

LAPPEENRANTA UNIVERSITY OF TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY

**Implementation of Signaling Gateway between Telephone Network
and the Internet**

The subject of this Master's thesis has been approved by the board of Department of Information Technology on 17.01.2001

The thesis has been inspected by docent Jarmo Harju. MSc Esa Vepsäläinen has supervised the author during the work.

Helsinki 05.11.2001

Jussi Savola
Seunalantie 3-5 B 7
00730 HELSINKI
+358 40 5513838

ABSTRACT

Author: Savola, Jussi
Name: Implementation of Signaling Gateway between Telephone
Network and the Internet
Department: Information technology
Year: 2001
Place: Helsinki

Master's thesis. Lappeenranta University of Technology. 51 pages, 23 figures, 1 table and 2 appendices.

Inspector: docent Jarmo Harju
Keywords: MEGACO, ISUP, PSTN, SIP, IP, H.323, signaling protocol

This thesis examines the requirements for a network node, which connects H.323, MEGACO and ISUP signaling protocols. Typically the described protocols are interfaced when connecting IP-based and traditional telephone networks together.

Firstly, the structure and signaling of PSTN network is examined. After that, focus is laid on internet protocols related to the scenario. The main body of the thesis contains an evaluation of the functionality needed for interconnecting the IP- and PSTN-based telephone networks.

The practical part of the work describes some of the message sequence charts that the signaling node performs. No particular interest is paid to description of the parameters of these messages.

TIIVISTELMÄ

Tekijä: Savola, Jussi
Nimi: Implementation of Signaling Gateway between Telephone
Network and the Internet
Osasto: Tietotekniikan osasto
Vuosi: 2001
Paikka: Helsinki

Diplomityö. Lappeenrannan teknillinen korkeakoulu. 51 sivua, 23 kuvaa, 1 taulukko ja 2 liitettä.

Tarkastaja: dosentti Jarmo Harju
Hakusanat: MEGACO, ISUP, PSTN, SIP, IP, H.323, signaalointiprotokolla

Tässä diplomityössä perehdytään verkkoelementiltä, joka yhdistää H.323, MEGACO- ja ISUP-protokollia käyttävät tietoliikenneverkot toisiinsa, vaadittaviin ominaisuuksiin ja toiminnallisiin. Tyypillisesti tällaista toiminnallisuutta tarvitaan IP- ja PSTN-verkkojen yhdistämisessä.

Tarkastelu aloitetaan kuvaamalla PSTN-verkon signointi ja rakenne, jatketaan kuvaamalla internet-protokollia käyttävä verkkoympäristö ja lopuksi perehdytään verkkoelementiltä vaadittaviin toiminnallisiin, jotta PSTN ja MEGACO-pohjaiset verkot toimivat yhteen.

Työn käytännöllisenä osuutena kuvataan osa viestisekvenssikaavioista, joita verkkoelementti toteuttaa puuttumatta kuitenkaan eri protokollien toimintaan viestien parametrien tasolla.

FOREWORD

This thesis has been written for the Lappeenranta University of Technology department of Information technology while working for Intellitel Communications Ltd.

I want to thank the following persons for technical assistance and creating an inspiring and supportive atmosphere: MSc Esa Vepsäläinen, MSc Pasi Kemppainen and many other Intellinauts, you know who you are. One of the main reasons for selecting the telecommunications as a primary area of studying is the influence of Jarmo Harju, thank you very much. I would especially like to mention the almost (?) endless patience of Satu Meriläinen.

The technology changed significantly in between the starting and finishing this thesis. Especially SIGTRAN (SIGnaling Transport) and SoftSwitching technologies may change the world and the operating principles of telephony networks. SoftSwitching, a large and complicated beast, may be a key factor in defining the telephone networks of tomorrow.

When telephone traffic was carried in telephone network and the little amounts of data traffic in their own networks, it was quite easy to see and master the "big picture". The diversifying networks and different technologies melting together will pose a great challenge for the people who continue the designing and implementation from now on.

