, June 2002, Obsoleted by RFCs 3261, 3262, 3263, 3264, 3265 http://www.ietf.org/rfc/rfc3261.txt

[219]B. Ramsdell (Editor), "S/MIME Version 3 Message Specification", IETF RFC 2633, June 1999, Obsoleted by RFC 3851 http://www.ietf.org/rfc/rfc2633.txt

[220] B. Ramsdell, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", Internet Request for Comments, RFC Editor, RFC 3851 (Proposed Standard), ISSN 2070-1721, July 2004, Obsoleted by RFC 5751

http://www.rfc-editor.org/rfc/rfc3851.txt

[221] B. Ramsdell and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", Internet Request for Comments, RFC Editor, RFC 5751 (Proposed Standard), ISSN 2070-1721, January 2010

http://www.rfc-editor.org/rfc/rfc5751.txt

[222]J. Peterson and C. Jennings, Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), IETF, Network Working Group, RFC 4474, August 2006 http://tools.ietf.org/html/rfc4474

[223]Israel M. Abad Caballero, *Secure Mobile Voice over IP*, M.Sc. Thesis, Royal Institute of Technology (KTH), Dept. of Microelectronics and Information Technology, Stockholm, Sweden, June 2003.

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/030626-Israel_Abad_Caballero-final-report.pdf

[224]Johan Bilien, *Key Agreement for Secure Voice over IP*, M.Sc. Thesis, Royal Institute of Technology (KTH), Dept. of Microelectronics and Information Technology, Stockholm, Sweden, Dec. 2003.

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/031215-Johan-Bilien-report-final-with-cover.pdf

[225]Joachim Orrblad, "Alternatives to MIKEY/SRTP to secure VoIP", Master of Science Thesis, KTH, Microelectronics and Information Technology, Telecommunication System Laboratory, Stockholm/Kista, March 2005

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/050330-Joachim-Orrblad.pdf

[226]Johan Bilien, Erik Eliasson, and Jon-Olov Vatn, “Call establishment Delay for secure VoIP”, WiOpt’04: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, University of Cambridge,UK, 24-26 March, 2004

RTP encryption

[227]D. Balenson, “Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers”, IETF RFC 1423, February 1993.

http://www.ietf.org/rfc/rfc1423.txt

[228]Rolf Blom, Elisabetta Carrara, Karl Norrman, Mats Näslund, “RTP Encryption for 3G Networks”, Communications Security Lab, Ericsson - IETF proceeding, December 2000, talk dated: Jan. 3, 2001.

http://www.ietf.org/proceedings/00dec/slides/AVT-3/tsld001.htm

[229]Rolf Blom, Elisabetta Carrara, Karl Norrman, and Mats Näslund, “RTP Encryption for 3G Networks, IETF draft, Expired: November 15, 2000 <draft-blom-rtp-encrypt-00.txt>

http://www.iptel.org/info/players/ietf/security/draft-blom-rtp-encrypt-00.txt

[230]Rolf Blom, Elisabetta Carrara, Karl Norrman, Mats Näslund, RTP Encryption for 3G Networks, In Proceedings of the Forty-Ninth Internet Engineering Task Force, Internet Engineering Task Force, San Diego, CA, USA, 10-15 December 2000, http://www.ietf.org/proceedings/00dec/slides/AVT-3/tsld001.htm

[231]Ville Hallivuori, "Real-time Transport Protocol (RTP) security", Tik-110.501 Seminar on Network Security, Helsinki University of Technology, 2000
http://www.tcm.hut.fi/Opinnot/Tik-110.501/2000/papers/hallivuori.pdf

[232]M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", IETF RFC 3711, March 2004, Updated by RFC 5506 [233] ftp://ftp.rfc-editor.org/in-notes/rfc3711.txt

[233]I. Johansson and M. Westerlund, "Support for Reduced-Size Real-Time Transport Control Protocol (RTCP): Opportunities and Consequences", Internet Request for Comments, RFC Editor, RFC 5506 (Proposed Standard), ISSN 2070-1721, April 2009 http://www.rfc-editor.org/rfc/rfc5506.txt

[234]M. Baugher, D. McGrew, M. Naslund. E. Carrara, and K. Norrman, The Secure Real-time Transport Protocol (SRTP), Internet Request for Comments, ISSN 2070-1721, RFC 3711, RFC Editor, March 2004, Updated by RFC 5506 [235], http://www.rfc-editor.org/rfc/rfc3711.txt

[235]I. Johansson and M. Westerlund, Support for Reduced-Size Real-Time Transport Control Protocol (RTCP): Opportunities and Consequences, Internet Request for Comments, ISSN 2070-1721, RFC 5506, RFC Editor,April 2009, http://www.rfc-editor.org/rfc/rfc5506.txt

[236]J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman, "MIKEY: Multimedia Internet KEYing", IETF RFC 3830, August 2004

http://www.ietf.org/rfc/rfc3830.txt

[237]M. Baugher and E. Carrara, "The Use of Timed Efficient Stream Loss-Tolerant Authentication (TESLA) in the Secure Real-time Transport Protocol (SRTP)", IETF, RFC 4383, February 2006

http://www.rfc-editor.org/rfc/rfc4383.txt

[238]Elisabetta Carrara, Security for IP Multimedia Applications over Heterogeneous Networks, Licentiate thesis, Royal Institute of Technology (KTH), Institution for Microelectronics and Information Technology, Trita-IMIT-LCN. AVH, 1651-4106; 05:01, May 2005

http://web.it.kth.se/~carrara/lic.pdf

NATs and Firewalls

[239] Fredrik Thernelius, "SIP, NAT, and Firewalls", M.Sc. Thesis, Royal Institute of Technology (KTH), Department of Teleinformatics, Stockholm, Sweden, May 2000.

[240]List of sources about SIP and Firewalls

http://www.cs.columbia.edu/sip/drafts_firewall.html

[241]P. Srisuresh, J. Kuthan, J. Rosenberg, A. Molitor, and A. Rayhan, "Middlebox Communication Architecture and framework", IETF RFC 3303, August 2002 http://www.ietf.org/rfc/rfc3303.txt

[242]B. Zhou and D. Liu, ALG consideration of SIP, Internet-Draft, IETF Network Working Group, March 1, 2010, Expired: September 2, 2010

http://tools.ietf.org/html/draft-zhou-sip-alg-00

[243]R. P. Swale, P. A. Mart, P. Sijben, S. Brim, and M. Shore, “Middlebox Communications (MIDCOM) Protocol Requirements”, IETF RFC 3304, August 2002 http://www.ietf.org/rfc/rfc3304.txt

[244]J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy, “Simple Traversal of UDP through NATs (STUN)”, RFC 3489, March 2003, Obsoleted by RFC 5389 http://www.ietf.org/rfc/rfc3489.txt

[245]J. Rosenberg, R. Mahy, P. Matthews, and D. Wing, “Session Traversal Utilities for NAT (STUN)”, Internet Request for Comments, RFC Editor, RFC 5389 (Proposed Standard), ISSN 2070-1721, October 2008, http://www.rfc-editor.org/rfc/rfc5389.txt

[246]J. Rosenberg, Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP), Internet Request for Comments, ISSN 2070-1721, RFC 5627, RFC Editor, October 2009, http://www.rfc-editor.org/rfc/rfc5627.txt

[247]Lawrence Keyes, “A Low Density Voice Over IP Gateway”, Master of Science in Information Technology thesis, Rochester Institute of Technology, B. Thomas Golisano College of Computing and Information Sciences, May 17, 2004

http://www.mxdesign.net/voip/voip/onfolio-files/Low%20Density%20Voice%20Over%20IP%20Gateway.pdf

[248]J. Rosenberg and H. Schulzrinne, “An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing”, RFC 3581, August 2003

http://www.ietf.org/rfc/rfc3581.txt

[249] “snom 4S NAT Filter: Admin Manual”, Version 2.09, 2004 snom technology Aktiengesellschaft http://www.snom.com/download/man_snom4s_natf_en_v209.pdf

[250]“NAT Traversal for Multimedia over IP Services”, White Paper, Newport Networks Ltd., last modified: Feb 18, 2005 11:15:54 AM

http://www.newport-networks.com/whitepapers/fwnatwpes6.html

[251]Saikat Guha, Yutaka Takeda, and Paul Francis, “NUTSS: A SIP based Approach to UDP and TCP Network Connectivity”, In Proceedings of SIGCOMM04 Workshops, Portland,

OR, Aug. 2004, pages 4348 https://www.guha.cc/saikat/files/papers/nutss.pdf

[252] A. La Torre Yurkov, Implementation of Traversal Using Relay Nat for SIP based VoIP, Master Thesis, Royal Institute of Technology (KTH), Institution for Microelectronics and Information Technology, Stockholm, Sweden, February 2006

http://www.minisip.org/publications/Thesis_LaTorreYurkov_feb2006.pdf

[253] R. Mahy, P. Matthews, and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", Internet Request for Comments, RFC Editor, RFC 5766 (Proposed Standard), ISSN 2070-1721, April 2010 http://www.rfc-editor.org/rfc/rfc5766.txt

[254] J. Rosenberg, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols",Internet Request for Comments, RFC Editor, RFC 5245 (Proposed Standard), ISSN 2070-1721, April 2010

http://www.rfc-editor.org/rfc/rfc5245.txt

[255] M. Komu, T. Henderson, H. Tschofenig, J. Melen, and A. Keranen, "Basic

Host Identity Protocol (HIP) Extensions for Traversal of Network Address Translators", Internet Request for Comments, RFC Editor, RFC 5770 (Experimental), ISSN 2070-1721, April 2010

http://www.rfc-editor.org/rfc/rfc5770.txt

[256]J. Rosenberg, A. Keranen, B. B. Lowekamp, and A. B. Roach, 'TCP Candidates with Interactive Connectivity Establishment (ICE)', Internet Request for Comments, vol. RFC 6544 (Proposed Standard), Mar. 2012 [Online]. Available: http://www.rfc-editor.org/rfc/rfc6544.txt

[257]M. Westerlund and C. Perkins, 'IANA Registry for Interactive Connectivity Establishment (ICE) Options', Internet Request for Comments, vol. RFC 6336 (Proposed Standard), Jul. 2011 [Online]. Available: http://www.rfc-editor.org/rfc/rfc6336.txt

[258]M. Petit-Huguenin and A. Keranen, Using Interactive Connectivity Establishment (ICE) with Session Description Protocol (SDP) offer/answer and Session Initiation Protocol (SIP), MMUSIC, Internet-Draft, July 15, 2013, Expires: January 16, 2014, draft-ietf-mmusic-ice-sip-sdp-00,

http://datatracker.ietf.org/doc/draft-ietf-mmusic-ice-sip-sdp/

[259]E. Ivov, H. Kaplan, and D. Wing, Latching: Hosted NAT Traversal (HNT) for Media in Real-Time Communication, Network Working Group, Internet-Draft, July 15, 2013, Expires: January 16, 2014, draft-ietf-mmusic-latching-03 http://datatracker.ietf.org/doc/draft-ietf-mmusic-latching/

[260]T. Reddy, P. Patil, and D. Wing, Happy Eyeballs Extension for ICE, MMUSIC, Internet-Draft, August 25, 2013, Expires: February 26, 2014, draft-reddy-mmusic-ice-happy-eyeballs-02

http://datatracker.ietf.org/doc/draft-reddy-mmusic-ice-happy-eyeballs/

[261]A. Keranen and J. Rosenberg, Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols, MMUSIC , Internet-Draft, July 15, 2013, Expires: January 16, 2014, draft-ietf-mmusic-rfc5245bis-00

http://datatracker.ietf.org/doc/draft-ietf-mmusic-rfc5245bis/

[262]M. Westerlund and T. Zeng, The Evaluation of Different Network Addres Translator (NAT) Traversal Techniques for Media Controlled by Real-time Streaming Protocol (RTSP), Internet-Draft, Network Working Group, May 29, 2013, Expires: November 30, 2013, draft-ietf-mmusic-rtsp-nat-evaluation-09

http://tools.ietf.org/html/draft-ietf-mmusic-rtsp-nat-evaluation-09

[263]J. Goldberg, M. Westerlund, and T. Zeng, A Network Address Translator (NAT) Traversal mechanism for media controlled by Real-Time Streaming Protocol (RTSP), Internet-Draft, Network Working Group, May 27, 2013, Expires: November 28, 2013, draft-ietf-mmusic-rtsp-nat-16

http://tools.ietf.org/html/draft-ietf-mmusic-rtsp-nat-16

[264]B. Stucker, H. Tschofenig, and G. Salgueiro, Analysis of Middlebox Interactions for Signaling Protocol Communication along the Media Path, Internet-Draft, MMUSIC, May 30, 2013, Expires: December 01, 2013, draft-ietf-mmusic-media-path-middleboxes-07.txt

https://datatracker.ietf.org/doc/draft-ietf-mmusic-media-path-middleboxes/

Privacy

[265] Alberto Escudero-Pascual, "Privacy in the next generation Internet, Data Protection in the context of European Union Data Protection Policy", Dr. Tekn. dissertation, Royal Institute of Technology, December 2002.
http://www.imit.kth.se/~aep/PhD/docs/escuderoa-PhD-20021030.pdf

[266] J. Peterson, "A Privacy Mechanism for the Session Initiation Protocol (SIP)", Internet Request for Comments, RFC Editor, RFC 3323 (Proposed Standard), ISSN 2070-1721, November 2002, http://www.rfc-editor.org/rfc/rfc3323.txt

[267] C. Jennings, J. Peterson, and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", Internet Request for Comments, RFC Editor, RFC 3325 (Informational), ISSN 2070-1721, November 2002, Updated by RFC 5876 http://www.rfc-editor.org/rfc/rfc3325.txt

[268] M. Barnes, "An Extension to the Session Initiation Protocol (SIP) for Request History Information", Internet Request for Comments, RFC Editor, RFC 4244 (Proposed Standard), ISSN 2070-1721, November 2005
http://www.rfc-editor.org/rfc/rfc4244.txt

[269]J. Elwell, “Updates to Asserted Identity in the Session Initiation Protocol (SIP)”, Internet Request for Comments, RFC Editor, RFC 5876 (Informational), ISSN 2070-1721, April 2010,

http://www.rfc-editor.org/rfc/rfc5876.txt

[270]M. Munakata, S. Schubert, T. Ohba, “User-Agent-Driven Privacy Mechanism for SIP”, Internet Request for Comments, RFC Editor, RFC 5767 (Informational), ISSN 2070-1721, April 2010

http://www.rfc-editor.org/rfc/rfc5767.txt

[271]Swedish Electronic Communications Act (SFS 2003:389), March 2003

http://www.pts.se/Archive/Documents/SE/Lag_2003-389_om_elektronisk_kommunikation.htm

[272]Communications Assistance for Law Enforcement Act. CALEA - 47 USC 1001-1010. Title 47--Telegraphs, Telephones, and Radiotelegraphs. Chapter 9--Interception of Digital and Other Communications

http://www.techlawjournal.com/agencies/calea/47usc1001.htm

[273]United States Department of Justice, Federal Bureau of Investigation and Drug Enforcement Administration, Joint Petition [to US FCC] for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, 10 March, 2004

http://www.steptoe.com/publications/FBI_Petition_for_Rulemaking_on_CALEA.pdf

[274] Jaya Baloo, Lawful Interception of IP Lawful Interception of IP Traffic, Draft 1, Black Hat Europe 2003, May 2003

http://www.blackhat.com/presentations/bh-europe-03/bh-europe-03-baloo.pdf

[275]Matt Holdrege, "Supporting Lawful Intercept in IP-based Networks", IEEE Homeland Defense Series, March 2002

http://www.ewh.ieee.org/r6/lac/csspsvts/briefings/holdrege.pdf

[276]Fred Baker, Bill Foster, and Chip Sharp, "Cisco Architecture for Lawful Intercept In IP Networks", IETF RFC 3924, October 2004

http://www.ietf.org/rfc/rfc3924.txt

[277]ETSI TS 101 331, *Telecommunications security; Lawful Interception (LI); Requirements of law enforcement agencies*, V1.1.1, August 2001.

[278]ETSI TS 33.108 *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Handover Interface for Lawful Interception,* V5.1.0, September 2002.

[279]ETSI TS 133 107 *Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful interception Architecture and Functions* (3G 33.107 version 3.1.0 Release 1999), V4.2.0, December 2001.

