KUNGL
TEKNISKA
HÖGSKOLAN

M.Sc. Thesis

IP Telephony: A Swedish Perspective

Examiner: Prof. Gerald Q. Maguire Jr.

OSKAR BERGQUIST
780707-0110
obe@kth.se

MAGNUS SJÖSTEDT
790716-0415
msj@kth.se

June 27, 2003

To our families

Abstract

The aim of this Masters Thesis project is to give the Swedish National Post and Telecom Agency, Post- och Telestyrelsen (PTS), an updated view on IP Telephony relative to the Swedish consumer market. The basic questions were raised by PTS and the focus is on the relevant topics from the agency's point of view. PTS is primarily interested in understanding what state IP Telephony is in and furthermore what IP Telephony can be used for in practice. What are the possibilities of different implementations and what will be their advantages and disadvantages?

Despite being on the scene for many years, IP Telephony is now on the verge of a break through. With the creation of gateways between IP and PSTN, various IP Telephony devices, and with the introduction of SIP (described in RFC2543) as a standard signalling protocol, perhaps today, IP Telephony has a significant potential on the consumer market. Many argue that 2003 will be the year that IP Telephony blossoms.

The fact that anyone can be their own operator, the role of the traditional operator versus the new operators, the separation of content and signalling transmission, as well as the efficient use of bandwidth are some of the topics covered in this report.

Due to the introduction of The Electronic Communications Act that comes into effect the 25th of July 2003, replacing The Telecommunications Act and The Radiocommunications Act, much of the focus in this report lies on regulatory issues. However, in order to get an insight in to the regulatory issues it is important to understand the underlying technology of IP Telephony as well as areas such as security, robustness, privacy, and emergency calls. Through a market analysis, an updated overview of the market for IP Telephony will be given, along with plausible future scenarios.

This report will provide the reader with answers not by focusing on the theoretical details of the technology itself, but rather in terms of it's practical use and limitations.

Sammanfattning

Syftet med denna rapport är att ge Post- och Telestyrelsen (PTS) en uppdaterad bild av den svenska IP-telefonimarknaden för privatpersoner. Då examensarbetet utfördes för PTS togs de grundläggande frågeställningarna fram av myndigheten och fokus för examensarbetet lades således på ämnen relevanta för PTS.

Trots att IP-telefoni har varit på tapeten i flera år, har tekniken ännu inte haft sitt genombrott på privatmarknaden. Existensen av slussar mellan IP och PSTN, samt utvecklingen av IP-telefoniutrustning och standardiserade protokoll (såsom SIP beskriven i RFC2543), har givit IP-telefoni förutsättningen att ta en signifikant roll på den svenska privatmarknaden. Många anser att 2003 är året då IP-telefoni kommer att ha sitt genombrott.

Utvecklingen och ändringen av den traditionella operatörsrollen, separationen av signaltrafik och samtalstrafik samt den effektiva och variabla användningen av bandbredd, är några av de faktorer som ger upphov till spännande frågeställningar.

Introduktionen av lagen för elektronisk kommunikation som träder i kraft den 25 Juli 2003, och ersätter både telelagen och lagen om radiokommunikation, har gjort att fokus till stor del riktas på de regulativa frågorna inom området. För att sätta sig in i dessa regulativa frågor krävs dock god insikt i tekniken bakom IP-telefoni samt förståelse i områden såsom säkerhet, robusthet, QoS och nödsamtal. En marknadsanalys bidrar med en uppdaterad bild av marknaden för IP-telefoni samt möjliga framtidscenarion.

Rapporten förser läsaren med svar genom att fokusera på teknikens praktiska användning och begränsningar snarare än att fokusera på de teoretiska detaljerna.

Acknowledgements

First and foremost the authors would like to send their appreciations to their examiner Prof. Gerald Q. Maguire Jr. for his insightful criticism throughout their work.

The authors would also like to thank all those, too numerous to name, who have helped them make this report possible.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Problem Statement

The aim of this master's thesis is to give the Swedish National Post and Telecom Agency, Post- och Telestyrelsen (PTS), an updated view on IP Telephony relative to the Swedish consumer market.

The problem is divided in three general areas

- Technology
- Regulatory Issues
- Market and Services

This report covers the most common protocols used in applications within the area of IP Telephony. The actual technlogy that lies behind IP Telephony is a broad but not very complex to understand for someone with a portion of knowledge of general computer communication. It is not the technology itself that for so many years have prevented IP Telephony from obtaining a wide spread use on the consumer market. Rather, much of the problem consists of finding an accepted standard for protocols used in these various applications, that fulfill the requirements of the consumers. Unfortunately many people today relate IP Telephony with bad quality and high delay. Factors such as insufficient bandwidth and obstacles in the network such as Network Address Translators (NATs) have also limited the spreading of IP Telephony. Quite a few of the Swedish ISPs provide their customers with only one public IP address. The result is that when a customer connects an IP Telephony device, this device occupies the only public address they have available. This raises questions about how IP Telephony works with NAT, an area in which quite a lot of work has been done (*see Section 3.2.1*).

Today each IP Telephony provider who wants to provide PC-to-phone services must struggle with the cumbersome work of associating IP addresses and phone numbers especially when moving between computer and telecommunication networks (*see Section 3.3*).

Will there be essential players on the market to take the responsibility of guarding/providing the gateway between the IP world and the world of PSTN (*see*

Chapter 4)? How long will this business be significant? Maybe it is then necessary for the influential players on the market to expand and start supporting the protocols applicable for IP Telephony (*see Section 3.1*).

The market that emerged in 1993 following the deregulation and the breakup of Televerket needed, for the sake of both producers and consumers, some form of regulation. These regulations came via The Swedish Telecommunications Act [3] and The Swedish Competition Act [4]. The Swedish Post & Telecom Agency was appointed as supervisory authority, to work in the interest of consumers and to make sure everybody would play by the rules (*see Section 2.1*).

The basic idea of The Telecommunications Act is to maintain a market of free entry. Free entry implies that an entrant suffers no disadvantage in terms of production technique or perceived product quality relative to an incumbent firm, and that potential entrants find it appropriate to evaluate profitability of entry in terms of incumbents pre-entry prices. The Act imposes a notification duty on parties who wish to conduct certain activities in a public telecommunications network. The increasing use of IP Telephony challenges the old norms and definitions of the regulatory foundation of telecommunications and it creates ambiguity and a certain room for interpretation. How does The Telecommunications Act affect IP Telephony (*see Section 5.2*)?

Along with the mandatory notification of The Telecommunications Act comes a number of obligations. One of these is the obligation to provide the possibility of cost free emergency calls. Knowing the exact location of the customers is **not** a requirement under The Telecommunications Act, although it would help in the dispatching of emergency units. However, the bill for the new regulations for electronic communications (see below) requires, to the extent technically feasible, the provision of location data to the party receiving emergency calls. It remains to be seen how the market will resolve this, but due to customer mobility and the structure of the Internet it will be hard for operators to know the exact location of their customers (*see Section 5.4*).

From July 25 2003, a new regulatory framework for electronic communications will be applied in all Member States of the EU. The implementation of these directives will, in Sweden, replace The Telecommunications Act as well as The Radiocommunications Act [2]. The aim of the new regulations is to create a harmonised regulatory framework for electronic communications and electronic communications services. With this new legislation, focus will be shifted from mandatory license to a more light-weight notification duty, while still promoting competition by imposing harder obligations on players with Significant Market Power (SMP). What implications will this new framework have on IP Telephony (*see Section 5.3*)?

Services that are obvious and demanded by users in the traditional networks such as preselection and number portability are also services needed to (initially) be provided in order to survive in the hybrid world as an IP Telephony operator. Having these services properly set up, the development of new services utilising the new technology and devices would be the next step (see Sections 3.9 and 3.10). It will be possibility to provide services with at least the same quality, trustworthiness and simplicity, as customers were used to from the traditional services in PSTN. There will also be room for high-quality/expensive services

as well as low-quality/cheap ones. Consequently, a closer quality-price relation is possible on this new market, i.e. a "you get what you pay for" situation will arise.

Today, regulatory agencies as well as market players are shifting away from unilateral telecom reasoning. A change which is necessary to maintain a market of free entry and also to be prepared for and rapidly be able to respond to market changes. However, as concluded in Alberto Escudero's dissertation: European Union Data Protection Policy, Location privacy in the next generation mobile Internet[74] the classification and the definition of data by traditional means without taking into account Internet's multilayered architecture might lead to an insufficient level of privacy protection for certain sensitive data. By traditional means is meant the obvious separation of signalling and content since in POTS signals and data are (often) transferred in two different channels. However, the Internet Protocols utilise a multi-layered architecture and what can be seen as traffic/signalling for one layer can indeed be seen as content for another layer and what can be seen as signalling traffic for an observer can be seen as content for another; depending on the information that he or she is looking for. The dissertation further argues that if new infrastructures will still be considered in traditional ways, the data collected can be understood only by having the different technologies in mind, i.e. privacy aspects can not be technology independant.

1.2 What is IP Telephony

A traditional PSTN telephone voice channel normally provides a fixed 64Kb connection, using PCM-encoded voice, and routes the call over a single path [1].

IP Telephony uses packet technology which means that the voice traffic which is part of conversations is divided into IP packets, traversing the network not necessarily using the same paths and regrouping at the destination. However, there is a significant difference, between data and traditional telecom traffic. For data traffic it is often of uttermost importance that each packet that was sent arrive at the destination. In fact, we are willing to accept some delay in order for this to happen. For voice traffic we can afford loosing a few bits (or even packets) here or there as long as the majority of the packets arrive on time. A certain delay is inevitable due to physical propagation, but it is important that this delay be bounded. For IP Telephony, unlike the fixed voice encoding used in PSTN, one can choose different compression techniques by using different compression/decompression (codecs) techniques, hence increasing or decreasing the quality of the conversation versus the bandwidth used. There are many codecs on the market today and a large number have been standardised. Using various codecs together with voice activity detection makes IP Telephony more efficient than traditional telephony concerning bandwidth on one hand, but also more variable when it comes to the quality perceived on the other hand.

With IP Telephony, if one feels that he or she wants to place a call with better quality and can afford the bandwidth for doing so, he or she has this possibility by selecting an appropriate codec, forward error correction scheme, using traffic shaping, etc. In general, one is free to choose the codec depending on the service to be provided. Depending on the features of the device the codec must be set either before the call, i.e. the device connecting must know which codec

the called device uses in order to place the call or if the device supports codec negotiation, it can connect to another device without necessarily knowing which codec will be used, but can negotiate this at call-setup, this is also known as automatic codec negotiation.

In the old days, people used to shrug their shoulders if their Internet connection did not work for a while, but when they lifted the handset of a phone connected to the fixed network they always expected to have a reliable, high-quality voice service available. Today, as the use of IP networks is widespread, much higher demands are placed on factors such as network reliability and quality. Some even argue that IP network reliability is now **higher** than PSTN reliability.

IP Telephony is found somewhere on the frontier between the two worlds of telecommunications and datacommunications and therefore the struggle of which protocols to use as a new standard to serve IP Telephony is not yet completely solved. A number of protocols have been developed by different camps to address the need for real-time session signalling over packet-based networks. As of today, there are two major standard protocols, H.323 and its set of components and the Session Initiation Protocol (SIP).

The International Telecommunication Union Telecommunication Standardisation Sector (ITU-T) developed H.323, a family of components related to the telecommunication industry. H.323 uses a number of binary protocols to set up a call. First of all, a supported client queries an H.323 gatekeeper for the address of another client. The gatekeeper retrieves the address and forwards it to the client, which then establishes a session with the new client using H.225. Once the session is established, another H.323 protocol, H.245, negotiates the available features of each client. The use of gatekeepers in H.323 networks is optional, although valuable since monitoring of the calls by the gatekeeper provides better control of the calls in the local network. Alternatively, clients can send call signalling messages directly to the peer endpoint(s). Because H.323 must first establish a session before it negotiates the features and functions of that session, call setup can take a long time. The amount of delay will depend upon the type of network because the different components that need to negotiate with each other can take several seconds. Depending on whether the gatekeeper is present or not a call setup can take about 6-7 Round Trip Times (RTTs), but using H.323 (version 2 or newer) with "Fast Connect" which may use a single exchange can reduce the delay to 2.5 RTTs [26, 27, 28, 29, 30, 43]. The actual RTT in ms obviously depends on factors such as what kind of network that is used- as well as the network load at the time the measurement is performed.

The Internet Engineering Task Force (IETF) developed the Session Initiation Protocol (SIP), a text based protocol for initiating interactive sessions between users. SIP reuses many of the familiar Internet elements such as RTP, RTCP, HTTP, SMTP, etc. Unlike H.323, SIP handles only the signalling and control, enabling it to to establish, modify, and terminate multimedia sessions. For describing the multimedia sessions SIP uses the Session Description Protocol (SDP) and hence call setup and the media transfer are separated, a little bit like that of traditional telephony. SDP is carried in the message body of SIP and is more of a session description than a protocol. It is a textual description that provides many details of the multimedia session, such as the originator of the session, a URL related to the session, the connection address for the session media(s), and other optional attributes. SDP also support use of IPv6 addresses

(see Section 2.6 for futher details of SIP).

For traditional telephony the ITU-T developed the Signalling System no.7 (SS7), a signalling system logically separated from the transmission network. SS7 is a packet switched signalling system which handles call setup (among other things) but also it prevents (or at least attempts to prevent) fraudulent network usage. The SS7 system generally terminates at the local exchange, thus it is not available to users' end-points [47].

In traditional telephony the network operator controls both the exchange of content and the call setup, where as in IP Telephony the SIP operator need not be involved in the media transfers. Hence, when using SIP one could imagine a separate IP Telephony operator who never carries any content. Some argue that pure traditional telecom operators who do not embrace new technologies such as IP Telephony will have a hard time surviving in the emerging market. This is especially true as most such operators charge based on the duration of the media session, often weighted by the physical distance between the end-points. While a SIP operator might only charge for use of their gateway to the PSTN and a monthly base fee.

Whereas SIP has been adopted by 3GPP (3G Partnership Project) and companies like Digisip [49], some software clients like Gnome Meeting [48] stick to H.323. Microsoft's Windows XP operating system included shifted from H.323 to SIP as the signalling protocol for its new, converged messaging application called Messenger [50].

Many people have argued that SIP is the right choice for the future, due to its uncomplicated structure and close relation to the Internet world. This is clear from the many SIP products coming onto the market (*see Section 3.10*).

A common solution for some companies providing IP Telephony services today is the use of proprietary protocols, hence diverging from the standards. This obviously limits calls between different operators unless there are gateways to enable the translation between the different protocols. For example, Cisco's proprietary SKNY protocol can be gatewayed to networks using other protocols.

To summarise, IP Telephony is the transport of communication services - voice, facsimile, and/or other traditional voice-based services - over IP based networks. However, there is a mixture between the common terms used within this area. Internet Telephony and VoIP are also often used to describe this communication transport. According to the ITU [34], IP Telephony takes place over IP based networks in general; while Internet Telephony, a subset of IP Telephony, is for communication between devices entirely or partially over the Internet. While, VoIP, another sub-set of IP Telephony, is frequently used to denote communications within private managed IP-based networks. Although, a mixture of the three terms are often generally referred to as "Internet voice" or "VoIP" *(see Figure 1.1)*. In spite of these somewhat fuzzy definitions, the focus should be on the specifics of the **service** being offered.

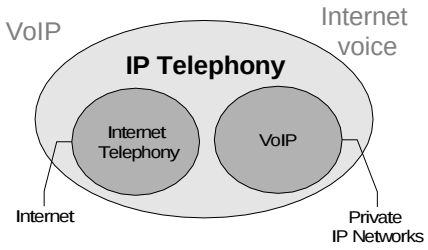

Figure 1.1: *Schematic Representation of the Terminology of IP Telephony*

1.3 Why IP Telephony

IP Telephony represents the next generation of telecommunication services. As the price for IP Telephony equipment decrease it rapidly becomes more cost competitive, thus providing many reasons for customers to switch from traditional telephony to IP Telephony:

- Money saving, especially on long distance calls
- The supply and variety of services will increase, as anyone can offer services!
- Possibility of multiple conversations simultaneously for the same price (i.e., conferencing)
- Flexibility (for users, devices, and sessions)
- Mobility (for users, devices, and sessions)
- Cost savings due to utilising a single infrastructure for both voice and data
- Scalability

In IP Telephony synergistic effects can also be produced by utilising the existing knowledge base that exists within the telecommunication and computer networking community.

1.4 History of IP Telephony

Many people argue that the start of IP Telephony on a user level came with Vocal Tec's[54] introduction of their first version of the Internet Phone in 1995 although mixing voice and data on a LAN goes back all the way to 1983 when experiments around this were carried out at AT&T Bell Laboratories[51] and the first paper on secure packet network voice was as early as March 1964 [52]. After the release of Vocaltec's software numerous players entered the market and in conjunction with the information technology expansion the Internet Telephony Consortium (ITC)[55] was created in 1996.

Despite being on the scene for many years, IP Telephony is now on the verge of

a break through. For example, in April 2003, Nässjö's local government moved completely to IP Telephony [53]. With the creation of gateways between IP and PSTN, together with other IP Telephony hardware, and with the introduction of H.323 and SIP as standard protocols, perhaps today, IP Telephony has significant market potential. Many argue that 2003 will be the year that IP Telephony blossoms.

Chapter 2

Background

2.1 The Convergence

As the development of electronic communications moves forward, the borders between initially separated sectors such as information technology, telecom, and media begins to blur. This phenomena is known as *the convergence* [11]. The convergence occurs within four main sectors: networks, services, devices, and markets. The service and device convergence are partially consequences of the network convergence. Based on this the prerequisites for a market convergence were created.

Network Convergence

Networks originally intended for different purposes and traditionally separated can now carry the same services. As an example, you can get Internet access from your cable TV network as well as through your power lines. The Internet plays an intricate role in the convergence process, as many traditional infrastructures are, so to speak, entangled in the web.

Service Convergence

Services can roughly be divided into two categories: communications services and content services. Communications services are services which conveys information between users, such as e-mail and telephony. While content services are services which provides or conveys content for others to take part of. Content services can be seen as one-way communications services, such as television and some web-sites. The service convergence is the merging of these two types of services.

Device Convergence

Device convergence means the merging of different devices with different functions. Devices that are able to handle all kinds of information and services, such as computers can function as TV receivers and mobile phones can function as advanced information processors.

Market Convergence

The network convergence as well as the service and device convergence can all be seen as direct effects of the development of technology. While market conver-

gence is more of an effect following the convergence in the other three sectors. The convergence in networks, services, and devices gives incentives and in some cases even makes it necessary for players on one market to engage in business in other adjacent markets.

IP Telephony is involved in all four sectors of the convergence process. Additionally, IP Telephony has one foot in telecommunications and the other in datacommunications, and the convergence is bringing them together.

2.2 The Swedish National Post & Telecom Agency

In 1993 the monopoly market of Swedish telecommunication was abolished and the operating arm of Televerket was converted into Telia AB while the regulatory arm became The National Post & Telecom Agency (PTS). This produced a transition period often referred to as the deregulation of the Swedish telecommunication market, even though the market shifted from an unregulated state monopoly (the market was, more or less, open to new entrents, but the barriers to entry, due to Televerket's possesion of the infrastructure for telecommunications, were far too great. Moreover, Televerket had to approve the use of all equipment in order for it to be connected to their network) to regulated competition. As a tool to regulate this free market, The Competition Act [4] and The Telecommunications Act [3] were passed. The Government appointed The Swedish National Post & Telecom Agency, and to some extent The Swedish Competition Authority, to act as the supervisory authorities on these matters.

> The Swedish National Post and Telecom Agency, Post- och Telestyrelsen, PTS, is the authority that supervises activities in the radio, telecom and datacom areas. Its goal is for everyone in Sweden to have access to effective and reasonably priced postal and telecom services, and to ensure that the radio spectrum is used in the best possible way. ... It is essential that everyone should have access to postal and telecom services, which should also function properly in the event of crises or military emergencies. Our work therefore also covers emergency planning, as well as looking after the interests of the disabled. [5]

This can be broken down into three main objectives:

- Promote competition to result in reasonable prices for all
- Promote efficient use of radio resources
- Work in the interest of consumers while providing for essential public purposes

The Swedish market for telecommunication is open for domestic as well as foreign actors. In order to conduct activities in this market notification needs to be sent to the supervisory authority, according to section 5 in The Swedish Telecommunications Act.

2.3 To the Reader

This report is primarily intended to be read by employees at PTS as well as individuals with a special interest in IP Telephony.

The reader should be acquainted with the interactions in the current market of electronic communication and possess basic knowledge in telecommunication and computer communication. Insight into The Telecommunications Act, The Electronic Communications Act, and other related legislations is also advantageous in order to understand the interaction between players, customers, and the supervisory authority.

There has been no prior work on IP Telephony by PTS. However, outside of PTS a lot has already been written about this topic: including professional market forecasts and reviews of end-user hardware and software. This work will be cited as necessary.

2.4 Why is this Problem Worth a M.Sc. Thesis Project?

The area of IP Telephony in the Swedish market is extensive and also raises a number of pressing social, political, and technical issues. So in order to answer the questions that arise we must use our ingenuity as well as our technical know-how.

Shedding light on topics such as security, robustness, and regulatory issues requires insight into a number of areas. Familiarity with the structure of the telecom market, in addition to a solid technical competence, provides the foundations that are necessary to achieve comprehensive results regarding the subject of IP Telephony. Completing the project requires observing and analysing the market regulations from a technical as well as a legal perspective.

The level of maturity of both the market and technology is continuously rising. At this moment we've hopefully reached a level where we can provide a balanced and relevant evaluation of the status of IP Telephony in Sweden.

Chapter 3

Technical Aspects

3.1 Protocols and Codecs

There is a broad variety of protocols that exist on the market today. Most of them serve specific tasks within the Voice over IP world but frequently, more than one protocol can serve the same purpose, i.e. they are in some sense competitors. The choice of which protocols to include in the scope of this document has not been an easy one. However, the choice that has been made is mainly the result of applying the three following criteria:

- Widespread use of the protocol
- Importance of applications using the protocol
- The expected future use of the protocol

The section further describes the standardised family of ITU-T recommended codecs called H.32x.

3.1.1 From Where does SIP Evolve?

The Session Initiation Protocol (SIP) was developed by the IETF Multiparty Multimedia Session Control (MMUSIC) working group and since September 1999 the IETF SIP working group. 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. The Session Initiation Protocol (SIP) WG[56] is chartered to continue the development of SIP. Throughout its work, the group strives to maintain the basic model and architecture defined by SIP. In particular:

- Services and features are provided end-to-end, whenever possible (unlike traditional telephony).
- Extensions and new features must be generally applicable, and not applicable only to a specific set of session types.
- Simplicity is the key.

- Reuse of existing IP protocols and architectures, and integrating with other IP applications, is crucial.

The SIP WG has created a draft standard version for SIP along with a number of other deliverables [56]. SIP is defined in RFC3261[16] (which updates the previous definition, RFC2543) and provides application layer signalling.