Helsinki, Finland 1.11.2001

Jussi Savola

TABLE OF CONTENTS

1	Introduction	1
2	Background	2
3	Internet Protocols	4
3.1	Internet Protocol (IP)	4
3.2	User Datagram Protocol	6
3.3	Transmission Control Protocol	6
3.4	Real Time Protocol	7
3.5	Real Time Control Protocol	7
4	MEGACO / H.248	8
4.1	Terms	9
4.2	History	10
4.3	Network architecture	12
4.4	Usage scenarios	14
4.5	Description of the protocol	15
4.5.1	Functionality	18
4.5.2	Encoding	19
4.5.3	Transfer	19
5	ISUP and other SS7 protocols	21
5.1	MTP	22
5.2	SCCP	23
5.3	TCAP	23
5.4	MAP, INAP, CAMEL	24
5.5	ISUP	24
5.5.1	History	25
5.5.2	Network architecture	25
5.5.3	Usage scenarios	26
5.5.4	Description of the protocol	27
6	H.323 and SIP	28
6.1	H.323 architecture	30

6.2 SIP.....	31
7 ISUP / MEGACO Interconnection.....	33
7.1 Applications.....	34
7.2 Benefits.....	35
7.3 Technical requirements.....	35
7.4 Normal call, message sequence and events	36
7.4.1 From H.323 to PSTN	36
7.4.2 From PSTN to H.323	39
8 Technical implementation	42
8.1 Network architecture	42
8.2 Hardware architecture.....	44
8.3 Software architecture	45
8.3.1 Host software	45
8.3.2 Application software	48
9 Conclusion.....	49
REFERENCES.....	52
APPENDICES.....	55

ABBREVIATIONS

ALF	Application Level Framing
API	Application Program Interface
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
CAP	Customized Application for Mobile networks Enhanced Logic
CASN	Compiler for ASN.1-syntax
CCBS	Customer Care and Billing System
CIC	Circuit Identification Code
CPU	Central Processing Unit
CVOPS	C-based Virtual OPerating System
DNS	Domain Name Service
DSS1	Digital Subscriber Signaling 1
ETSI	European Telecommunication Standards Institute
FPLMTS	Future Public Land Mobile Telecommunication System
GT	Global Title
GW	GateWay
HTTP	HyperText Transport Protocol
IETF	Internet Engineering Task Force
INAP	Intelligent Network Application Part
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISUP	ISDN User Part
ITU-T	International Telecommunication Union – Telecommunication Standardization sector
LAN	Local Area Network
MAP	Mobile Application Part
MEGACO	MEdia GAteway COntrol protocol
MG	Media Gateway

MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MIU	MTP2 Interface Unit
MPLS	Multi Protocol Label Switching
MTP	Message Transfer Part
NNI	Network-Network Interface
NNTTP	NetNews Transport Protocol
NSP	Network Service Part
OMC	Operations and Maintenance Centre
OPC	Originating Point Code
OS	Operating System
OSI	Open Systems Interconnection
PBX	Private Branch Exchange
PC	Point Code
PCM	Pulse Code Modulation
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
RFC	Request For Comments
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SCCP	Signaling Connection Control Part
SCTP	Stream Control Transmission Protocol
SGCP	Simple Gateway Control Protocol
SIGTRAN	SIGnaling TRAnsport
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SPOF	Single Point Of Failure
SS7	Signaling System no. 7
SSN	Sub-System Number

SSP	Service Switching Point
SCN	Switched Circuit Network
TCAP	Transaction Control Application Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TDMA	Time Division Multiple Access
THK	TeleHallintoKeskus
TUP	Telephone User Part
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UNI	User-Network Interface
VoDSL	Voice over Digital Subscriber Line
VoIP	Voice over Internet Protocol
VTASK	Virtual TASK
WWW	World Wide Web

1 Introduction

Recent years have shown the rise of the Internet Protocol (IP) based data communication networks. IP, as a protocol, has been around for a long time, but new application scenarios have laid new requirements for the IP based networks.

Public Switched Telephony Network (PSTN) has been in use for more than hundred years and has proved itself as a working concept. PSTN is widely available on a global basis and has evolved to omnipresent digital network, which spans the globe. Both wireline and wireless terminals and networks are currently available.

PSTN contains interworking mechanisms for intervendor operation and globally functional, unambiguous addressing scheme. Voice over IP networks are still largely missing these features, but the situation is evolving continuously.