[280]Global LI Industry Forum, Inc. http://www.gliif.org/

[281]http://www.gliif.org/standards.htm

[282]Ranjith Mukundan, “Media Servers and App Servers: Insights from IP Services Research and Proof-of-Concept Implementions”, SIP Summit 2005, Honolulu, Hawaii, 18 January 2005.
http://www.wipro.com/pdf_files/SIP_Summit_2005_Wipro-MediaSrv-AppSrv_PPT.pdf

[283]J. Rosenberg and C. Jennings, “The Session Initiation Protocol (SIP) and Spam”, Internet Request for Comments, RFC Editor, RFC 5039 (Informational), ISSN 2070-1721, January 2008,

http://www.rfc-editor.org/rfc/rfc5039.txt

[284]VeriSign Switzerland SA, “Integration and Treatment of VoIP and other IP-Enabled Services LI specifications”, Joint ETSI TC LI and 3GPP SA3 LI meeting, document td003, Povoa de Varzim, Portugal, 22 - 23 July 2004

http://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_LI/Joint_Meetings/2004_07_Povoa/TD03%20integration.pdf

[285]IAB and IESG, “IETF Policy on Wiretapping”, Internet Request for Comments, RFC Editor, RFC 2804 (Informational), ISSN 2070-1721, May 2000 http://www.rfc-editor.org/rfc/rfc2804.txt

[286]Bo Martinsson, Per Bergstrand, Marcus Boklund, Dejan Jaksic, Camilla Philipson Watz, Roland Svahn, and Cecilia Östrand, ‘Which services and networks are subject to the Electronic Communications Act? Guidance’, Swedish Post and Telecom Agency (PTS), vol. PTS-ER-2009:12, p. 60,

March 2009, Available at

http://www.pts.se/upload/Rapporter/Internet/2009/services-e-com-act-2009-12.pdf

[287] Romanidis Evripidis, Lawful Interception and Countermeasures: In the era of Internet Telephony, Masters thesis, Royal Institute of Technology (KTH), School of Information and Communications Technology, Stockholm, Sweden, COS/CCS 2008-20, September 2008

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/080922-Romanidis_Evripidis-with-cover.pdf

[288] Md. Sakhawat Hossen, "A Session Initiation Protocol User Agent with Key Escrow: Providing authenticity for recordings of secure sessions", Masters thesis, Royal Institute of Technology (KTH), School of Information and Communications Technology, Stockholm, Sweden, TRITA-ICT-EX-2010:1, January 2010

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/100118-Md._Sakhawat_Hossen-with-cover.pdf

[289] Muhammad Sarwar Jahan Morshed, "Voice over IP and Lawful Intercept: God cop/Bad cop", Royal Institute of Technology (KTH), School of Information and Communications Technology, Stockholm, Sweden, TRITA-ICT-EX-2010:28, February 2010,

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/100221-Muhammad_Sarwar_Jahan_Morshed-with-cover.pdf

[290]European Parliament and the Council of the European Union, Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105, April 13, 2006, pp. 0054 - 0063
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML

[291]Prajwol Kumar Nakarmi, Evaluation of VoIP Security for Mobile Devices: In the context of IMS, Masters thesis, Royal Institute of Technology (KTH), School of Information and Communications Technology, Stockholm, Sweden, TRITA-ICT-EX-2011:111, June 2011,
http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/110617-Prajwol_Kumar_Nakarmi-with-cover.pdf

[292]John Mattsson and Tian Tian, MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY), Internet Request for Comments, ISSN 2070-1721, RFC 6043, RFC Editor, March 2011, http://www.rfc-editor.org/rfc/rfc6043.txt

[293]3GPP. Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA). TS 33.220, 3rd Generation Partnership Project (3GPP), June 2010.

[294]3GPP. SSO for Application Security for IMS - based on SIP Digest. TR 33.914, 3rd Generation Partnership Project (3GPP), May 2011.

VoIP Security

[295]Himanshu Dwivedi, *Hacking VoIP: Protocols, Attacks, and Countermeasures*, No Starch Press, illustrated edition, March 21, 2008, 220 pages, ISBN-10: 1593271638 or ISBN-13: 978-1593271633

[296] Patrick Park. *Voice over IP Security*, Cisco Press; 1 edition, September 19, 2008, 384 pages, ISBN-10: 1587054698 or ISBN-13: 978-1587054693

[297]David Endler and Mark Collier, *Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions*, McGraw-Hill Osborne Media; 1 edition, November 28, 2006, 539 pages, ISBN-10: 0072263644 or ISBN-13: 978-0072263640

[298]Dustin D. Trammell, VoIP Attacks!, Slides from a talk at Computer Security Institute Annual Conference (CSI 2007), 6 Movember 2007
http://druid.caughq.org/presentations/VoIP-Attacks.pdf

[299]Yun-Sheng Yen and I-Long Lin. VoIP Digital Evidence Forensics Standard Operating Procedure. IJRRCS. March 2011;2(1):173-179.

[300]Rodrigo do Carmo, Mohamed Nassar, and Olivier Festor. "Artemisa: an Open-Source Honeypot Back-End to Support Security in VoIP Domains", 12th IFIP/IEEE International Symposium on Integrated Network Management 2011, 23-27 May 2011, pages 361-368.
http://hal.inria.fr/docs/00/59/48/57/PDF/TS_14c_78368.pdf

SIP recording

[301] K. Rehor (editor), L. Portman (editor), A. Hutton, and R. Jain, Use Cases and Requirements for SIP-Based Media Recording (SIPREC), Internet Request for Comments, ISSN: 2070-1721, RFC 6341, RFC Editor, August 2011, http://www.rfc-editor.org/rfc/rfc6341.txt

[302]A. Hutton, L. Portman, R. Jain, and K. Rehor, "An Architecture for Media Recording using the Session Initiation", Internet Draft, IETF, SIPREC Working group,

draft-ietf-siprec-architecture-02, 13 April 2011, Expires: 15 October 2011, http://tools.ietf.org/html/draft-ietf-siprec-architecture-02

[303] A. Johnston and A. Hutton, “SIP Call Control - Recording Extensions”, Internet Draft, IETF, SIPREC working group, draft-johnston-siprec-cc-rec-00, 3 July 2010, Expired: 4 January 2011 http://tools.ietf.org/html/draft-johnston-siprec-cc-rec-00

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 13: SIP Telephony

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:32

SIP Telephony

SIP Telephony (SIP-T) -- for details see RFC 3204 [312] (Updated by RFCs 3459 [313] and 5621 [314]).

Gateway between the SIP world and the PSTN world looks like a SIP user agents to other SIP entities and like a terminating telephone switch to the PSTN.

Advantages	Provides ISUP transparency (by carrying ISUP message as multipart MIME messages in the SIP messages between SIP-T gateways)
Disadvantages	Does **not** interwork with SIP
	Perpetuates ISUP!

For example of call flows between SIP and PSTN see [315].

Stream Control Transmission Protocol (SCTP) can be used to carry telephony signalling [319].

Telephony Routing over IP (TRIP)

- TRIP [316] is a gateway to Location Server (LS) protocol
- Designed for an interdomain gateway
- Allows the gateway to advertise what PSTN number range it is a gateway for

For within a domain there is a version for between a gateway and a proxy: TRIP-lite

A Location Server is responsible for a Internet Telephony Administrative Domain (ITAD).

See also: **Telephony Routing over IP (TRIP)** on page 566

and Telephony Gateway REgistration Protocol (TGREP) [318].

Call Control Services

Generally include advanced telephony services such as:

- Call Transfer, both Attended and Unattended
- Call Park/Un-Park
- Multistage Dialling
- Operator Services
- Conference Call Management
- Call Mobility
- Call Pickup

See the slides starting on **Intelligent Network service using SIP** on page 215.

Call Center Redesign using SIP

- Replace the call center switch via VoIP
- Interactive Voice Response (IVR) - using a media server (for pre-recorded clips) and SIP signalling
- Automatic Call Distribution (ACD) - replace with scripts using Call Processing Language (CPL)
- Agent Workstation - a PC with a SIP client
- The agent has access via Web and various databases to information, which can be indexed by the agent using information from the SIP request.

Additional SIP Telephony services

- SIP for the Hearing Impaired
- Emergency Services
- Precedence signalling (military, government, emergency services, …)
  - RFC 3487 [304] gives the requirements for resource priority mechanisms for SIP
- Message Waiting, Voice Mail, and Unified Messaging
  - See for example Interactive Intelligence's Communité® ("ka-mune-i-tay") http://www.inin.com/products/communite/communite.asp
- Call Waiting
- SIP *continuing* presence service
  - The I-Am-Alive (IAA) database [311] is a distributed database system that users can query after-the-event to determine the status of a person - it does not require the session properties of SIP
  - Is there a SIP corollary - for *continuing* presence?

Emergency Telecommunication Service (ETS)[320]

Telephony Signaling when used in Internet-based telephony services in addition to the general requirements specified in RFC 3689 [307] needs to support a number of additional requirements RFC 3690 [308]:

- Telephony signaling applications (used with Internet-based telephony) **must** be able to carry labels.
- The labels **must** be extensible
  - to support various types and numbers of labels.
- These labels **should** have a mapping to the various emergency related labels/markings used in other telephony based networks, e.g., PSTN
  - To ensure that a call placed over a hybrid infrastructure (i.e., PSTN+Internet) can carry the labels end-to-end with appropriate translation at PSTN/Internet boundaries.
  - Only authorized users or operators **should** be able to create non-ordinary Labels (i.e., labels that may alter the default best effort service).
  - Labels **should** be associated with mechanisms to providing strong end-to-end integrity
  - Operators **should** have the capability of authenticating the label

- Application layer IP telephony capabilities **must not** preclude the ability to do application layer accounting.
- Application layer mechanisms in gateways and stateful proxies that are specifically in place to recognize ETS type labels **must** be able to support “best available” service (i.e., better than “best effort”).

See also RFC 4375 [309] and RFC 4542 [310].

Emergency Services (E911)

We need to support 3 things according to Henning Schulzrinne[305]:

- There must exist an emergency address (similar to 911, 112, help, …)
- find Public Safety Answering Point (PSAP)
  - outbound proxy -- only if there is a well bounded geographic area servered by this proxy
  - use DNS where the user or device enters a relevant name: e.g., pittsburgh.pa.911.arpa
  - SLP - but scope not likely to coincide with ESR
  - call volume:
    - Sweden: SOSAlarm.se has 20 call centers distributed aound Sweden with ~18 million calls/year with ~20% of them calls to 112 the rest are automatic alarms;
    - US: National Emergency Number Association (NENA) reports >500,000 calls/day or 190 million a year (more than 80% are not emergencies ⇒ 311 non-emergency number)
- obtain caller's **identity** and **geographical address**
  - this is done to minimize prank calls
  - caller provides in request
    - Geographic position: N 59° 24.220' E017° 57.029' +/- 77m and/or
    - Geographic Location: "5th floor, Isafjordsgatan 22, Kista, Stockholm, Sweden"
  - or PSAP queries caller
  - or PSAP queries third party based on caller identity

note: Enhanced 911 (E911) - mandated by FCC for cellular phones in US

Public Safety Answering Point (PSAP)

For example MapInfo has an E911 database called "PSAP Pro" which contains the following PSAP information for the U.S. :

- 10-digit emergency numbers
- Address information
- Administrative phone number
- Fax number
- Contact person
- Latitude and longitude
- Jurisdictional boundaries

~4,400 records: both primary PSAPs and sheriff's departments and offices in areas not served by a PSAP.

from http://www.mobileinfo.com/news_2001/issue03/mapinfo_psap.htm

So finding the nearest one can be done based on geography, but is it the most relevant or useful one? In Sweden SOS Alarm works with the digital maps from CoordCom.

Location Interopeability Forum became part of Open Mobile Alliance (OMA) and no longer exists separately: http://www.openmobilealliance.org/tech/affiliates/lif/lifindex.html

Vonage 911 service

http://www.vonage.com/no_flash/features.php?feature=911

- User must pre-designate the physical location of their Vonage line and update Vonage when the user moves
- 911 dialing is not automatically a feature of having a line
  - users must pre-activate 911 dialing
  - user may **decline** 911 dialing
- A 911 dialed call will be connected to a general access line at the Public Safety Answering Point (PSAP)
  - thus they will **not** know you phone number or location
- Service may **not** be available due to
  - a local power failure (your IP phone needs power)
  - you local ISP not being able to offer service
  - one of the transit networks not being able to offer service
  - the voice gateway to the PSTN not being in service
  - …

Vonage equips PSAPs with VoIP

Vonage Equips Over 100 New Counties and 400 Calling Centers With E911 in Just One Month, Vonage Press Release, March 7, 2006

http://www.vonage.com/corporate/press_index.php?PR=2006_03_07_0

- "Nearly 65 Percent of Vonage Customers Now Have E911"
- "In February alone, Vonage equipped an additional 400 calling centers in over 100 new counties with E911 -- bringing the total number of calling centers across the nation with E911 service to over 3400, which is more than half of the nation's calling centers. While it took Vonage less than a year to turn on E911 in more than one-half of the nation's PSAP's, it took the wireless industry 10 years to accomplish the same feat."
- "In the event Vonage is unable to connect to the 911 system or for customers who are using mobile devices such as wifi phones or softclients, Vonage offers a national emergency call center which enables customers to get local help when they need it."

+888

United Nations Office for Coordination of Humanitarian Affairs (OCHA) assigned the E.164 geographic country code +888 for used by UN emergency responders

> "The +888 number range has been allocated to OCHA for the purpose of facilitating the provision of an international system of naming and addressing for terminals involved in disaster relief activities in an area of a country that has been cut off from the national telecommunications system of that country until such time as normal telecommunications can be restored. The use of these numbering resources will therefore be relatively short-lived and the resource may be re-used at a later date for another location."

Jeff - VoipDIY.com, "United Nations OCHA Teams-up With Voxbone to Facilitate Disaster Relief Communications on the iNum +883/+888 Network" , 24 October 2012

Emergency Services Branch on Open IMS core

Added:

- Emergency-CSCF (E-CSCF) and
- Location Retrieval Function (LRF)
- Requires the capability to do an emergency registration

http://www.openimscore.org/emergency

Follows 3GPP TS 23.167 (IP Multimedia Subsystem (IMS) emergency sessions), TS 24.229 (IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3), and TS 29.228 (IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents)

Geographic Location/Privacy Working Group (GEOPRIV)

GEOPRIV (http://www.ietf.org/html.charters/geopriv-charter.html) an IETF working group tasked with establishing a means of disseminating geographic data that is subject to the same sorts of privacy controls as presence is today.

The requirements for GEOPRIV are given in RFC 3693 [321]. Security threats are examined in RFC 3694 [322].

"A Presence-based GEOPRIV Location Object Format" is defined in RFC 4119 [323] based on earlier work done in formulating the basic requirements for presence data -- the Presence Information Data Format (PIDF) and a means of distributing these object described in RFC 4079 [326].

References and Further Reading

Emergency services

[304]Henning Schulzrinne, “Requirements for Resource Priority Mechanisms for the Session Initiation Protocol (SIP)”, IETF RFC 3487, February 2003

[305]See Henning Schulzrinne , “SIP for Emergency Services”, 48th IETF (Pittsburgh), http://www.cs.columbia.edu/sip/talks/ietf0008_911.pdf

[306]Europe’s 112 web site: http://www.sos112.info/

[307]K. Carlberg and R. Atkinson, “General Requirements for Emergency Telecommunication Service (ETS)”, IETF RFC 3689, February 2004

ftp://ftp.rfc-editor.org/in-notes/rfc3689.txt

[308]K. Carlberg and R. Atkinson, “IP Telephony Requirements for Emergency Telecommunication Service (ETS)”, IETF RFC 3690, February 2004

ftp://ftp.rfc-editor.org/in-notes/rfc3690.txt

[309]K. Carlberg, “Emergency Telecommunications Services (ETS) Requirements for a Single Administrative Domain”, Internet Request for Comments", RFC Editor, RFC 4375 (Informational), ISSN 2070-1721, January 2006, http://www.rfc-editor.org/rfc/rfc4375.txt

[310]F. Baker and J. Polk, “Implementing an Emergency Telecommunications Service (ETS) for Real-Time Services in the Internet Protocol Suite”, Internet Request for Comments, RFC Editor, RFC 4542 (Informational), ISSN 2070-1721, May 2006, Updated by RFC 5865

http://www.rfc-editor.org/rfc/rfc4542.txt

[311]N. Tada, et al., “IAA System (I Am Alive): The Experiences of the Internet Disaster Drills”, Proceedings of INET-2000, June 2000.