3.1.2 The SIP Protocol

The protocol is used to establish, modify, and terminate multimedia sessions. SIP (*see Figure 3.1*) is a HTTP-like textual protocol that can utilise UDP, TCP, TLS, SCTP, etc. as underlying transport. It uses Uniform Resource Indicators (URIs) to designate calling and called parties. SIP is an alternative to H.323, and comprises a set of components, protocols, and procedures that provide multimedia communication services such as real-time audio, video, and data communications over packet networks. H.323 was proposed by ITU-T before IETF developed SIP and SIP covers only the signalling parts of H.323. SIP provides the ability to discover remote users and establish interactive sessions. It can run directly on top of any protocol offering reliable or unreliable byte stream or datagram services whereas H.323 requires the use of a reliable transport protocol. SIP itself does not provide QoS. It uses SDP (Session Description Protocol) to provide information about a call (*see Section 3.1.6*).

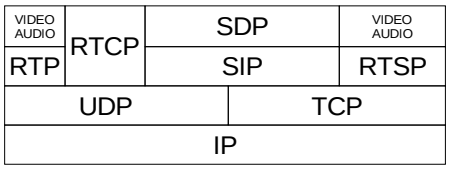

Figure 3.1: *The SIP Stack*

SIP Request Types and Responses

The SIP request types are called methods and in its basic specification SIP includes the following six requests: **INVITE, ACK, OPTIONS, CANCEL, BYE,** and **REGISTER**. SIP responses use a numerical code (*see Table 3.1*).

SIP status codes are similar to HTTP's status codes. Additional SIP methods beyond those defined in the basic specification have been defined in other RFCs. For more information on SIP extentions and features see the Internet Draft "Guidelines for Authors of Extensions to the Session Initiation Protocol (SIP)" by J. Rosenberg and H. Schulzrinne[71].

SIP URIs

The SIP URIs have the same form as e-mail addresses, i.e. user@domain and there are two different URI schemes for usage with SIP. The first and the most

Response Code	Response Type
1XX	Informational
2XX	Final
3XX	Redirection
4XX	Client error
5XX	Server error
6XX	Global failure

Table 3.1: *SIP Responses and Requests[17]*

common one, introduced in RFC2543 is of the form:

sip:magnus@sip.brothas.net

The second, newer scheme, introduced in RFC3261 is a secure SIP URI of the form:

sips:oskar@sip.brothas.net

SIPS requires TLS over TCP for transport security. Furthermore, there are two types of SIP URIs depending on whether you want to contact a specific user or a specific device. The Address of Record (AOR) identifies a user, e.g. magnus@sip.brothas.net and consequently needs DNS SRV records to locate SIP Servers for the brothas.net domain. The Fully Qualified Domain Name (FQDN) identifies a specific device, e.g. magnus@213.89.184.7 where the IP address corresponds to a device that supports SIP.

The first step in routing a SIP request is to compute the mapping between the first form of URI and a specific user at a specific host/address although there is no need to compute the mapping when a device is already identified. This is a very general process and the source of much of SIP's power, providing support for mobility and portability. It can be done utilising: DNS SRV lookup, ENUM, or Location Server lookup.

3.1.3 A SIP Message in Detail

A simple SIP timeline datagram (*see Figure 3.2*) consists of an INVITE message, the media transmission, a BYE message, and several acknowledgements.

The corresponding SIP INVITE message in textual format, and how it looks like when it is transmitted in practice is discussed in this section.

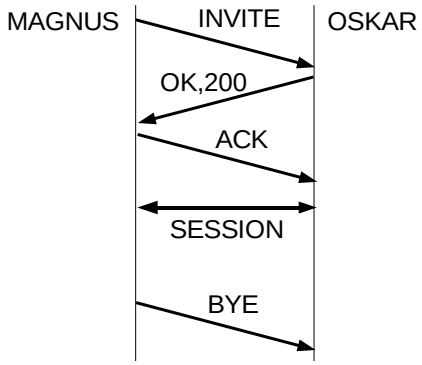

Figure 3.2: *A Simple SIP Timeline*

An example of a SIP INVITE message from Oskar (User ID 1001) to Magnus (User ID 1000) follows:

SipClient: Receiving message...

SipClient: Received: 09:44:10.127

INVITE sip:magnus@213.89.184.107 SIP/2.0
Via: SIP/2.0/UDP 213.89.184.200:5060;branch=bebff297cf7d976ff48c6ed63113c64b.4
Via: SIP/2.0/UDP 213.89.184.200:5060;branch=baf03c837903910f1f102797acc25565.2
Via: SIP/2.0/UDP 213.89.185.178:5062
To: <sip:1000@213.89.184.200>
From: "Oskar" <sip:1001@213.89.184.200>;tag=6F348680
Call-ID: 1921023076@213.89.185.178
CSeq: 1168 INVITE
Max-Forwards: 69
Subject: sip:1001@213.89.184.200
Record-Route: <sip:magnus@213.89.184.200:5060;maddr=213.89.184.200>
<sip:1000@213.89.184.200:5060;maddr=213.89.184.200>
Contact: <sip:oskar@213.89.185.178:5062;transport=udp>
User-Agent: KPhone/3.11
Content-Type: application/sdp
Content-Length: 189

v=0
o=username 0 0 IN IP4 213.89.185.178
s=The Funky Flow
c=IN IP4 213.89.185.178
t=0 0
m=audio 32988 RTP/AVP 0 97 3
a=rtpmap:0 PCMU/8000
a=rtpmap:3 GSM/8000
a=rtpmap:97 iLBC/8000

SipClient: Searching for a user
SipClient: Creating new call for user "magnus" <sip:1000@213.89.184.200>
SipCall: Incoming request
SipCall: New transaction created
SipTransaction: Incoming Request
SipClient: Sending UDP Response
SipClient: Sending to '213.89.184.200' port 5060
SipClient: Sending: 09:44:10.129

Method or request type: the first component on the first line of a SIP message contains the method or request type, in the above case INVITE. See table 3.1 for the methods and request types defined in the basic specification. The request-URI indicates who the request is for, in this example sip:oskar@200.201.202.203. The last component of the first row shows the version number. In this case the SIP version number is SIP/2.0.

Via headers: These headers show the path the request has taken in the SIP network. The bottom via header is inserted by the User Agent which initiated the request. The top via headers are inserted by proxies in the path. The Via headers are used to route responses back the reverse of this path.

Max-Forwards: a counter decremented by each proxy that forwards the request. When the counter reaches zero, the request is discarded and a "Too Many Hops" response is sent.

To header field: contains the address-of-record whose registration is to be created or updated. The To field may not be re-written by proxies [15].

From header field: contains the address-of-record of the person responsible for the registration. For first-party registration, it is identical to the To header field value [15].

Request-URI: This URI could be a SIP URL or a general URI. It indicates the user or service to which this request is being addressed. Unlike the To field, the Request-URI may be re-written by proxies [15].

Call-ID: a number is a globally unique identifier. It uniquely identifies the session and is of the form: string@hostname or IP address.

CSeq: The Command Sequence (CSeq) Number is initialised at the start of the call. It is incremented for each subsequent request and used to distinguish a retransmission from a new request. The CSeq number is followed by the request (SIP method). Registrations with the same Call-ID are consequently obliged to have increasing CSeq numbers although the server does not reject out-of-order requests.

Contact header field: The request may contain a contact header field. Future non-register requests for the URI given in the "To header" field should be directed to the address or addresses given in the contact header[15].

Content-Type: indicates the type of message body attachment, in this case SDP. Other types could be: text/plain, application/cpl+xml, etc.

Content-Length: indicates length of the message body in octets (bytes). A content-length of 0 bytes indicates that there is no message body.

Next follows some session properties such as what kind of content data that is to be sent (in this case it is plain audio) and which codec that is to be used (in this case we use the G.711 μ-law 64 Kbps Codec) and finally the message shows how the clients creates the call and sends the message on to the registrar (IP 213.89.184.200).

3.1.4 Components in the SIP Network

The general basic components in a SIP network *(see Figure 3.3)* will be discussed. The SIP user agents are capable of sending and receiving SIP requests and are usually also the devices that originate the SIP requests. SIP user agents (UAs) consist of two parts: User Agent Clients (UACs) which initiate SIP requests and User Agent Servers (UASs) which respond to SIP requests. Examples of SIP clients could be: SIP phones, PC/Laptops and PDAs with SIP software clients, etc. The PSTN Gateway is also a user agent. SIP Proxy Servers can be either outbound or inbound and forward (proxy) requests closer to the destination on behalf of other user agents. Outbound proxy servers are used by a UA to route an outgoing request and inbound proxy servers are servers that support a domain by receiving incoming requests. These proxy servers can be either transaction- and/or call stateful, which means they remember their queries and answers, and can also forward several queries in parallel or they can be stateless, which means they ignore SDP and do not handle any media content.

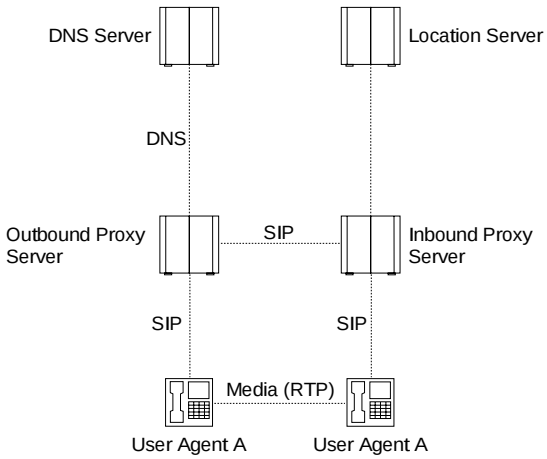

Figure 3.3: *The Basic Components of a SIP Network*

A SIP redirect server directs the client to contact an alternate URI[15]. It works by mapping the address into zero or more new addresses and returning these addresses to the client. Unlike a proxy server, it does **not** initiate its

own SIP requests. Unlike a user agent server, it also does not accept calls. A registrar is a server that accepts REGISTER requests[15]. A registrar is typically co-located with a proxy or a redirect server and *may* offer location services. When the registrar receives the SIP REGISTER request it updates the Location Server (LS). UA registering (i.e. the process and the need to register) will be described further in the report. The LS contains a database of the locations of SIP User Agents and is queried by SIP proxies when they route SIP messages. As mentioned previously, the LS is updated when UAs registers. However, SIP can also uses DNS SRV (Service) Records to locate inbound Proxies.

3.1.5 Locating a Callee

If A attempts to contact B when B is not registered A will be notified that B has not signed in. Similarly A can ask to be told (notified) when B signs in. A device in the SIP network registers in order to establish their current device and location. Only the LS they "belong to" needs to know this information. The LS can also use policies to limit the distribution of the location information rather than giving it out to everyone.

3.1.6 SDP

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

SDP is a textual protocol carried as a message body in SIP messages. SDP specifies the Real-time Transport Protocol (RTP) to be used subsequently to transfer media packets over IP[72]. SDP itself is defined by RFC2327[84] which was updated by RFC3266[85] in June 2002. RFC3266 describes, among other things, how SDP also supports the use of IPv6 addresses. SDP is carried encoded in MIME as a message body in SIP messages.

A successor of SDP, called SDPng has been developed by the MMUSIC Working Group. Its use has been expanded to include, among other things, media description for SIP-initiated multimedia sessions and particularly IP telephone calls. SDPng uses XML syntax and could be seen as designed to address the major flaws of SDP.

3.1.7 SAP

The Session Announcement Protocol (SAP) is primarily intended for initiating multicast multimedia sessions and to provide information needed for session setup for the presumptive participants[58]. RFC2974 defines SAP and states that:

> In order to assist the advertisement of multicast multimedia conferences and other multicast sessions, and to communicate the relevant session setup information to prospective participants, a distributed session directory may be used. An instance of such a session directory periodically multicasts packets containing a description of

the session, and these advertisements are received by other session directories such that potential remote participants can use the session description to start the tools required to participate [58]

The SAP announcer periodically multicasts an announcement packet to the scope of the session it announces, thus a SAP listener listens to the scopes it is within and learns about upcoming sessions.

3.1.8 H.323

H.323 is a standard that specifies the components, protocols, and procedures that provide multimedia communication services - realtime audio, video, and data communications - over packet networks, including IP based networks. H.323 is part of a family of ITU-T recommendations called H.32x that provides multimedia communication services over a variety of networks [70]. The different components described by the H.323 standard are summarised in the Table 3.2

Component	Description
H.323	System document
H.225.0	Handles call control, signalling, and synchronisation of media streams
H.245	Handles opening and closing channels for media streams
H.450.x	Defines signalling and procedures used to provide telephony-like services
H.235	Defines the security framework (authentication, encryption etc.) to H.323 systems
H.332	Provides large scale, or loosely-coupled conferencing based upon H.323
H.261	Video codec for audiovisual services at P x 64 Kbps
H.263	Specifies a new video codec for video over POTS
G.711	Audio codec, 3.1 KHz at 48, 56, and 64 Kbps (normal telephony)
G.722	Audio Codec, 7 KHz at 48, 56, and 64 Kbps
G.723	Audio Codec, for 5.3 and 6.3 Kbps modes
G.728	Audio Codec, 3.1 KHz at 16 Kbps
G.739	Audio Codec, 8 Kbps audio code

Table 3.2: *Components of H.323*

The absence of an existing standard for voice over IP resulted in products that were incompatible which in turn resulted in the first version of H.323 in October 1996. Some of the basic devices in the H.323 standard are similar to those components that constitutes the basic structure of a SIP network. H.323 specifies four different kinds of components that provide point-to-point and point-to-multipoint multimedia services when networked together

- Terminals (end-devices on the network such as PCs, stand-alone devices running an H.323-stack, or applications supporting H.323. The terminals are required to support RTP/RTCP since H.323 uses this protocol to transmit audio and video packets).
- Gateways (provides connectivity between an H.323 network and a non-H.323 network, e.g. between an H.323 terminal and the PSTN).

- Gatekeepers (the most important of the four components in the network, acts as the central point for all calls within its zone and provides call control services for registered H.323 endpoints).
- Multipoint Control Units (MCUs) (provides support for three or more H.323 terminals. The MCU consists of a Multipoint Controller (MC) that negotiates codec and manages conference resources, and zero or several Multipoint Processors (MPs) that take care of the media streams).

H.323 Version 4 was approved in November 2000 and contained enhancements in a number of important areas, including reliability, scalability, and flexibility.

3.1.9 SIP vs. H.323

As described above, SIP and H.323 provides a similar set of services. In the recent years though, SIP has surpassed H.323 as the number one IP Telephony protocol. This section will compare the two protocols on complexibility, extensibility, scalability and features. Moreover it will present a table that describes the major differences between the two protocols.

Complexity

H.323 defines hundreds of components while SIP defines only 32 headers in its base specification and 5 headers in the call control extensions. Using four headers (To, From, Call-ID, and CSeq, all described above) and three request types (INVITE, ACK, and BYE, all described above) a basic SIP IP Telephony Implementation can be created. As opposed to SIP's textual format, H.323 uses binary representation for its messages and hence it requires special code-generators to parse and disallows manual entry and reviewing of messages. Also, H.323's complexity arises due to the great number of components it includes and their need to interoperate since many services require interactions between several of them. As an example call forwarding uses H.450, H.225.0, and H.245. SIP, on the other hand, uses a single request that contains all necessary information. Another problem with H.323 is the duplication of services. As described previously H.323 makes use of RTP/RTCP for handling media content. As an example, RTCP itself provides various conference and feedback control functions with great scalability at the same time as H.245 provides its own simple mechanisms for the same purpose. Obviously the latter becomes redundant, hence causing service duplication.

Extensibility

The topic of extensibility is a key metric for IP Telephony protocols as the features provided evolve quickly over time as new application are developed. SIP has built in a rich set of compatibility functions. Unknown headers and values are ignored by default and instead clients can, using the Require header, indicate features that the server **must** support. The server checks the features included in the Require header and if any of them are not supported it returns and error code and a list of the features it does not understand. The feature names are hierarchical and can be registered with Internet Assigned Numbers Authority

(IANA)[73] and consequently any developer can create new features in SIP. Also, the textual encoding in SIP means that header fields are self-describing. Header field names like "To", "From", and "Subject" are self-evident and hence as new header fields are added, developers on the outside can determine their usage just by the name, and add support for the field if they want. Finally, SIP is similar to HTTP and consequently HTTP extensions mechanisms can be reused also for SIP. H.323 also provides extensibility mechanisms. However, these are somewhat limited partially due to the fact that H.323 has no mechanism for letting terminals exchange their support for different extensions. In addition, H.323 requires full backward compatibility for previous versions which means as features come and go the size of the protocol will only increase. SIP allows older features and headers to disappear as they are no longer needed keeping the protocol clean. Another aspect of extensibility is modularity. SIP is reasonably modular since it includes only basic call signalling, user location, and registration. Advanced signalling, for example, is part of SIP but within a single extension. H.323 on the other hand, defines an integrated protocol suite for a single application. H.323 encompasses everything from basic call signalling, to QoS, capability exchange, etc, all intertwined with the various sub-protocols of H.323, which makes it less modular than the SIP protocol. SIP's modularity can be used in conjunction with H.323, by e.g. letting a user locate another user using SIP and after this letting the actual communication taking place with H.323.

Scalability

Scalability differs between the protocols in a number of different levels:

- Large Number of Domains (H.323 was originally designed for use on a single LAN and even if a newer version of H.323 defines the concept of a zone, H.323 has scalability problems for large numbers of domains)
- Server Processing (both in H.323 and SIP systems, gatekeepers and SIP servers respectively, and gateways will be required to handle an eventual large number of calls. Furthermore, SIP transactions can be either stateful or stateless and carried over TCP and UDP where in the latter case, no connection state is required, hence requiring less processing by the server and improving scalability. H.323 requires gatekeepers to keep call state for the entire duration of a call and also, since connections are TCP based, the gatekeepers must also maintain its TCP connections for the entire call, eventually posing scalability problems for large gatekeepers.
- Conference Sizes (H.323 does support multiparty conferences, thus requiring a central control point (MC) to process the signalling, even for the smallest conferences. Since MC functionality is optional in H.323 even three party conferences are sometimes not supported. Also, in the case of a conference, should the user who provides the MC functionality quit for some reason, the entire conference will be terminated. Although not directly included in SIP, the protocol scales to all different conference sizes and there is no requirement for a central MC.)
- Feedback (H.245, H.323's control channel protocol, includes procedures for receivers to control media encodings, transmission rates and error recovery.

This kind of feedback is valuable for a two-party point-to-point conference, but looses its functionality for multipoint conferencing. SIP, instead, relies on RTCP for feedback and the feedback RTCP provides scales from a two person point-to-point conference to huge style multicast conferences.)

Services

A comparison of the support for different services by the two protocols is somewhat difficult since this is constantly changing as new services are created. However, one can draw a couple of conclusions even so. Both SIP and H.323 provide, in addition to call control services, capability exchange services. Concerning this type of service, H.323 provides a much richer set of functionality. However, SIP provides richer support for personal mobility services i.e. the redirection of a callee to different locations and caller preferences about e.g. the nature of the terminal to be contacted. H.323 also supports different conference control services (as discussed previously) whereas SIP relies, instead, on other protocols for this service.

A Comparison

Although the comparison of H.323 and SIP in the previous sections gives an overview of the differences between the two protocols there are a few additional features viewing their difference also important to take into consideration (*see Table 3.3*)

Feature	SIP	H.323
Encoding	Textual	Binary
Call setup delay	1.5RTT	1.5RTT (optimal)
Complexity	Low (see previous discussion)	High (see previous discussion)
Extensibility	High (see previous discussion)	Low (see previous discussion)
Scalability	High (see previous discussion)	Low (see previous discussion)
Architecture	Modular	Monolithic
Instant Message Support	Yes	No
Firewall Support	Adequate	Adequate
Addressing	Any URL	Host or gatekeeper-resolved alias
Transport protocol	UDP,TCP, and STCP	UDP and TCP
Inter-domain call routing	Hierarchically by DNS	Statically by Annex G/H.323

Table 3.3: *Comparison of H.323 and SIP[30]*

3.1.10 RTP and RTCP

The Real-Time transfer Protocol (RTP) was approved as an Internet standard in late 1995 and is defined in RFC1889 and RFC1890. RTP was developed to provide end-to-end network transport functions and features for applications with real-time properties such as audio, video or simulation data. It provides a mechanism to time-stamp packets so that random delays resulting from other factors on the network can be compensated for by the use of buffers at the destination locations, hence redistributing the packets. Although a flexible protocol,

RTP does not provide any QoS guarantees, but rather, it relies on lower-layer services to do so. The resource ReSerVation Protocol (RSVP), also explained in this report, can be mentioned here, as it provides the mechanism to reserve network resources that are necessary to transport real-time traffic carried by RTP. However, the actual monitoring of the content transmitted via RTP is done by the Real-Time Control Protocol (RTCP) to provide minimal control and identification functionality. RTP itself only serves to carry data that has real-time properties. Both RTP and RTCP, however, are designed to be independent of the underlying transport and network layers. Unlike other protocols, RTP is intended to be malleable to provide the information required by a particular application. Hence the RTP protocol framework as standalone is not complete but rather it is completed by additions and modifications to the header as needed. Consequently, RTP for a particular application will require one or more companion documents, for example, a profile specification document, which defines a set of payload type codes and their mapping to payload formats (e.g. media encodings etc) and a payload format specification document, which defines how a particular payload, such as an audio or video encoding, is to be carried in RTP. This often results in an integration of it into the application processing rather than as a separate layer. If it turns out that additional functionality is needed to all profiles, a new version of RTP should be defined to make permanent changes to the fixed header [47][72].

3.1.11 RTSP

The Real Time Streaming Protocol (RTSP), defined in RFC2326[81] is an application-level protocol for control over the delivery of data with real-time properties. RTSP provides a framework to enable controlled delivery of real-time data, such as audio. The purpose of the protocol is to provide a means for choosing delivery channels such as UDP, multicast UDP and TCP, and provide a means for choosing delivery mechanisms based upon RTP and the protocol supports the following operations:

- Retrieval of media from media server
- Invitation of a media server to a conference
- Addition of media to an existing session

As RTSP is only a tool for controlling audio (or video) streams it does not typically deliver the media streams itself. Further, RTSP does not depend on the underlying transport mechanism and streams controlled by RTSP can use RTP. The number of streams to be controlled are defined by a presentation description and the RTSP protocol is in general similar in syntax to HTTP which means: new methods and parameters can be easily added to RTSP, RTSP can be parsed by standard HTTP or MIME parsers, and that RTSP can reuse web security mechanisms (all HTTP authentication mechanisms such as digest authentication, discussed previously,are directly applicable). In RTSP, both the media client and media server can issue requests. Also, RTSP requests are not stateless i.e. they may set parameters and continue to control a media stream long after the request has been acknowledged [81]. It is important to distinguish RTP from RTSP. RTSP is used by users communicating with a unicast server. RTSP allows the users to communicate with the streaming server and take

action such as pause, fast forward, reverse, and absolute positioning, which is beyond the scope of SIP, H.323, and RTP. RTSP does not deliver data, though the RTSP connection may be used to tunnel RTP traffic for ease of use with e.g. firewalls (as an open standard, RTSP has allowed the industry to concentrate its efforts on a single streaming infrastructure). RTP and RTSP will likely be used complementary in many systems, although both protocols can exist in isolation of each other. For more reading on the use of RTP with RTSP see the section in RFC2326[81] that treats this topic in more detail.