This thesis focuses on the interface between PSTN and IP networks. Telephone networks in most industrial countries use Integrated Services User Part (ISUP) signaling for establishing, maintaining and tearing down a call. The same protocol is used also for maintaining the welfare of the voice-bearing network. [1]. ISUP is used in Network – Network Interface (NNI). This means that the network components use it when communicating among each other. End users and terminals can not directly access these interfaces. Media Gateway Control Protocol / H.248 (MEGACO) is also internal to the network; end users have no contact with the protocol. In comparison, UNI (User Network Interface) protocols are used in between the end terminal and the network which provides the services.

MEGACO and ISUP are both used inside the network and are not visible to end-users. They both are used for interconnecting the network elements of the corresponding networks. MEGACO is not symmetric as ISUP. Still, the comparison of their functionality and features and possible interworking is a relevant topic.

This thesis does not handle the various protocols and technologies that end-users may encounter. Instead, the focus is in the core network, not on the terminal equipment and their interfaces. There are multiple commercial solutions for the small to midsize environments, but not very much emphasis has been put to core network functionality. This thesis extends the media over IP concept to large scale and to carrier class networks.

Some light has to be shed on the H.323 protocol as well, as MEGACO is local within the Gateway environment. A promising rival for H.323 is Session Initiation Protocol (SIP), but for this paper, H.323 is examined.

This thesis starts by examining the core of the technology, first examining IP-based protocols from the bottom up, then it takes a quick look at higher level protocols. Also the basic SS7 protocols are examined and finally all of this is linked together.

UMTS and other future implementations of the “telephony call from A to B” idea may very well be laid on the IP basis. [2] Legacy PSTN is however not going to disappear at least for a long time and so it is mandatory to provide interworking between these networks. Telecom operators have invested significant amounts of resources to building the current PSTN networks and it is quite clear that the transition, if it happens, will not happen “over night”.

2 Background

The traditional Public Switched Telephony Network (or Plain Old Telephone Service, POTS) has been built on circuit switching ideology. A fixed capacity resource is thus reserved for a call for the duration of the call. In the early years, this resource was wire and there was a pair of wires per call. Later, multiple calls were carried on a single pair, using Time Division Multiplexing (TDM) and Frequency Division Multiplexing (FDM) [3].

Eventually the PSTN was digitalized but the basic idea, static amount of bandwidth (or resource) per call, was maintained. Logically the circuit still exists, even though the analogue data is digitized and multiplexed among other calls into a same wire, radio link or fiber. Normally a capacity of 64000 bits/second (samples are eight bit and taken 8000 times per second) is reserved for a call and these are multiplexed to higher levels in the Synchronous Digital Hierarchy (SDH). Very convenient level of hierarchy is E1, which contains 31 payload channels and a timing signal ($31+1 = 32$; $32 * 64 \text{ k} = 2048 \text{ k} = 2\text{Mbit/sec}$). The same media (E1) is used in e.g. ISDN-PRI (Integrated Services Digital Network PRImary rate) environment, where one of the payload channels is used for Digital Subscriber Signaling number 1 (DSS1) or other ISDN variant.

In contrast, the telephony (and other streaming media oriented) services which are build over IP networks and their transmission mechanisms carry data on packets instead of allocated circuits. The whole principle of IP networks is packet oriented. Streaming protocols have been developed for the IP environment but they do not change the fact that the network underneath is based on packet transmission. Real Time Protocol (RTP) is often used for carrying a voice stream.

Packet based networks often carry other data as well; company LAN file sharing, intranet traffic, WWW-traffic and other applications often share the same medium as the voice and other media streams. This sharing of the transmission media imposes a remarkable challenge for developers of IP based media networks. Massive bulk transfer of data imposes completely different requirements on the data transmission. For example, large WWW or FTP transfer requires large bandwidth but does not care about jitter or latency, but voice over IP traffic has completely opposing needs (moderate bandwidth, low jitter, low latency). To put all this into same network is challenging, and lots of work has been done in this area (Voice enabled routers, MPLS and other technologies).

Large scale networks may dedicate certain amount of bandwidth for media streams problems (or are purposefully dedicated for media transfer) thus resolving the resource adequacy, but still conversion has to be done on circuit switched network and packet network boundary. Certain devices, Media Gateways (MG) are a specified solution for this problem. By standardizing the external interfaces of the MGs, independency of the hardware suppliers may be obtained.

3 Internet Protocols

Internet Protocol family is the basis and foundation for the Internet as well for other internets. These packet switched protocols have proven to be suitable for multiple purposes and to a variety of applications.