SIP Telephony

[312]E. Zimmerer, J. Peterson, A. Vemuri, L. Ong, F. Audet, M. Watson, and M. Zonoun, “MIME media types for ISUP and QSIG Objects”, IETF RFC 3204, December 2001, Updated by RFCs 3459 and 5621

http://www.ietf.org/rfc/rfc3204.txt

[313]E. Burger, “Critical Content Multi-purpose Internet Mail Extensions (MIME) Parameter”, Internet Request for Comments, RFC Editor, RFC 3459 (Proposed Standard), ISSN 2070-1721, January 2003, Updated by RFC 5621 http://www.rfc-editor.org/rfc/rfc3459.txt

[314]G. Camarillo, “Message Body Handling in the Session Initiation Protocol (SIP)”, Internet Request for Comments, RFC Editor, RFC 5621 (Proposed Standard), ISSN 2070-1721, September 2009

http://www.rfc-editor.org/rfc/rfc5621.txt

[315] A. Johnston, S. Donovan, R. Sparks, C. Cunningham, and K. Summers, "Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows", IETF RFC 3666, December 2003

http://www.ietf.org/rfc/rfc3666.txt

TRIP

[316]J. Rosenberg, H. Salama, and M. Squire, “Telephony Routing over IP (TRIP)”, IETF RFC 3219, January 2002 http://www.ietf.org/rfc/rfc3219.txt

[317]J. Rosenberg and H. Schulzrinne, “Framework for Telephony Routing”, IETF RFC 2871, June 2000. http://www.ietf.org/rfc/rfc2871.txt

[318]M. Bangalore, R. Kumar, J. Rosenberg, H. Salama, D.N. Shah, “A Telephony Gateway REgistration Protocol (TGREP)”, Internet Request for Comments, RFC Editor, RFC 5140 (Proposed Standard), ISSN 2070-1721, March 2008 http://www.rfc-editor.org/rfc/rfc5140.txt

[319]L. Coene and J. Pastor-Balbas, “Telephony Signalling Transport over Stream Control Transmission Protocol (SCTP) Applicability Statement”, IETF, RFC 4166, February 2006 http://www.rfc-editor.org/rfc/rfc4166.txt

[320]K. Carlberg, I. Brown, and C. Beard, “Framework for Supporting Emergency Telecommunications Service (ETS) in IP Telephony”, IETF, RFC 4190, November 2005 ftp://ftp.rfc-editor.org/in-notes/rfc4190.txt

Geopriv

[321]J. Cuellar, J. Morris, D. Mulligan, J. Peterson, and J. Polk, “Geopriv Requirements”, Internet Request for Comments, RFC Editor, RFC 3693 (Informational), ISSN 2070-1721, February 2004

http://www.rfc-editor.org/rfc/rfc3693.txt

[322]M. Danley, D. Mulligan, J. Morris, and J. Peterson, “Threat Analysis of the Geopriv Protocol”, Internet Request for Comments, RFC Editor, RFC 3694 (Informational), ISSN 2070-1721, February 2004

http://www.rfc-editor.org/rfc/rfc3694.txt

[323]J. Peterson, “A Presence-based GEOPRIV Location Object Format”, Internet Request for Comments, RFC Editor, RFC 4119 (Proposed Standard), ISSN 2070-1721, December 2005, Updated by RFCs 5139 [324] and 5491 [325] http://www.rfc-editor.org/rfc/rfc4119.txt

[324]M. Thomson and J. Winterbottom, “Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)”, Internet Request for Comments, RFC Editor, RFC 5139 (Proposed Standard), ISSN 2070-1721, February 2008

http://www.rfc-editor.org/rfc/rfc5139.txt

[325]J. Winterbottom, M. Thomson, and H. Tschofenig, “GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations”, Internet Request for Comments, RFC Editor, RFC 5491 (Proposed Standard), ISSN 2070-1721, March 2009

http://www.rfc-editor.org/rfc/rfc5491.txt

[326]J. Peterson, “A Presence Architecture for the Distribution of GEOPRIV Location Objects”, Internet Request for Comments, RFC Editor, RFC 4079 (Informational), ISSN 2070-1721, July 2005 http://www.rfc-editor.org/rfc/rfc4079.txt

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1
Module 14: SIP Conferencing

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:32

Conferencing

- Multimedia conferencing
  - Synchronized Multimedia Integration Language (SMIL) to enable other media (e.g., text, graphics and URLs) to be added to audio/video streams for synchronized display[349]
  - SMIL documents are XML 1.0 documents
- Multipoint conferencing
  - can exploit multicast where available
- Call control for conferencing
- Floor control [330]
  - this a particular focus of Push-to-talk service [333]
  - see Florian Maurer's push-to-talk service for minisip (formerly available from http://push2talk.floHweb.ch)
  - An example of a floor control protocol is given in RFC 4582 [331]
- RFC 4575 [332] defines a SIP Event Package for Conference State

Conferencing Models [327]

Type of Conference	Description	Scale
Endpoint mixing	One end point acts as a mixer for all the other end points	small
SIP Server and distributed media	Central SIP server establishes a full mesh between all participants - each participant does their own mixing	medium
Dial-in conference	All participants connect to a conference bridge which does the mixing for each participant	medium
Ad hoc centralized conference	Two users transition to a multiparty conference, by one of them using third-party signaling to move the call to a conference bridge	medium
Large multicast conference	user join the multicast based on the multicast address (which they got via: • annoucement on the web • e-mail • Session Annoucement Protocol (SAP) [348]	small to very large

Commercial conference bridge authenticate the users joining the conference.

SIP Conferencing

RFC 4353 [328] defines SIP procedures for the following common operations:

- Creating Conferences (see RFC 5366 [341] for providing an initial list of participants)
- Adding/Removing Participants
- Destroying Conferences
- Obtaining Membership Information
- Adding/Removing Media
- Conference Announcements and Recordings

RFC 5850 [342] defines "A Call Control and Multi-Party Usage Framework for the Session Initiation Protocol (SIP)".

RFC 4579 [338] defines SIP Call Control - Conferencing for User Agents

A variety of conferencing scenarios are described in RFC 4597 [340].

Realizing conferences

Conferences can be realizes in many ways:

- Centralized Server, Endpoint Server, or Distributed Conferencing
- Media Server Component
- Distributed Mixing
- Cascaded Mixers
- Transcoding media at a conference bridge (see RFC 5370 [334])

Centralized Conferencing Framework

A framework for centralized conferences is defined in RFC 5239 [346]

Distributed Conferencing (DCON)

Distributed conferencing is an area where there is a lot of active development today, see the many Internet Drafts - such as “Requirements for Distributed Conferencing” [347].

Conference and IVR server control

The Media Server Control Protocol Requirements are defined in RFC 5167 [337] .

The Media Server Control Markup Language (MSCML) and Protocol specified in RFC 5022 [344] enables the conference focus to mix and control input from a media server. This can be used to play a video clip, display a picture (for example a slide), etc.

See also the Media Server Markup Language (MSML) defined in RFC 5707 [345]. The XMLSchema for Media Control is defined in RFC 5168 [339].

Media types

RFC 3551: RTP Profile for Audio and Video Conferences with Minimal Control provides a basic RTP profile.

RFC 4245: High-Level Requirements for Tightly Coupled SIP Conferencing defines the media types for the languages of the W3C Speech Interface Framework [329]:

- Voice Extensible Markup Language (VoiceXML),
- Speech Synthesis Markup Language (SSML),
- Speech Recognition Grammar Specification (SRGS),
- CallControl XML (CCXML), and
- Pronunciation Lexicon Specification (PLS).

Speaker recognition in a conference

Abstract:

A system and method for identifying a participant during a conference call include the capability to receive a packet containing data that represents audible sounds spoken by one of a plurality of participants in a conference call and to determine a speaker of the audible sounds using voice profile information of the participants. The system and method further include the capability to provide identification information of the speaker to the other participants in the conference call contemporaneously with providing audible sounds based on the data to those participants.

Shmuel Shaffer and Michael E. Knappe, US patent 6,853,716 [350]

Web conferencing

Apache OpenMeetings: Open source web conferencing http://openmeetings.apache.org/ offering:

- Audio and Video Conferencing
- Meeting recording and Screen sharing
- File Explorer (managed folders in each conference room)
- Moderating System
- Multi-Whiteboard and Chat
- User and room management
- Private message center
- Plan meetings with integrated calendar
- Conduct polls and votes on issues
- Backup all user generated content into a single ZIP file

References and Further Reading

SIP Conferencing

[327]J. Rosenberg and H. Schulzrinne, “Models for Multi Party Conferencing in SIP”, Internet Draft, July 1, 2002, {expired}

http://www.ietf.org/internet-drafts/draft-ietf-sipping-conferencing-models-01.txt

[328]J. Rosenberg, "A Framework for Conferencing with the Session Initiation Protocol (SIP)", IETF, RFC 4353, February 2006

http://www.rfc-editor.org/rfc/rfc4353.txt

[329]O. Levin and R. Even, High-Level Requirements for Tightly Coupled SIP Conferencing, Internet Request for Comments, ISSN 2070-1721, RFC 4245, RFC Editor, November 2005, *http://www.rfc-editor.org/rfc/rfc4245.txt*

[330]P. Koskelainen, J. Ott, H. Schulzrinne, and X. Wu. “Requirements for Floor Control Protocols”, IETF, RFC 4376, February 2006

http://www.rfc-editor.org/rfc/rfc4376.txt

[331]G. Camarillo, J. Ott, and K. Drage, “The Binary Floor Control Protocol (BFCP)”, Internet Request for Comments, RFC Editor, RFC 4582 (Proposed Standard), ISSN 2070-1721, November 2006 http://www.rfc-editor.org/rfc/rfc4582.txt

[332]J. Rosenberg, H. Schulzrinne, and O. Levin, “A Session Initiation Protocol (SIP) Event Package for Conference State”, Internet Request for Comments, RFC Editor, RFC 4575 (Proposed Standard), ISSN 2070-1721, August 2006, http://www.rfc-editor.org/rfc/rfc4575.txt

[333]M. Garcia-Martin,"A Session Initiation Protocol (SIP) Event Package and Data Format for Various Settings in Support for the Push-to-Talk over Cellular (PoC) Service", IETF, RFC 4354, January 2006

ftp://ftp.rfc-editor.org/in-notes/rfc4354.txt

[334]G. Camarillo, “The Session Initiation Protocol (SIP) Conference Bridge Transcoding Model”, Internet Request for Comments, RFC Editor, RFC 5370 (Proposed Standard), ISSN 2070-1721}, October 2008

http://www.rfc-editor.org/rfc/rfc5370.txt

[335] O. Levin and R. Even, "High-Level Requirements for Tightly Coupled SIP Conferencing", IETF RFC 4245, November 2005,

ftp://ftp.rfc-editor.org/in-notes/rfc4267.txt

[336] H. Schulzrinne and S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control", Internet Request for Comments, RFC Editor, RFC 3551 (Standard), ISSN 2070-1721, July 2003, Updated by RFC 5761 http://www.rfc-editor.org/rfc/rfc3551.txt

[337] M. Dolly and R. Even, "Media Server Control Protocol Requirements", Internet Request for Comments, RFC Editor, RFC 5167 (Informational), ISSN 2070-1721, March 2008 http://www.rfc-editor.org/rfc/rfc5167.txt

[338]: A. Johnston and O. Levin, "Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents", Internet Request for Comments, RFC Editor, RFC 4579 (Best Current Practice), ISSN 2070-1721, August 2006

http://www.rfc-editor.org/rfc/rfc4579.txt

[339]O. Levin, R. Even, and P. Hagendorf, “XML Schema for Media Control”, Internet Request for Comments, RFC Editor, RFC 5168 (Informational), ISSN 2070-1721, March 2008 http://www.rfc-editor.org/rfc/rfc5168.txt

[340]R. Even and N. Ismail, “Conferencing Scenarios”, Internet Request for Comments, RFC Editor, RFC 4597 (Informational), ISSN 2070-1721, August 2006 http://www.rfc-editor.org/rfc/rfc4597.txt

[341]G. Camarillo and A. Johnston, “Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)”, Internet Request for Comments, RFC Editor, RFC 5366 (Proposed Standard), ISSN 2070-1721, October 2008, http://www.rfc-editor.org/rfc/rfc5366.txt

[342]R. Mahy, R. Sparks, J. Rosenberg, D. Petrie, and A. Johnston, “A Call Control and Multi-Party Usage Framework for the Session Initiation Protocol (SIP)”, Internet Request for Comments, RFC Editor, RFC 5850 (Informational), ISSN 2070-1721, May 2010 http://www.rfc-editor.org/rfc/rfc5850.txt

[343]J. Van Dyke, E. Burger, and A. Spitzer, “Media Server Control Markup Language (MSCML) and Protocol”, Internet Request for Comments, RFC Editor, RFC 4722 (Informational), ISSN 2070-1721, November 2006, Obsoleted by RFC 5022 http://www.rfc-editor.org/rfc/rfc4722.txt

[344]J. Van Dyke, E. Burger, and A. Spitzer, “Media Server Control Markup Language (MSCML) and Protocol”, Internet Request for Comments, RFC Editor, RFC 5022 (Informational), ISSN 2070-1721, September 2007

http://www.rfc-editor.org/rfc/rfc5022.txt

[345]A. Saleem, Y. Xin, and G. Sharratt, “Media Server Markup Language (MSML)”, Internet Request for Comments, RFC Editor, RFC 5707 (Informational), ISSN 2070-1721, February 2010

http://www.rfc-editor.org/rfc/rfc5707.txt

[346]M. Barnes, C. Boulton, and O. Levin, “A Framework for Centralized Conferencing”, Internet Request for Comments, RFC Editor, RFC 5239 (Proposed Standard), ISSN 2070-1721, June 2008

http://www.rfc-editor.org/rfc/rfc5239.txt

[347]S P. Romano, A. Amirante, T. Castaldi, L. Miniero, and A. Buono, Requirements for Distributed Conferencing, IETF Network Working Group, Internet-Draft, June 20, 2011, Expires: December 22, 2011, draft-romano-dcon-requirements-09,

http://tools.ietf.org/html/draft-romano-dcon-requirements-09

Session Annoucement Protocol

[348]M. Handley, C. Perkins, and E. Whelan, "Session Announcement Protocol", IETF RFC 2974, October 2000

http://www.ietf.org/rfc/rfc2974.txt

SMIL

[349] Synchronized Multimedia Integration Language (SMIL) 1.0 Specification, W3C Recommendation 15-June-1998 http://www.w3.org/TR/REC-smil/

Speaker recognition in a conference

[350]Shmuel Shaffer and Michael E. Knappe, "System and method for identifying a participant during a conference call", Assignee: Cisco Technology, Inc. (San Jose, CA), United States Patent 6,853,716, February 8, 2005, Filed: April 16, 2001.

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 15: Mixed Internet-PSTN Services

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:32

Mixed Internet-PSTN Services

- PSTN and Internetworking (PINT)
- Servers in the PSTN Initiating Requests to Internet Servers (SPIRITS)
- Telephony Routing over IP (TRIP)
- Opticall AB's Dial over Data solution

PSTN and Internetworking (PINT)

PSTN and Internetworking (PINT)[351] - action from the internet invokes a PSTN service (note: this is **one way** invocation), examples:

- Request to Call ⇒ "Click to Connect" from a web page
- Request to Fax Content ⇒ "Click to FAX"
- Request to Speak/Send/Play Content
- …

Based on SIP extensions (SIPext), which in actuality are SDP extensions (i.e., the body of SIP messages). Redefines some methods (`INVITE`, `REGISTER`, and `BYE`) and introduces three new methods:

- `Subscribe` - request completion status of a request
- `Notify` - receive status updates
- `Unsubscribe` - cancel subscriptions

PINT extensions to SDP: Network type (TN) and Address type: RFC2543 (SIP)

Servers in the PSTN Initiating Requests to Internet Servers (SPIRITS)

SPIRITS protocol [354] - implementing a family of IN services via internet server (rather than in the PSTN)

For example, internet call waiting (ICW) - calling a busy phone in the PSTN network could pop up a call waiting panel on the client that is using this telephone line, this replaces earlier solutions such as:

- for example, Ericsson's PhoneDoubler, Ericsson Review, No. 04, 1997
  http://www.ericsson.com/about/publications/review/1997_04/article55.shtml
- PDF of the entire article:
  http://www.ericsson.com/about/publications/review/1997_04/files/1997041.pdf

SPIRITS unlike PINT allows **two way** interaction between Internet and PSTN.

See also [364].

Note that the IETF SPIRITS working group has concluded their work.

Telephony Routing over IP (TRIP)

Telephony Routing over IP (TRIP) [360] Finding a route from the Internet to a gateway nearest to where the call should be terminated

Telephony Routing Protocol is modeled after the Border Gateway Protocol (BGP)

See also TRIP MIB definitions iin RFC 3872 [362] and providing TRIP with a way to provided prioritized services to certain callers (generally special goverment employees) - RFC 5115 [363].

Opticall AB's Dial over Data solution

This approach uses a SIP proxy + VoIP gateway to couple calls to and from the PSTN, SIP trunks, SIP handsets, etc. in order to reduce the cost of calls. For details see the masters theses by Max Weltz [365], Li Zhang [366], Xiao Wu [367], Tao Sun [368], and others.

References and Further Reading

PINT

[351] S. Petrack and L. Conroy, "The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services", IETF RFC 2848, June 2000

http://www.ietf.org/rfc/rfc2848.txt

[352] H. Lu, M. Krishnaswamy, L. Conroy, S. Bellovin, F. Burg, A. DeSimone, K. Tewani, P. Davidson, H. Schulzrinne, K. Vishwanathan. "Toward the PSTN/Internet Inter-Networking--Pre-PINT Implementations", IETF RFC 2458 , November 1998

http://www.ietf.org/rfc/rfc2458.txt

[353] M. Krishnaswamy and D. Romascanu, "Management Information Base for the PINT Services Architecture", IETF RFC 3055, February 2001 http://www.ietf.org/rfc/rfc3055.txt

SPIRITS

[354] V. Gurbani (Editor), A. Brusilovsky, I. Faynberg, J. Gato, H. Lu, and M. Unmehopa, "The SPIRITS (Services in PSTN requesting Internet Services) Protocol", IETF RFC 3910 , October 2004 http://www.ietf.org/rfc/rfc3910.txt

[355]I. Faynberg, H. Lu, and L. Slutsman, “Toward Definition of the Protocol for PSTN-initiated Services Supported by PSTN/Internet Internetworking”, IETF, Network Working Group, Internet draft, October 1999, Expired: April 2000 https://datatracker.ietf.org/doc/draft-faynberg-spirits-protocol/

[356]H. Lu, I. Faynberg, J. Voelker, M. Weissman, W. Zhang, S. Rhim, J. Hwang, S. Ago, S. Moeenuddin, S. Hadvani, S. Nyckelgard, J. Yoakum, and L. Robart, “Pre-Spirits Implementations of PSTN-initiated Services”, IETF RFC 2995, November 2000 http://www.ietf.org/rfc/rfc2995.txt

[357]L. Slutsman, I. Faynberg, H. Lu, and M. Weissman, “The SPIRITS Architecture”, IETF RFC 3136, June 2001 http://www.ietf.org/rfc/rfc3136.txt

[358]I. Faynberg, J. Gato, H. Lu, and L. Slutsman, “Service in the Public Switched Telephone Network/Intelligent Network (PSTN/IN) Requesting InTernet Service (SPIRITS) Protocol Requirements”, IETF RFC 3298, August 2002 http://www.ietf.org/rfc/rfc3298.txt

[359]IETF Service in the PSTN/IN Requesting InTernet Service working group http://www.ietf.org/html.charters/spirits-charter.html

TRIP

[360]J. Rosenberg, H. Salama, and M. Squire, “Telephony Routing over IP (TRIP)”, RFC 3219, January 2002 http://www.ietf.org/rfc/rfc3219.txt

[361]J. Rosenberg and H. Schulzrinne, “A Framework for Telephony Routing over IP”, Internet Request for Comments, RFC Editor, RFC 2871 (Informational), ISSN 2070-1721, June 2000 http://www.rfc-editor.org/rfc/rfc2871.txt

[362]D. Zinman, D. Walker, and J. Jiang, “Management Information Base for Telephony Routing over IP (TRIP)”, Internet Request for Comments, RFC Editor, RFC 3872 (Proposed Standard), ISSN 2070-1721, September 2004 http://www.rfc-editor.org/rfc/rfc3872.txt

[363]K. Carlberg and P. O'Hanlon, “Telephony Routing over IP (TRIP) Attribute for Resource Priority”, Internet Request for Comments, RFC Editor, RFC 5115 (Proposed Standard), ISSN 2070-1721, January 2008 http://www.rfc-editor.org/rfc/rfc5115.txt

ISUP

[364]G. Camarillo, A. B. Roach, J. Peterson, and L. Ong, "Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping", IETF RFC 3398, December 2002

ftp://ftp.rfc-editor.org/in-notes/rfc3398.txt

Dial over Data

[365]Max Weltz, Dial over Data solution, Masters thesis, Royal Institute of Technology (KTH), School of Information and Communications Technology, COS/CCS 2008-02, February 2008

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/080221-MaxWeltz_ExjobbReport-with-cover.pdf

[366]Zhang Li, Service Improvements for a VoIP Provider, Masters thesis, Royal Institute of Technology (KTH), School of Information and Communications Technology, TRITA-ICT-EX-2009:104, August 2009

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/090829-Zhang-Li-with-cover.pdf

[367]Xiao Wu, SIP on an Overlay Network. Masters thesis, Royal Institute of Technology (KTH), School of Information and Communications Technology, TRITA-ICT-EX-2009:105, September 2009

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/090915-XiaoWu-with-cover.pdf

[368]Tao Sun, Developing a Mobile Extension Application: OptiCaller Application and Provisioning System. Masters thesis, Royal Institute of Technology (KTH), School of Information and Communications Technology, TRITA-ICT-EX-2009:177, October 2009

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/091015-Tao_Sun-with-cover.pdf

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 16: AAA and QoS for SIP

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:32

Authentication, Authorization, Accounting (AAA)

This become a major issue especially in conjunction with QoS since for better than best effort service, someone probably has to pay for this high QoS - AAA is necessary to decide who you are, if you are allowed to ask for this service, and how much you should be charged. See [378] and “Authentication, Authorization and Accounting Requirements for the Session Initiation Protocol”[371].