3.1.12 Presence Protocols

Presence information conveys the ability and willingness of a user to communicate across a set of devices. A presence protocol is a protocol for providing a presence service over the Internet or any IP network. RFC2778[93] describes a model for presence and instant messaging. Presence information is collected and afterwards distributed to interested parties. Two leading standard protocols for presence awareness and instant messaging are:

- SIMPLE (SIP for Instant Messaging and Presence Leveraging Extensions)
- XMPP (eXtensible Messaging and Presence Protocol)

The SIP Messaging and Presence Leveraging Extensions (SIMPLE) Working Group was formed in March 2001 and focuses on the application of SIP to the suite of services collectively known as Instant Messaging and Presence (IMP).

XMPP is an open, XML-based protocol developed as early as during the late 1990s and then submitted to the IETF for standards consideration. The purpose of the IETF XMPP working group is to adapt XMPP for use as an IETF Instant Messaging and Presence technology and in April XMPP reached working group final-call status within the IETF. The protocol is within months of reaching final ratification as an IM and presence awareness standard, according to PeterSaint-Andre, executive director of the Jabber Software Foundation[94], the Jabber-sponsored, open-source organisation fostering XMPP's development, in an article published by InfoWorld [92].

The two protocols are as of today fighting about who should conquer the market for their very purpose. Whereas Microsoft and IBM have thrown their weight behind SIMPLE, a groundswell of support is rising behind XMPP, as Hewlett-Packard, Intel, Hitachi, Sony, and others invest in the technology. Intel's Wireless Communications and Computing Group chose XMPP-based IM vendor Jabber in March 2003. HP plans to deepen its XMPP support with a forthcoming distribution and systems integration deal with Denver-based Jabber [92].

However, the progress of SIMPLE through the IETF is expected to be completed *after* XMPP and many mean that the SIMPLE protocol is still too immature for the market; adding to the momentum of SIMPLE, though, is that Sun Microsystems, another big-name infrastructure player, plans this month to deliver SIMPLE support in its newly released Sun ONE (Open Net Environment) Instant Messaging Server 6.0.

Companies turned directly towards consumers, such as Yahoo, and AOL, have not yet made their choice, and are also unlikely to do so in a near future since

companies like these have invested millions of dollars in proprietary protocols. What will remain as standard on the market within this area remains to be seen. Maybe the best of synergistic effects between proprietary protocols, XMPP, and SIMPLE will all contribute to the new standard for instant messaging and presence awareness on the market.

3.1.13 Gateway Protocols

This section mainly discusses two IETF gateway control protocols, Simple Gateway Control Protocol (SGCP) and Media Gateway Control Protocol (MGCP or H.248 and Megaco)[82], used to control Voice over IP Gateways from external call-control elements.

SGCP assumes an architecture whose call-control intelligence is outside of the gateway and is handled by external call-control elements, called call agents. Several call-agents can participate in constructing a call but the synchronisation between various call-agents is presumed, and not covered by SGCP. The basic concepts of SGCP are **endpoints**, sources of data that physically or logically exist within an entity, and **connections** that can be either point-to-point or multipoint. Groups of connections constitute a **call** and is set up by call agents. SGCP consists of end-point and connection handling functions. The SGCP service enables the call agent to instruct the gateway on connection creation, modification, and deletion using five different protocol commands: *NotificationRequest, Notify, CreateConnection, ModifyConnection, DeleteConnection*. SGCP can also inform the call agent about events occurring in the gateway.

SGCP was fused with Internet Protocol Device Control (IPDC) to form MGCP. MGCP, also known as H.248 and Megaco, is a standard protocol for handling the signalling and session management needed during a multimedia conference. Megaco and H.248 refer to an enhanced version of MGCP. It is an emerging standard that will enable voice, fax, and multimedia calls to be switched between the public switched telephone network and emerging IP networks. The standard is defined by the IETF in RFC3015[82] and by the ITU-T in Recommendation H.248. The Megaco framework could potentially enable service providers to offer a wide variety of converged telephone and data services and the model removes the signalling control from the gateway and puts it in a media gateway controller (MGC), which can then control multiple gateways. MGCP utilises the connection model, similar to SGCP, where the basic constructs are physical or logical end-points and/or point-to-point or multipoint connections The model includes the possibility for the controller to determine the location of each communication end-point and/or connection and its media capabilities so that a level of service can be chosen depending on the capabilities of the parts participating in the conference.

3.1.14 Codecs

The term codec is an acronym that stands for compression/decompression. A codec is an algorithm, that reduces the number of bytes consumed by large files and programs, such as the voice packets in IP Telephony. As mentioned previously, for IP Telephony unlike the fixed voice encoding used in PSTN, one

can choose different compression techniques by using different codecs, hence increasing or decreasing the quality of the conversation versus the bandwidth used. This section will discuss the topic of codecs and how this subject has developed in more detail.

The two basic variations of 64 Kbps Pulse Code Modulation (PCM converts analog sound to digital by sampling the analog sound 8000 times per second and converting each sample into a numerical code) commonly used today are μ-law (used in North America) and a-law modulation (used in Europe). The two methods however, differ solely in minor compression details. Worth noting is that when making a long distance call, any required μ-law to a-law conversion is the responsibility of the μ-law country. Another compression technique often used is the Adaptive Differential Pulse Code Modulation (ADPCM) which, unlike PCM, encodes the **differences** in amplitude, as well as the rate of change of that amplitude. PCM and ADPCM are examples of waveform codecs, compression techniques that exploit redundant characteristics of the waveform itself. New compression techniques, employing signal processing procedures that compress speech by sending only simplified parametric information about the original speech excitation and vocal tract shaping require less bandwidth to transmit the information and have been deployed over recent years. The different techniques (*see Table 3.4*) are generally referred to as source codecs. As mentioned previously, in the introduction, a variety of standardised codecs exist on the market today. The ITU-T standardises CELP, MP-MLQ, PCM, and ASPCM

Acronym	Codec Compression Method
PCM	Pulse Code Modulation
ADPCM	Adaptive Differential Pulse Code Modulation
LDCELP	Low Delay Code Excited Linear Prediction
CS ACLEP	Conjugate Structure Algebraic Code Excited Linear Prediction
MP MLQ	Multi Pulse, Multi Level Quantisation
ACELP	Algebraic Code Excited Linear Prediction

Table 3.4: *Codec Compression Methods[79]*

coding schemes in its G-series recommendation. Some of the most popular voice coding standards for packet voice are viewed below [17] [79]:

G.711 describes the 64 Kbps PCM voice coding discussed previously and is today the format used for digital voice delivery in PSTN and through PBXs.

G.726 describes ADPCM coding at 40, 32, 24, and 16 Kbps and which can be used between IP Telephony networks and PSTN provided that the latter has ADPCM capabilities.

G.728 describes a 16 Kbps low-delay variation CELP voice compression.

G.729 describes CELP compression which enables voice to be coded into 8 Kbps.

G.723.1 describes a compression technique used to compress speech or other audio signal components of multimedia service at a low bit rate. Two bitrates are associated with this coder: A 5.3 Kbps coder based on MP MLQ technology and a 6.3 Kbps coder based on CELP.

For more details and information about codecs, visit the homepage of the Codec Central[80], a general resource for information about various codec technologies and their applications.

Voice quality can be tested in two ways: subjectively by humans performing subjective voice testing and objectively by computers performing objective voice testing such as total harmonic distortion and signal-to-noise ratios. However, the latter does not always correlate well to a human perception of voice quality and hence a common subjective benchmark used to determine the quality of sound produced by specific codecs is the Mean Opinion Score (MOS). MOS-tests are performed with a wide range of listeners judging the quality of a voice sample (corresponding to a particular codec) on a scale of 1 (bad) to 5 (excellent). The scores are then averaged to get the MOS. Table 3.5 shows the results of comparison between a number of codecs in the G-series, performed by Cisco Labs. In general, the MOS rating of a speech codec decreases with decreasing bit rate. When it comes to IP Telephony devices, Cisco 3600, for example, supports

Compression Method	Bit Rate	MOS Score
G.711 PCM	64	4.1
G.726 ADPCM	32	3.85
G.728 LD CELP	16	3.61
GSM	13	3.54
G.729 CS ACELP	8	3.92
G.729 x 2 Encodings	8	3.27
G.729 x 3 Encodings	8	2.68
G.729a CS ACELP	8	3.7
G.723.1 MP MLQ	6.3	3.9
G.723.1 ACELP	5.3	3.65

Table 3.5: *Codec Comparison (Source: Cisco Labs)*

a number of codecs: "G.711 a-law 64 Kbps","G.711 μ-law 64 Kbps", and "G.729 8 Kbps". 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)", and "ITU G.729 standard, 8k rate".

Codec Negotiation, another interesting topic which provides the ability for a VoIP gateway to connect to other VoIP devices without necessarily knowing which codec is used for a call setup. This feature also allows Cisco gateways to dynamically adjust to changes on remote devices. As long as the codec used by the remote VoIP device matches the capabilities list of the VoIP gateway, the call is completed. With the introduction of IOS Version 12.0(5)T, Cisco VoIP gateways support codec negotiation. Through codec negotiation a codec can also be changed during conversation, as supported by e.g. Cosmobridge's IP Gateway System CTG3400.

However, many vendors support proprietary protocols and codecs such as the the Japanese company Japan Kyastem Co.,Ltd, that has developed a codec selected by VoiceAge called ACELP®.wide, a wideband speech codec that claims to be able to compress at rates of 9.6, 12.8, 16, and 18.6 (Kbps) and further claims to render voice with un-compromised quality at a bitrate of 12.8 Kbps, while working on a very short frame length of 20 ms. The disadvantage of using proprietary protocols and codecs is of course, among other things, that devices

in different networks will be (directly) incompatible with each other and there will be a need for some sort of gateway for conversion, and also in the long term, due to factors like increased development and purchase costs and problems with licence issues.

On the other hand it is also possible to understand why companies choose to develop proprietary protocols since through this they gain a certainty that the protocols will really work with their equipment while at the same time they force the customers to stick with their products.

However, there are various drawbacks with compressing voice and one must be careful when designing voice networks with low bit rate compression. One of the main drawbacks is signal distortion due to multiple encodings (called tandem encodings). For example, when a G.729 voice signal is tandem encoded three times, the MOS score drops from 3.92 (very good) to 2.68 (unacceptable). Another drawback is codec induced delay with low bit rate codecs.

3.2 IP Telephony Security Issues

In order to provide message integrity and privacy the security features of SIP are important. This section deals with how SIP behaves behind and together with NATs and firewalls, the possibilities of encrypting media setup as well as media content, and finally authentication. For further reading see RFC3261, J. Rosenberg et. al., June 2002 [16] where the details of SIP security are described.

3.2.1 NATs and Firewalls

Companies and consumers use firewalls (*see Figure 3.4*) to protect their LANs from unwanted traffic. Everything that is inbound (this is always seen from the internal networks point of view) or outbound will be filtered. Those packets that do not fulfill the rules set will be filtered out and dropped in order to enforce the security policy set in the filters.

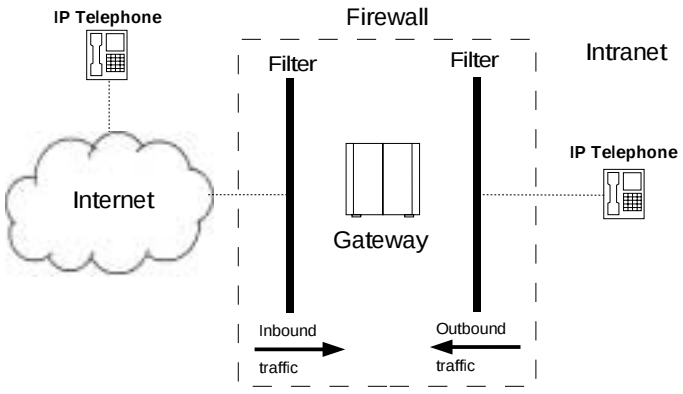

Figure 3.4: *The Principles of a Firewall Using IP Telephony Equipment*

Network Address Translation (NAT) is a method for mapping IP addresses from one realm to another, providing transparent routing to end hosts, usually used by companies to map several private addresses onto a lesser number of public addresses. Another example where NATs are used is that of consumers possessing cable or DSL modems, wishing to connect multiple computers using the single address provided by the cable company or DSL company. However, NATs[103] were originally a short-term solution to the long-term problem of the lack of IP addresses in IPv4. A general hope is that NATs will disappear with the deployment of IPv6, a slow ongoing process. The basic various flavours of NATs[61] are called static NATs, dynamic NATs, and NAPTs (Network Address and Port Translation), these amongst others are described in RFC2663[61].

There has been a great amount of work done about getting various kinds of applications through NATs and firewalls. The problem of SIP traffic traversing through NATs and firewalls is similar to getting any other application through a NAT or a firewall, only more troublesome, since addresses and port numbers are inside both SIP and SDP, and different types of NATs sometimes change these parameters in the IP headers, hence problems may arise unless the NAT is SIP aware.

Services like HTTP and FTP work on well known ports and they do not give firewall administrators much of a problem. However, SIP is a problem even though SIP also works on a well known port, 5060. In finding the answer to why SIP can be particularly troublesome one must remember that SIP is only used for setting up sessions, it provides a tool for helping users to find each other and to distribute information between them. The information that describes the session (usually defined by the SDP protocol) is what makes traversing NATs and firewalls partially difficult. SDP describes what kind of media stream you want to setup and to where, i.e. which port and address to use. The ports that are used for these media streams are ephemeral and dynamic, consequently firewalls do not know if an audio stream is destined for a certain address and if a given port should be let through, denied, or dropped. Given the existence of NATs, and while waiting for IPv6, one way to handle incoming and outgoing SIP traffic is to utilise a SIP Application-Level Gateway (ALG), the most sophisticated kind of firewall gateway, such as the IX66 firewall with SIP support developed by Intertex[108]. Unlike circuit leveled gateways, that only relay information received from one side to the other without interpreting the content, ALGs, as the name tells us, are application aware. An ALG, by definition, is an application specific translation agent that allows an application on a host in one address realm to connect to its counterpart running on a host in different realm transparently[61].

A possible SIP call from Magnus to Oskar, using a SIP ALG proxy within the (possibly private) network and a firewall permitting SIP/SDP, and RTP traffic to and from the Application Level Gateway (ALG) proxy (*see Figure 3.5*), could consequently be carried out without trouble.

For further reading about this topic, and details on the implementation of a SIP ALG, see Fredrik Thernelius M.Sc Thesis, "SIP, NAT, and Firewalls", May 2000[24].

A simpler solution to the NAT problem, although with many drawbacks such as complicated configuration and risk of a variety of Denial of Service (DoS) attacks, is to configure the NAT with a DeMilitarised Zone (DMZ) host. A

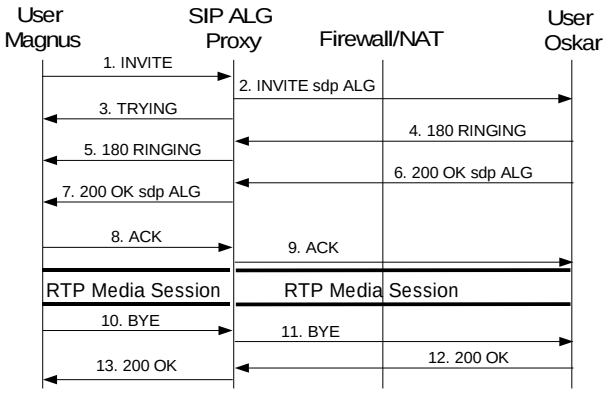

Figure 3.5: *SIP Application Level Gateway (ALG) for Firewall Traversal*

DMZ is a computer host or small network inserted as a neutral zone between a company's private network and the outside public network. The DMZ host receives all incoming packets that have not previously established an outside connection. By telling the DMZ host the home IP address of the phone (i.e. the phone's IP address on the private LAN) it can then forward all incoming messages to the phone.

Other solutions were proposed by J. Rosenberg et. al. in an Internet draft about NAT and Firewall Scenarios and Solutions for SIP[64]. One is to upgrade the client phone or PC application to include support for the STUN (Simple Traversal of UDP through NATs) protocol[65], and optionally the SDP extensions for NAT[66], SDP extensions for connection oriented media[68], and SIP extensions for NAT[67]. The STUN protocol allows a client to discover whether it is behind a NAT, and if so what type of NAT it is. Using the STUN protocol the device will then be informed of its public IP address.

To summarise, there are quite a few solutions to solve the problem of SIP traffic traversing NATs that exist today. However, it seems there is no *stand alone* solution that can, itself, satisfy the entire requirement within this topic, but rather all current practices lacks features and suffer from certain limitations. Hopefully it will become as common for gateways to support SIP as it is for them today to support HTTP and FTP. Also, as mentioned previously, with the introduction of IPv6 the need for NATs will be reduced and the problem of SIP traffic traversing NATs should diminish.

3.2.2 Encryption and Authentication

Encryption of the actual SIP signaling has no bearing on the protocols used for media transfer. In fact the encryption of media associated with a session can be encrypted end-to-end independently of any associated SIP signaling. SDP enables encryption of media streams by adding the encryption key, "k", to each media description. Moreover, the Secure Real-time Transport Protocol (SRTP) can provide confidentiality and message authentication if the protocol used for

transmitting the media is RTP[72].

However, SIP is not an easy protocol to secure due to its use of intermediaries as well as its expected usage between elements that the user may not trust at all. Also SIP is meant to work on a user-to-user basis which makes security issues far from trivial. Confidentiality using encryption will probably be demanded for the SIP protocol, in similar ways as for the traditional protocols like HTTP and FTP. Encryption and authentication may be either end-to-end- or hop-by-hop encryption. The latter may use either transport or network-layer authentication. At first it may seem that end-to-end authentication is simpler to implement, although it leaves a considerable amount of information in the clear. Hop-by-hop authentication allows total confidentiality of the SIP message, but demands a potentially more complex underlying security infrastructure. The complexity of hop-by-hop authentication referred to here is not so much a weakness with SIP, but rather the difficulty lies in the infrastructure needed to ensure the trusted network nodes. However, when using end-to-end encryption, total confidentiality can not be fulfilled as some of the header fields are needed for the message to be understood by intermediate SIP entities. Hence, lower layer security implementations (such as VPNs) would need to be considered for global end-to-end security across Internet. In order for such global security to take place, VPN aware SIP proxies would need to be part of the network infrastructure conveying the messages, whereas to achieve security within a private network it would be enough to connect all workstations and devices through a single VPN.

SIP header fields can be encrypted in an S/MIME message body, since SIP messages carry MIME bodies, and the MIME standard includes mechanisms for securing MIME contents to ensure both integrity and confidentiality. Implementors must once again be aware that the traffic may pass insecure network intermediaries before arriving to the destination. These intermediaries might rely on viewing or modifying the bodies of SIP messages (especially SDP), and consequently secure MIME may prevent these intermediaries from functioning.

A SIP or SIPS URI identifies a communications resource. Like all URIs, SIP and SIPS URIs may be placed in web pages, email messages, etc. They contain sufficient information to initiate and maintain a communication session with the resource. In addition to being a general specification of a resource, the SIPS URI additionally specifies the resource to be contacted securely. Transport Layer Security (TLS) is used between the UAC and the domain associated with the URI. From there, secure communication is used to reach the user, where the specific security mechanism depends on the policy of the domain. Any resource described by a SIP URI can be upgraded to a SIPS URI by changing the scheme, if it is desired to communicate with that resource securely.

SIP provides stateless authentication based on the HTTP digest authentication. This type of HTTP digest authentication provides message authentication and replay protection, but it does not provide message integrity or confidentiality. Both user-to-user and user-to-proxy authentication is provided and the digest authentication scheme is almost exactly identical to the HTTP scheme described in RFC2069[59].

3.3 ENUM in Sweden

ENUM is a telephone number mapping function that translates telephone numbers to valid Internet based addresses. "ENUM" has a number of meanings:
It is the name of a protocol that resolves telephone numbers to fully qualified domain names using a DNS-based architecture, and as defined in ITU Recommendation E.164[86]. It is the title of RFC2916[77], the approved protocol document that discusses the use of DNS for the storage of E.164 numbers and the available services connected to an E.164 number. It is also the name of a chartered working group of the Internet Engineering Task Force (IETF) chartered to develop protocols that map telephone numbers to resources found on the Internet using the Domain Name System. The specific Internet domain defined for the purpose of this kind of electronic number mapping is e164.arpa. The IETF ENUM Working Group has defined the ENUM protocol, also defined in RFC2916[77], and discussed above. The E.164 Number Mapping standard uses DNS to map standard E.164 telephone numbers to a list of Universal Resource Locators (URL). A protocol like SIP can then use those URLs to initiate sessions. The result of the query is a set of DNS Naming Authority Pointer Resource Records (NAPTR RR)[78]. The NAPTR record is used for identifying available ways of contacting a specific node identified by that name. The key fields in the NAPTR RR are explained below [77]:

The order field: specifies the order in which records MUST be processed when multiple NAPTR records are returned in response to a single query

The preference field: specifies the order in which records SHOULD be processed when multiple NAPTR records have the same value of order

The service field: specifies the resolution protocol and resolution services that will be available if the rewrite specified by the regexp or replacement fields is applied

The flags field: contains modifiers that affect what happens in the next DNS lookup, typically for optimizing the process

The regexp field: one of two fields used for the rewrite rules, and is the core concept of the NAPTR record

The replacement field: the other field that may be used for the rewrite rule

The background of ENUM originates from that a prospective caller may wish to discover which services and protocols are supported by the terminal named by a given telephone number. Similarly, the holder of an E.164 number or device may wish to control what URIs that are associated with that number. E.164 numbers are globally unique resources on PSTNs, ISDNs, and PLMNs used to identify different services such as ordinary phones, fax machines, pagers, data modems, email clients, text, terminals for the hearing impaired, etc.

During the year 2001 the Swedish Government appointed PTS[87] to have the administrative responsibility for, and to carry out a national test with, ENUM. The reason for this test is to gain experience before an eventual permanent commercial introduction of ENUM on the Swedish market. PTS must present their work to the Government latest July, 31, 2003.

In RFC2916[77], which talks about the transformation of E.164 numbers into DNS names, it is stated that ENUM should be implemented in a way which will make E.164-numbers available through DNS by using the general .e164.arpa domain. It is further stated that the Internet Assigned Numbers Authority (IANA) [73] should have the technical responsibility for the delegation of the .e164.arpa domain, this according to the Internet Architecture Board (IAB)[89] who has the administrative responsibility for the domain. Names within this zone are to be delegated to parties according to the ITU-T recommendation E.164[86]. Delegations in the zone e164.arpa (not delegations within delegated domains of e164.arpa) should be done after expert review, and the Internet Engineering Steering Group (IESG)[90] will appoint a designated expert. Possessing the technical responsibility for the domain .e164.arpa, IANA[73] has delegated the technical responsibility to the RIPE Network Coordination Centre (RIPE NCC) in Amsterdam. RIPE NCC is is one of Four Regional Internet Registries (RIR) that exist in the world today, providing allocation and registration services that support the operation of the Internet globally (the IANA allocates blocks of IP address space to RIRs who in turn allocate blocks of IP address space to Local Internet Registries that assign the addresses to end users). RIPE NCC can carry out the delegations **only** after instructions from ITU and in accordance with the Internet Architecture Boards (IABs)[89] specified intructions. The RIPE NCC however, will not evaluate any requests for delegation that it happens to receive apart from the correctness of the technical information submitted in the request. It is the ITU-T Telecommunication Standardisation Bureau (ITU-T TSB)[88] that evaluates delegation requests and questions and anyone interested in discussing E.164 matters which are not DNS related to contact ITU-T TSB. TSB's task is to provide secretarial support for the work of the ITU-T Sector and services for the participants in ITU-T work, to diffuse information on international telecommunications worldwide, and to establish agreements with many international Standards Development Organisations. The RIPE NCC will furthermore not perform any evaluation of requests for delegation of domains under e164.arpa. This as well is the responsibility of ITU-T TSB[88].