This paper assumes the usage of IPv4 protocol. New version of IP is already standardized and it is known as IPv6. The most important difference in between IPv4 and IPv6 is the size of the network entity address field. IPv4 contains 32 bit addresses, whereas IPv6 employs 128 bits for the address. IPv6 also has many other advantages compared to IPv4. Some of the new features are related to flow control and security. [4]

The following picture stacks the different protocols in the same scope.

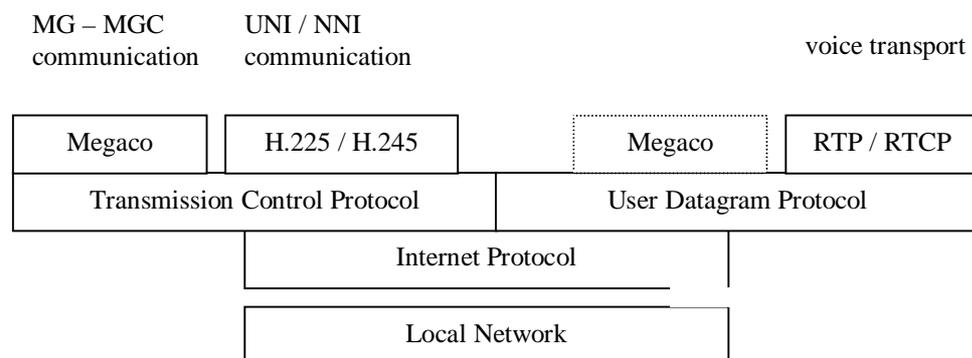


Figure 1: Relevant IP protocols layered

3.1 Internet Protocol (IP)

IP defines mechanisms for transporting a packet from one network node to another, not much else. This is the reason for multiple different higher level protocols on top of IP.

IP protocol itself is defined in the RFC 791 [5] as early as 1981.

The structure of IP frame header is described in the figure 2 below:

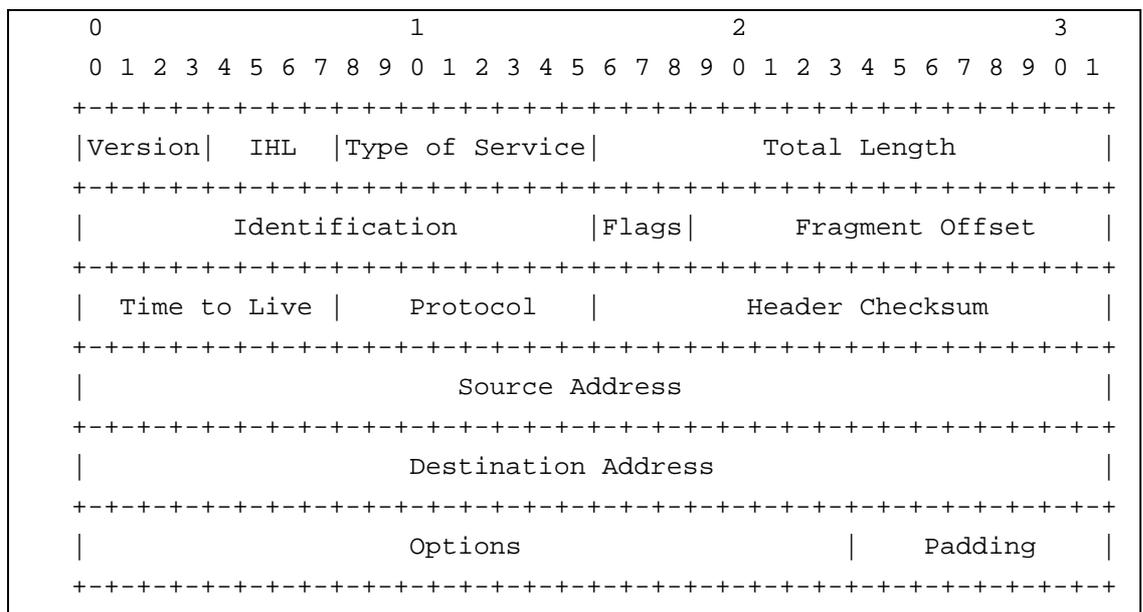


Figure 2: IP Frame header structure

As the figure 2 depicts, the header information in IP frame may be 24 octets. The actual payload is appended to the header and can be of varying length.