SIP Accounting

For definition of terms see RFC 2975 [375]

Purposes:

- controlling resource usage (e.g., gateways to PSTN via which someone could place very expensive international or ‘premium rate’ calls)
- real-time
  - fraud detection
  - pre-paid subscriptions
- off-line
  - monthly/quarterly billing
  - deriving usage patterns ⇒ planning upgrades (resource dimensioning) , input for fraud detection, …

Resources to account for:

- resources used by SIP itself
- resource consumed once initiated by SIP
- services initiated and controlled by SIP {voice mail, media translation/transcoding, …}

Open Settlement Protocol (OSP)

(mostly) off-line settlement between operators based on Call Detail Records

Open Settlement Protocol developed as part of ETSI project TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) [376]

Based on exchange of Extensible Markup Language (XML) messages via HTTP

```
<!DOCTYPE Message [
    <!ELEMENT Message(( PricingIndication |
                        PricingConfirmation|
                        AuthorisationRequest |
                        AuthorisationResponse |
                        AuthorisationIndication |
                        AuthorisationConfirmation|
                        UsageIndication |
                        UsageConfirmation |
                        ReauthorisationRequest |
                        ReauthorisationResponse )+ ) >
                    ... ]>
```

Achieving QoS

- Over provision!
  - Simplest approach
- If this fails, then use TOS field or Diffserv
  - Much of the problem is on the access network - hence TOS or Diffserv even only on these links may be enough
- If this fails, then use RSVP
  - Much more complex - especially when done over several operator's domains

Some measured delays

Actual performance of SIP phone to SIP phone and software applications over a LAN, shows that the performance of SIP phones is well within acceptable delay.

Measurements of mouth to ear one-way delay, from "Aside: SIP phone QoS" slide 15 of [70]

end-point A	end-point B	A⇒B	B⇒A
GSM	PSTN	115 ms	109 ms
3Com	Cisco	51 ms	63 ms
NetMeeting	NetMeeting	401 ms	421 ms
Messanger XP	Messanger XP	109 ms	120 ms

Underlying Quality

Some statistics from Qwest for POP to POP measurements[1]

Table 1: February Monthly Averages

	Atlanta			Chicago			Dallas			Denver			Los Angeles (LA)			New York (NY)			Sunnyvale		
	loss (%)	latency (ms)	jitter (ms)	loss	latency	jitter	loss	latency	jitter	loss	latency	jitter	loss	latency	jitter	loss	latency	jitter	loss	latency	jitter
Atlanta				0.00	39.64	0.05	0.00	24.13	0.05	0.00	45.21	0.05	0.00	52.10	0.08	0.00	20.35	0.00	0.00	61.10	0.14
Chicago	0.00	39.46	0.09				0.00	24.10	0.08	0.00	23.32	0.07	0.00	56.13	0.33	0.00	20.17	0.01	0.00	48.10	0.09
Dallas	0.00	24.13	0.05	0.00	24.12	0.05				0.00	21.21	0.07	0.00	40.77	0.07	0.00	44.24	0.02	0.00	46.14	0.10
Denver	0.00	45.16	0.09	0.00	23.32	0.05	0.00	21.23	0.08				0.00	32.16	0.06	0.00	44.13	0.00	0.00	25.08	0.06
LA	0.00	52.07	0.06	0.00	56.09	0.20	0.00	40.68	0.07	0.00	32.22	0.06				0.01	76.09	0.02	0.00	8.01	0.07
NY	0.00	20.36	0.00	0.00	20.21	0.01	0.00	44.23	0.00	0.00	44.24	0.00	0.01	76.17	0.00				0.00	68.19	0.00
Sunnyvale	0.02	61.14	0.09	0.01	48.20	0.08	0.00	46.17	0.10	0.01	25.12	0.08	0.00	8.14	0.09	0.00	68.24	0.00			

1. Numbers takes from http://209.3.158.116/statqwest/statistics.jsp

Voice Quality

Some major tests:

- Mean Opinion Score (MOS)- defined in ITU-T P.800 [370]
  - ITU test based on using 40 or more people from different ethnic or language backgrounds listening to audio samples of several seconds each
  - Human listeners rating the quality from 1 to 5; 5 being perfect, 4 “toll-quality”, …
- Perceptual Speech Quality Measurement (PSQM) - ITU-T P.861
  - A computer algorithm - so it is easy to automate
  - scale of 0 to 6.5, with 0 being perfect
  - Designed for testing codecs
  - test tools from JDSU[380], QEmpirix, Finisar, … - cost US$50k and up
- PSQM+
  - Developed by Opticom
  - for VoIP testing
- PESQ (Perceptual Evaluation of Speech Quality)
  - submitted to ITU-T by Psytechnics, Opticom, and SwissQual
  - 0.95 correlation with human listeners
  - ITU-T P.862 standard Dec. 2003
- Perceptual Analysis Measurement System (PAMS)
  - Developed by British Telecommunications ~1998

- ITU-T's P.563
  - Passive monitoring
  - 0.85 to 0.9 correlation with human listeners
  - ITU standard May 2004
- Psytechnics algorithm: psyvoip
  - passive listening
  - uses RTP statistics
- "E Model" - ITU-T G.107
  - passive monitoring

Rating voice quality in practice

One approach is to occasionally ask IP phone users to indicate how the quality of their call was at the end of the call $\Rightarrow$ MOS scoring!

Another is exemplified by Susan Knott, global network architecture for PricewaterhoursCoopers:

> "But I've found that if my vice president of finance can talk to my CIO [over a VoIP connection], and they both say the quality of the connection is OK, then I say that's good enough."
>
> Phil Hochmuth, "Quality question remains for VoIP", NetworkWorld, Vol. 19, Number 40, October 7, 2002, pp. 1 and 71, quote is from page 71.

VoIP problem handling

Christina Sidiropoulou has written a masters thesis “VoIP Operators: From a Carrier Point of View” [405] describing out VoIP problem tickets can be handled by a carrier.

She describes how a problem is escalated and when.

QoS Proprietary vs. Standards based

Past

Agere Systems, Inc. VoIP “Phone-On-A-Chip” used a proprietary voice packet prioritization scheme called Ethernet Quality of Service using BlackBurst (EQuB), an algorithm (implemented in hardware) ensures that voice packets are given the highest priority in their collision domain.

2002

Their Phone-On-A-Chip solution now implements a software-based IEEE 802.1q tagging protocol (i.e. Virtual local area network (VLAN) tagging) for outgoing Ethernet frames.[1]

1. Agere Systems. T8302 Internet Protocol Telephone Advanced RISC Machine (ARM®) Ethernet QoS Using IEEE® 802.1q,Advisory July 2001.

QoS for SIP

SDP can be used to convey conditions which must be met:

- direction for QoS support: send, receive, or bidirectional
- along with a “strength” parameter: optional or mandatory

If conditions can be met then a `COMET` is sent.

See also RFC 4412 [393].

VoIP traffic and Congestion Control

RFC 3714: IAB Concerns Regarding Congestion Control for Voice Traffic in the Internet [385] - describes the concerns of the IAB due to the persistance of VoIP clients which continue to send RTP streams **despite** high packet loss rates WRT[1]:

- the risks of congestion collapse (along the end-to-end route) and
- fairness for congestion-controlled TCP traffic sharing the links.

When a steady-state packet drop rate >> a specified drop rate the flow should be terminated or suspended. Thus:

- RFC3551: RTP Profile for Audio and Video Conferences with Minimal Control - should be changed to say:
  - "… RTP receivers ~~SHOULD~~ MUST monitor packet loss to ensure that the packet loss rate is within acceptable parameters." and hence "MUST detect and respond to a persistent high loss rate"
- CODECs - should adapt so as to reduce congestion

Suggested heuristic: VoIP applications should suspend or terminate when:

- RTCP reported loss rate is greater than 30%, or
- N back-to-back RTCP reports are missing

1. With Respect To

Delay and Packet Loss effects

Effect of delay and packet loss on VoIP when using FEC has been studied by many researchers [387], [388], [389], [390].

A rule of thumb: When the packet loss rate exceeds 20%, the audio quality of VoIP is degraded beyond usefulness (cited as [S03] in [385]).

Normally in telephony, when the quality falls below a certain level users give up (i.e., they hang up). Does this occur in the absence of a cost associated with not hanging up?

$\therefore$ according to [385]:

if loss rate is *persistently unacceptably high* relative to the current sending rate
& the best-effort application is *unable to lower* its sending rate:

$\Rightarrow$ flow **must** discontinue:

- multicast session $\Rightarrow$ receiver withdraws from the multicast group
- unicast session $\Rightarrow$ unicast connection termination

When to continue (try again)

Probabilistic Congestion Control (PCC) [391] based on:

- calculating a probability for the two possible states (on/off) so that the expected average rate of the flow is TCP-friendly
- to perform a random experiment that succeeds with the above probability to determine the new state of the non-adaptable flow, and
- repeat the previous steps frequently to account for changes in network conditions.

The off periods need to be fairly distributed among users and the on period need to be long enough to be useful.

When to try again is determined by: **Probing the network while in the off** state (the authors of [391] have not implemented this yet).

Note that PCC only applies when there is a significant level of statistical multiplexing on the link (otherwise the use of statistics is not meaningful).

Other examples of probe based measurements are described at [392].

More about congestion

D. Willis and B. Campbell in “Session Initiation Protocol Extension to Assure Congestion Safety”, and (expired) Internet-Draft, October 13, 2003 examine:

- UAC may require that any proxy processing its requests **must** transmit those requests over a transport protocol providing congestion management
  - with a "Proxy-Require: congestion-management" header field
- In turn the UAS receiving these requests can be required to respond in similar fashion
- If a proxy finds that it has no route supporting congestion management it may reject the request with a 514 response (“No available route with congestion management”)
- If the request would be fragmented, the proxy can reject it with a 516 response ("Proxying of request would induce fragmentation")
- If the originating request did **not** require congestion-managed transport, then a UAS may reject a request that would result in a respons that requires congestion-managed transport.

RTP (over UDP) playing fair with TCP

Real-time multimedia communications wants (adapted from):

- timely delivery (vs. reliable but late delivery via TCP)
- smooth & predicatable throughput

This lead to proposals to use a transport layer such as Datagram Congestion Control Protocol (DCCP) [396] - as this implements TCP Friendly Rate Control (TFRC) [395].

However, this has some problems - including[400]:

- when a flow traverses a low statistically multiplexed network link (e.g., DSL link) using drop-tail queueing, TFRC traffic can starve TCP traffic
- oscillation on a short time scale
- if the RTT is less than the CPU interrupt cycle, then TRFC is hard to implement!

TCP-Friendly Window-based Congestion Control (TFWC)

Soo-Hyun Choi (together with his advisors) introduce TCP-Friendly Window-based Congestion Control (TFWC)[399][400].

This is based upon ACK clocking, sent using an ACK vector (to allow missing packets).

The claim is that TFWC is much fairer than TFRC when competing TCP flows and it is simple to implement in applications (in their case: VIC[1] and RAT)

1. Code for TFWC over VIC can be found at http://tfwc.sourceforge.net/download.html

VoIP quality over IEEE 802.11b

Two exjobb reports:

Juan Carlos Martín Severiano, “IEEE 802.11b MAC layer’s influence on VoIP quality: Measurements and Analysis”[401]

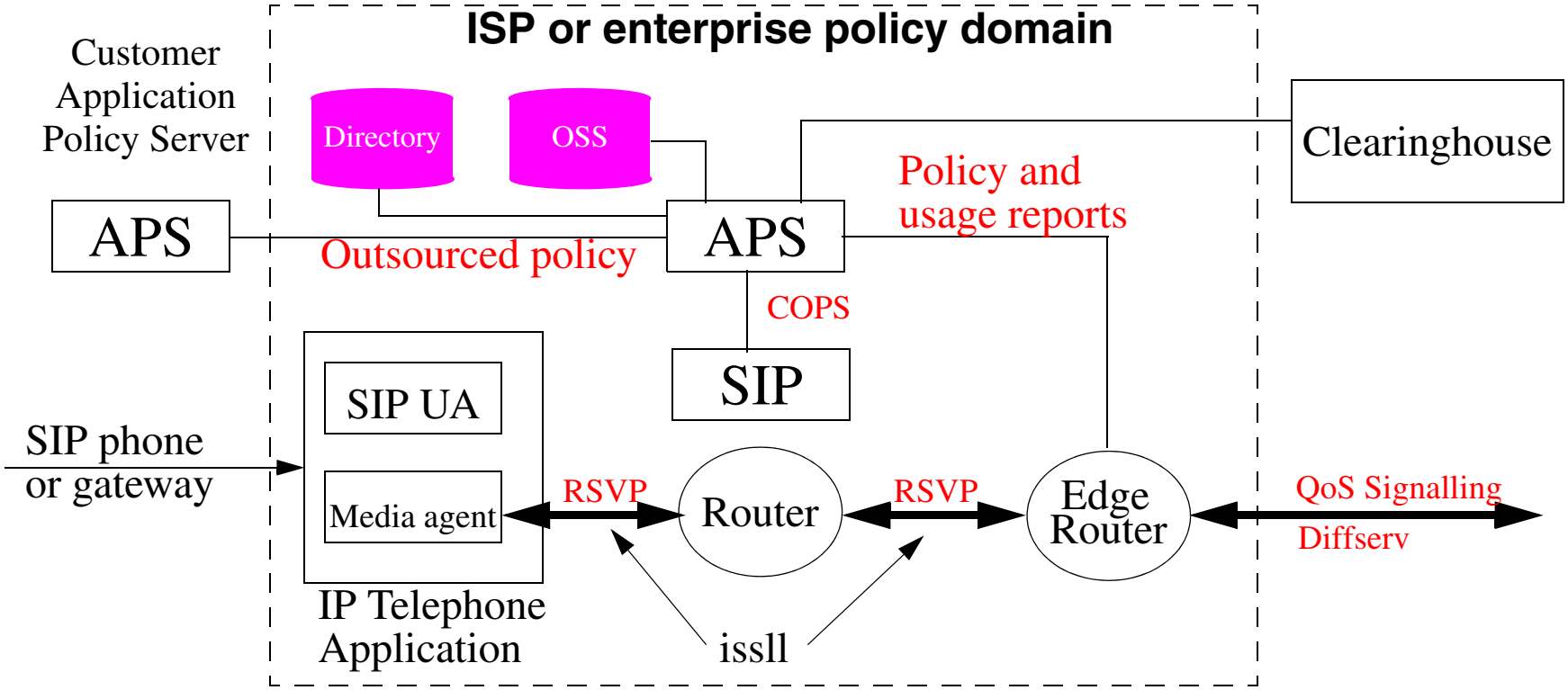
Victor Yuri Diogo Nunes, “VoIP quality aspects in 802.11b networks” [402]

Measurements of VoIP QoS

For an overview of VoIP and QoS see the doctoral dissertation of Ian Marsh [403]. Additional measurements of VoIP QoS are given in his licentiate thesis[404].

Application Policy Server (APS)

Gross, et al. proposed the use of an Application Policy Server (APS) [379]



IETF Integrated Services over Specific Lower Layers (issll) Working group (http://www.ietf.org/html.charters/issll-charter.html) is defining protocols to control the link layer.

VoIP performance managment and optimization

See the book Adeel Ahmed, Habib Madani, and Talal Siddiqui. *VoIP performance management and optimization: A KPI-based approach to managing and optimizing VoIP networks, Cisco Press, 2011* [406]

This book use key performance indicators (KPI) as metrics for managing and optimizing a VoIP system.

Figure 1-3 on page 9 of this book shows a set of voice quality issues and their potential causes. It further details these in Table 1-1 on page 15-17.