PTS has acquired delegation of the domain .6.4.e164.arpa for purpose of the national test. In a mail[91] dated November, 28, 2002, PTS requests, on behalf of their Director-General, the delegation of the ENUM country code zone .6.4.e164.arpa for Sweden, that corresponds to the Swedish Country Code (CC) 46, according to the ENUM Request Form Template from RIPE NCC.

For further reading about ENUM in Sweden see the report done by PTS, "ENUM - funktion som översätter telefonnummer till Internetbaserade adresser. En beskrivning samt möjligt införande i Sverige"[10] that was handed over to the Swedish Government April, 1, 2001. To follow current ENUM activities see the section of PTS' homepage that handles the topic of ENUM.

3.4 IP Telephony Quality of Service (QoS)

QoS is a vital part of IP Telephony as a key application. One of the main disadvantages of IP Telephony is the difficulty to guarantee a certain **network** QoS. For IP Telephony, one definition of providing QoS is *to provide a guaranteed timely delivery of specific application data or resources to a particular destination.* The simplest and least complex way to provide network QoS is probably

through over provisioning. However, this section will discuss some of the more advanced models developed to provide **application** QoS in IP Telephony networks.

3.4.1 Authentication, Authorisation, Accounting (AAA) and QoS

In conjunction with QoS, for better than best effort service, using AAA with SIP is a growing issue. It is clearly possible in theory, as mentioned previously, to pay for a better QoS but how does this function in practice with a protocol such as SIP. This section will shortly shed some light on some of the various concepts one must take into consideration while implementing AAA.

AAA is used to decide who you are, if you are allowed to ask for a specific service, and how much you should be charged for using it. Since SIP is only a signalling protocol, and SIP sessions have need for session authentication, authorization and accounting, some kind of external mechanism is needed in order to perform AAA. SIP entities need to access AAA information such as checking if the password provided by a user is correct, or storing accounting records related to a particular session. Instead of co-locating a database together with each of the SIP entities in the network a common AAA server accessible by all entities in the network is suggested. SIP entities communicate with the server through the use of a SIP-AAA interface, which obviously poses certain restrictions on this interface, such as the possibility of SIP entities in different domains to communicate with the same AAA server, the allowance for an AAA server to update the information about a user that a SIP entity has, the possibility for the AAA traffic to be securely transported, etc.

Accounting in IP Telephony networks is more than simple charging. The purpose of accounting in SIP networks is mainly to control the resource usage (for example, gateways to PSTN from which someone could place a very expensive international call). The resources to account for are generally resources used, consumed, and/or once initiated by SIP session as well as services initiated and controlled by SIP such as voice mail and media translation.

In the next section two different causes of action, on how to actually obtain QoS, are discussed.

3.4.2 QoS Models

The Integrated Services (Intserv) model

The Intserv model is based on the use of the ReSerVation Protocol (RSVP) and a host uses RSVP to request a specific Quality of Service (QoS) from the network, on behalf of an application data stream. RSVP, by definition, discriminates between users, by providing some users with better service at the expense of others and hence we can expect a need for policy and access controlling mechanisms. RSVP carries the request through the network, visiting each node the network uses to carry the stream. At each node, RSVP attempts to make a resource reservation for the stream.

To make a resource reservation at a node, the RSVP daemon communicates

with two local decision modules, admission control and policy control. Admission control determines whether the node has sufficient available resources to supply the requested QoS. Policy control determines whether the user has administrative permission to make the reservation. If either check fails, the RSVP program returns an error notification to the application process that originated the request. If both checks succeed, the RSVP daemon sets parameters in a packet classifier and packet scheduler to obtain the desired QoS. The packet classifier determines the QoS class for each packet and the scheduler orders packet transmission to achieve the promised QoS for each stream. [75]

RSVP however has its drawbacks in that it is a complex protocol. Part of the complexity lies in that each routing node must be aware of the QoS mechanism used and user applications must also have the protocol implemented. RSVP though, runs over both IPv4 and IPv6.

The Differentiated Services (DiffServ) model

The DiffServ model for QoS was developed to differentiate IP traffic so that the traffic's relative priority could be determined on a per-hop basis. By using DiffServ, traffic is classified based on priority. Then the traffic is forwarded using one of the IETF-defined per-hop behaviour (PHB) mechanisms. The PHB mechanism aggregate IP frames with similar applications' demands by using the same Differentiated Services Code Point (DSCP) within the IP frame. The aggregated frames then moves in the same direction over a given link. A DSCP is a modification of the Type Of Service (TOS) byte in the IP header. Six bits of this byte are being reallocated for use as the DSCP field, where each DSCP specifies a particular per-hop behaviour that is applied to a packet. The DSCP is then mapped to the PHB. This technique allows service providers to control how the DSCP code-points are mapped to PHBs, and each time a packet enters a network domain it may be remarked. This approach allows traffic with similar service characteristics to be passed with similar traffic guarantees across multiple networks, even if the multiple networks do not provide the same service the same way. This is an important feature because the Internet is really a network of multiple service provider networks [76].

The Differentiated Server architecture is further explained in RFC2475 and RFC3260.

3.5 PSTN-IP Gateways

The gateway works as an interface between the PSTN network and the Internet. An analog call goes over the local PSTN to the nearest gateway which terminates the incoming synchronous voice calls and transcodes them from one digital format to another by compressing the voice, encapsulating them into packets, and sending it as IP packets. The gateway transmits the packets onto the Internet for transport to a gateway server at the receiving end. Similarly, incoming IP voice packets are unpacked, decompressed, buffered, and then sent out as synchronous voice to the PSTN connection. A gateway between the SIP world and the PSTN world looks like a SIP user agent to other SIP devices and like a terminating telephone exchange to the PSTN. The advantage of such a gateway is that it provides ISDN User Part (ISUP) transparency by carrying

ISUP message as multipart MIME messages in the SIP messages between SIP-T gateways. ISUP is part of the Signalling System 7 (SS7) suite developed by CCITT and it defines the protocol and procedures used to setup, manage, and release trunk circuits that carry voice and data calls over the public switched telephone network. ISUP is a protocol used between switches in PSTN networks. ISUP is used for both ISDN and non-ISDN calls; although calls that originate and terminate at the same switch do not use ISUP signalling.

As of today, the disadvantages of having an IP Telephony network existing in isolation from the traditional telephone networks are obvious. Consequently, it is vital for a wide spread use of IP Telephony (such as a SIP telephony network) to interwork with the PSTN and hence there is a need for PSTN-SIP gateways. However, an interesting question to ask oneself is how **large** a SIP user database needs to be (i.e. the proportion of users possessing a SIP-adress) before the PSTN-SIP gateway looses its relevance? Maybe 50%, 75%, or 80%, but clearly *not* 100%. It it obvious that this changes from user to user, and mainly depends on the habits of the user, who he or she usually calls, and which services he or she demands. For example, one user might use the phone to frequently phone only a limited group of friends and once they all have SIP-addresses, do they really need the PSTN? Similarly, do they need a phone number in the traditional sense of an E.164-number since they can use the universal SIP-address and a multifunctional device to handle **all** services, such as telehony, answering machine, fax, voicemail, etc, in one. Another user also possessing a SIP Telephony device at home, though, might find it valuable to phone abroad, or a place such as a small village, where SIP and IP Telephony have not yet developed. To satisfy the needs of this second user the existence of PSTN-SIP gateways is clearly necessary.

Another important characteristic of a SIP telephony network is routability of SIP requests - a SIP request that sets up a telephone call should contain sufficient information in its headers to enable it to be appropriately routed to its destination by proxy servers in the SIP network. Most commonly this entails that parameters of a call such as the dialled number should be carried over from SS7 signalling to SIP requests. However, during implementation one must be careful so that unlisted numbers are not revealed as was the case with the Swedish company Bredbandsbolaget (BBB) shown by tests performed by Stefan Alfredsson at Karlstads University[109]. Routing in a SIP network may in turn be influenced by mechanisms such as Telephony Routing over IP (TRIP)[63] or ENUM[77].

For further information on the use of SIP and telephony related applications see the work done by the IETF Session Initiation Protocol Project INvestiGation (SIPPING) working group whose objective is to "document the use of SIP for several applications related to telephony and multimedia, and to develop requirements for any extensions to SIP needed for those applications"[62].

3.6 PSTN and Internetworking

A PSTN/Internet Interworking (PINT) Service denotes a transaction, starting with the sending of a request from an IP client including the relaying of the request into a telephone network and finishing with the telephone network performing the particular request. Examples of such services are: "Click to call"

or "Click to fax" from a web page. Services using the PINT protocol[69] are distinguished by the fact that they always involve two separate networks, an IP network and a Global Switched Telephone Network (GSTN). The PINT protocol operates using SIP and SDP together with some extensions and enhancements. As an example, three new methods, SUBSCRIBE, UNSUBSCRIBE, and NOTIFY are added to the existing SIP requests allowing a PINT client to receive information about the status of a telephone call session invoked by a PINT session.

PINT allows only a one way interaction with the PSTN. As opposed to PINT services, there are also servers in the PSTN network that can initiate requests to Internet servers. The Services in the PSTN/IN Requesting InTernet Services (SPIRITS) Working Group[83] addresses how PSTN can request actions to be carried out in the IP network. Examples of such services are: "Incoming Call Notification (Internet Call Waiting)" and "Internet Caller-Id Delivery". SPIRITS, unlike PINT services, allow for two way interaction between Internet and PSTN.

3.7 IP Telephony Devices

3.7.1 Devices Supporting IP Telephony

It is out of the scope of this report to make a detailed survey of IP equipment on the market today. This section will rather introduce the reader to some of the most common products that exist today, and give examples of companies that provide them. As the pace of development of this kind of products is very rapid, a survey as described above would quickly be outdated. Some of the products that exist on the market today are listed below:

- IP Telephones (such as Cisco 7900-series and Snom's 200 IP telephone)
- IP Telephony Gateways (such as Patton Electronics SmartNode Voice over IP Gateways)
- IP Telephony Servers (such as IP Unity's Harmony6000™Product Family)
- IP Telephony Firewalls and NATs (such as Acme Packet Net-Net Session Routers)
- Fax over IP products (such as Brooktrout's real-time fax over IP products)
- Different kinds of Network Appliances using extensions to the Session Initiation Protocol (such as Telcordia Technologies' SIP for toasters)
- Handheld devices and PDAs supporting IP Telephony (such as the Fujitsu Transaction Solutions Inc.'s iPAD handheld with iFon software and Cisco's Wi-Fi Phone)

A number of devices in each of the above genres exist on the market today and the types and extensions of these devices is expanding with at least the same pace as the technology itself.

3.7.2 Devices and Factors Inhibiting IP Telephony

Despite the compelling appeal and acknowledged benefits of IP Telephony, there are a few key factors that inhibit widespread adoption. From a technical point of view the structure of IP Telephony is rather simple and the major obstacle seems to be that of calls traversing through NATs and firewalls (*as described in Section 2.8.1*). Moreover, one must bear in mind that over three hundred million existing digital business telephones today are installed around the world, thus the switch to switch to IP Telephony will not happen overnight. Furthermore, customers tend to resist changes as they are used to their familiar handsets and ways of communicating. Furthermore customers tend to resist new changes as they are used to their familiar handsets and ways of communicating. However, many of the IP telephony adapters are designed to directly connect to existing handsets and many IP Telephony devices are of similair design as the existing handsets. The IP end-point devices today are also relatively expensive compared to PSTN end-devices and implementing and guaranteeing QoS in the network structure that IP Telephony relies upon is thought to be difficult, although there is little proof it is really needed.

3.8 Non-voice IP Telephony Services

Non-voice IP Telephony services might not be the initial focus for spreading IP Telephony as a replacement for the PSTN voice service. However, as the voice market saturates there will probably be a demand for various non-voice services. In the general it may not be appropriate to try to emulate PSTN services as they are often derived from the centralised single service nature of the PSTN. Non-voice services may be built using scripts that the IP telephone executes and that result in different types of information viewed on the display of the IP telephone. Some of the IP phones today include embedded web browsers and exterior displays, and possess the ability to interprete XML. Some examples of non-voice services are:

- Unified messaging
- Faxing (using PSTN internetworking)
- Scheduler
- E-mail and voice-mail lists
- Personal address book
- Weather reports
- Stock information
- Daily news
- Viewing images from remote cameras (e.g. for security)

The flexibility of IP Telephony, and the possibility for anyone to create applications for IP devices will probably bring IP Telephony services together with intelligent software applications and result in a great number of non-voice services on the market within a short time.

3.9 Robustness

A traditional PSTN telephone is fed with 42 Volts (in Sweden) using the same telephone wires as those leading to the telephone socket. Consequently a traditional telephone will still work during a power cut failure. But what happens to IP Telephony during such a power cut?

For RJ45 cables (the Ethernet cables) all wires are not occupied (for up to 100 MBit/s networks) and hence the remaining wires can be used for feeding various devices with electricity. This is called Power of Ethernet (PoE) and since 1999 IEEE has a working group investigating how to supply electricity to various Ethernet devices in an efficient and economic way. The newly established PoE consortium conducted its first round of interoperability testing on a matrix of Powered Devices and Power Sourcing Equipment in April 2003. Until now the problem has been, as with any emerging technology, for products to comply with a single standard. While the IEEE standard for Power over Ethernet has yet to be completely formalised, a final draft is available for review and the last step in the ratification process is expected in June 2003.

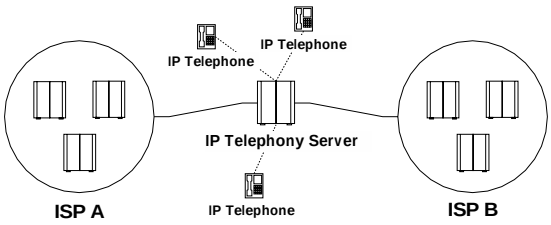

Figure 3.6: *The Possibilities for Redundancy in IP Telephony*

PoE is a technology for wired Ethernet LANs that allows the electrical current, necessary for the operation of each device, to be carried by the data cables rather than by power cords. This minimises the number of wires that must be strung in order to install the network. The result is lower cost, less downtime, easier maintenance, and greater installation flexibility than with traditional wiring. For PoE to work, the electrical current must go into the data cable at the power-supply end, and come out at the device end, in such a way that the current is kept separate from the data signal so neither interferes with the other. The current enters the cable by means of a component called an injector. If the device at the other end of the cable is PoE compatible, then that device will function properly without modification. If the device is not PoE compatible, then a component called a picker or tap must be installed to remove the current from the cable. This "picked-off" current is routed to the power jack. To minimise the possibility of damage to equipment in the event of a malfunction, the more sophisticated PoE systems employ fault protection. This feature shuts off the power supply if excessive current or a short circuit is detected.

Concerning the robustness of a network, it is also important to think about how to build the infrastructure. One common reason as of today, for connections to

IP networks such as Internet, to stop working are due to interruptions on the physical cable from the ISP. A reason for such a stoppage could be e.g. that the cable gets cut off by an excavator during a job in the area. A common safety measure considered minimise this type of accidents among all kinds of cables (for data, telecommunication, electricity, etc) is to physically separate the location of the cables. In order to further increase the robustness of the network one can deploy redundancy. Redundancy is created by connecting a computer network to the external IP network by **more** than one cable. If these cables furthermore are physically located at different places the risk for the communication going down due to an interruption will consequently decrease. Moreover, if the different physical cables originate from different ISPs (*see Figure 3.6*) the risk of being caused by such an it eruption becomes even smaller. In addition to solutions using more physical cables, wireless connections can also be added in order to increase the redundancy. All the above mentioned types of redundancy results in a robustness for IP Telephony that is not possible to the same extent in PSTN networks.

Chapter 4

The Market

The electronic communications sector does not consist of one homogenous market, but rather several submarkets of various sizes och characteristics. More precisely, the entire sector can, according to PTS, be divided into 16 relevant markets. IP Telephony is involved in several of these markets.

This chapter will be based upon two particular views on the evolution of the public telephony network of today. It will visualise the possible interactions between IP Telephony networks and traditional switched telephony networks. With this in mind, a few representative players, which the authors have been in more or less close contact with, will be presented and their roll in the evolution process will be discussed. This representation is intended to give a better feel for the IP Telephony market as a whole, and to point in which general direction it is heading.

4.1 Two Sides of the Same Coin

As mentioned, the authors believe that there are two major ways in which the traditional public switched network will transform. These two transformations does not at all exclude each other, they are simply a result of two directions in which the different players of the market are heading. The most likely event is that these two branches will evolve side by side until they finally, sometime in the future, merge into a one homogenous network.

The two evolutional branches are denoted: *Transit Upgrade* and *The Island Kingdom*.

4.1.1 Transit Upgrade

In this scenario, IP based solutions will to a greater and greater extent control the traffic that is now in the hands of traditional switched systems. Exchanges in all different levels and parts of the PSTN will gradually be replaced by IP based systems *(see Figure 4.1)*. By doing this, the network operators will cut traffic costs due to an increase in efficiency. The efficiency gain is a result of the IP network's superior bandwidth usage in comparison with traditional switched networks. In the end, this will consequently lower consumer prices. In the long

run, switching to IP based solutions will additionally facilitate upgrades and ease integration with other systems. The new IP systems would have to be able to communicate with the old exchanges of the switched part of the entire network, though not directly to end-users.

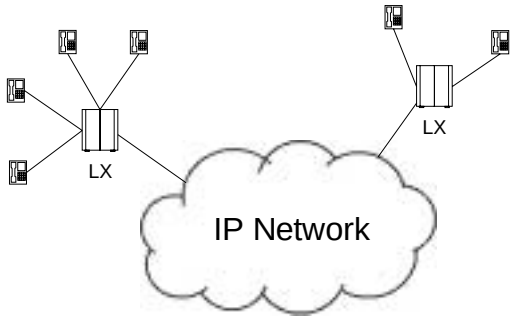

Figure 4.1: *Transit Upgrade*

It is likely, despite the fact that the inner working of the public network will be dominated by high-tech IP switches, that a large part of the traditional local loop will remain unchanged. These twisted copper wires have an extensive lifespan due to numerous reasons. First and foremost, there is no economic incentive nor any direct need for a wide-spread abolishment of the usage of the local loop. Especially along with the EU directives (LLUB[1] and additional directives implemented in The Electronic Communications Act), with the aim of increasing competition in the local loop and breaking up monopolies on fixed telephony subscriptions, there might be even less of an incentive for operators to try to circumvent a usage of the copper wires.

The direct advantages of this scenario, in terms other than costs and consumer prices, will mainly be felt by network operators rather than consumers. This is partly due to the limitations in the local loop and the plain old telephony sets (POTS) connected to it. Limitations such as the lack of value-added services and scalability.

This scenario could be seen as a gradual transformation of the PSTN to a network consisting of an IP networking core. This transformation would improve the efficency of the PSTN mainly by affecting telephony traffic "in transit", hence the name.

4.1.2 The Island Kingdom

In this scenario, operators and consumers move further away from the traditional public switched networks by implementing and using pure end-to-end IP solutions for telephony services. Operators offer IP Telephony services to consumer directly via their Internet connection. As long as it is profitable and relevant operators will offer interconnection with the traditional PSTN by the use of PSTN-IP gateways *(see Figure 4.2)*. Via IP Telephony the operators

[1]LLUB - Local Loop Unbundling

can lower costumer prices by offering Internet connection and IP telephony in a bundle. Different kinds of high-speed broadband access as e.g. xDSL, could give the local loop a needed boost in capacity and usability. In addition to this, the intentional break up of the monopoly on fixed telephony subscriptions, as mentioned in the previous scenario, may encourage ISPs and others to start offering IP Telephony to their customers, thus making customers' "regular" telephony subscription redundant.

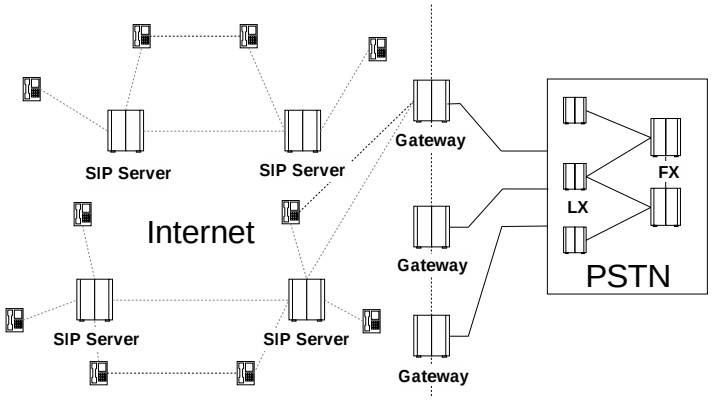

Figure 4.2: *The Island Kingdom*

The advantages of having one single network for voice and data are obvious, and the possibilities are many. Consumers will most likely experience more diversified services, both in terms of value-added and price. The quality and the potential for IP Telephony highly depend upon the specifications of the IP networks used. Either a general network QoS and an application QoS are applied or IP Telephony operators have consumers use their private IP network, to guarantee the dual QoS, and will meet a certain Service Level Agreement (SLA).

A prerequisite for this scenario to occur is an expansion of broadband connections and a more competitive pricing on IP phones and peripheral equipment. Additionally, an aid for it to expand is also that IP Telephony software could be included in the standard installation of an operating system, such as the SIP client Messenger in Windows XP.

Within this scenario, numerous IP Telephony Service Providers (IPTSPs) will eventually pop up and offer telephony services. Today, a large portion of the calls made from commercial IPTSPs still terminate in the PSTN, via the their PSTN-IP gateways. Apart from handling signalling for calls between users of the same service provider, the infrastructures of IPTSPs are mainly used for this purpose. If this evolutional branch *The Island Kingdom* continues to grow, this may no longer be the case. Instead, users will contact each other, with the aid of their respective provider, over the Internet. The IPTSPs' servers, the "islands", will handle signalling and via DNS they will interconnect user from all over the "kingdom".

4.2 Players

4.2.1 TeliaSonera

Since December 9, 2002, Telia is a part of the TeliaSonera group. Telia and Sonera are creating a leading telecommunications group in the Nordic and Baltic regions called TeliaSonera. TeliaSonera operates under the Telia brand in Sweden and Denmark, under the Sonera brand in Finland, and under the NetCom brand in Norway. Telia provides a service called *Mikrosamtal* that lets their customers gateway their international calls over the Internet by first calling a special number and after this specifying the international number they wish to dial. It is possible to subscribe to the service by registering on Telia's homepage, and no special equipment except a regular phone is needed. Prices are slightly lower than Telia's regular prices for international calls and there are no costs in addition to the costs for the calls one makes. The QoS is satisfactory, at least for the countries with which the authors have tried the service.