The maximum total length of the data packet in Ethernet type networks is typically approximately 1500 bytes per frame, whereas serial links may restrict the maximum to even as short as 296 bytes per frame. IP-based network can often be seen as “IP-substrate” which is not dependent on the actual media. The transmission media naturally enforces certain restrictions e.g. on the datagram size and transmission rate, but often the differences are not relevant on the application level.

3.2 User Datagram Protocol

User Datagram Protocol (UDP) provides mechanism for transporting user datagrams from one network entity to another. UDP does not provide reliable transfer; the term “best effort” can be used to describe its functionality. The sender has no mechanism for knowing whether the sent data reached its destination.

UDP is not connection oriented, so the user of UDP is forced to introduce application level sequencing and guaranteed delivery for critical data.

UDP is defined in RFC 769. [6]

3.3 Transmission Control Protocol

Transmission Control Protocol (TCP) provides reliable and sequenced flow of data from one network entity to another. TCP, being connection oriented protocol, includes relatively complex timer and state automaton mechanisms and thus is not optimal choice for every purpose. Transport of time critical media data, for example, is a scenario, where TCP does not excel. Media connection setup, parameter negotiation and session teardown are good candidates to TCP applicability.

TCP is defined by RFC 793. [7]

3.4 Real Time Protocol

Real Time Protocol (RTP) is run over UDP, which, in turn is run over IP. As UDP introduces only a little overhead to raw data transfer, and as media packets can not wait for retransmissions, UDP is a natural choice for delivering media data.

RTP enters timestamps and time criticality headers to data so that the applications can rearrange the data packets, if they arrive out of order within their buffer space.

RTP by itself does not provide any guaranteed Quality of Service mechanisms. As RTP is end-to-end protocol and run over standard UDP, the intermediate IP-routers and switches do not need to take any special measures when transporting the traffic. [8]

On RTP transport, the voice data is carried in some encoded format. There are several alternative formats, a-law PCM and μ -law PCM being the most well known. These formats are not compressed, but several compressed formats are defined as well. A-law (most of the world) and μ -law PCM (America) both define how analogue voice signal is encoded into octets. These formats are heritage from the PSTN world.

RTP is defined in RFC 1889. [9]

3.5 Real Time Control Protocol

Real Time Control Protocol (RTCP) packets, which are inserted into the media flow transported on RTP, contain additional information about the welfare of the media stream. The RTCP contains information on lost packets and the data flow synchronization. RTCP is also used when using a voice compression protocol, which do not send any data during silence. This "blanco" stream of RTCP messages is used

to indicate both ends of the connection that the connection is still alive, even though no media packets are being transferred.

RTCP is defined in RFC 1889. [9]

When examining RTP traffic with a protocol analyzer, it is good to know that RTP traffic is aimed to UDP even port number (e.g. 1668) and the corresponding RTCP traffic is sent to odd numbered port one above the RTP port (e.g. 1669).

4 MEGACO / H.248

Media Gateway Control Protocol is defined jointly by IETF [10] and ITU-T (H.248). The two organizations publish a document, which is textually the same.

MEGACO defines the protocol used between elements of a physically decomposed multimedia gateway. Such elements are Media Gateway Controller (MGC) and Media Gateway (MG) as defined in RFC 2805.