One of the features that Cisco's IOS has introduced is IP Service Level Agreements (IP SLA) - this can both collection information and be used to create a loopback so that traffic can be generated on the leaves of the network (for load testing).

VoIP metrics have also been added to Cisco's NetFlow version 9.

References and Further Reading

[369]CCITT Recommendation P.800, Methods for Subjective Determination of Transmission Quality, specifically Section 7: Subjective Opinion Tests, paragraph 3.1.2.3 Silence (gap) characteristics, CCITT, 1988. http://starlet.deltatel.ru/ccitt/1988/ascii/5_1_06.txt {A later version of the standard is [370]}

[370]ITU-T, Methods for Subjective Determination of Transmission Quality}, ITU-T, Recommendation P.800, March 1993

[371] J. Loughney, G. Camarillo, "Authentication, Authorization, and Accounting Requirements for the Session Initiation Protocol (SIP)", IETF RFC 3702, February 2004 http://www.ietf.org/rfc/rfc3702.txt

[372]G. Camarillo, W. Marshall, and J. Rosenberg, "Integration of Resource Management and Session Initiation Protocol (SIP)", IETF RFC 3312, October 2002. Updated by RFCs 4032 & 5027 http://www.ietf.org/rfc/rfc3312.txt

[373]G. Camarillo and P. Kyzivat, Update to the Session Initiation Protocol (SIP) Preconditions Framework, RFC Editor, RFC 4032 (Proposed Standard), ISSN 2070-1721, March 2005 http://www.rfc-editor.org/rfc/rfc4032.txt

[374]F. Andreasen and D. Wing, Security Preconditions for Session Description Protocol (SDP) Media Streams, RFC Editor, RFC 5027 (Proposed Standard)", ISSN 2070-1721, October 2007, http://www.rfc-editor.org/rfc/rfc5027.txt

[375] B. Aboba, J. Arkko, and D. Harrington, Introduction to Accounting Management, IETF RFC 2975, October 2000. http://www.ietf.org/rfc/rfc2975.txt

[376]Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON): Inter-domain pricing, authorisation, and usage exchange; ETSI DTS/TIPHON-03004 V1.4.0 (1998-09).

[377]W. Marshall, M. Osman, F. Andreasen, and D. Evans , “Architectural Considerations for Providing Carrier Class Telephony Services Utilizing SIP-based Distributed Call Control Mechanisms”, IETF SIPPING WG, Internet Draft, 15 January 2003
http://www.ietf.org/internet-drafts/draft-dcsgroup-sipping-arch-01.txt

[378] A. Johnston, D. Rawlins, H. Sinnreich, Stephen Thomas, and Richard Brennan, "Session Initiation Protocol Private Extension for an OSP Authorization Token", IETF Internet Draft, June 2004, Expired: December 2004 http://www.ietf.org/internet-drafts/draft-johnston-sip-osp-token-06.txt

[379] G. Gross, H. Sinnreich, D. Rawlins, and S. Thomas, "QoS and AAA Usage with SIP Based IP Communication", IETF Internet Draft, March 2000, draft-gross-sipaq-00.txt replaced by draft-gross-sipaq-01 on 2001-04-13 {expired October 2001}

[380] JDSU (formerly Agilent) Voice Quality Tester (VQT) J1981B

http://www.jdsu.com/

[381] CT Labs, "Speech Quality Issues & Measurement Techniques Overview", CT Labs, Inc., Revision: 10-23-2000

http://www.ct-labs.com/Documents/Speech_Quality_Testing.pdf

[382] netIQ's Vivinet Manager Suite http://www.netiq.com/products/vm/default.asp

[383] Cisco's "Monitoring Voice over IP Quality of Service"

http://www.cisco.com/warp/public/105/voip_monitor.html

[384]Mona Habib and Nirmala Bulusu, “Improving QoS of VoIP over WLAN (IQ-VW)”, Project Research Paper, for CS522 Computer Communications, University of Colorado at Colorado Springs, December 2002.

http://cs.uccs.edu/~cs522/projF2002/msoliman/doc/QoS%20of%20VoIP%20over%20WLAN.doc

[385]S. Floyd and J. Kempf (Editors), “IAB Concerns Regarding Congestion Control for Voice Traffic in the Internet”, IETF, RFC 3714, Network Working Group, March 2004. ftp://ftp.rfc-editor.org/in-notes/rfc3714.txt

[386] Sally Floyd and Kevin Fall, “Promoting the use of end-to-end congestion control in the Internet”, IEEE/ACM Transactions on Networking, vol. 7, no. 4, pp. 458-472, Aug. 1999.

[387]Wenyu Jiang and Henning Schulzrinne, “Modeling of Packet Loss and Delay and Their Effect on Real-Time Multimedia Service Quality”, NOSSDAV, 2000. http://citeseer.nj.nec.com/jiang00modeling.html

[388]Wenyu Jiang and Henning Schulzrinne, “Comparison and Optimization of Packet Loss Repair Methods on VoIP Perceived Quality under Bursty Loss”, NOSSDAV, 2002. Available from http://www1.cs.columbia.edu/~wenyu/

[389]Wenyu Jiang, Kazummi Koguchi, and Henning Schulzrinne, "QoS Evaluation of VoIP End-points", ICC 2003. Available from http://www1.cs.columbia.edu/~wenyu/

[390]A. P. Markopoulou, F. A. Tobagi, and M. J. Karam, "Assessing the Quality of Voice Communications Over Internet Backbones", IEEE/ACM Transactions on Networking, V. 11 N. 5, October 2003.

[391] Jörg Widmer, Martin Mauve, and Jan Peter Damm. "Probabilistic Congestion Control for Non-Adaptable Flows", Technical Report 3/2001, Department of Mathematics and Computer Science, University of Mannheim. formerly available from

http://www.informatik.uni-mannheim.de/informatik/pi4/projects/CongCtrl/pcc/

[392]Thomas Lindh, "Performance Monitoring in Communication Networks". Doctoral Thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, TRITA-IMIT-LCN AVH 04-02, 2004.

[393]H. Schulzrinne and J. Polk, Communications Resource Priority for the Session Initiation Protocol (SIP), RFC Editor, RFC 4412, ISSN 2070-1721, February 2006 http://www.rfc-editor.org/rfc/rfc4412.txt

[394]D. Willis and B. Campbell, “Session Initiation Protocol Extension to Assure Congestion Safety”, Internet-Draft, October 13, 2003, Expired: April 12, 2004 formerly available from http://www.ietf.org/internet-drafts/draft-ietf-sip-congestsafe-02.txt

[395]S. Floyd, M. Handley, J. Pahdye, and J. Widmer, TCP Friendly Rate Control (TFRC): Protocol Specification, IETF, Network Working Group, RFC 5348, September 2008 http://www.ietf.org/rfc/rfc5348.txt

[396]E. Kohler, M. Handley, and S. Floyd, Datagram Congestion Control Protocol (DCCP), IETF, Network Working Group, RFC 4340, March 2006, Updated by RFCs 5595 & 5596 http://www.ietf.org/rfc/rfc4340.txt

[397]G. Fairhurst, The Datagram Congestion Control Protocol (DCCP) Service Codes, RFC Editor, RFC 5595, ISSN 2070-1721, September 2009 http://www.rfc-editor.org/rfc/rfc5595.txt

[398]G. Fairhurst, Datagram Congestion Control Protocol (DCCP) Simultaneous-Open Technique to Facilitate NAT/Middlebox Traversal, RFC Editor, RFC 5596, ISSN 2070-1721, September 2009, http://www.rfc-editor.org/rfc/rfc5596.txt

[399]Soo-Hyun Choi, Design and Analysis for TCP-Friendly Window-based Congestion Control, University College London, Department of Computer Science, October 10, 2006 http://www.cs.ucl.ac.uk/staff/S.Choi/pubs/transfer_report.pdf

[400]Soo-Hyun Choi and Mark Handley, Designing TCP-Friendly Window-based Congestion Control for Real-time Multimedia Applications, Slides from their presentation at the 7th PFLDNeT, May 2009.
http://www.hpcc.jp/pfldnet2009/Program_files/3-3.pdf

[401]Juan Carlos Martín Severiano, "IEEE 802.11b MAC layer's influence on VoIP quality: Measurements and Analysis", MS thesis, Royal Institute of Technology (KTH)/IMIT, Stockholm, Sweden, October 2004.
http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/041024-Juan_Carlos_Martin_Severiano.pdf

[402]Victor Yuri Diogo Nunes, "VoIP quality aspects in 802.11b networks", MS thesis, Royal Institute of Technology (KTH)/IMIT, Stockholm, Sweden, August, 2004.

[403] Ian Marsh, Quality aspects of Internet telephony, Doctoral Dissertation, Royal Institute of Technology (KTH), Skolan för Elektro- och systemteknik, TRITA-EE, ISSN 1653-5146; 2009:025, SICS Dissertaion Series, ISSN 1101-1335; 51 2009

http://kth.diva-portal.org/smash/get/diva2:219379/FULLTEXT01 or

http://www.sics.se/~ianm/PhD/thesis.pdf

[404] Ian Marsh, Quality aspects of audio communication, Licentiate thesis, Royal Institute of Technology (KTH), Microelectronics and Information Technology) Trita-IMIT-LCN. AVH; 03:01, 2003

http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-1592

[405] Christina Sidiropoulou, VoIP Operators: From a Carrier Point of View, Masters thesis, Royal Institute of Technology (KTH), School of Information and Communication Technology, TRITA-ICT-EX-2011:166, July 2011,

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/110729-Christina_Sidiropoulou-with-cover.pdf

[406] Adeel Ahmed, Habib Madani, and Talal Siddiqui. *VoIP performance management and optimization: A KPI-based approach to managing and optimizing VoIP networks*. Indianapolis, IN: Cisco Press, 2011, 448 pages, ISBN-13: 978-1-58705-528-7.

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1
Module 17: SIP Applications

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:32

Session Initiation Protocol Project INvestiGation (SIPPING)[1]

SIP for applications related to telephony and multimedia. One of the significant features of using SIP for building applications is that it is much easier to build **open, distributed,** and **scalable services** that the traditional method of Intelligent Networks (IN); thus putting services into the hands of user!

Specific tasks for SIPPING were:

1 PSTN and/or 3G telephony-equivalent applications that need a standardized approach

- informational guide to common call flows
- support for T.38 fax
- requirements from 3GPP for SIP usage
- framework of SIP for telephony (SIP-T)
- call transfer and call forwarding
- AAA application in SIP telephony
- mapping between SIP and ISUP

1. Former working group - it no longer exists.

2 Messaging-like applications of SIP

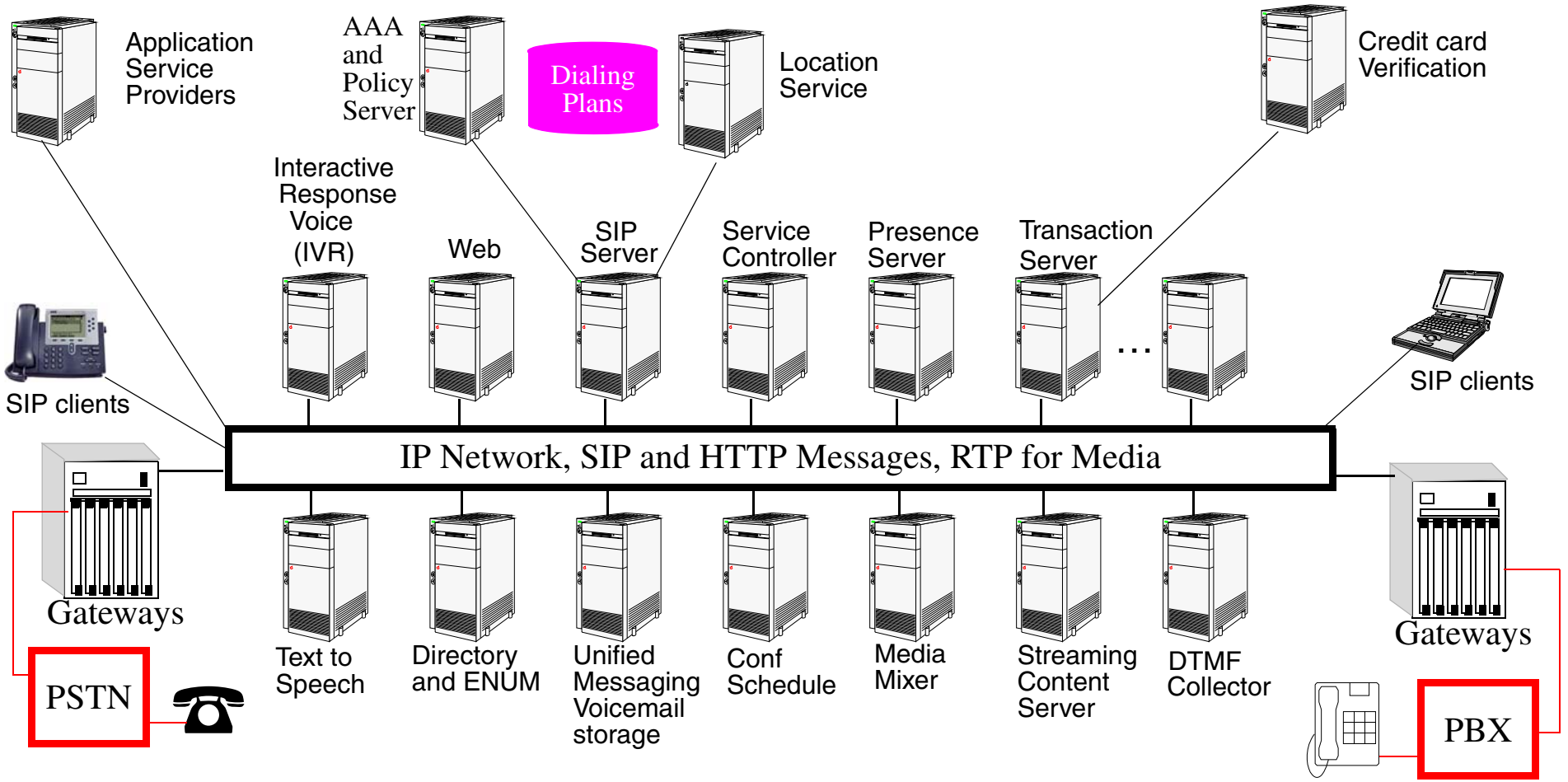
- support for hearing-/speech-impaired calling
- User Requirements for the Session Initiation Protocol (SIP) in Support of Deaf, Hard of Hearing and Speech-impaired individuals (RFC 3351) http://www.ietf.org/rfc/rfc3351.txt
- development of usage guidelines for subscribe-notify (RFC 2848, SIP events) to ensure commonality among applications using them, including SIMPLE WG's instant messaging.

3 Multi-party applications of SIP

4 SIP calling to media servers

- develop a requirements draft for an approach to SIP interaction with media servers, e.g., whether a voicemail server is just a box that a caller can send an INVITE to.

Application Service Components

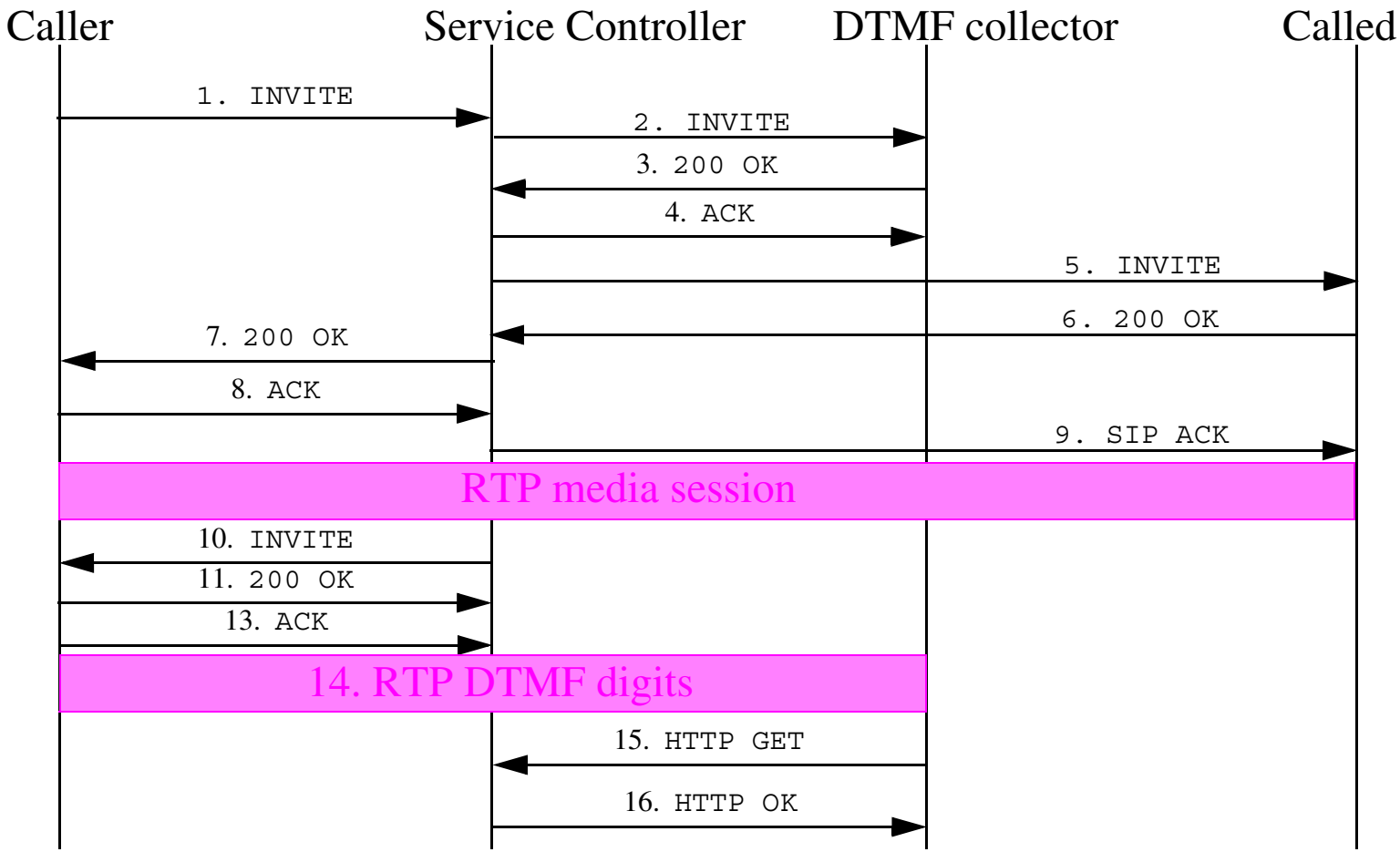


Advantages

- Decomposition
  - No complex APIs, just HTTP and SIP ⇒ rapid development
  - User can provide input to the service controller via Web servers, DTMF digit collector, voice portal (via VoiceXML), DTMF input, ... ⇒ just about any internet attached device can be used to provide input.
  - Easy to scale
  - New services can combine the "best of the best" (thus allowing developers to specialize)
  - Servers and services can be located anywhere on the internet and operated by anyone
- Decoupling
  - Loosely coupled and distributed
    - Flexible location of servers
    - if properly designed, implemented, and operated ⇒ higher reliability and resilience
  - Separation of businesses (leads to a rich variety of outsourcing, reseller, … models)
  - Since the functions are highly independent ⇒ rapid development
- Anyone can introduce a new service

However, if you want to use service components of others, then you may need to work out a suitable agreement (which will probably include an agreement about authorization) ⇒ security can be more complex.