Telia has no incentive to undermine their PSTN, which generates a large portion of their revenue. They would naturally benefit from the *Transit Upgrade* scenario. Switching to IP solutions would, in the long run, cut costs while keeping existing consumers, which is a prerequisite to survive in the toughened competition that likely will emerge. Telia manages, through Skanova, the largest fibre optic network for broadband in Sweden. In addition to Telia's broadband services (ADSL), this could be seen as a opportunity to prosper in *The Island Kingdom* scenario. But to offer IP Telephony, other than to business customers, would likely compete far too much with their own telephony services on the PSTN. Since Telia's competitors mainly uses price to compete, Telia uses IP Telephony to offer value-added services to their business customers in order to be more competitive.

4.2.2 Bredbandsbolaget

Bredbandsbolaget (BBB) [106] is a market leader in the area of broadband communication in Sweden and offers fibre to the building, Ethernet-LAN broadband services to households and small companies. BBB also offers broadband access via the traditional telephony network. The company is present in Sweden and Norway.

During the spring 2003 BBB have begun to install IP Telephony as a service in households around Sweden. First out were the customers in Örebro who currently have access to the IP Telephony service. The service requires, apart from the broadband connection provided by BBB, also an adapter in order to convert the signals from an analogue telephone. A computer is not needed to use the service. The telephony service is presently only available for Ethernet-LAN broadband users.

There was no time to evaluate this service, although in the magazine InternetWorld (no 3, 2003) the service was referred to as "Recommended". Unfortunately, BBB have a policy about not giving comments or prognoses about the market of IP Telephony, therefore no further information concerning their business can be given.

Bredbandsbolaget, have previously only offered Ethernet-LAN to households

and small companies via fibre, until May 2003 when they started offering broadband via TeliaSonera's local loop. This expansion in activity has fortified their position on the broadband market and consequently contributed to the growth of *The Island Kingdom* branch. Furthermore, as they are an Internet Service Provider that starts offering telephony services, and not the other way around, they will probably have an easier task of surviving in this scenario. By offering IP Telephony and Internet connection in a bundle, and by making it possible for customers to receive a single bill for Internet connection and telephony, BBB will most certainly be a competitor on the fixed telephony market.

4.2.3 Digisip

Digisip is the first independent IP Telephony operator in Sweden that concentrates on private consumer services. Digisip delivers both broadband calls and connections to the PSTN. The service is independent in the sense that it does not matter which broadband operator the user is connected to. Digisip does not own any network infrastructure and hence factors such as QoS, etc, are solely up to the existing connection of the user. In order to use the service independent of the computer the user must utilise a IP Telephony device, an IP Telephony adapter, or another SIP client. Today Digisip supports the Cisco ATA 186-I2 and ATA 188-I2. The founder of the company, Hans Eriksson, is one of the Swedish IP Telephony pioneers and has previously done research at SICS, and worked with IP Telephony at Telia, as well as being a cooperator at Pulver.com.

Digisip utilises IP Telephony and the spreading of broadband access to provide low-price telephony services. Even though Digisip's primary revenue is generated by PSTN interoperability, as end-to-end IP calls only are covered by a small fix initial cost, they would probably prosper more in a pure IP environment. Digisip could in such an environment better be able to offer services that utilises the possibilities of IP Telephony.

4.2.4 Free World Dialup / Pulver.com

Today's Free World Dialup is the third generation of Free World Dialup services to offer the ability to make free calls over the Internet. The first Free World Dialup service began in 1995.

Within the Free World Dialup (FWD) community one can make free phone calls over the Internet using a 'regular' telephone, an IP telephone, or a computer program. The FWD service has over 26,000 subscribers from over 100 countries. Free World Dialup does not provide access to the traditional telephone networks or cellular networks.

The one thing needed to get started is an Internet connection (broadband or even modem) and a SIP phone. Both softphones, such as KPhone and Windows Messenger, and hardware devices, like Cisco's ATA-186 and Cisco 7960 are supported.

FWD is a part of Pulver.com which was founded by visionary Jeff Pulver. Pulver.com is an idea factory for the IP Communications industry, and works through conferences, newsletters, liaison roles, advise to start-ups, summits, and test projects. FWD differs from the other players previously enumerated,

as they are not running a telephony business in a traditional sense. As FWD is a worldwide service and 100% Internet based, not much attention is given to the traditional telephony networks. FWD tries to show the flexibility and transcending capabilities of what pure Internet telephony can offer. Although not totally different from the predictions of *The Island Kingdom*, it is a more Internet utopian perspective. In light of the varying, and sometimes inferior, telephony service quality provided (not due to FWD, but rather due to limited network resources. FWD merely sets up the call), this community gives a hint of how the world of communications could evolve.

Chapter 5

Regulatory Issues

This chapter deals with the Acts that form the basis of the regulations that affect IP Telephony. Each of the two most influential acts will be described in a section. Each of these sections will start with an outline, followed by a subsection stating and commenting on definitions. With the definitions at hand, a subsection concerning obligations will follow. These opening subsections are intended to give an IP Telephony outlook while reading the actual acts. Finally, each act's section is concluded by a short subsection with comments and consequences, that summarises the act from a IP Telephony perspective as well as from a more general point-of-view.

The Electronic Communications Act, a legislation based on EU directives, will be the main focus in this chapter. The Electronic Communications Act will, in the summer of 2003, replace The Telecommunications Act as well as The Radio Communications Act. Though a relatively comprehensive review is made of The Telecommunications Act, it is merely present for the purpose of comparison. The review will hopefully give an insight into the changes that individual players, and even markets as whole, might go through. The Radiocommunications Act may indirectly affect IP Telephony, but will, in spite of this, not be covered to any significant extent.

Furthermore, this chapter includes sections on matters that deserve special attention. Matters that are regulated in The Telecommunications Act as well as The Electronic Communications Act, and which are pre-selection, number portability, and emergency calls.

5.1 General Views on Regulation

The matter of regulating IP Telephony has divided the general IP Telephony involved public into two camps. Two camps, that oversimplified could be seen as: *Those who like it, and those who do not.* The disapproving ones often tend to see IP Telephony as a child of the Internet and all that comes with that. Accordingly, they find it unwise (sometimes even unconstitutional) to treat IP Telephony as something other than just another Internet applications, hence unregulatable by national legislations. These opinions are often rooted in fact

that they see Internet as something completely different (and free) rather than a commoditised form of communication. It is not entirely uncommon to encounter a "*Don't touch my Internet*" mentality within this camp.

In contrast, the other camp tends to see IP Telephony more in term of the service actually provided. They see no reason not to treat IP Telephony in a similar fashion as other forms of telephony services, presupposing they share characteristic concerning quality, price, availability, etc. Accordingly, demands are to primarily be based upon public significance of the service. Whether the service is conveyed by air, fibre optics, Internet or no Internet, should, according to members of this second camp, make no difference.

5.2 The Telecommunications Act

The Telecommunications Act aims to guarantee that private individuals, legal entities, and public authorities have access to efficient telecommunications at the lowest feasible cost to the national economy (costs for both consumers, producers, as well as government are taken into account). The Acts' regulations intend, partly to encourage competition in the area of telecommunications and partly to safeguard national tele-political goals. To ensure this, the Act contains rules on mandatory notification and mandatory licences for some activities, on examination of licence applications and licence conditions, on the provision of telecommunications services, on telecommunication tariffs, on interconnection, on numbering, and on official recognition of telecommunications operators.

The outlines of the tele-political goals of the Government are stated in Section 2 and 3 of The Telecommunications Act. They are as following:

1. anyone shall be able to use, at his/her permanent place of residence or regular business location and at an affordable price, telephony services within a public telecommunications network,
2. everybody shall have access to telecommunications services on equivalent terms,
3. telecommunications shall be sustainable and accessible during crises and wartime, and
4. when implementing the Act it will be endeavoured to create scope for and maintain efficient competition within all parts of the telecommunications sector as a means of achieving the objectives specified above.

5.2.1 Definitions

Section 1 of The Telecommunications Act verbatim includes these definitions, amongst others, for the purpose of the Act:

telecommunications message: sound, text, pictures, data, or other information conveyed by aid of radio transmission or light emission or electromagnetic oscillations utilising a specially devised conductor,

telecommunications network: an installation intended for the conveyance of telecommunications messages,

telecommunications activities: conveyance of telecommunications messages via telecommunications networks or the provision of network capacity for such activities,

telecommunications service: the conveyance of a telecommunications message on behalf of a third party,

telecommunications operator: party who conducts commercial telecommunications activities,

network capacity: transfer capacity in a telecommunications network or part thereof,

telephony service: telecommunications service which consist of speech transmission and which permit transmission of telefax messages and data communication via low-speed modems,

mobile telecommunications service: telecommunications service with radio-aided connection of subscribers in a mobile network termination point [3].

The following describes the applicability of these definitions when applied to IP Telephony and IP traffic in general [6].

telecommunications message

This term holds importance as many other definitions are based upon the definition of this term. The term telecommunications message refers to some sort of conveyance of information. A conveyance independent of the way the information is transported, i.e. packet switched as well as both circuit and cell switched information is included in the definition. Whether the receiver of the information is a machine or an individual should make no difference.

Depending on the definition of *a specially devised conductor* and what it is in allusion to determines what the term telecommunications message comprises. A specially devised conductor can be seen as that which aids in the conveyance of information from point A to point B, e.g. wires, fibre optic cables, radio transmitters and receivers. In this case the allusion holds no real importance. A specially devised conductor can also be seen as that which conveys the information **all** the way from point A to point B, leaving out radio transmitters and receivers and including e.g. wires in the definition. If the latter definition is adapted it leaves us with the problem of allusion. If the phrase **only** is in allusion to information conveyed by aid of electromagnetic oscillations the term is wide (this is the predominant interpretation and the one adapted by the legal experts at PTS). The interpretation of *telecommunications message* with this allusion makes it similar to the interpretation of that which follows the first definition of *specially devised conductor*, in terms of what is included. However, if the phrase is in allusion to information conveyed by aid of all three ways the term is more narrow, e.g. free space radio and optics are **not** covered as there is no specially devised conductor.

telecommunications network

The fact that the information on a network is conveyed, for example, in packets should have no influence on the judgement on whether it is a telecommunications network or not. However, if it is not **intended** for the conveyance of telecommunications messages, e.g. power lines, then it is **not**, under this definition, to be considered a telecommunications network.

telecommunications activities

Even though The Telecommunications Act focuses on regulating the supply of telecommunications services to others, the conveyance of one's own telecommunications messages constitutes telecommunications activities. But telecommunications activities on one's own behalf is not dealt with in any larger extent in the Act.

telecommunications service[1]

Telecommunications services can, from a technical perspective, be divided into three categories: basic services, add-on services, and value added services. The basic service, when it comes to the Internet, could be described as a transportation service, i.e. the conveyance of IP packets from one user to another. The basic Internet service (IP service) could closely be resembled to such a transportation service. IP Telephony is an Internet service just like services such as e-mail and file transfers.

Add-on services, though not defined in The Telecommunications Act, ought to be some form of modified basic service. An add-on service cannot be provided separately, but rather in a bundle with a basic telecommunications service. In the case of TCP/IP, add-on services are services that can be provided utilising the IP service of the operator. Examples of such services are time stamping and digital signatures as a mean for authentication.

Value added services are not defined in The Telecommunications Act either. These services concern the processing of information at the receiver end or the inquiring for information and similar services. These services do not fall under the liability of the operator.

Basic services and add-on services constitute telecommunications services in The Telecommunications Act sense. Value added services often do not constitute a telecommunications service, but can utilise a basic service as an underlying transportation service.

telecommunications operator

According to these definitions an operator is thus someone who conducts commercial activities, conveying information over an installation of some sort (e.g. some types of wired network or wireless network, and assuming the predominant definition of *telecommunications message*), intended for conveyance of telecommunications messages, or providing a network for such activities. Hence, this definition includes operators that conduct telecommunications activities by the provision of telecommunications services via the Internet or other IP networks, as long as it is conducted on a commercial basis. Those generally called Internet Service Providers (ISPs) are thus included in the definition, with exception to parties, who conduct commercial conveyance of telecommunications messages via a network **not** included in the definition of a telecommunications network,

[1] Telelagen och Internet[6] s. 145.

such as an ISP utilising power lines.

network capacity

ISPs are generally not seen as the providers of network capacity, but rather the providers of a service of conveyance of telecommunications messages. Providing this service does not come with the need for any mandatory notification as long as it is the conveyance of data and other activities that do not require allocation of capacity from the numbering plan for telephony. Service providers that uses a leased line for e.g. an Internet connection are not subject to mandatory notification by merely providing network capacity. However, the provider of the leased line is required to send notification to the supervisory authority, if the line is within a public telecommunications network.

telephony service

Telephony service is defined in The Telecommunications Act as the telecommunications service which consists of speech transmission and which permits transmission of telefax messages and data communication via low-speed modems. The term low-speed modems should refer to A/D converted data traffic below 2400 bit/s. Furthermore, the definition does not take into account how the subscriber connects to the network and includes fixed network termination point and radio-aided connection, i.e. mobile telephony.

mobile telecommunications service

Mobile telecommunications services are telecommunications services with radio-aided connection of subscribers to a mobile network termination point. The definition has recently been changed to clarify that it does not include so called fixed radio access, where a fixed network termination point is established by the aid of radio to the local loop. This means wireless LAN access points are not included in this definition. All mobile telecommunications services are included in the definitions regardless of underlying infrastructure. Unlike the definition of a telephony service, mobile telecommunications service contains all kinds of telecommunications services including data communications services.

5.2.2 Obligations

Section 5 of The Telecommunications Act, concerning mandatory notifications, states that, within a public telecommunications network, the following services can only be provided following notification to the supervisory authority:

1. telephony services to a fixed network termination point,
2. mobile telecommunications services,
3. other telecommunications services requiring allocation of capacity from the numbering plan for telephony under Section 37 and,
4. network capacity.

Section 5 of The Telecommunications Act also states the following important clause:

> The Government or, if authorised by the Government, the supervisory authority may issue regulations concerning exemptions from mandatory notification.

Parties subject to the mandatory notification of Section 5 are liable, verbatim according to Section 23,

1. to conduct the activity on the preconditions arising by virtue of the international agreements that Sweden has acceded,
2. to have regard in the activity to the needs of persons with disabilities for special telecommunications services,
3. to contribute to enabling telecommunications messages to be conveyed, without cost to the user, to public emergency services,
4. to recognise the needs of the Swedish Total Defence for telecommunications in times of alert,
5. to submit annual reports on those parts of the activity which are subject to the obligation to give notification, following application of principles especially adapted to the activity, and to make such reports available to the supervisory authority or the party nominated by the authority,
6. to provide, on reasonable terms, to any party who, for the purpose of providing enquiry services so requests, such information about the telephone subscription of a private individual or legal entity as is not subject to the obligation of confidentiality according to Section 45, first paragraph, item 1 of this Act,
7. to provide in its activities, on reasonable terms, information to the public about the telephone subscription of private individuals or legal entities with any other party subject to the obligation to give notification to the extent that they are not subject to an obligation of confidentiality according to law, and
8. to provide, for statistical purposes, information about the activity.

The room for interpretation that IP Telephony creates leads to questions of whether or not a provider of IP Telephony needs to abide by Section 5. On one hand, registering with PTS might provide a certain credibility from both the customer's point of view as well as from potential companies wishing to cooperate with each other since they know that certain criteria have been fulfilled. On the other hand it is these criteria that may stand in the way of a growth, that would be beneficial for both consumers and producers.

Moreover, according to section 7 of The Telecommunications Act a licence is required in order to be authorised to provide, the following, within a public telecommunications network: telephony service to a fixed network termination point, mobile telecommunications services, and network capacity. That is, if the activity is of a degree which is substantial considering area covered, the number of users, or other comparable circumstances. What constitutes an activity

of *substantial* degree is not easily defined. However, the existence of a licence duty depends upon a joint analysis, by the supervisory authority, of all relevant premises.

Section 15 verbatim stipulates that, a party with a licence to pursue telecommunications activities may be subject to conditions concerning obligations for the licence holder, including:

1. to provide on certain conditions telephony services to a fixed network termination point to anyone requesting such service,
2. to provide, having regard to available capacity and on certain conditions, network capacity other than for mobile telecommunications services to anyone so requesting,
3. to provide information about the owner of the activity,
4. to conduct the activity continuously and with good capacity, access and quality, and so as to promote the efficient use of frequency,
5. to fulfil in a certain way what is prescribed in Section 23 or 34,
6. to publish on reasonable terms in its own telephone directory information about individual telecommunications subscriptions with entities subject to mandatory notification, to the extent that such information is not subject to an obligation of confidentiality according to law,
7. to, without special compensation, maintain automatic telephones, to the extent which as regards number and geographical coverage satisfies public needs, and
8. to provide operator assistance services on reasonable terms.

In addition to Section 15 a licence holder must, according to Section 17, pursue the telecommunications activities in such a manner that decisions concerning secret telecommunications interception and secret telecommunications monitoring may be executed and without the execution being revealed. When it comes to end-to-end IP Telephony this could prove to be a bit of a challenge, as content and signalling are separated. But, under The Telecommunications Act, activities conducted by ISPs are not, to any large extent, exposed to any mandatory licence which in turn does not require that they provide for secret telecommunications interception and monitoring. As for IP Telephony operators which only handles signalling, they can not be forced to disclose any media content, as they never handle any of this traffic. Furthermore, in the case of SIP a user can encrypt the SDP content of the signalling which may make the operator unable to reveal the addresses used by the media content traffic.

Besides the sections mentioned above The Telecommunications Act includes numerous sections concerning mandatory licence. Section 10 of The Telecommunications Act says:

> The supervisory authority may grant exemption from the mandatory licence obligation under Section 7 if there are special reasons for this.

Section 5 and Section 10 give the supervisory authority, in this case PTS, the important possibility to grant exemptions from the mandatory notification and licence of The Act. These exemptions can be made in favour of free competition or at other occasions, when seen fit.

5.2.3 Comments and Consequences

As this section on The Telecommunications Act is merely for comparison, the comments and consequences on it will be fairly brief.

The Telecommunications Act is constructed without IP Telephony (at least not in its present meaning) in mind. Even though it manages to regulate parts of it, there are numerous questions which are left unanswered. For small early stage IP Telephony operators, the mandatory notification that comes with The Telecommunications Act is more likely to be used as a proof of quality, in order to promote business, and an act of good will than anything else.

The Telecommunications Act has been around for quite some time (since 1993) and, though amended at several occasions (as late as June, 2002), the crude core of the Act is still based on a rudimentary terminology. Consequently the authors agree that the transition to The Electronic Communications Act on July 25, 2003, will give a well-needed injection to the market of electronic communications. In spite of this, the Act has served some its purpose.

5.3 The Electronic Communications Act

A new regulatory framework for electronic communications networks and services will be put into practice in all Member States from July 25, 2003.

By July 24 all Member States must adapt their national legislation and implement the directives with the exception of the Data Protection directive, for which the date is October 31, 2003.

> The new regulatory framework is intended to provide a coherent, reliable and flexible approach to the regulation of electronic communication networks and services in fast moving markets. The directives provide a lighter regulatory touch where markets have become more competitive yet ensure that a minimum of services are available to all users at an affordable price and that the basic rights of consumers continue to be protected [18].

The Swedish government has, on the basis of these EU directives, compiled a bill concerning electronic communications [13] based on a Swedish Government Official Report (Statens Offentliga Utredningar, SOU)[12]. This bill comprises all electronic communications networks and electronic communications services. The new Act, called The Electronic Communications Act, that follows the bill replaces The Telecommunications Act and The Radiocommunications Act.

The proposed act has its basis in a general notification duty for the provision of public communications networks and public accessible electronic communications services. The proposal involves an expansion of the notification duty in relation to The Telecommunications Act.

5.3.1 Definitions

The bill concerning electronic communications contains a proposal for The Electronic Communications Act. Chapter 1 Section 7 of this proposal includes these definitions[2], amongst others, for the purpose of the Act:

auxiliary installation: a device, a function or other which does not constitute as an electronic communications service nor an electronic communications network, but is in connection with such and enables or supports that service or the provision of services via that network,

call: a connection for the conveyance of speech which allows two-way communications in what the user perceives as real-time,

electronic communications network: a system for conveyance and in applicable cases equipment for connecting or switching, and other resources which admits conveyance of signals via wire, via radio, optically, or via other electromagnetic conveyance media independent of the type of informations conveyed,

electronic communications service: a service, usually commercially provided, entirely or mainly consisting of the conveyance of signals in electronic communications networks,

network termination point: a physical point where a subscriber connects to a public communications network.

operator: one in possession or in other ways in charge of a public communications network or auxiliary installations,

public communications network: an electronic communications network entirely or principally used for the provision of publicly available electronic communications services,

public telephony network: an electronic communications network used for the provision of publicly available telephony services and which enables the conveyance of speech, telefax messages, data communications and other forms of communications between network termination points,

telephony service: an electronic communications service that implies the possibility to place or receive calls through one or several numbers within a national or international numbering plan, including emergency calls.

The following generally comments and furthermore describes the applicability of the enumerated definitions when applied to IP Telephony and IP traffic in general. To the extent possible, these definitions will also be compared to equivalent definitions in The Telecommunications Act.

auxiliary installation

A term used to patch the holes that the reach of the term *electronic communications network* might leave behind. All other equipment, system or installation used in and around electronic communication that is excluded in the latter term

[2]Translated from Swedish by one of the authors.

is thus included in this one. Unambiguously a term that is meant to be technology independent and to hold significance throughout time. SIP servers, if not categorised as a part of an *electronic communications network*, they most likely fall under this category.

call

An attempt to move towards technology independence and focus more on the service actually provided. As a mean to achieve this goal the (dangerously) subjective phrase *perceives as real-time* is used. It is unclear of where, when, and how the judgement, on whether it is real-time or not, is made. A *call* could in mid-conversation, according to this definition, cease to be a *call*, when no longer perceived as real-time. Furthermore, this is a new term to Swedish telecommunications regulation - it has no equivalent in the old legislation.

electronic communications network

Naturally, this term is wider in scope than that in The Telecommunications Act stated definition of a *telecommunications network*. It includes peripherals such as equipment for connecting and switching. Any ambiguities are eradicated and therefore, as apposed to the equivalent definition of the preceding legislations, borderline networks, e.g. power lines, are included. A network no longer need to be intended for the conveyance, but rather only need to **admit** conveyance to be included in the definition.

electronic communications service

A **very** comprehensive term which includes everything from the provision of mobile telephony to e-mail. Even more basic services are included, such as the conveyance of IP packets.

network termination point

A term also used in The Telecommunications Act, there albeit unspecified. It includes fixed network termination points as well as mobile network termination points. According to Televerket, the fixed network termination point for residential users, was the main plug in the residence.

operator

While the term *telecommunications operator* includes both the providers of services on a network as well as the providers of the networks themselves, the term *operator* only consists of those possessing (or in charge of) the networks or auxiliary installations. Hence, a term more narrow than its Telecommunications Act counterpart. Albeit, it could be made much wider depending on the use of the term *auxiliary installation*. Hence, in the case of IP Telephony, both those who handle content and those in charge of signalling can be seen as operators.

public communications network

The scope of this term depends upon the scope of *publicly*. The concept of *public*, in this sense, does not necessarily mean each and everyone. But rather it would be sufficient that a priorly demarcated category of users can utilise the network for it to constitute as publicly available[3]. The fact that an electronic communications network need to be **entirely** or **principally** used for the provision of publicly available electronic communications services for it to constitute as a public communications network will exclude certain networks. In the light

[3]Telelagen och Internet[6] s. 154.

of this, e.g. an IP network over power lines, which constitutes as an electronic communications network does not constitute as a public communications network.

public telephony network

An electronic communications network used for the provision of publicly available telephony services and which enables all forms of communications between network termination points. As in the case of *public telephony network* the term *public* plays, in this definition, an equally important role. Furthermore, on account of the ambivalent definition of the term *telephony service*, it is ambiguous as to what constitutes as a public telephony network.

telephony service

A definition that makes IP Telephony seem caught in the middle. End-to-end IP telephony, without the use of numbers from a national or international numbering plan, is **not** included, while PSTN-IP gatewayed telephony is. The vague definition of a *call* contributes to this definition's mixed approach to IP Telephony. As signalling and content in IP Telephony are separated, and likely controlled/provisioned by different parties, it is not completely obvious who is providing the actual telephony service. Although, the party in charge of signalling seem most likely, as they are the ones that utilise numbering plans to provide their services.