Collecting DTMF digits for use within a service



Response “3. 200 OK” looks like:

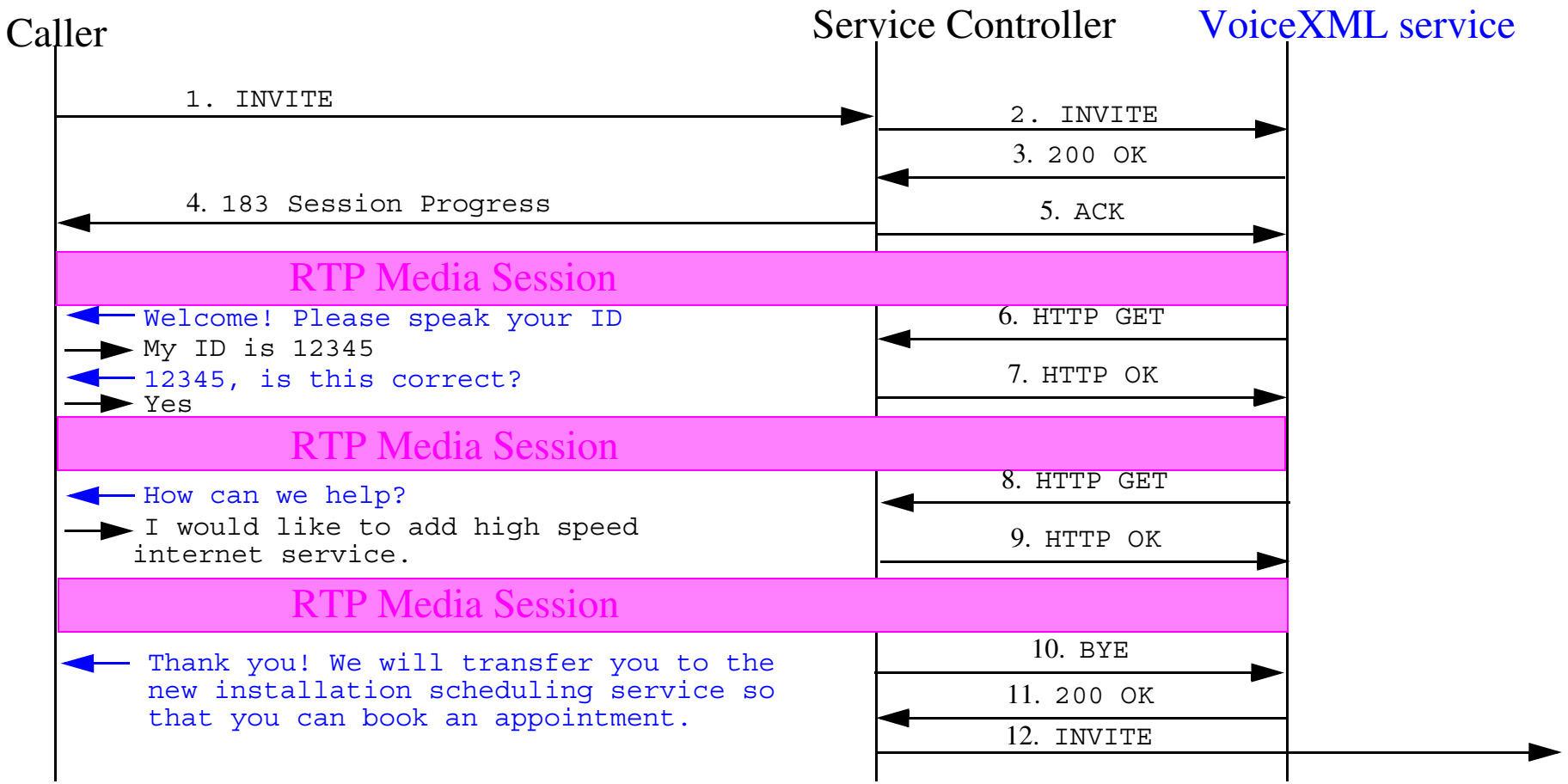
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 100.101.102.103
To: User A <sip:UserA@here.com>
From: UserB <sip:UserB@there.com>
Call-ID: a84b4c76e66710100.101.102.103
CSeq: 1 INVITE
Contact: <sip:UserB@there.com>
Content-Type: application/sdp
Content-Length: …

v=0
o=UserA 289375749 289375749 IN IP5 110.111.112.113
S=-
c=IN IP4 110.111.112.113
t=0 0
m=audio 5004 RTP/AVP 0
```

Controller issues a “re-Invite” at 11 which looks like:

```
INVITE sip:UserB@there.com SIP/2.0
Via: SIP/2.0/UDP 100.101.102.103
To: UserB <sip:UserB@there.com
From: User A <sip:UserA@here.com>
Call-ID: a84b4c76e66710100.101.102.103
CSeq: 1 INVITE
Contact: <sip:UserB@there.com>
Content-Type: application/sdp
Content-Length: …

v=0
o=UserA 289375749 289375749 IN IP5 100.101.102.103
S=-
c=IN IP4 100.101.102.103
t=0 0
m=audio 5004 RTP/AVP 0
m=audio 53000 RTP/AVP 0
c=IN IP4 200.201.202.203
a=rtpmap:96 telephone-event
```

Note the 2nd “m=audio” line in the SDP (see Sinnreich Johnston page 257), this second connection is the RTP connection to the DTMF digit collector.

Voice Portal Service using Interactive Voice Response (IVR)



The service controller proxies the caller to the IVR system.

Managing Services

Avgeropoulos Konstantinos in “Service Policy Management for User-Centric Services in Heterogeneous Mobile Networks”[408] proposes the use of SIP as signaling protocol for **policy based management** of a user’s multiple UAs.

He proposes a new SIP entity, called the **SIP Service Manager** (SSM).

Context aware SIP services

See for example these masters theses:

- Bemnet Tesfaye Merha, Secure Context-Aware Mobile SIP User Agent [409]
- Ke Wang, Exploiting Presence [410]
- Xueliang Ren, A Meeting Detector to Provide Context to a SIP Proxy [411]

See the licentiate thesis:

- Alisa Devlic, Context-addressed communication dispatch [412]

Unified communications

Unified communications (UC) - **integration** of both real-time (IM, presence, IP telephony, multimedia conferencing, …) and non-real-time communications (e-mail, SMS, MMS, fax, …).

- Sender sends a communication in their preferred format & Receiver receives the communications in their preferred format
- Integrates communication with business processes
- all via a consistent user interface (even when using different devices and media)

Interview with Mats Lundgren, Bygg UC med genomtänkt kundrelation, TDC Ahead, Winter 2008/2009, pages 12-15

http://download.opasia.dk/pub/song-sverige/ahead/Ahead_vinter_0809_TDC.pdf

SIP Web APIs

H. Sinnreich and A. Johnston in an internet draft entitled “SIP APIs for Communications on the Web” [415] - propose a SIP API to enable web developers to easily build services which utilize SIP - see the related for on Simple SIP - which also facilitate exploitation of the possibilities of so-called rich internet applications.

Simpler approach to SIP applications

"Simple SIP Usage Scenario for Applications in the Endpoints" RFC 5638 [413] describes how to exploit processing in the endpoints rather than emulating telephony to simplify the implementation of application and reduce the number of SIP documents that one needs to comply with.

Simple SIP = only the required functions for rendezvous and session setup + security

Goal is to leverage rich internet applications (RIAs) approach rather than trying to be like telephony! RIAs leverage the web browser as the user interface and facilitate the combination (mashups) of various information sources. SIP URIs should be able to be used as flexibly as other URIs in new RIA applications.

Relegates telephony aspects of SIP to something that is done in the gateway to the PSTN and not something that has to be built into every SIP UA.

Lots more services

See the list of SIP applications documents related to IBM's WebSphere Application Server, via the following web page (last accessed 2010.08.20)

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/welc6tech_sip_links.html

<< more to be added here - as time permits >>

Avoiding declarative service IDs

J. Rosenberg in “Identification of Communications Services in the Session Initiation Protocol (SIP)” RFC 5897 [414] argues that services should **not** be identified by a service identifier (such as a new Service-ID header).

References and Further Reading

SIPPING

[407]J. Rosenberg and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers”, IETF RFC 3263, June 2002

http://www.ietf.org/rfc/rfc3263.txt

[408]Avgeropoulos Konstantinos, “Service Policy Management for User-Centric Services in Heterogeneous Mobile Networks”, M.Sc. Thesis,Royal Institute of Technology (KTH), Institution for Microelectronics and Information Technology, Stockholm, Sweden, March 2004

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/040401-Konstantinos_Avgeropoulos-with-cover.pdf

[409]Bemnet Tesfaye Merha, Secure Context-Aware Mobile SIP User Agent, Masters Thesis, Royal Institute of Technology (KTH), School of Information and Communication Technology, Stockholm, Sweden, TRITA-ICT-EX-2009:63, July 2009

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/090705-Bemnet_Tesfaye_Merha-with-cover.pdf

[410]Ke Wang, Exploiting Presence, Masters thesis, Royal Institute of Technology (KTH), School of Information and Communications Technology, Stockholm, Sweden, COS/CCS 2008-27, December 2008

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/081205-Ke_Wang-with-cover.pdf

[411]Xueliang Ren, A Meeting Detector to Provide Context to a SIP Proxy, Masters thesis, Royal Institute of Technology (KTH), School of Information and Communications Technology, Stockholm, Sweden, COS/CCS 2008-24, October 2008

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/081025-Xueliang_Ren-with-cover.pdf

[412]Alisa Devlic, Context-addressed communication dispatch, Licentiate thesis, Royal Institute of Technology (KTH), School of Information and Communications Technology, Stockholm, Sweden, TRITA-ICT-COS:0902, ISSN 1653-6347; April 2009.

http://web.it.kth.se/~devlic/licentiate%20thesis/Alisa_Devlic-licentiate-thesis.pdf or

http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-10282

[413]H. Sinnreich, A. Johnston, E. Shim, and K. Singh, Simple SIP Usage Scenario for Applications in the Endpoints, RFC Editor, RFC 5638, ISSN 2070-1721, September 2009 http://www.rfc-editor.org/rfc/rfc5638.txt

[414]J. Rosenberg, Identification of Communications Services in the Session Initiation Protocol (SIP), RFC Editor, RFC 5897 (Informational), ISSN 2070-1721, June 2010 http://www.rfc-editor.org/rfc/rfc5897.txt

SIP Web API

[415]H. Sinnreich (Editor) and A. Johnston, SIP APIs for Communications on the Web, Internet Draft, IETF SIP Core Working Group, June 21, 2010, Expired: December 2010 http://tools.ietf.org/id/draft-sinnreich-sip-web-apis-01.txt

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 18: More than Voice

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:32

Non-voice Services and IP Phones

Phone Services: built using scripts which the IP phone executes to acquire information and display it

For example, some of the Cisco IP telephones (7940 and 7960) have a web browser which understands XML and a 133x65 pixel-based LCD display to display output.

Sample services:

- Conference room scheduler
- E-mail and voice-mail messages list
- Daily and weekly schedule and appointments
- Personal address book entries ($\Rightarrow$ any phone can become “your” phone)
- Weather reports, Stock information, Company news, Flight status, Transit schedules, …
- Viewing images from remote camera (for security, for a remote receptionist, …)

XML

XML objects include: CiscoIPPhoneMenu, CiscoIPPhoneText, CiscoIPPhoneInput, CiscoIPPhoneDirectory, CiscoIPPhoneImage, CiscoIPPhoneGraphicMenu, CiscoIPPhoneIconMenu, CiscoIPPhoneExecute, CiscoIPPhoneError and CiscoIPPhoneResponse.

Cisco IP Phone Services Software Developer's Kit[1]

1. Formerly available from http://cisco.com/warp/public/570/avvid/voice_ip/cm_xml/index.html

Invoking RTP streams

On the Cisco phones it is possible to invoke RTP streaming (transmit or receive) via URIs in above services. RTP information for the stream types must be of the form:

CODEC	G.711 mu-Law
Packet size	20 ms

More details

see ‘Thinking Outside the “Talk” Box: Building Productivity-Boosting Applications for Your Cisco IP Phones’ by Anne Smith, Cisco Packet, Third Quarter, 2002, pp. 21-23[1]

The book includes a CD which has a CallManager Simulator - so you can write applications with just a web server and a Cisco IP phone.

The SDK[2] should be available via http://developer.cisco.com)

1. Formerly available from http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac170/about_cisco_packet_technology09186a00801016d6.html
2. Formerly available from http://cisco.com/warp/public/570/avvid/voice_ip/cm_xml/cm_xmldown.shtml

Services for sale - building a market

Purchase existing services or contract for new third party XML services or support for Cisco's IP Telephony products: HotDispatch.

They have 91 Existing products as of 20 October 2002

HotDispatch has partnered with Cisco to provide IP Telephony **marketplace**, this is an example of a Community Knowledge Marketplace.

Network Appliances

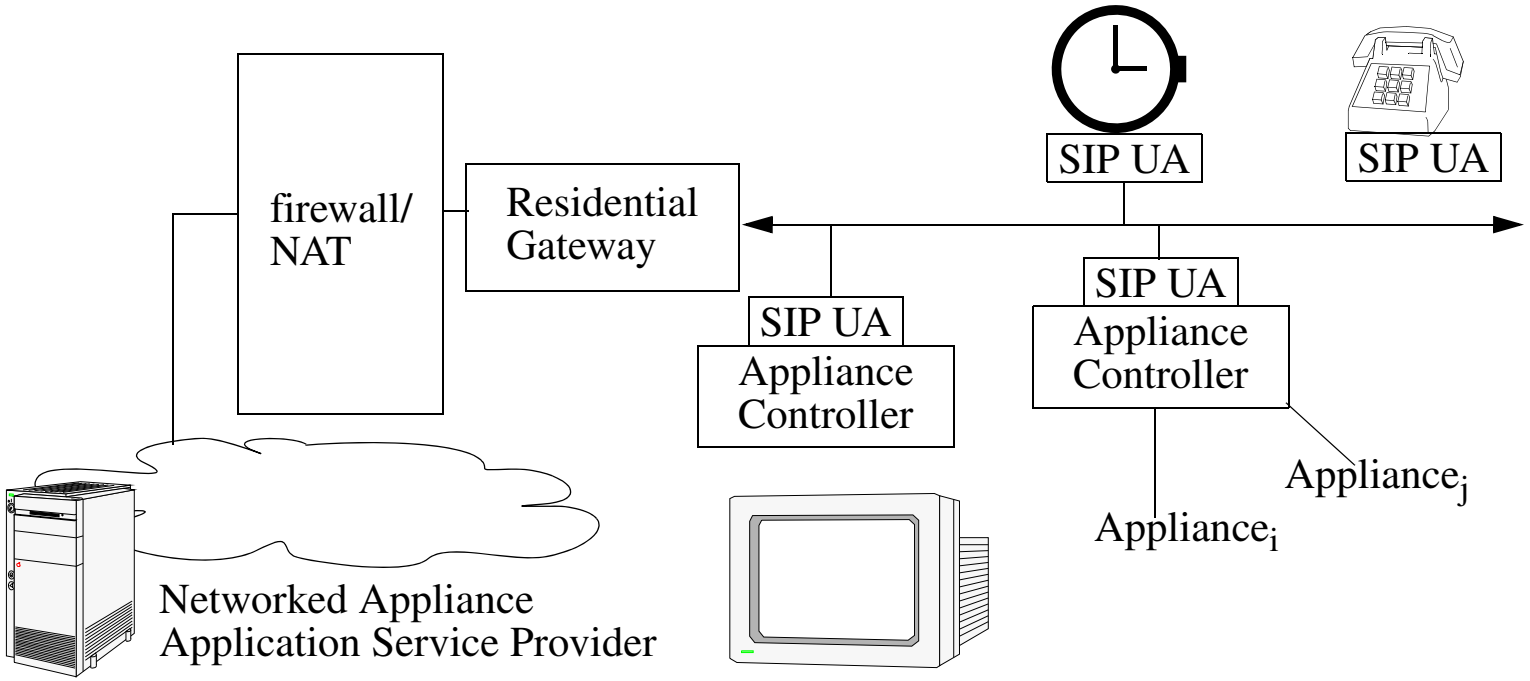


Figure 49: Using SIP for Service Portability (adapted from figure 2 of Moyer, Maples, Tsang, and Ghosh)

See: Stan Moyer, Dave Maples, Simon Tsang, and Abhrajit Ghosh, "Service Portability of Networked Appliances", IEEE Communications Magazine, January 2002, pp. 116-121.

Proposed Extension of SIP

Add **DO** message type

Adding a new optional header: History-Info

- provides information as to how and why a call arrives at a specific application or user [427]

Build upon Event extensions (specifcally **SUBSCRIBE** and **NOTIFY**)

- For example, you can subscribe to know when a user is invited to a session or there is a change in a state of an INVITE initiated dialog [426]

Add a new payload type via the new MIME type: **Device Message Protocol** (DMP) -- this payload is translated into device specific payload at the SIP User Agent.

Note that you could also send **SOAP** payload either separately or as part of DMP.

Service Location Protocol (SLP) URL

To: [SLP:/d=lamp, r=office, u=maguire]@it.kth.se

Note that the information inside the [ ] can be encoded in BASE-64 and encrypted, those making it opaque to entities outside the domain.

See [422].

Example service

This example is adapted from the above article, and the service is a network-based alarm clock service:

- delivers user specific information (latest news, weather, etc.)
- at a user selected time
- to the user's "alarm clock" network appliance

Specifically:

1. `REGESTER register@home.net`
   `To: [slp:/d=alarmclock, r=bedroom, u=maguire]@ua.chips.home.net`
   From: `[slp:/d=alarmclock, r=bedroom, u=maguire]@ua.chips.home.net`
   Content-type: application/ddp
   [Device address]
2. `INVITE sip:[slp:/d=alarmclock, r=bedroom, u=maguire]@home.net SIP/2.0`
   From: sip:announcement@alarmclock.net
   `To: [slp:/d=alarmclock, r=bedroom, u=maguire]@ua.chips.home.net`
   Via: `alarmclock.net`
   Content-type: application/sdp
   [SDP for uni-directional RTP stream]

3. `INVITE sip:[slp:/d=alarmclock, r=bedroom, u=maguire]@home.net SIP/2.0`
   From: sip:announcement@alarmclock.net
   `To: [slp:/d=alarmclock, r=bedroom, u=maguire]@ua.chips.home.net`
   `Via: home.net`
   Via: `alarmclock.net`
   Content-type: application/sdp
   [SDP for uni-directional RTP stream]
4. `INVITE sip:[slp:/d=alarmclock, r=bedroom, u=maguire]@home.net SIP/2.0`
   From: sip:announcement@alarmclock.net
   `To: [slp:/d=alarmclock, r=bedroom, u=maguire]@ua.chips.home.net`
   `Via: chips.home.net`
   `Via: home.net`
   Via: `alarmclock.net`
   Content-type: application/sdp
   [SDP for uni-directional RTP stream]
5. The alarm clock responds with its RTP parameters and the RTP session plays the annoucement to the user via the “alarm clock” network appliance

Example of service portability

This example is adapted from the above article, Chip visits his friend Mark:

- delivers user specific information (latest news, weather, etc.)
- at a user selected time
- to the user's "alarm clock" network appliance
- But the service now has to be delivered to the correct "alarm clock"
  - Either Chip takes his alarm clock with him or
  - Utilizes Mark's guest alarm clock as his alarm clock

1. `REGESTER register@home.net`
   `To: [slp:/d=alarmclock, r=bedroom, u=maguire]@ua.chips.home.net`
   From: `[slp:/d=alarmclock, r=bedroom, u=maguire]@ua.chips.home.net`
   Contact: *; expires=0

   The above cancels the service to Chip's home alarm clock

2. `REGESTER register@home.net`
   `To: [slp:/d=alarmclock, r=bedroom, u=maguire]@ua.chips.home.net`
   `From: [slp:/d=alarmclock, r=bedroom, u=maguire]@ua.chips.home.net`
   `Contact: sip:[slp:/d=alarmclock, r=guest_bedroom, u=maguire]@ua.marks.home.net]`
   `Content-type: application/ddp`
   `[Device description (including address)]`

3. INVITE sip:[slp:/d=alarmclock, r=bedroom, u=maguire]@home.net SIP/2.0
   From: sip:announcement@alarmclock.net
   To: [slp:/d=alarmclock, r=bedroom, u=maguire]@us.chips.home.net
   Via: alarmclock.net
   Content-type: application/sdp
   [SDP for uni-directional RTP stream]

   Now the SIP Proxy at home.net looks up [slp:/d=alarmclock, r=bedroom, u=maguire]@home.net and determines that it is [slp:/d=alarmclock, r=guest_bedroom, u=maguire]@ua.marks.home.net] so it forwards the messages to the SIP proxy at marks.home.net

4. INVITE sip:[slp:/d=alarmclock, r=guest_bedroom, u=maguire]@ua.marks.home.net] SIP/2.0
   From: sip:announcement@alarmclock.net
   To: [slp:/d=alarmclock, r=bedroom, u=maguire]@ua.chips.home.net
   Via: home.net
   Via: alarmclock.net
   Content-type: application/sdp
   [SDP for uni-directional RTP stream]

5. INVITE sip:[slp:/d=alarmclock, r=guest_bedroom, u=maguire]@ua.marks.home.net] SIP/2.0
   From: sip:announcement@alarmclock.net
   To: [slp:/d=alarmclock, r=bedroom, u=maguire]@ua.chips.home.net
   via: marks.home.net
   Via: home.net
   Via: alarmclock.net

Content-type: application/sdp
[SDP for uni-directional RTP stream]

6. Mark's guest bedroom alarm clock responds with its RTP parameters and the RTP session plays the annoucement to the user via the "alarm clock" network appliance

Text

Interleaved text

RTP can be used to carry real-time text conversations, the contents use ITU-T Recommendation T.140.[425]

Timed Text

The 3rd Generation Partnership Project (3GPP) has defined "timed text" as “time-lined, decorated text media format with defined storage in a 3GP file”[424].

“Timed Text can be synchronized with audio/video contents and used in applications such as captioning, titling, and multimedia presentations.”[424]

SOS and other URNs

H. Schulzrinne in “A Uniform Resource Name (URN) for Emergency and Other Well-Known Services” RFC 5031 [428] describes a service URN scheme for context-dependent services.

Just a dialing 911 in North America or 112 in Europe is mapped to the local emergency services “address”, there are other well known services that could be supported by having a well-known URN to be used with SIP.

These can be combined with Location-to-Service Translation protocol (LoST), RFC 5222 [429] to map the URN to the local instance of the “address”.

Examples:

- urn:service:sos
- urn:service:sos.ambulance
- urn:service:sos.fire
- urn:service:sos.police

Not all emergencies should go to the local authorities nor should they all be voice sessions

Consider a user with a portable monitoring device for a chronic health problem, this monitor might detect that the user's blood chemistry is going out of the expected range and automatically set up a session between the users montor and the user's physician or other health care professions - or perhaps even an on-line expert system.

Meta data

Gurbani, Burger, T. Anjali, H. Abdelnur, and O. Festor in an internet draft entitled "The Common Log Format (CLF) for the Session Initiation Protocol (SIP)" [430] emphasize the value of having a standard log format - in terms of enabling tools that can manipulate (and mine) this data - *independent* of the SIP entity that produces the data.

They describe why call data records are **not** sufficient.

References and Further Reading

Phone Services

[416]Darrick Deel, Mark Nelson, Anne Smith, *Developing Cisco IP Phone Services: A Cisco AVVID Solution*, Cisco Press, Feb. 15, 2002, 288 pages, ISBN 1-58705-060-9 http://www.ciscopress.com/bookstore/product.asp?isbn=1587050609

[417]Cisco IP Phone Services Application Development Notes, Oct. 1, 2002, http://www.cisco.com/application/pdf/en/us/guest/products/ps556/c1671/ccmigration_09186a00800f0d66.pdf

Network Appliances

[418]S. Tsang, et al., “Requirements for Networked Appliances: Wide-Area Access, Control, and Internetworking”, IETF Draft draft-tsang-appliances-reqs-01.txt, Sept. 2000, Expired March 2001

[419]Open Services Gateway Iniative (OSGi), http://www.osgi.org

[420] S. Moyer, et al., “Framework Draft for Networked Appliances Using the Session Initiation Protocol”, IETF draft, July 2000, {expired}

http://tools.ietf.org/html/draft-moyer-sip-appliances-framework-02.txt

[421]S. Tsang, D. Marples, and S. Moyer, "Accessing Networked Appliances using the Session Initiation Protocol", In Proc. of ICC 2001, 11-14 June 2001, Helsinki, Finland.

[422]E. Guttman, C. Perkins, J. Veizades and M. Day, “Service Location Protocol, version 2”, RFC 2608, June 1999, Updated by RFC 3224

http://www.ietf.org/rfc/rfc2608.txt

[423]E. Guttman, Vendor Extensions for Service Location Protocol, Version 2, RFC Editor, RFC 3224 (Proposed Standard), ISSN 2070-1721, January 2002

http://www.rfc-editor.org/rfc/rfc3224.txt

Text

[424] J. Rey and Y. Matsui, RTP Payload Format for 3rd Generation Partnership Project (3GPP) Timed Text, RFC 4396, February 2006

http://www.rfc-editor.org/rfc/rfc4396.txt

[425]G. Hellstrom and P. Jones, “Real-Time Transport Protocol (RTP) Payload for Text Conversation Interleaved in an Audio Stream”, IETF, RFC 4351, January 2006 ftp://ftp.rfc-editor.org/in-notes/rfc4351.txt

[426]J. Rosenberg, H. Schulzrinne, and R. Mahy (editors), An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP), IETF, RFC 4235, November 2005 ftp://ftp.rfc-editor.org/in-notes/rfc4235.txt

[427]M. Barnes (Editor), An Extension to the Session Initiation Protocol (SIP) for Request History Information, IETF, RFC 4244, November 2005

ftp://ftp.rfc-editor.org/in-notes/rfc4244.txt

[428]H. Schulzrinne, A Uniform Resource Name (URN) for Emergency and Other Well-Known Services, RFC Editor, RFC 5031, ISSN 2070-1721, January 2008 http://www.rfc-editor.org/rfc/rfc5031.txt

[429]T. Hardie, A. Newton, H. Schulzrinne, and H. Tschofenig, LoST: A Location-to-Service Translation Protocol, RFC Editor, RFC 5222, ISSN 2070-1721, August 2008 http://www.rfc-editor.org/rfc/rfc5222.txt

Log file format

[430]V. Gurbani (Ed.), E. Burger (Ed.), T. Anjali, H. Abdelnur, and O. Festor, The Common Log Format (CLF) for the Session Initiation Protocol (SIP): Framework and Data Model Internet-Draft, SIPCLF, March 9, 2012, Expires: September 10, 2012, draft-ietf-sipclf-problem-statement-11

http://tools.ietf.org/html/draft-ietf-sipclf-problem-statement-11

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 19: VOCAL

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with Luan Dang, Cullen Jennings, and David Kelly, *Practical VoIP: Using VOCAL*, O'Reilly, 2002, ISBN 0-596-00078-2.

Last modified: 2013.09.01:14:32

VOCAL System Overview

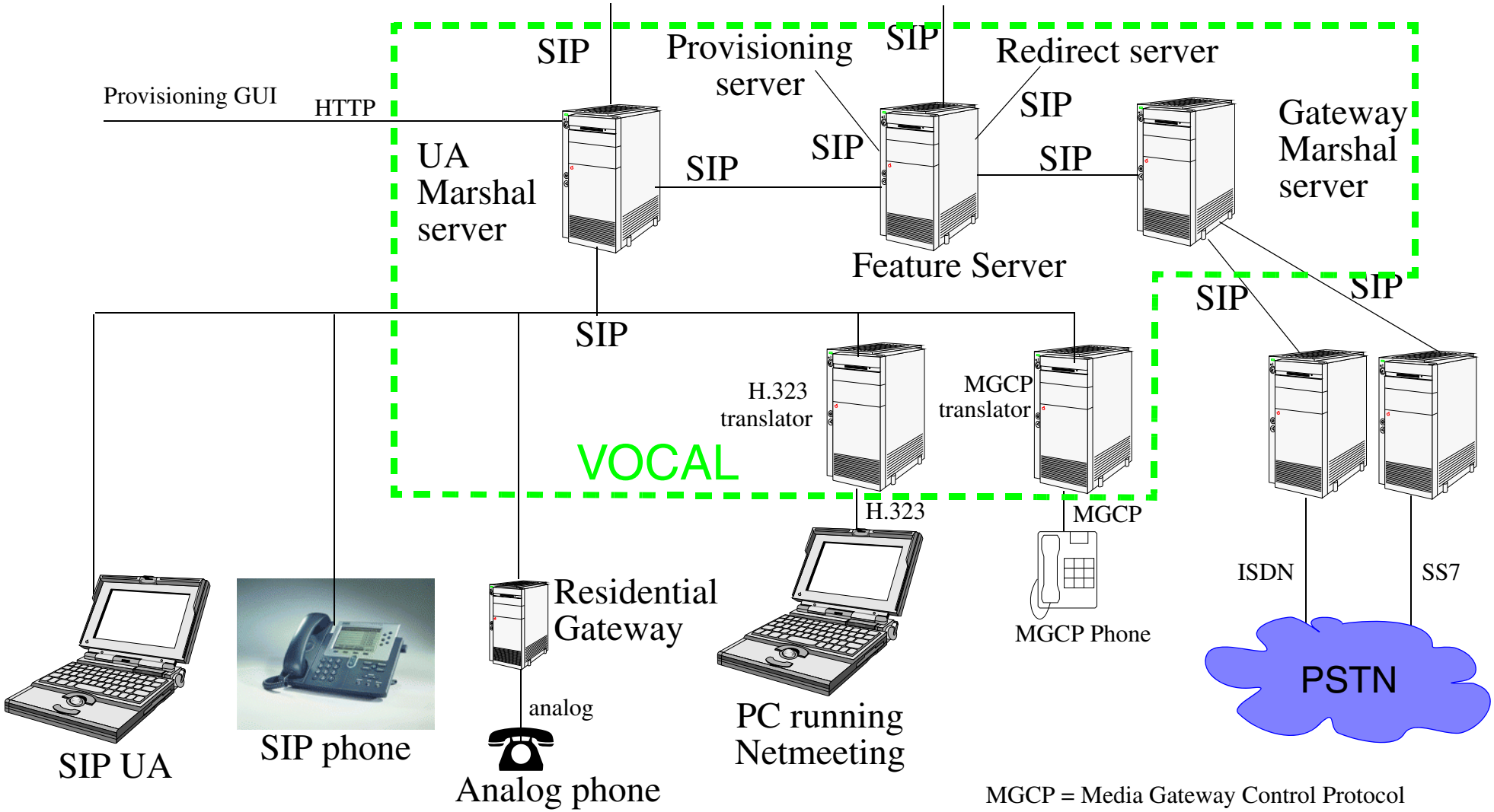


Figure 50: VOCAL: Simplified overview

VOCAL Servers

- Marshal server (MS)
  - User Agent (UA) Marshal server
    - interface to/from IP phones connected to this network
    - can do different types of authentication on a per-user basis
  - (PSTN) Gateway Marshal servers
    - provides interworking with PSTN
  - Internet Marshal server
    - interface to/from a SIP proxy server on another IP network
    - authenticate calls via Open Settlement Protocol (OSP)
    - can request QoS via Common Open Policy Service (COPS)
  - Conference Bridge Marshal server
    - interface to/from third party conference servers
- Feature server (FS)- to provide advanced telephony services
- Redirect server (RS) - keep track of registered users and provide routing to/from them
- Provisioning server (PS) - for configuration
- Call Detail Record (CDR) server - stores start/end information about calls for billing and other purposes

Scaling of a VOCAL system