5.3.2 Obligations

With The Electronic Communications Act comes an expanded notification duty, in comparison to The Telecommunications Act, while the requirements regarding licences are partially revoked.

Chapter 2, Section 1, of the proposal, concerning notification states[4]:

> A public communications network, usually commercially provided, or other publicly available electronic communications services may only be provided following notification to the authority appointed by the Government (the supervisory authority).

A notification duty as comprehensive as the definition of *electronic communications service*. What does, in reality, this notifications duty comprise? Or perhaps more appropriately, what does, in reality, this notifications duty **not** comprise?

Moreover, Section 2, same chapter, stipulates[4]:

> For activities solely consisting of the conveyance of signals via wire for broadcasting of sound radio programmes to the public or other activities, as specified in Chapter, 1, Article 1, third paragraph, first sentence of the Fundamental Law on Freedom of Expression, are not subject to mandatory notification under Section 1.
>
> The Government or, if authorised by the Government, the supervisory authority may issue regulations concerning further exemptions from the mandatory notification of Section 1.

[4]Translated from Swedish by one of the authors.

With the new legislation the licence duty will in numerous cases be replaced by a notification duty. What is left from the mandatory licence of The Telecommunications Act is the use of radio transmitters and numbers from a national numbering plan.

Chapter 5 Section 7, of proposal for The Electronic Communications Act, concerning general obligations states that one who provides a publicly available telephony service shall[5]:

1. make sure the service and the public telephony network to a fixed network termination point satisfies reasonable demands on functionality and technical safety, as well as durability and availability at extraordinary events during peacetime,

2. contribute to enabling interruption-free conveyance of emergency calls, free of charge for the user,

3. to the extent technically feasible, provide location data to the party receiving emergency calls,

4. under conditions that are fair, cost-based, and non-discriminatory satisfy every reasonable request to hand out subscriber information, not subject to secrecy or a duty of confidentiality according to law, to one who conducts or intends to conduct subscriber information activity,

5. free of charge provide a subscriber a specified telephone bill that concerns the use of a public telephony network to a fixed network termination point or thereto belonging publicly available telephony services, unless the subscriber has requested that the bill should be unspecified,

6. make sure end-users in other countries within the European Economic Area can reach Swedish numbers, whose numbering structure lacks geographic significance, if it is technically or economically viable and the called subscriber has chosen, not for commercial reasons, to limit the access for calls from certain geographic areas,

7. have regard in the activity to the needs of persons with disabilities for special services.

   Calls that are free of charge for the calling subscriber may not be stated in telephone bill.

   The Government or the public authority appointed by the Government may issue regulations on the manner in which the obligations shall be satisfied and on matters concerning exemptions from the obligations.

The actual application of the term *telephony service* controls the effect that these general obligations will have on IP Telephony. Further on, an in-depth analysis of the consequences of the obligations concerning emergency calls will be given (*see Section 5.4*).

As its predecessor, The Electronic Communications Act also contains obligations concerning secret telecommunications interception. Chapter 6 Section 19

[5]Translated from Swedish by one of the authors.

states that an activity shall be pursued in such a manner that decisions concerning secret telecommunications interception and secret telecommunications monitoring may be executed and without the execution being revealed, if the activity concerns the provision of:

1. a public communications network not solely intended for the conveyance of signals via wire for broadcasting of sound radio programmes to the public or other activities, as specified in Chapter, 1, Article 1, third paragraph, first sentence of the Fundamental Law on Freedom of Expression,

2. services within a public communications network, which consists of:

   a) a publicly available telephony service, to a fixed network termination point, which admits the conveyance of local, national, and international calls, telefax, and data communication with a certain stated lowest transfer rate, which admits functional access to the Internet,

   b) a publicly available electronic communications service to a mobile network termination point.

   The content of and information about the telecommunications messages subject to interception or monitoring shall be made available so that information may be easily dealt with. A telecommunications message refers to sound, text, pictures, data or other information conveyed by aid of radio transmission or light emission or electromagnetic oscillations utilising a specially devised conductor.

   The Government or, if authorised by the Government, the supervisory authority may issue regulations concerning matters addressed in the first and second paragraph, and in individual cases exemptions from the obligations of the first paragraph.

The recurring statement, that media content and signalling are separated in IP Telephony, is once again relevant. As mention previously (*see Section 5.2.2*), this separation make IP Telephony operators, which only handles signalling, unable to disclose any media content, as they never handle any of this traffic. Moreover, users can utilise encryption on different levels to further complicate matters of interception and monitoring.

5.3.3 Comments and Consequences

The prime directive of The Electronic Communications Act, roughly the same as that of the Telecommunications Act, is to promote competition and to maintain a market of free entry. The act can be seen as a sector specific, ex ante regulation. Where a market is found to be effectively competitive, specific regulation should no longer be needed.

The Electronic Communications Act loosens the grip of the smaller players on the market by switching weight from mandatory licence to the lighter notification duty, while keeping the grip of the more dominant players by enforcing obligations concerning e.g. interconnection and other forms of access. An example that concerns these other forms of access is the ability for the supervisory authority to enforce players with Significant Market Power (SMP) to retail subscriptions for fixed telephony, to other operators. Prior to this legislation, The

Telecommunications Act stated that players with SMP were obligated to provision a leasing of their lines, on cost based tariffs. This new enhanced obligation, though crafted in the pursuit for perfect competition on the market of fixed network telephony, may end up in causing long-winded lawsuits. All will be revealed in due time.

The two different approaches in dealing with market players, depending on their market significance, has undoubtedly created an ambiguity as to whether or not the new act brings increased or decreased regulations.

Due to the comprehensive nature of The Electronic Communications Act, it could prove to be burdensome for PTS, though yet highly dependent upon the structure of the policy framework adapted. Along with this potential burden comes a great deal of potential power - a power to shape the rules of the market in an ad hoc fashion.

How and what do you regulate? Where do you draw the line? Should you draw a line at all? It would seem natural to design the framework to lessen the burden and to minimise or even eliminate distortion of competition, while working in the interest of consumers. Should this be done by keeping an open but rigid policy, so that entrants and incumbents know the rules they can play by? Or, should the policy give more free rein, thus creating a flexible and powerful supervisory authority, but adding to the risk of distortion of competition and at the same time giving market players a level of uncertainty? Although, in the long run, ad hoc rulings, that might seem inconsistent, could prove to do much less harm to the competition than a rigid and unfortunately levelled policy, that could backfire.

The Electronic Communications Act is intended to treat IP Telephony as any other telephony service. From a regulatory perspective the judgement of whether or not a call is conveying in real time can be put aside. A two-way communication which by consumers will be perceived as not to be occurring in real time will inevitably be deemed unusable by most. Therefore, it does not need to be regulated.

Depending on the outcome of the market (*see Section 4.1*) different regulatory measures have to be taken. In the scenario *Transit Upgrade*, where the traditional switched systems are replaced by IP systems, end-users are not affected to any larger extent by the transition to IP technology. Consequently, regulations affecting end-users do not significantly need to differ from that of traditional switched telephony services. But it should be kept in mind to ensure that proper and effective interconnection is rendered possible. With IP networks there are no technical obstacles for this to happen. Furthermore, one must be aware of the fact that IP Telephony technology has the ability to strengthen the hold the incumbent network operators have on the market.

The Island Kingdom scenario, explains how end-users start using pure IP Telephony instead of traditional circuit switched telephony. In this case, the focus is to a greater extent on the users and the ISPs, rather than traditional telephony operators. As voice is integrated with data and the use of different services from different providers are facilitated, the role of telephony service provider is dispersed. Furthermore, with the separation of signalling and content in IP Telephony, this dispersion is made obvious. One or more parties, the ISPs, may convey the media traffic, while anothers, the IPTSPs, handle the signalling. From a regulatory point of view, it is important to note that, in order to make

IP Telephony calls **from** Sweden one does not need to use registrars (*see Section 3.1.4*) **in** Sweden.

In conclusion, it is hard to predict the impact that the new legislation will have on the market of today and tomorrow. It is though safe to say that some players will barely notice the transition from The Telecommunications Act (and The Radiocommunications Act) to The Electronic Communications Act, while others might be more directly affected.

5.4 Emergency Calls (112)

SOS Alarm are by appointment of the Swedish government responsible for receiving all emergency telephone calls (112 - emergency calls). Initially the service was administrated by Televerket, but since 1974 it has been maintained by SOS Alarm. SOS Alarm is owned by the Swedish government, the Swedish Association of County Councils, and the Swedish Association of Local Authorities. SOS Alarm's centres can be found at 20 locations throughout Sweden.

A party subject to the mandatory notification of Section 5 of The Telecommunications Act is liable under Section 23 to i.e. contribute to enabling telecommunications messages to be conveyed to public emergency services, and to do this without a per call cost to the user. In addition to an obligation like that of The Telecommunications Act, The Electronic Communications Act also contains an obligation to provide, to the extent technically feasible, location data to the party receiving emergency calls. These two obligations are stated in Chapter 5 Section 7, concerning general obligations, and are applicable to those who provide publicly available telephony services.

The Electronic Communications Act includes two definitions that specifically hold significance:

emergency calls: calls to public emergency services through a number within a determined numbering plan for telephony.

location data: data which is treated in an electronic communications network and which provides the geographic position of a user's terminal equipment.

5.4.1 Problems

With PSTN-IP gateway capabilities or other means of reaching PSTN from an IP network there is no explicit problem of conveying the actual emergency call to an emergency service centre. The problem rather lies in the ability to switch the emergency call to the correct (in this context, closest) emergency service centre. In addition to the problem of switching, there lies a difficulty in resolving the location and identity (if needed) of an IP Telephony emergency caller. The problem of switching will be addressed first.

To understand the complexity of the problems, that arise when current solutions for switching emergency calls to the correct emergency service centres are applied to IP Telephony, one has to understand how a non-IP Telephony emergency call is processed. When someone, in Sweden and within TeliaSonera's PSTN, places a call to the common national emergency number – 112, likewise

the common European emergency number – the B-number (the A-number is the telephone number **from** which the call originates, while the B-number is the telephone number **to** where the call is intended) goes through a conversion in the local exchange (LX) based on a county ID (*swe.* kommun-ID. Geographic code for both fixed and mobile telephony), which in turn depends on the geographic location of the LX. Further along the chain, in the transit switches (FXs, *swe.* förmedlingsstationer) the call can be switched, on the basis of this new B-number, to the correct emergency service centre. Along with the call the centre receives this B-number, which gives the general geographic area from where the call originates. When an emergency call comes from another operator or from a mobile telephony network it enters at FX level, preceded by its B-number being appended with a prefix and a county ID. Thereafter the call is handled in the same manner as any other emergency call. Consequently, switching, in the manner as stated in the scenarios above, presupposes that the caller is in the same geographic area as the switch, which converts the B-number. In the case of IP Telephony, this might accordingly be the nearness to the PSTN-IP gateway.

With IP Telephony this is not at all a certainty. The caller might not even be in the same country, let alone the same county as the gateway. An emergency call originating from an IP Network will be switched to the emergency service centre that corresponds to the location of the PSTN-IP gateway in question *(see Figure 5.1)*. But how important or relevant is it for an emergency call to be sent to the closest emergency service centre? Since the emergency centre could subsequently re-route the request to the most suitable centre **following** communication with the caller.

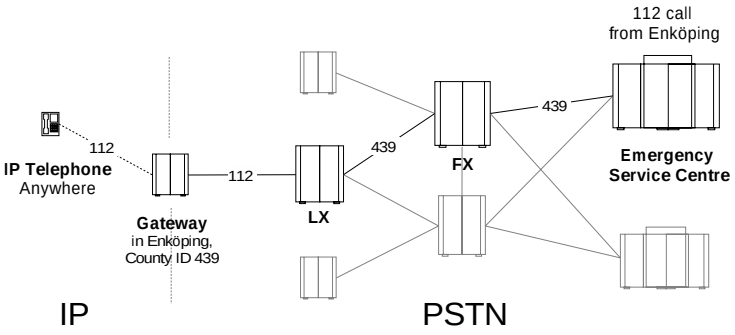

Figure 5.1: *Switching of an Emergency Call Originating from an IP network*

The second problem concerning emergency calls is regarding the ability to resolve the geographic location and identity of a caller. This information could prove to be crucial to the efficiency of the emergency service, and frequently a matter of life or death. The identity of a caller, in addition to the fact that it gives an ability to locate the caller and customise the emergency aid, also minimises prank calls. When an emergency call originates from the PSTN the A-number is forwarded via SS7. Thus the emergency service centre is able to look up the subscriber's address in a telephony directory and therefore is capable of dispatching the appropriate aid to the appropriate location, **without** further communication. This scenario is still plausible if the call originates from

an IP network, although it assumes that the IP Telephony operator in question keeps records of its subscribers, which is not always the case. Perhaps more importantly to note, even if a call from a certain subscriber goes through the same PSTN-IP gateway it does not mean it has the same origin, i.e. the subscriber does not necessarily need to place the call at their address of record.

5.4.2 Solutions

The following presents more or less viable solutions to the problems that arise when emergency services are utilised in combination with IP Telephony. Some proposed solutions will try to solve the problem of switching an emergency call to the appropriate emergency service centre, while others will address the issue of resolving the origin (more accurately than county level) of a emergency call.

First of all, some relatively short term solution that apply to the situation for today's emergency calls:

- By implementing the county ID plan earlier in the conveyance chain of the emergency call, i.e. append the prefix and the appropriate county ID before the emergency call enters the PSTN, the emergency call could be switched to the correct emergency centre. The implementation should be done at a point close to the origin of the call, possibly even the IP device used to place the call. This would solve the issue of switching, but at the same time raise new issues and reallocates existing ones. The problem of how to actually extract the physical location of an device still stands.
- A similar solution to the one above, but instead ENUM (*see Section 3.3*) is used to the largest possible extent within IP networks. This may be a more durable and more Internet adapted solution, but it still leaves the matters of the previous solution unresolved.
- If an outbound proxy is limited to serving only a well bounded geographic area, switching an emergency call to the correct emergency centre would no longer be a problem. But naturally it would consequently inhibit the flexibility of the proxy.

In addition to these suggestions, the following might be long term solutions:

- The introduction of an emergency service centre capable of receiving pure end-to-end IP emergency calls, will eliminate the need for any IP-PSTN traversal. In order for it to function the centre's system must include support for a wide number of protocols and formats (including the transmission of location data), and be able to receive emergency calls under any circumstances. A case such as the one of some of today's online banking services (a **very** different scenario, but possibly with some coinciding characteristics. Both are vital, but to a different extent), where one is unable to perform online banking tasks due to the choice of software (despite it being standard compliant), is obviously intolerable.
- As hinted in the previous suggestion, an inauguration of standardised and even automated methods for transmitting location data to an emergency service centre located either in the PSTN or within Internet. This is more of a prerequisite than a viable solution.

5.4.3 Comments and Consequences

In order for an expansion of end-user IP Telephony the access to full-fledged emergency services is of uttermost importance. In a long term perspective there **must** at least exist: a single emergency address similar to 112 of PSTN, or other satisfactory means of utilising suitable emergency services within an IP Telephony network. However, other networks for electronic communications (existing and emerging) could be confided to handle emergency services. IP Telephony and related services although clearly have the potential to provide capabilities for emergency services beyond the scope of traditional telephony. Here are a few examples:

- Multimedia (video, medical data)
- Authenticated access to medical data base access
- Remote control of medical devices and various equipment for emergency aid
- Encryption of sensitive information
- Transmission of miscellaneous data during emergency communication session to facilitate emergency aid

Moreover, an ability to provide an emergency communication session, at times when networks reach traffic saturation, with a higher probability of completion over non-emergency traffic might also be important. Although, this priority can be hard to perform as the traffic can be highly encoded, which makes it difficult to separate emergency traffic from non-emergency traffic.

The Electronic Communications Act contains an obligation to provide, to the extent technically feasible, location data to the party receiving emergency calls. Comprised in *technically feasible*, in addition to the obvious, is that the demands on economic reasonableness are to be met as well [13]. As the supervisory authority can make exemptions from the obligation it will consequently have to take factors such as cost and usability into consideration when making a judgement concerning whether or not a party needs to abide by the obligation or not. The obligation is intended to improve the level of protection and security for the user, and it will most certainly give birth to varying solutions for resolving location data, ranging in implementation cost and accuracy.

Whoever's lap these issues will fall into - the IP Telephony service providers, the PSTN-IP gateway providers, the PSTN service providers, or perhaps the party receiving the emergency calls - it will most likely be a cumbersome task.

This leaves us with the issue of switching an emergency call to the correct emergency centre. As stated before, how important or relevant is this? The structure of today's emergency service systems are naturally highly integrated into the PSTN and that might not be optimal for the communications networks of tomorrow. If all emergency calls no longer would be sent to the closest centre, the entire emergency system would probably have to focus more on redirecting and coordinating dispatches, much like the distributed call centres of today. Implementing IP Telephony would facilitate this and furthermore it would improve performance by better integrating voice and data technology. In a not too distant tomorrow, a set of completely synchronised and uniformly

performing emergency centres will have the capability to accurately perform on a various number of networks and in numerous extreme scenarios.

5.5 Pre-selection

Pre-selection is dealt with in section 40 of The Telecommunications Act, which stipulates:

> A licence holder providing within a public telecommunications network telephony services to fixed network termination points or digital mobile telephony services shall ensure that the subscriber can gain access to telecommunications services provided by another party with whom the licence holder interconnects. It shall be possible for the subscriber to select such services by a permanent selection (pre-selection). It shall be possible to bypass the pre-selection in the case of individual telephone calls.

The Electronic Communications Act includes similar obligations, though in its case aimed at players with SMP (*see Section 5.3.3*).

Pre-selection can be divided into two separate areas: pre-selection for media content and pre-selection for signalling.

The basic transportation of IP packets can be regarded as a services provided by the ISPs. End users pay ISPs to get access to the Internet, i.e. the ISPs convey packet from end users out on the Internet. Consequently, the pre-selection for packet transportation, from end users to the Internet, is thus a rigid matter. Because media content in IP Telephony is end-to-end, the only third parties involved between both end points, are the ISPs. As a result of this, pre-selection for media content can be seen as the routing of the media packets from one user to another. However, the affect the user can have on this routing is limited.

Obligations concerning pre-selection that are imposed on traditional telephony are, on a signalling level, easily satisfied by IP Telephony. There is nothing inhibiting users from having multiple addresses from multiple IPTSPs and applying an ad hoc usage of these depending on the nature of the call.

5.6 Number Portability

This section will address the issue of number portability and the different mappings that might occur when IP Telephony comes into the picture. In fixed and mobile telephony number portability has become a regularity, and a convenient service people expect. If users move to IP Telephony, how will the number portability be affected?

As in the case of pre-selection (*see Section 5.5*), number portability can be seen in more than one way. The Electronic Communications Act, in similarity to The Telecommunications Act, includes obligations on number portability.

Chapter 5 section 9 states[6]:

> A party providing publicly available telephony services shall ensure that the telephony network allows a subscriber to retain his or her telephone number on changing service provider. If the subscriber so requests, telephone numbers used for such service shall be transferred to another party in order that such party shall provide these services. Telephone numbers whose number structure has geographic significance only need to be transferred for provision of telephony services within the same area code district.

The legislations concerning number portability still just concerns *numbers* and **not** addresses, although extending the scope raises some interesting points.

As hinted previously number portability in IP Telephony is not as straightforward as in traditional telephony. There are two basic parts of mapping involved in number portability:

1. E.164 mapping to SIP URL
2. SIP URL to a client (i.e., an IP address)

If a user decides to retain his or her E.164 number, when moving from a traditional telephony operator to a SIP operator (with a PSTN-IP gateway), there are several ways this could be done.

The user's portable E.164 number could be transferred to the new operator, by mapping this number to a operator specific non-portable E.164 number. The operator specific E.164 number could in turn be mapped by the operator to a SIP URL, associated with the user, using ENUM. The translation between the two E.164 numbers would, in Sweden, be done by the number portability centre (SNPAC - Swedish Number Portability Administrative Centre) and performed in the same manner as they would with any other numbers.

As an alternative, this process could be done in a single step, where the user's portable E.164 is directly mapped into a SIP URL by the number portability centre. A prerequisite for this is though that the number portability centre has to start supporting this kind of mapping. In exchange for this, the consumers get a better flexibility and the SIP operator no longer needs to allocate another E.164 number for each new user.

A final alternative would be to let the users themselves determine the mapping of their portable E.164 number, and in a sense transfer his or her number to the number portability centre itself. The number portability centre could act as a registrar for this number and it could be directly mapped into the user's IP address, and thus making the process independent of both SIP operators and traditional telephony operators. Although, worth noting is the fact that IP addresses are network topology bounded and thus non-portable for users. But as the number portability centre acts as a registrar, the user can simply re-register when changing IP address.

IP Telephony signalling uses a "user@domain" format akin to e-mail, expressed as a URL, to name end points. This makes the users more closely tied to a

[6]Translated from Swedish by one of the authors

service provider than users are in the traditional E.164 system. While this kind of non-portability for SIP URLs is tolerable (and perhaps necessary) for names associated with organisations, where validity of the name is often linked to a function performed by the present holder of the address, this is inconvenient for residential end users. To solve this problem, users need to acquire their own domain names, or in some other way unambiguously link themselves to an address.

Chapter 6

In Practice

As PTS did not have the possibility of providing us with an environment in which we were able to perform test calls, such as a test laboratory, the opportunity to perform tests was somewhat limited. The aim of our implementation and experiments was to give us a feeling of what was actually happening in practice during an IP Telephony conversation. This is not meant to be an in depth analysis to come up with innovative results, but rather to give a view of how simple it is for anyone with basic knowledge in telecommunication and computer communication to set up a basic IP Telephony system and become an IP Telephony operator. Also, the quality of an IP Telephony call using various SIP operators have been evaluated.

6.1 SIP Servers and Clients

This section takes a closer look at the SIP software we used during the implementation. At our disposition we had 2 laptops and 1 stationary computer of satisfactory performance.

6.1.1 SIP Servers

The choice of SIP Server was not a difficult one. After an evaluation of what was offered on the market and excluding all *non* open source software as well as software for operating systems other than Linux/GNU the choice fell on the following:

- The Vovida Open Communication Application Library (VOCAL) provided by Vovida.org

The choice of VOCAL was based on it being the most discussed SIP Server on the market, at the time this thesis project was carried out. It is a fully-fleshed system of components, and the VOCAL Base System satisfied more than our needs in terms of various features.