From table 3-1 of *Practical VoIP: Using VOCAL*

Server types	6-host system	14-host system	26-host system
Redirect servers	1	2	5
Feature servers	1	2	5
Marshal servers	2	4	10
Call Detail Record servers	1/2	2	2
Provisioning servers	1	2	2
Policy servers	1/2	2	2
Total number of hosts	6	14	26
Capacity in calls per second	35	70	175
Capacity in busy-hour call attempts (BHCA)	125,000	250,000	630,000

Each host is a 700MHz Pentium III with 512 MB or RAM.

- Note that unlike a PBX or Public Exchange, the capacity in calls per second (or BHCA) is **independent** of the call durations, since the **call traffic** is carried directly between the endpoints via RTP and **does not use** the VOCAL system!

For comparison with a PBX

- NEC's PBX: EAX2400 IMX - Integrated Multimedia eXchange, model ICS IMGdxh uses a Pentium control process and the claimed[1] BHCA is 25,600.
- Tekelec's softswitch[2] "VXiTM Media Gateway Controller" claims[3] a capacity which scales from 250,000 to over 1 million BHCA - a Class 5 exchange.
- Lucent's 5E-XC™ Switch High Capacity Switch - supports 4 million BHCA, 250K trunks, and 99.9999% availability [434]
- Frank D. Ohrtman Jr. says that a Class 4 Softswitch should handle 800,000 BHCA, support 100,000 DS0s (i.e., 100K 64 bps channels), with a reliability of 99.999%, and MOS of 4.0 (i.e., high quality voice)[431].
  - His pricing data shows that softswitches are about 1/4 the price per DS0 of Class 4 exchanges (e.g., Nortel DMS250 and Lucent 4ESS vs. Convergent Networks's ICS2000 and SONUS GSX9000) -- additionally the softswitches are physically much smaller.
  - Many claim that softswitch and VoIP reliability already **exceeds** that of central office exchanges; because with VoIP it is cheaper to implement redundancy and easier to build physically distributed systems; plus more features {sooner}, while also providing potentially better quality (i.e., better than "toll" quality)!

Radcom's MegaSIP test software generates 3,500,000 BHCA calls per server.

---

1. Was available from http://www.stfi.com/STF_part3e.html
2. "A softswitch is the intelligence in a network that coordinates call control, signaling, and features that make a call across a network or multiple networks possible."[431]
3. Was available from http://www.tekelec.com/productportfolio/vximediagatewaycontroller/

Marshal server (MS)

A SIP proxy server which provides:

- authentication of users
- generates call detail records (CDRs)
- provides a entry point for SIP messages into the VOCAL system
  - thus the other elements of the VOCAL system don't need to authenticate each message
- monitor heart beats - can uses this for load balancing across RSs
- SIP transaction stateful, but not call (dialog) stateful

Allows better scaling, since these servers can be replicated as needed; while allowing the redirect server to focus just on keeping registration information.

Redirect Server (RS)

- receives SIP `REGISTER` messages from User Agents (UAs)
- keeps track of registered users and their locations (i.e., registrations)
- provides routing information for SIP `INVITE` messages
  - based on caller, callee, and registration information (for either or both parties)
  - based on where the `INVITE` message has already been
- Supports redundancy
  - Utilizes multicast heartbeat
    - starts by listening for 2s for another RS
    - if found, then it synchronizes with this RS and will act as a redundant backup RS (following synchronization)
    - if not found, then it starts transmitting its own heartbeat
  - a given RS must mirror `REGISTER` messages (received from the MS) to the other RSs

Feature Server (FS)

- Implements Call Forward, Call Screening, Call Blocking
  - The “Core Features” are implmented “within the network”
    - for example, you can’t implement features in aphone which is not there!
    - you can’t give an end system the caller’s ID, but guarantee that they **don’t** display it, …
- Execute arbitrary Call Processing Language (CPL) scripts written by users
  - CPL is parsed into eXtensible Markup Language (XML) document object model (DOM) trees, these are then turned into state machines (in C++), then executed.

Residential Gateway (RG)

A residential gateway (RG) provides "… Internet access throughout the home and remote management of common household appliances such as lights, security systems, utility meters, air conditioners, and entertainment systems."[1]

Open Services Gateway Initiative (OSGi™) Alliance http://www.osgi.org/ is attempting to define a standard framework and API for network delivery of managed services to local networks and devices.

An alternative to using a residential gateway to attach analog phones are devices such as the Cisco Analog Telephone Adaptor (ATA) 186 [435].

In VOCAL: "SIP Residential Gateway is an IP Telephony gateway based on SIP which allows a SIP user agent to make/receive SIP call to/from the Public Switched Telephone Network (PSTN)."[2]

---

1. from http://www.national.com/appinfo/solutions/0,2062,974,00.html - "National Semiconductor signed a definitive agreement in August 2003 to sell its Information Appliance (IA) business unit, consisting primarily of the Geode™ family of microprocessor products, to Advanced Micro Devices (AMD)"

2. http://www.vovida.org/fom-serve/cache/761.html

Residential Gateways

A very important aspect of such gateways is provisioning them, for example via the Broadband Forum's CPE WAN Protocol, TR-069 standard. This enables the operators to control the boxes, perform updates, set the device's configuration, etc. This protocol is based upon SOAP over HTTP.

Provisioning is very important when an operator my have 10^5 to 10^7 devices installed at their customers premises.

References and Further Reading

[431]Frank D. Ohrtman Jr., *Softswitch: Architecture for VoIP*, McGraw-Hill Professional, 2002, ISBN: 0071409777.

[432]Radcom, MegaSIP data sheet, Bristol, England
was available from http://www.radcom.com/radcom/test/pdf/ds_pa_megasip.pdf

[433]Abacus2 Test equipment, Spirent Communications, Calabasas, CA, USA, www.spirentcom.com - generates and switches more than 20 million calls per hour

[434]5ESS Switch High Capacity Switching Applications, 5E-XCi v1, Sept. 2003
http://www.lucent.com/livelink/090094038004f536_Brochure_datasheet.pdf

[435]Cisco Analog Telephone Adaptor (ATA) 186
http://www.cisco.com/warp/public/cc/pd/as/180/186/

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 20: SIP Express Router and other Software

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:32

SIP Express Router (SER)

http://www.iptel.org/ser/ SER is an open-source implementation which can act as SIP registrar, proxy or redirect server. SER features:

- an application-server interface,
- presence support,
- SMS gateway,
- SIMPLE2Jabber gateway,
- RADIUS/syslog accounting and authorization,
- server status monitoring,
- Firewall Communication Protocol (FCP)[1] security, …
- Web-based user provisioning (serweb)

For configuration help see: http://www.mit.edu/afs/athena/project/sip/sip.edu/ser.shtml

For performance of a SER server see [438]

1. http://www.iptel.org/fcp/

Many SIP Express Routers

The OpenSER project has split in to a number of projects, see:

- Open SIP Server (OpenSIPS) http://www.opensips.org/
- Kamailio http://www.kamailio.org/

SER amd Kamailo are part of the sip-router project (http://sip-router.org).

Additionally there are lots of other projects, see

http://www.voip-info.org/wiki/view/Open+Source+VOIP+Software

or use your favorite search engine!

SipFoundry

http://www.sipfoundry.org/ was formed on March 29, 2004 - goal improving and adopting open source projects related to SIP

Pingtel Corp. contributed their sipX family of projects (distributed under the LGPL). This includes:

sipXphone	SIP soft phone
sipXproxy	pair of applications that together form a configurable SIP router.
sipXregistry	SIP Registry/Redirect server
sipXpublisher	server to handle SIP SUBSCRIBE/NOTIFY handling + flexible plugin architecture for different event types.
sipXvxml	VXML scripting engine supporting creation of IVR and other VXML applications (including auto-attendant and voice mail)
sipXconfig	SIP configuration server
sipXpbx	full PBX solution; combining sipXproxy, sipXregistry, sipXpublisher, sipXvxml, and sipXconfig
sipXtest	testing tools and frameworks

Other SIP Proxies

- JAIN-SIP Proxy
  - Formerly available from http://snad.ncsl.nist.gov/proj/iptel/
  - JAIN-SIP proxy, JAIN-SIP IM client, SIP communicator, SIP trace viewer, JAIN-SIP gateway, JAIN-SIP 3PCC, …
- SaRP SIP and RTP Proxy
  - *http://sarp.sourceforge.net*
  - written in Perl
- Siproxd SIP and RTP Proxy
  - *http://sourceforge.net/projects/siproxd/*
  - an proxy/masquerading daemon for the SIP protocol
- partysip
  - *http://www.nongnu.org/partysip/partysip.html*
  - Has a plugin to enable use of SCTP transport
- Yxa: Written in the Erlang programming language
  - *http://www.stacken.kth.se/projekt/yxa/*

…

SIP Tools

- Callflow
  - http://callflow.sourceforge.net/
  - Generates SIP call flow diagrams based on an ethereal capture file
- SIPbomber
  - http://freecode.com/projects/sipbomber
  - a SIP proxy testing tool for server implementations (i.e., proxies, user agent servers, redirect servers, and registrars)
- Sipsak
  - http://sipsak.org/
  - sipsak a comand line tool for developers and administrators of SIP applications
- PROTOS Test-Suite
  - https://www.ee.oulu.fi/research/ouspg/PROTOS_Test-Suite_c07-sip
  - SIP Testing tools from the "PROTOS - Security Testing of Protocol Implementations" project

SIP Clients

- kphone
  - http://sourceforge.net/projects/kphone/
  - IPv4 and IPv6 UA for Linux, also supports Presence and Instant Messaging
  - UA for Linux - for KDE
- Linphone
  - http://www.linphone.org/?lang=us&rubrique=1
  - UA for Linux - for GNOME
- CounterPath Corporation's X-Lite - free demo version for Windows and Linux
  - http://www.counterpath.com/x-lite.html
  - The also have a "Business-class SIP Softphone"
- minisip
  - http://www.minisip.org/
- …

Microsoft Lync

Unified communications:

- IM + presence
- Telephony
- Video conferencing
- Meetings
- Integration with Skype

http://office.microsoft.com/en-us/lync/

http://www.microsoft.com/sverige/lync/default.html (in Swedish)

CPL and Ontology extentions to SER

See:

- A. Devlic, “Extending CPL with context ontology”, In Mobile Human Computer Interaction (Mobile HCI 2006) Conference Workshop on Innovative Mobile Applications of Context (IMAC), Espoo/Helsinki, Finland, September 2006. http://www.it.kth.se/~devlic/article.pdf
- Sergi Laencina Verdaguer, “Model driven context awareness”, M.Sc. Thesis, School of Information and Communication Technology, Royal Institute of Technology (KTH), 28 January 2007

  http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/070130-Sergi_Laencina_Verdaguer-with-cover.pdf

Green VoIP

Currently VoIP gateways and devices run 24/7 365 days per year $\Rightarrow$ lots of power consumed

Can this be reduced?

- Goce Talaganov's recent M.Sc. thesis: Green VoIP : A SIP Based Approach [439] - looks at splitting the functions between a local lower power device that can power down for some part of the day
- Need to understand how to extend this to exploit Wake on LAN for all the many analog telephone gateways and other devices - How much power can be saved?

References and Further Reading

[436] http://www.google.com/search?q=%2BSIP&hl=en&lr=&ie=ISO-8859-1

[437] Amos Nungu, VoIP Service Provider (Internet Telephony Service Provider using SIP Protocol), Masters thesis, School of Information and Communication Technology, Royal Institute of Technology (KTH), April 2005

[438] Mohammad Zarifi Eslami, Masters Thesis, Department of Communication Systems, School of Information and Communication Technology, Royal Institute of Technology, December 2007
http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/071220-Mohammad_Zarifi_Eslami-with-cover.pdf

[439] Goce Talaganov, Green VoIP : A SIP Based Approach, Masters's thesis, KTH Royal Institute of Technology, School of Information and Communication Technology (ICT), Communication Systems (CoS), Stockholm, Sweden, Trita-ICT-EX-2012:162, July 2012, 130 pages,

http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-98795

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/120702-Goce_Talaganov-with-cover.pdf

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1
Module 21: Non-SIP applications

KTH Information and
Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:32

Skype

Skype™ Technologies http://www.skype.com/

- "Skype is free Internet telephony that just works."

Downloads	Simultaneous users	Date
562,405,650	52,400,993	2013.09.01 at 13:39 CEST
3,045,390,529	38,284,981	2012.08.23 at18:50 CEST
2,188,315,138	26,475,036	2011.08.16 at 17:00 MEST
2,438,790,535	18,386,099	2010.08.20 at 20:00 MEST
1,587,992,602	15,627,990	2009.08.19 at 17:20 MEST
844,062,744	11,306,336	2008.03.24
522,932,765	5,512,395	2007.03.27
	~9 million	2007.01.29
~200,000,000		2005.11.08
	> 5 million	2006.01.23 [440]

- in 2005: ~1 Million downloads/day, downloads at peak are ~0.5 Gbit/sec

Statistics as an RSS feed at: http://share.skype.com/stats_rss.xml updated every few minutes

L. De Cicco, S. Mascolo, and V. Palmisano have written a paper'A mathematical model of the Skype VoIP congestion control algorithm' [441] where they looking at how Skype changes it sending rate based upon packet loss rate.

Cisco's Skinny

Cisco's Skinny Call Control Protocol (SCCP) is used in Cisco's CallManager - a proprietary protocol between the CallManager and their VoIP phones. Audio is carried via RTP over UDP.

Skinny messages use TCP port 2000.[1]

Skinny was originally developed by Selsius Corporation.

1. The message types formerly could be found at http://www.javvin.com/protocolSCCP.html.

H.323 and MGCP

International Telecommunication Union (ITU-T)'s H.323

- further details at: http://www.h323forum.org/

Internet Engineering Task Force (IETF)'s Media Gateway Control Protocol (MGCP) defined in RFC 3435 [442] and updated by RFC 3661 [443]- used for controlling telephony gateways.

Asterisk

Asterisk is an open source PBX system, see http://www.asterisk.org/

Asterisk can function as a PBX (Switch), gateway, feature or media server.

Asterisk supports SIP, H.323, their own Inter-Asterisk Exchange (IAX) protocol, Media Gateway Control Protocol (MGCP), and Skinny Client Control Protocol (SCCP).

- Inter-Asterisk eXchange (IAX2) - a protocol for calls between Asterisk servers (also implemented by some IP phones) has replaced IAX.

For an example of a system implemented using Asterisk and SER see Max Weltz's thesis [444].

References and Further Reading

[440]Jaanus, “5 million online Skypers”, in News, Events, Milestones, Skype, January 23, 2006 http://share.skype.com/sites/en/2006/01/5_million_online_skypers.html, last modified March 12, 2006 14:05:25

[441]L. De Cicco, S. Mascolo, and V. Palmisano, ‘A mathematical model of the Skype VoIP congestion control algorithm’, presented at the 47th IEEE Conference on Decision and Control, 2008. CDC 2008., Cancun, 2008, pp. 1410–1415 [Online]. Available:

http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4739324 .

[442] F. Andreasen and B. Foster, Media Gateway Control Protocol (MGCP), Version 1.0, IETF RFC 3435, January 2003, Updated by RFC 3661.

http://www.ietf.org/rfc/rfc3435.txt

[443]B. Foster and C. Sivachelvan, Media Gateway Control Protocol (MGCP) Return Code Usage, RFC Editor, RFC 3661 (Informational), ISSN 2070-1721, December 2003 http://www.rfc-editor.org/rfc/rfc3661.txt

[444]Max Weltz, Dial over Data solution, Masters Thesis, Department of Communication Systems, School of Information and Communication Technology, Royal Institute of Technology (KTH), February 2008

http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/080221-MaxWeltz_ExjobbReport-with-cover.pdf

IK2554 Practical Voice Over IP (VoIP): SIP and related protocols
Fall 2013, Period 1

Module 22: Conclusions and your projects

KTH Information and Communication Technology

Lecture notes of G. Q. Maguire Jr.

Last modified: 2013.09.01:14:32

Conclusions

VoIP is both feasible and increasingly being adopted as a substitute for fixed line telephony (and as the basis for mobile telephony).

SIP is more complex that it first seemed, but it is still approachable.

Secure VoIP is possible, but like all security it takes effort.

There are lots of details, but there is also a lot of existing code, implementations, and documents.

Seven Myths About VoIP

Let us consider Steven Cherry's, "Seven Myths About Voice over IP: VoIP is turning telephony into just another Internet application - and a cheap one at that"[20]

Myth	Status
"VoIP is free"	Not quite, but given a flat rate Internet subscription the incremental cost is small.
"The only difference between VoIP and regular telephony is the price"	About the only thing they have in common is "voice" content and "calls".
"Quality of service isn't an issue nonadways, because there's plenty of bandwidth in the network"	latency, jitter, and packet loss can still matter, but over-provisioning goes a long way to avoiding probems
"VoIP can't replace regular telephony, because it still can't guarantee quality of service"	MPLS and QoS aware routing are used to provision VoIP services
"VoIP is just another data application"	Issues about providing 911, lawful intercept, etc.
"VoIP isn't secure"	SRTP + MIKEY + tunnels ==> very high security
"A Phone is a Phone is a Phone"	Modern phones are computers - with all the problems and advantages that brings!

VoIP service criteria today

The maturity of commerical VoIP service can be seen in the criteria being used (see for example [445]):

- **Ratings**: Overall Rating, Ratings, Service Plan and Fees, Features, Ease of Installation/Setup, Help/Support
- **Package + pricing**: Free Phone Adapter, Activation fee/ Setup fee, Cancellation fee
- **Service Plan fees & minutes**: Unlimited Minutes, Long Distance Calls (outgoing), Select International Calls, Free In-Network Calls, Business Plans
- **Basic calling features**: Voicemail, Caller ID, 3-Way Calling, Speed Dial, Call Waiting, Call Forwarding, Call Return (*69)
- **Enhancing calling features**: Call Transfer, Call Blocking, 911 Service, Do Not Disturb, Free 411 Directory Assistance, Find Me
- **Service features**: Keep Existing Number, Choose Area Code, Online Account Management
- **Additional services**: Add a Line, Softphone, Toll-Free Number, Directory assistance, Virtual phone number, FAX support, FAQ, Technical help/support, email/telephone help/support

VoIP maturity

Generations:

0 research

1 initial adoption

2 massive adoption and maturity
organizations replacing first generation VoIP solutions

3 ??? - what comes next?

An other sign of maturity - increasing regulation

The U.S. FCC requires VoIP service providers to [446]:

- provide E911 service
- pay universal service fees
- enable wiretaps (under CALEA)
- implement customer proprietary network information (CPNI) requirements

Your projects

Discussion of topics

Reminder: Write **complete references** and **do not use anyone else's work with out clearly identifying it!**

I encourage you to use Zotero and my style sheet:

http://www.ict.kth.se/courses/II2202/ExampleStyle-with-access.csl

For information about writing and oral presentation see the course notes for II2202 (available from *http://www.ict.kth.se/courses/II2202/II2202-Coursepage-2013.html*).

References

[445] VoIP Services Review 2011 - TopTenREVIEWS, TechMediaNetwork.com, 2011, http://voip-service-review.toptenreviews.com/

[446] Alex Goldman, How The FCC Killed VoIP, Internet Statistics: Blog Archive, 2011.02.06, http://net-statistics.net/wordpress/2011/02/how-the-fcc-killed-voip/