VOCAL

According to Vovida.org, VOCAL Version 1.5.0 had only been evaluated and tested on Redhat Linux 7.3 running kernel 2.4.18 and hence we decided to set up a Red Hat Linux 9.0 (Shrike) distribution on one of our stationary Compaq PII computers acting as SIP Server/Registrar. The Vovida Open Communication Application Library (VOCAL) base system can be obtained from VOCAL's[97] homepage and here it is also stated that:

> "The Vovida Open Communication Application Library (VOCAL) is an open source project targeted at speeding the adoption of Voice over Internet Protocol (VoIP) implementations by helping developers within the community build VoIP features, applications, and services. The VOCAL software includes a Session Initiation Protocol (SIP) based Redirect Server (RS), Feature Server (FS), Provisioning Server (PS) ,Marshal Server (MS), and Voice Mail Server (vmserver)."

The Vovida package is relatively easy to install, but obviously requires some post install configuration. However, there was a good book all about it to help us out, called *Practical VoIP: Using VOCAL*[14]. Once installed, VOCAL provides a user friendly web-tool for handling e.g. the user database, monitoring the system status, etc.

SIP Express Router (SER)

An alternative to VOCAL, worth remembering, and also evaluated during our choice of SIP server was the SIP Express Router (SER)[112], a light weight alternative to VOCAL. SER was developed by iptel.org and is being provided under terms of GPL, and claims to run on Sun/Solaris, PC/Linux, PC/BSD, and IPAQ/Linux platforms. SER supports both IPv4 and IPv6 and features an application-server interface, presence support, SMS gateway, SIMPLE2Jabber gateway, RADIUS/syslog accounting and authorisation, and server status monitoring.

6.1.2 SIP Clients

The choice of SIP client was more difficult. Perhaps it was mostly a matter of choice, since a great number of SIP clients exists on the market today. Different SIP clients offer different functionality (such as encryption, video conferences, presence, codecs, etc.). The broad array of SIP clients vary from the simplest ones without GUI to more complex well designed ones with all imaginable features.

The SIP clients we used possessed a satisfactory GUI (to have something well designed to demo for PTS and other interesting parties) and included all the functionality we needed.

The SIP clients were implemented as softphones on our laptops, running a light weight distribution of Linux/GNU called CRUX[105].

KPhone

KPhone was the SIP Client mainly utilised in our experiments. With KPhone we obtained the measurements presented in Section 6.3.1. KPhone is a SIP user agent for Linux/GNU, with which you can initiate IP Telephony connections over an IP network. KPhone can be obtained from Wirlab's homepage[95]. It supports Presence and Instant Messaging (IM), and to some extent also video calls between two hosts (although the latter is something we never tried to implement). The original KPhone was written by Billy Biggs, modifications made by Pekka Raisio, Jouni Vuorela and Juha Heinanen at Wirlab. KPhone is easy to install, has a nice GUI, and it (obviously) requires some of the KDE-libraries to function well. KPhone provides three different codecs and beeps via the terminal when there is a incoming phone call. Although stable in general, KPhone seemed to crash from time to time.

Linphone

During our implementation we have had many discussions with Simon Morlat, the author of Linphone and initially we believed that Linphone was going to be the SIP Client mainly used in our evaluations. Linphone is a French simple web-phone, much like KPhone, with a nice GUI that provides the possibility to make two party-calls using an IP network.

Simon claims that Linphone works best with ALSA-drivers[100] and requested in an e-mail to us to "Please use alsa-drivers (the best audio driver of the world)". Unfortunately, even after switching to ALSA-drivers there was still a problem with the communication between Linphone and the sound hardware in our laptops and we decided to instead continue with KPhone.

The advantage of Linphone, though, is that it provides a greater choice of codecs than KPhone. However, this was not a problem since the three codecs supplied by KPhone were satisfactory for performing the tests we wanted. Linphone can be obtained from Linphone's homepage[96].

SIPSet

The Vovida SIPset client was used during the initial phase of our evaluation since it is part of the Vovida-family. However, it was not used during the tests since it is a very limited SIP client and more of a test-tool than a real softphone. SIPSet is a simple SIP User Agent which can be run with or without the included GUI, and SIPSet Version 1.5.0 provides the possibility to make calls through a SIP proxy, to register to receive calls through a SIP proxy, to make and receive calls directly with another user agent, etc.

SIPSet is part of the Vovida-family and can be used as a softphone, to make and receive phone calls from a PC equipped with Linux and audio input and output. SIPSet can be obtained from Vovidas' homepage.[97]

6.2 A Call

We performed calls using two different types of network infrastructures (WLAN and a fixed network) and three different types of SIP operators. The components of the test environment were always set up the same way (see Figure 6.1), using a registrar and two laptops as SIP clients.

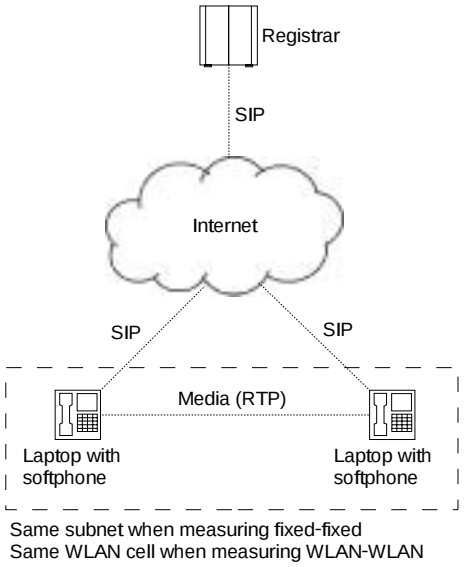

Figure 6.1: *Overview of the Test Environment*

However, the network infrastructure, SIP operators, and to some extent also the SIP clients (although changing the SIP clients does not directly influence the result) were exchanged as we repeatedly performed call tests (see Section 6.3). The two types of networks used were the following:

- Using accounts at KTHOPEN[101] (For wireless access)
- Using accounts at UPC's broadband service Chello (For fixed access)

We got accounts at two SIP operators in addition to the one we had created on our local SIP Server. The different SIP operators we used were the following:

- Our local registrar
- Jeff Pulver's Free World Dialup (FWD) network
- The SIP Center Network Server (maintained and hosted by Ubiquity Software Corporation; founders of The SIP Center[113])

Registering (i.e. to get accounts) at these additional registrars was for free and a rather simple procedure. After registration one can setup the SIP client to contact that specific registrar by providing the IP-address and the username

and password. In KPhone there was a possibility to have profiles, i.e. the client could be started with an argument depending on which registrar the user wants to connect to.

Initially we used only our local registrar to make calls to each other measuring the quality. Although the local registrar possessed a public IP address and was connected to the Internet it was not (after a while) very exiting to perform calls between just the two of us. Consequently, following this successful testing we got accounts at the FWD Network and at the SIP Center Network Server. We performed calls between the two fixed networks, between the two wireless networks, and between the fixed and the wireless network, using the three different registrars as described above. The Free World Dialup project was launched during the winter 1995 by Jeff Pulver. Registering with the above operators (for free) obviously gave us access to a larger SIP user database which made it possible to perform SIP calls to users registered on the same network, but located in different countries.

6.3 Analysis of Testing

We measured the quality in terms of our own perception of the quality, using three different three codecs supported by KPhone: *G.711 μ-law 64 Kbps codec, the GSM codec, and the free speech iLBC codec*[104].

We performed tests during different parts of the days to see if the load on the network had any influence on the quality of the conversation. We also performed calls with all three registrars using the three codecs respectively to a voice mail box where a .WAV-files was placed as a point of reference. During the time of the testing the two laptops were both in the same subnet while performing the fixed-fixed network tests and in the same WLAN cell while performing wireless-wireless network tests. In the two above cases the two laptops were always in Stockholm, and attached to the same router. However, when performing tests between the fixed and the wireless network the laptops were **not** in the same subnet and were also **not** attached to the same router.

The quality in terms of our own perception of the sound quality was measured using the same scale as in Table 3.5, i.e. the Mean Opinion Score (MOS) on a scale (*see Section 3.1.14*) from 1 (bad) to 5 (excellent).

Some measurements of round trip times in the different networks and to and from the various operators were measures using **traceroute**. Basically, the traceroute command sends small packets to the appropriate gateway and records how long the round-trip took in milliseconds. This process is repeated at least 3 times at each gateway. The output of traceroute is in the following order: hop count, gateway name, gateway IP address, RTT for each of the packets.

A traceroute between the two laptops on the fixed network is viewed below:

```
traceroute to 213.89.185.178 (213.89.185.178), 30 hops max, 40 byte packets:

1.  c213-89-185-178.cm-upc.chello.se (213.89.185.178) 0.387 ms 0.319 ms 0.288 ms
```

A traceroute between the two laptops (in the same cell) on the wireless network is viewed below:

```
traceroute to 130.237.5.30 (130.237.5.30), 30 hops max, 40 byte packets:

1.  p30.kthopen.kth.se (130.237.5.30) 75.360 ms 1.596 ms 3.340 ms
```

A traceroute between one of the laptops on the fixed network and one of the laptops at the wireless network is viewed below:

```
traceroute to 130.237.5.113 (130.237.5.113), 30 hops max, 38 byte packets:
1.  c213-89-184-1.cm-upc.chello.se (213.89.184.1) 9.495 ms 11.817 ms 10.286 ms
2.  gsr2-srp4-0.upc.se (213.200.190.130) 16.085 ms 10.899 ms 10.140 ms
3.  se-sto01a-rd2-gige-2-2.aorta.net (213.46.176.1) 12.232 ms 8.939 ms 11.235 ms
4.  se-sto-rd-02-pos-1-0.chellonetwork.com (213.46.176.21) 17.406 ms 11.365 ms 9.334 ms
5.  se-sto01a-rd1-pos-5-0.aorta.net (213.46.176.17) 15.635 ms 12.478 ms 9.342 ms
6.  stk-pr-2-srp1-0.sunet.se (194.68.132.19) 12.381 ms 11.473 ms 10.667 ms
7.  stockholm1-SRP4.sunet.se (130.242.94.8) 12.845 ms 12.364 ms 12.199 ms
8.  stockholm3-POS0.sunet.se (130.242.82.26) 16.691 ms 12.197 ms 10.097 ms
9.  kth1-SRP1.sunet.se (130.242.85.67) 20.616 ms 18.014 ms 11.239 ms
10.  cn4-kth1-b.gw.kth.se (130.237.211.234) 15.953 ms 13.641 ms 13.622 ms
11.  ea2-cn4-p2p.gw.kth.se (130.237.211.198) 14.392 ms 20.982 ms 14.591 ms
12.  bf2-ea4-p2p.gw.kth.se (130.237.211.226) 14.997 ms 14.004 ms 12.423 ms
13.  p113.kthopen.kth.se (130.237.5.113) 22.783 ms 12.699 ms 12.344 ms
```

A traceroute between one of the laptops on the fixed network and the local registrar (also connected to the fixed network) is viewed below:

```
traceroute to 213.89.184.200 (213.89.184.200), 30 hops max, 40 byte packets:
1.  c213-89-184-200.cm-upc.chello.se (213.89.184.200) 0.621 ms 0.303 ms 0.260ms
```

A traceroute between one of the laptops on the wireless network and the local registrar (connected to the fixed network) is viewed below:

```
traceroute to 213.89.184.200 (213.89.184.200), 30 hops max, 40 byte packets:
1.  login1.kth.se (130.237.5.1) 3.106 ms 2.835 ms 17.363 ms
2.  ea4-bf2-p2p.gw.kth.se (130.237.211.225) 3.573 ms 3.669 ms 1.401 ms
3.  cn4-ea2-p2p.gw.kth.se (130.237.211.197) 3.571 ms 4.699 ms 3.367 ms
4.  kth1-cn4-b.gw.kth.se (130.237.211.233) 7.956 ms 1.168 ms 5.075 ms
5.  stockholm3-SRP2.sunet.se (130.242.85.65) 3.618 ms 1.665 ms 3.602 ms
6.  stockholm1-POS6.sunet.se (130.242.82.25) 4.293 ms 3.800 ms 2.830 ms
7.  stkpr3-SRP4.sunet.se (130.242.94.7) 3.986 ms 4.303 ms 1.686 ms
8.  se-sto01a-rd1-srp-1-1.aorta.net (194.68.132.89) 3.806 ms 5.665 ms 3.854 ms
9.  213.46.176.42 (213.46.176.42) 4.768 ms 2.264 ms 4.014 ms
10.  gsr1-gige-1-0.upc.se (213.46.176.6) 4.077 ms 4.067 ms 2.070 ms
11.  to-c7200-1-srp1-0.upc.se (213.200.190.134) 6.707 ms 4.274 ms 2.601 ms
12.  c213-89-184-200.cm-upc.chello.se (213.89.184.200) 14.012 ms 13.240 ms 15.549 ms
```

A traceroute between one of the laptops on the fixed network and the SIP Center registrar (on a different subnet and attached to a different router) is viewed below:

```
traceroute to sip.sipcenter.com (80.248.33.37), 30 hops max, 40 byte packets:
1.  c213-89-184-1.cm-upc.chello.se (213.89.184.1) 6.440 ms 5.767 ms 6.362 ms
2.  gsr2-srp4-0.upc.se (213.200.190.130) 6.675 ms 12.501 ms 9.605 ms
3.  se-sto01a-rd2-gige-2-2.aorta.net (213.46.176.1) 8.198 ms 8.001 ms 9.030ms
4.  se-sto-rd-02-pos-1-0.chellonetwork.com (213.46.176.21) 10.398 ms 7.043 ms 8.804 ms
5.  nl-ams01a-rd1-gige-4-0.aorta.net (213.46.160.225) 56.162 ms 52.884 ms 5566 ms
6.  * uk-lon01a-rd2-pos-1-2.aorta.net (213.46.160.150) 170.277 ms 164.353 ms
7.  uk-lon01a-rd1-pos-1-0.aorta.net (213.46.174.1) 163.867 ms 162.945 ms 16199 ms
```

```
8.  uk-lon01a-ri1-ge-2-0-0.aorta.net (213.46.174.30) 162.121 ms 165.999 ms 2.475 ms
9.  GigabitEthernet5-0.linx1.lon1.level3.net (195.66.224.77) 163.831 ms 167.5 ms 164.133 ms
10.  unknown.Level3.net (212.113.3.29) 166.094 ms 162.987 ms 163.226 ms
11.  * so-7-0-0.mp2.London1.Level3.net (212.113.3.9) 165.990 ms 163.410 ms
12.  so-3-0-0.mp2.Amsterdam1.Level3.net (212.187.128.13) 172.636 ms 176.365 ms 171.869 ms
13.  gige8-0.ipcolo1.Amsterdam1.Level3.net (213.244.165.39) 173.336 ms 171.64ms 172.903 ms
14.  ippowerhouse-gw.level3.net (212.72.45.2) 174.683 ms 174.218 ms 174.320ms
15.  80.248.32.37 (80.248.32.37) 176.696 ms 170.495 ms 173.197 ms
16.  80.248.33.37 (80.248.33.37) 172.363 ms 171.780 ms
```

A traceroute between one of the laptops on the wireless network and the SIP Center registrar (on a different subnet and attached to a different router) is viewed below:

```
traceroute to sip.sipcenter.com (80.248.33.37), 30 hops max, 40 byte packets:
1.  login1.kth.se (130.237.5.1) 4.818 ms 2.769 ms 2.773 ms
2.  ea4-bf2-p2p.gw.kth.se (130.237.211.225) 3.461 ms 3.513 ms 2.571 ms
3.  cn4-ea2-p2p.gw.kth.se (130.237.211.197) 3.636 ms 4.937 ms 3.436 ms
4.  kth1-cn4-b.gw.kth.se (130.237.211.233) 3.268 ms 5.228 ms 3.360 ms
5.  stockholm3-SRP2.sunet.se (130.242.85.65) 3.648 ms 3.410 ms 3.817 ms
6.  stockholm1-POS6.sunet.se (130.242.82.25) 6.467 ms 1.926 ms 4.148 ms
7.  s-gw.nordu.net (193.10.252.181) 3.903 ms 3.779 ms 2.058 ms
8.  POS1-0.hsipaccess1.Stockholm1.Level3.net (213.242.69.17) 3.933 ms 5.862 ms 1.899 ms
9.  ae0-15.mpls1.Stockholm1.Level3.net (213.242.68.33) 4.201 ms 3.972 ms 2.024 ms
10.  so-3-0-0.mp2.Amsterdam1.Level3.net (212.187.128.13) 31.941 ms 31.979 ms 31.786 ms
11.  gige11-1.ipcolo1.Amsterdam1.Level3.net (213.244.165.83) 31.957 ms 31.986 ms 31.967 ms
12.  ippowerhouse-gw.level3.net (212.72.45.2) 38.620 ms 38.408 ms 38.225 ms
13.  80.248.32.37 (80.248.32.37) 39.007 ms 39.590 ms 41.115 ms
14.  80.248.33.37 (80.248.33.37) 39.263 ms 39.212 ms 39.065 ms
```

The RTTs between the laptops did not suggest any delay for a IP Telephony call neither between the fixed networks, nor between the wireless networks, nor between the fixed and the wireless network.

In the above routes there were no significant packet loss. However, the packet loss, and the type of network and codec used have great influence on IP Telephony MOS scores (and consequently also in QoS measures) as discussed e.g. in ETSI Workshop on QoS in Next Generation Networks (Speech Coders - a VoIP perspective) by Alan Duric[110] and Speech Coders - a VoIP perspective by Roar Hagen[111]. These reports show, among other things, how network congestions and packet loss affects MOS scores and furthermore the report comes up with real measurements of jitter and packet loss during an IP Telephony phone call between different places in The United States, China, and Hong Kong.

6.3.1 Results

From the results of our measures (*see Table 6.1*) of our own perception of the quality during the call one can draw a couple of conclusions. No major unexpected values were encountered during the implementation.

Registering with different operators we were able to make a comparison of how operators might differ from each other. In our case there was no difference and

Network	G.711 μ-law Codec	GSM Codec	iLBC Codec[104]
WLAN-WLAN	4	3.5	3
WLAN-Fixed	4	3.5	3
Fixed-Fixed	4	3.5	3

Table 6.1: *Results from Testing Quality of IP Telephony Calls*

therefore we have not included the SIP operator in Table 6.1. It is not evident that it is always true since various operators will probably provide different services and handle SIP traffic differently.

The above results compare well with MOS Scores (*see Table 3.5*). The MOS score for the 64 Kbps G.711 μ-law codec is 4.1 (as compared to 4 above) and the MOS score for the 13 Kbps GSM codec is 3.54 (as compared to 3.5 above). However, the 13.33 Kbps iLBC (internet Low Bitrate Codec) is not included in Table 3.5. iLBC is a **free** speech codec suitable for robust voice communication over IP. Unlike current low bit rate codecs such as ITU G.729, G.723.1, GSM-EFR, and 3GPP-AMR (developed for traditional telephony) based on the CELP (Code Excited Linear Prediction) paradigm i.e. they are stateful, they have memory, and error propagation results from lost or delayed packets, iLBC treats every packet individually, making it suitable for packet communications.

It is important to understand that the operators handle and influence **only** the SIP traffic as the RTP traffic (the media content) travels end-to-end between the users and is consequently out of the scope of the operators.

Looking at the results it is furthermore obvious that the type of network (WLAN or fixed) also does not change the perceived quality of the call. These (relatively fast) networks are more than satisfactory for IP Telephony calls using the codecs above. However, when we phoned countries such as Russia, France, and Yugoslavia using the FWD registrar, we experienced both significant delay and packetloss.

Finally we would once again like to emphasise (and in this way hopefully encourage readers) that the relative simplicity and the possibility for every consumer in the traditional network to become their own operator in the world of IP Telephony means a decentralisation and a shift in the traditional roles of the telecommunication world.

6.3.2 Conclusion

As discussed previously (*see Section 6.2*) and as proven by the experiments above, it is easy for a user to switch between different registrars such as the SIP Center registrar and the FWD registrar. This gives rise to a number interesting questions concerning regulatory issues such as: Should there be regulations of the registrars? Should there be regulation with respect to clients? Do normal business regulations take care of your expectations for commercial services from the network, from the registrar, and if you purchase a client?

For example, even if PTS regulates registrars that exist in Sweden, since a user can use any registrar anywhere on the Internet. The choice of registrar is equivalent for the user (except for maybe the propagation delays).

Worth noting is also that while a user can have only a Swedish E.164 number

(i.e. +46 xxx xxxx) mapping in Sweden there is nothing that stops him or her from using a SIP URL such as "user@hpt.hr" with a different country code. How important will it be to have a phone number in the traditional sense? Furthermore it is possible to have multiple numbers as from a company such as Digisip a user can have a block of numbers since only the first N digits matter to Digisip and the rest can be mapped by the user's SIP proxy. In addition to this a user can have multiple numbers from multiple registrars in multiple countries and while each of them might be regulated by different regulators the different phone numbers might map to the same SIP URL (which points to a server in yet another country).

Hence, as one might regulate local network operators within a country's jurisdiction, there is no clear regulatory frame work outside this country (see the work of Alberto Escudero concerning European Union Data Protection Policy[74]). Suppose one might be able to get a court order in Sweden and force an operator such as Digisip to reveal SIP traffic between their server and a specific user. Since Digisip as an operator does not handle any of the content they can not consequently be forced to disclose the actual media being sent. In addition, since user can use encrypted SDP content (*see Section 3.2.2*) Digisip may not even be able to reveal the addresses used by the RTP traffic. A similar situation could occur for instant messaging content since the SIP body can be protected by S/MIME (*see Section 3.2.2*).

There is obviously little which the regulators can do about regulating the clients, nor any clear precedent in which they have done so, since the traditional rules which regulates the public network were based on physical damage to the network rather than its higher level effects. It is clearly impossible, for example, to forbid someone to program a SIP client and distribute it as free software over the Internet.

Chapter 7

Conclusions and Future Work

This chapter is intended to tie up all the loose ends and summarise the respective conclusions of the previous chapters. In all aspects, this conclusion predicts the future for IP Telephony.

It will also include topics that influence and affect IP Telephony, but were not included in the earlier parts of the report.

7.1 King of the Hill

If the intentions of PTS and the goals for The Electronic Communications Act are reached, there will be free entry to the market to a much larger extent than today, which asymptotically will lead to a market of perfect competition. In practice, this will lead to more operators which in turn will lead to reduced prices for consumers and consequently will give customers the ability to choose from a greater variety of networks, services, and operators.

The authors believe that there are two ways in which IP Telephony can be utilised to transform traditional switched networks of electronic communications, although one does not have to exclude the other (*see Section 4.1*):

Transit Upgrade
: Exchanges in different levels of the network will gradually be replaced by IP based solutions. Large parts of the local loop will, due to incumbent operators and the existence of a solid infrastructure, remain fairly untouched.

The Island Kingdom
: In this scenario consumers will abandon the traditional telephony and traverse to a pure IP telephony services.

As these different scenarios evolve the market will naturally evolve accordingly. The twining of these scenarios, which is the most probable outcome for the future, makes it hard to predict winners and losers in the future market of

electronic communications. A pure "The Island Kingdom" scenario would most likely lead to numerous IPTSPs emerging and trying to grab the biggest possible chunk of the consumer market as they are capable of. A dispersal of users akin to that of the e-mail provision of today, is not entirely unlikely. In the case of "Transit Upgrade" the scene might be somewhat different. The increased efficiency, that IP Telephony technology brings to the incumbent network operators, may reduce margins for their competitors, that today might thrive from the opportunities that rise from e.g. law enforced cost-based interconnection deals.

7.2 Buying the Pig in the Poke

As previously discussed (*see Section 6.3.2*) the difficulty in regulating different operators possessing registrars and other network components as these might be geographically located in a completely different area without the user noting much of a difference (except for the propagation delay) results in the difficulty for PTS to maintain supervision. Another problem is for the users to be sure that they are really getting the expected service that they are paying for. One thing which PTS could do would be to establish test programs, which user's can use to decide themselves if they are getting this expected service, much like the testing of ISP through put (such as TPTEST developed by the The Swedish ICT-Commission[114]) that exists already today in which users via their Internet connections can determine their bandwidth to and from various places where test servers are placed. A secondary activity might be keeping a web page of quality evaluations conducted by PTS or third party testing labs, of the quality of specific operators, as an information service for the public.

In addition to the above various client measurement tools for real time analysis of the network characteristics (such as round-trip times and jitter) can be made available by PTS, much like what Lars Aronsson talks about in an e-mail[115] to the Elektrosmog[116] mailing list on 25 October 2002, where he suggests having a utility which would run in the background and display round-trip time and jitter displaying a "signal quality meter" on the screen, using a scale of 0-3 (red, useless quality), 4-7 (yellow, satisfactory quality), and 8-10 (green, excellent quality). If the above scenarios are applied it would help the consumers to maintain awareness of the quality of the services they utilise. This would, in outline with the aim of PTS, bring forth competition on the market. However, specific Societal services such as emergency calls can not be supervised by these means. For these kind of services the supervisory authority must find alternate ways to make them available to the consumers.

7.3 Public vs. Private networks

Deploying IP Telephony within public and private networks are two rather different tasks. Mainly the question concerns the control and overview an administrator has in the limited private networks as opposed to the free uncontrolled world of the public networks. In the previous case, it is possible to provide a certain predefined QoS as the characteristics of the infrastructure of the network as well as the number of users, etc are known. Since there are many

different protocols for various tasks an administrator can decide to set up and support a standardised family of protocols for various services demanded by the users. Furthermore it is possible to provide the same end-devices with the same features and capabilities to all users within the limited network.

Providing the above mentioned three parameters in public networks is a much more difficult task as there is no single authority that controls the entire network. Consequently, with several IP telephony architectures (i.e. a public network), the signalling and media information will traverse several IP networks controlled by different entities (different service providers, different operators) which make it very difficult to control.

7.4 The Intelligence of the Endpoints

Device convergence (*see Section 2.1*) means the merging of different devices with different functions and in order for this to happen the placement of intelligence will have to be moved. In traditional PSTN networks, the phones are no more than a simple terminal and the telephony switch holds the actual intelligence. For IP Telephony much of this intelligence is moved to the end-points, i.e. the SIP clients. At the same time as this is positive on one hand as the users get more influence on the setup of the devices themselves at the same time as these devices will be rather powerful, it also increases the requirements of actually understanding the device the user is dealing with on the other hand. Everyone knows how an analogue phones function and there is no bigger difference between the phones themselves. There is no similar guarantee on the end-devices in the IP Telephony world as they can possess different characteristics, features, and support different services. This obviously raises the demand for support on these products and this might lead to the phenomenon similar to the computing world today where most people can not start the program after someone has deleted the shortcut from their desktop. Our mothers would never ask us to explain to them how to make a phone call using the analogue phone at home but most probably they will do so after purchasing e.g. a Cisco IP Telephone.

7.5 Prices and Costs

The complicated economic matters involved in regulation is to some extent beyond the scope of this report, but none the less important to the development of the market of electronic communications.

The increased competition, that the regulation of the market for electronic communications is supposed to bring forth, should lower consumer prices. To ensure that the actions taken will actually give the intended results, the terminology and the angle of approach used in the legislation is naturally of great importance.

For example, a company imposed with competition improving actions, that obligates incumbents to provision interconnection at cost-based prices, can put the competition out of play simply by keeping their costs at a high level. In addition to creating barriers to entry and reducing the margins for parties utilising this interconnection, it obviously does nothing to lower consumer prices. Thus, SMPs might have to be held under scrutiny and stricter obligations may

be needed to improve competition. The Electronic Communications Act has the ability to impose this and it remains to be seen what effect it will have on consumer prices.

7.6 The Call

One of the main questions evolving around this topic (*see Section 3.5*) is how much longer it will be important for users to have a E.164 number in traditional means? Also, as discussed previously, (*see Section 3.5*) how much longer will the gateways between the IP Telephony world and the PSTN network play an important role?

The authors believe that there may take some time before the consumers will switch completely to pure IP Telephony solutions (*see Section 4.1.1*) depending on the utilisation of the technology and the strategies deployed by the incumbent operators. In order to speed up the expansion of IP Telephony usage, a IP Telephony software client could be included as standard in most common operating systems (*see Section 4.1.2*).

7.7 Future Work

We have identified a number of topics in which more work has to be done. The topics that follow, are topics that originate from areas that have been given low priority in our work due to lack of time, their relative irrelevance, or because they have been outside of the scope of this project. A brief discussion of these different topic areas is given in each of the subsequent sections.

7.7.1 Accounting

Accounting in IP Telephony networks is more than simple charging. Accounting may be a (simple) list of services accessed, servers accessed, duration of session, etc. Charging for SIP sessions could be extremely complex and requires some additional study. Another question is **why** the charging is this complex and does it necessarily **have** to be and furthermore **who** will we billing the users, the latter of which an attempted answer will follow. As the operators do not handle any of the content (and if they do not have their own networks such as Digisip[49]) the only thing they could charge the users for (during pure IP Telephony calls) is the setup of the phone call as well as various services that they might provide. However, if the operators are acting ISPs at the same time providing IP Telephony such as Bredbandsbolaget[106] they can obviously charge the users for the traffic traversing their network.

The authors believe that this might lead to that ISPs will charge the users for the **amount** of traffic instead of having a fixed cost and according to this the users can choose what quality they want on their calls, what type of media it should be (audio, video), etc.

7.7.2 The Risks of IP Telephony

IP telephony brings the terms phreaker and hacker closer together than ever before. Several characteristics of IP telephony make it easier for a hacker to try to compromise and/or control different aspects or parts of the IP telephony-based network. Compared to the PSTN, IP telephony-based networks face a greater security threat as a result of a combination of various factors. For example, the increased intelligence of the end-points (*see Section 7.2*) and hence and ability to interact with different IP telephony components and services as well as different networking components within the IP telephony network, means that a malicious user using such an endpoint, or a modified client, will have the same ability to interact with these components. This is in contrast with the PSTN, where a phone is only able to interact with its telephony switch. The ability of an endpoint to interact with more IP telephony-based elements and network components poses a greater risk of misuse for an IP telephony-based network compared with the PSTN, where the switch a phone is connected to is the most likely to be attacked.

7.7.3 Extensive QoS testing

More extensive and in depth analysis of QoS measures would have been performed in case the time would have allowed it. Examples of interesting measures are how the quality of a call such as the delay and jitter changes while the network gets congested and the packet loss increases with respect to different types of codecs.

Bibliography

[1] William Stallings (1997) *Data and computer communications.* Prentice Hall, ISBN 0-13-571274-2.

[2] *The Swedish Radiocommunications Act (1993:599)* http://www.pts.se/dokument/getFile.asp?FileID=1715, accessed 2003-04-07

[3] *The Swedish Telecommunications Act (1993:597)* http://www.pts.se/dokument/getFile.asp?FileID=2320, accessed 2003-03-26

[4] *The Swedish Competition Act (1993:20)* http://www.kkv.se, accessed 2003-03-26

[5] *PTS' homepage* http://www.pts.se, accessed 2003-02-20

[6] *Telelagen och Internet* http://www.pts.se/dokument/getFile.asp?FileID=1167, accessed 2003-04-13

[7] *Telefonnummer på framtida marknader - PTS-ER-2002:1*

[8] *Tillit till IT vid Internetanvändning - PTS-ER-2002:24 - 1 november 2002*

[9] *I backspegeln - Erfarenheter av tio år med telelagen - PTS-ER-2003:5*

[10] *ENUM - funktion som översätter telefonnummer till Internetbaserade adresser - En beskrivning samt möjligt införande i Sverige - PTS Mars 2001*

[11] *SOU 1999:55* Statens offentliga utredningar 1999:55.

[12] *SOU 2002:060* Statens offentliga utredningar 2002:60

[13] *Proposition 2002/2003:110* Regeringens proposition 2002/03:110 Lag om elektronisk kommunikation, m.m.

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

[15] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, *RFC 2543 - SIP: Session Initiation Protocol*. http://rfc.sunsite.dk/rfc/rfc2543.html, accessed 2003-02-26

[16] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, *RFC 3261 - SIP: Session Initiation Protocol*. ftp://ftp.rfc-editor.org/in-notes/rfc3261.txt, accessed 2003-02-27

[17] Jonathan Davidson, James Peters, and Brian Gracel, (2000) *Voice over IP Fundamentals*. Cisco Press; 1st edition, ISBN 1578701686

[18] *New Regulatory Framework* http://europa.eu.int/information_society/topics/telecoms/regulatory /new_rf/text_en.htm, accessed 2003-02-27

[19] *NOSKI Protocol Stack ISP* http://www.softfront.co.jp/en/product/embedded/sipstack.html, accessed 2003-02-27

[20] Ken Camp, (2003) *IP Telephony Demystified*. McGraw-Hill Professional, ISBN 0071406700

[21] *General information about IP Telephony* http://www.dotcom.se/ip_telefoni/ip_telefoni.asp, accessed 2003-03-01

[22] Anders Roxenhag, (December 2000) *VoIP and IPSec* M.Sc. thesis, Department of Microelectronics and Information Technology, KTH

[23] T. Dominique, (January 2001) *Information Service Based on SIP* M.Sc. thesis, Department of Microelectronics and Information Technology, KTH

[24] F. Thernelius, (May 2000) *SIP, NAT, and Firewalls* M.Sc. thesis, Department of Teleinformatics, KTH

[25] *Internet Telephony - The Regulatory Issues (McCarthy Tétrault LLP* http://www.mccarthy.ca/pub_docs/docview.asp?file=mt

[26] *SIP / H.323 Comparison* http://www.nuera.com/applications/sipH323pfv.cfm, accessed 2003-03-20

[27] *H.323 versus SIP: A Comparison* http://www.packetizer.com/iptel/h323_vs_sip/, accessed 2003-03-20

[28] *SIP: Comparison of SIP and H.323* http://www.cs.columbia.edu/~hgs/sip/h323-comparison.html, accessed 2003-03-20

[29] *Comparison of H.323 and SIP for IP Telephony Signaling* http://www.cs.columbia.edu/~hgs/papers/others/Dalg9909_Comparison.pdf, accessed 2003-03-20

[30] *SIP versus H.323* http://www.iptel.org/info/trends/sip.html, accessed 2003-03-20

[31] *SIP - Specific Event Notification RFC3265, June 2002, Obsoletes RFC2543, Updates RFC3265*
ftp://ftp.rfc-editor.org/in-notes/rfc3265.txt, accessed 2003-03-15

[32] *Internet Official Protocol Standards (SD1)*
ftp://ftp.rfc-editor.org/in-notes/std/std1.txt, accessed 2003-03-15

[33] *Background materials from ITU - misc. topics*
http://www.itu.int/osg/spu/ni/iptel/, accessed 2003-03-15

[34] ITU, (2001) *ITU Internet Reports IP Telephony.* ISBN 92-61-08621-7

[35] *ENUM in Sweden*
http://www.nic-se.se/, accessed 2003-03-16

[36] *Internet Engineering Task Force*
http://www.ietf.org/, accessed 2003-03-20

[37] *3GPP - A global initiative*
http://www.3gpp.org, accessed 2003-03-20

[38] *Security threats and models*
http://www.vide.net/conferences/spr2002/presentations/chatterjee.ppt , accessed 2003-02-15

[39] *IP-telefoni i Sverige*
http://www.ip-telefoni.se/, accessed 2003-03-20

[40] *The Market*
http://www.mindbranch.com/listing/tl-tele.html, accessed 2003-02-15

[41] G.Q. Maguire Jr. (2003) *2G5564 Practical Voice over IP (VoIP), lecture slides*, KTH
http://vvv.it.kth.se/edu/Ph.D/2G5564/VoIP-20030226.pdf, accessed 2003-03-20

[42] *The OpenH323 Project*
http://www.openh323.org/, accessed 2003-02-20

[43] *The H.323 Forum*
http://www.h323forum.org/, accessed 2003-03-31

[44] *Edvina.net*
http://www.edvina.net, accessed 2003-03-25

[45] *The WLAN forum*
http://www.wlan-forum.net, accessed 2003-03-25

[46] Walter J. Goralski and Matthew C. Kolon (2000) *IP Telephony.* McGraw-Hill, ISBN 0-07-135221-X

[47] Gilbert Held (1998) *Voice over Data Networks.* McGraw-Hill, ISBN 0-07-028135-1

[48] *Gnome meeting's homepage*
http://www.gnomemeeting.org/, accessed 2003-03-24

[49] *Digisip's homepage*
http://www.digisip.se/, accessed 2003-03-24

[50] *Windows Messenger for Windows XP*
http://messenger.msn.com/, accessed 2003-03-24

[51] *AT&T Bell Laboratories*
http://www.research.att.com/, accessed 2003-03-31

[52] Paul Baran, *On Distributed Communications Networks* , IEEE Transactions on Systems, March 1964.

[53] *Telia Pressrelease - 880445927*
http://han16ns.telia.se/telia/thk/thkpre52.nsf/vNyhetEfocus/9D9A84CC76BD32EC41256D0900314637, accessed 2003-04-16

[54] *VocalTec - The Voice of Next Generation Networks™*
http://www.vocaltec.com/, accessed 2003-03-31

[55] *The Internet Telephony Consortium*
http://itel.mit.edu/itel/newind.html, accessed 2003-03-31

[56] *Session Initiation Protocol (SIP) Working Group*
http://www.ietf.org/html.charters/sip-charter.html, accessed 2003-03-31

[57] *SMU School of Engineering - Internet Communications using SIP*
http://smuhandouts.com/8393/SIPTutorial.pdf, accessed 2003-04-01

[58] *SAP - Session Anouncement Protocol*
ftp://ftp.rfc-editor.org/in-notes/rfc2974.txt, accessed 2003-04-03

[59] *An Extension to HTTP : Digest Access Authentication*
ftp://ftp.rfc-editor.org/in-notes/rfc2069.txt, accessed 2003-04-04

[60] *The IP Network Address Translator (NAT), RFC1639, May 1994*
ftp://ftp.rfc-editor.org/in-notes/rfc1631.txt, accessed 2003-04-07

[61] *IP Network Address Translator (NAT) Terminology and Considerations, RFC2663, August 1999*

[62] *Session Initiation Proposal Investigation (sipping)*
http://www.ietf.org/html.charters/sipping-charter.html

[63] *J. Rosenberg, H. Salama, and M. Squire, Telephony Routing over IP (TRIP) , IETF RFC 3219, January 2002*

[64] *J. Rosenberg, R. Mahy, and S. Sen, NAT and Firewall Scenarios and Solutions for SIP, IETF Internet Draft, June 24, 2002*

[65] *J. Rosenberg, J. Weinberger, C. Huitema, and R. Mahy, STUN - simple traversal of UDP through NATs, IETF Internet Draft, April 2002.*

[66] *C. Huitema, RTCP attribute in SDP, IETF Internet Draft, February 2002*

[67] *J. Rosenberg, J. Weinberger, and H. Schulzrinne, SIP extensions for NAT traversal, IETF Internet Draft, November 2001*

[68] *D. Yon, Connection-oriented media transport in SDP, IETF Internet Draft, May 2002*

[69] *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*

[70] *International Engineering Consortium - H.323 Tutorial* http://www.iec.org/online/tutorials/h323/index.html, accessed 2003-04-14

[71] *J. Rosenberg and H. Schulzrinne, Guidelines for Authors of Extensions to the Session Initiation Protocol (SIP), IETF Internet Draft, November 2002*

[72] *H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson, RTP: A Transport Protocol for Real-Time Applications, IETF RFC1889, January 1996*

[73] *The Internet Assigned Numbers Authority* http://www.iana.org/, accessed 2003-04-20

[74] *Alberto Escudero Pascual, European Union Data Protection Policy 'Location privacy in the next generation mobile Internet', IMIT - IT University, April 2002*

[75] *RSVP Protocol Overview* http://www.isi.edu/rsvp/overview.html, accessed 2003-04-25

[76] *Network Fusion - The leader in Network Knowledge* http://www.nwfusion.com/, accessed 2003-04-25

[77] *P. Faltstrom, E.164 number and DNS, RFC2916, September 2000*

[78] *M. Mealling, R. Daniel, The Naming Authority Pointer (NAPTR) DNS Resource Record, RFC2915, September 2000*

[79] *Cisco Systems, Understanding Codecs: Complexity, Hardware Support, MOS, and Negotiation, December 2002* http://www.cisco.com/warp/public/788/voip/codec_complexity.pdf, accessed 2003-05-07

[80] *Codec Central* http://www.siggraph.org/education/materials/HyperGraph/video/codecs/Default.htm, accessed 2003-05-07

[81] *H. Schulzrinne, A. Rao, R. Lanphier, Real Time Streaming Protocol (RTSP), RFC2326, April 1998*

[82] *F. Cuervo, N. Greene, A. Rayhan, C. Huitema, B. Rosen, J. Segers, Megaco Protocol Version 1.0, RFC3015, November 2000)*

[83] *Service in the PSTN IN Requesting InTernet Service SPIRITS Working Group*

[84] *M. Handley, V. Jacobson, SDP: Session Description Protocol, RFC2327, April 1998*

[85] *S. Olson, G. Camarillo, A. B. Roach, Support for IPv6 in Session Description Protocol (SDP), RFC3266, June 2002*

[86] *ITU-T Recommendation E.164, The international public telecommunication numbering plan (05/97)*

[87] *Regeringens beslut, Uppdrag att genomföra ett nationellt försök avseende ENUM, 2001-12-06*
http://www.pts.se/dokument/getFile.asp?FileID=2759, accessed 2003-05-18

[88] *The ITU-T Telecommunication Standardization Bureau (TSB)*
http://www.itu.int/ITU-T/info/tsb/info.html, accessed 2003-05-18

[89] *Internet Architecture Board (IAB)*
http://www.iab.org/, accessed 2003-05-18

[90] *The Internet Engineering Steering Group*
http://www.iesg.org/iesg.html, accessed 2003-05-18

[91] *PTS' request for delegation of the ENUM country code zone*
http://www.ripe.net/ripencc/mail-archives/enum-request-arch+46/2002/msg00000.html, accessed 2003-05-25

[92] *Cathleen Moore, XMPP rises to face SIMPLE standard, InfoWorld, April 18th 2003*
http://www.infoworld.com/article/03/04/18/16imstandards_1.html, accessed 2003-05-27

[93] *M. Day, J.Rosenberg, H. Sugano, A Model for Presence and Instant Messaging, RFC2778, February 2000*

[94] *Jabber Software Foundation*
http://www.jabber.org/, accessed 2003-05-27

[95] *Wirlabs' homepage*
http://www.wirlab.net/kphone/,accessed 2003-06-02

[96] *Linphone's homepage*
http://linphone.org/, accessed 2003-06-02

[97] *VOVIDA.ORG - Your Source for Open Source Communication*
http://www.vovida.org/, accessed 2003-06-02

[98] *Xten Networks' homepage*
http://xten.com/, accessed 2003-06-02

[99] *Pulver.com*
http://www.pulver.com/, accessed 2003-06-02

[100] *Advanced Linux Sounds Archtecture*
http://www.alsa-project.org/, accessed 2003-06-02

[101] *KTHLAN - the Local Area Network of Royal Inst of Technology*
http://www.lan.kth.se/

[102] *Requirements for Emergency Telecommunication Capabilities in the Internet* Internet Draft - "work in progress", Expires: April 2003
http://www.ietf.org/internet-drafts/draft-ietf-ieprep-requirements-01.txt

[103] *K. Egevang and P. Francis, The IP Network Address Translator (NAT), IETF RFC1631, Mayb 1994*

[104] *iLBC Freeware Project Homepage*
http://www.ilbcfreeware.org/, accessed 2003-06-05

[105] *CRUX's homepage*
http://www.crux.nu/, accessed 2003-06-05

[106] *Bredbandsbolaget's homepage*
http://www.bredband.com/, accessed 2003-06-05

[107] *Freeworld Dialup's homepage*
http://www.freeworldialup.com/, accessed 2003-06-05

[108] *Intertex's homepage*
http://www.intertex.se/, accessed 2003-06-13

[109] Stefan Alfredsson, 2003 *Practical Voice over IP - project report*
http://www.cs.kau.se/ alfs/voip/, accessed 2003-05-20

[110] Alan Duric *Speech Coders - a VoIP perspective (ETSI Workshop on QoS in Next Generation Networks)* Global IP Sound
http://www.etsi.org/qosworkshop/ETSI_NGN_QoS_Workshop/
V%20-%20Alan%20Duric%20-%20SpeechCoders_aVoIP_perspective.pdf

[111] Roar Hagen *Speech Coders - a VoIP perspective* Gloval IP Sound
http://www.itu.int/itudoc/itu-t/workshop/converge/s6am-p4_pp7.ppt

[112] *The SIP Express Router's homeage*
http://www.iptel.org/ser/, accesses 2003-06-01

[113] *The SIP Center homepage*
http://www.sipcenter.com/, accessed 2003-06-01

[114] *The Swedish ICT-Commission's homepage*
http://www.itkommissionen.se/index.html, accessed 2003-06-20

[115] *An idea to investigate, displaying current quality*
http://vvv.it.kth.se/edu/Ph.D/2G5564/Idea1.html, accessed 2003-06-20

[116] *Elektrosmog's homepage*
http://www.elektrosmog.nu/, accessed 2003-06-20

Appendix A

Appendix

A.1 Acronyms and abbreviations

DNS	Domain Name System
FAX	Facsimile Service
FTP	File Transfer Protocol
H.323	Protocol defined in ITU-Recommendation H.323
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
NAPTR	Naming Authority PoinTeR
PSTN	Public Switched Telephone Network
RFC	Request For Comment
RIPE NCC	Reseaux IP Europeens Network Control Center
RR (DNS)	Resource Record
SIP	Session Initiation Protocol
URI	Uniform Resource Identifier
VoIP	Voice over IP
AOR	Address of Record
ALG	Application Level Gateway
CODEC	compression/decompression
DNS	Domain Name Server
FQDN	Fully Qualified Domain Name
IEEE	Institute for Electric and Electronic Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
LAN	Local Area Network
MIME	Multipurpose Internet Mail Extensions
MOS	Mean Opinion Score
NAT	Network Address Translation

PDA	Personal Digital Assistant
PoE	Power over Ethernet
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request For Comments
RTCP	Real Time Control Protocol
RTSP	Real Time Streaming Protocol
RTP	Real-time Transport Protocol
RTT	Round-Trip Time
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMP	Significant Market Power
SNPAC	Swedish Number Portability Administrative Center
SS7	Signal System 7
TCP	Transmission Control Protocol
TLS	Transport Layer Security
URI	Universal Resource Identifier
UDP	User Datagram Protocol
URL	Universal Resource Locator
WLAN	Wireless LAN