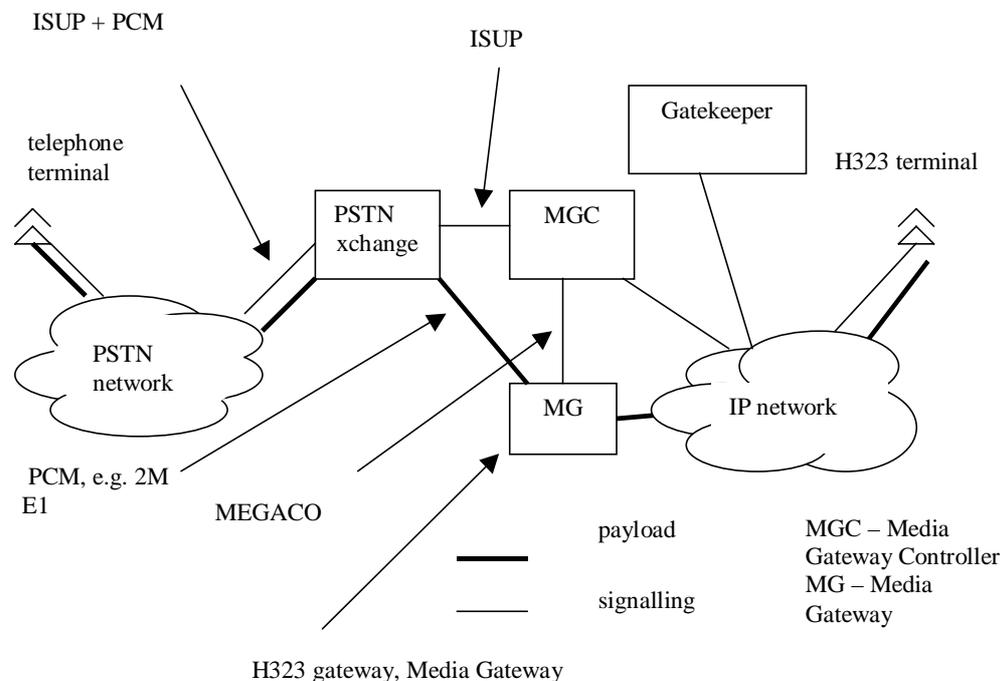


Figure 3: MEGACO architecture seen from H.323 point of view

MEGACO is able to handle the concept of traffic to and from packet networks (e.g. ATM and IP) and circuit switched networks (e.g. analogue tone signaling, ISUP, ISDN and others). Principally, the protocol is able to handle traffic from any to any network; the networks can even be the same.

MEGACO does not handle the actual end to end routing of the call; other mechanisms must be employed for that functionality. MEGACO has only local significance; it defines only the interface between MG and MGC. Naturally, the MGs can span a large geographic area provided that there is a reliable network for MEGACO traffic connecting the network entities together.

4.1 Terms

Media Gateway is a network entity that is capable of converting media presented in some type of network to format which is suitable in another type of network. These networks can be e.g. circuit switched network (e.g. 64 kbps PCM encoded voice channel in PSTN) and packet network (e.g. RTP stream in an IP network). There are no limitations imposed for additional functionality, MG can also provide Interactive Voice Response (IVR) functionality and video transmission. MG can also provide conferencing functionality [10].

Media Gateway Controller is an entity, which has the responsibility of controlling the media gateways. MGs are thus enslaved to MGC, somewhat in the same way as Service Switching Points are enslaved to the Service Control Points in the Intelligent Network architecture but more tightly. MGC can be connected to signaling related to media streams, e.g. the ISUP channel, which controls the voice channels or DSS1 in the ISUP primary rate environment.

SCN FAS and **SCN NFAS signaling gateways** are, correspondingly, Switched Circuit Network (Non) Facility Associated Signaling gateways. This thesis

concentrates on SCN NFAS as the ISUP is Non-Facility Associated Signaling (i.e. the signaling is logically separated from the payload).

4.2 History

Before MEGACO, there was lots of work done in the industry, IETF and ITU-T to standardize to interface between the Media Gateway devices and a centralized control node.

Firstly, IPDC (proposed by Level 3, 3Com, Alcatel, Cisco and others) and SGCP (Telcordia) were brought together by the IETF to form MGCP (Media Gateway Control Protocol), under the responsibility of the Megaco (Media Gateway Control) working group. [25]

The background for separating “the muscle” and “the brain” lies partly in the weaknesses of H.323; it did not scale up from LAN proportions and contained complex gateway devices. In addition, H.323 was not very compatible with PSTN world protocols and mechanisms.

Simple Gateway Control Protocol (SGCP) is a simple client-server protocol implemented on top of UDP over IP. SGCP is used in cable network environments and remarkable degree of inter vendor interoperability has been reported.

To further confuse matters, existing implementations of this protocol are based on various stages of this initiative; IPDC, SGCP and MGCP form the vast majority of implementations.

Megaco does represent an enhancement of MGCP: it can support thousands of ports on a gateway, multiple gateways and accommodation for connection-oriented media like TDM and ATM. [25]

MGCP is very close relative to MEGACO; most of the concepts are the same, although some differences in the model can be noted. Below, in figure 4, is one approximation of the protocol family development path.

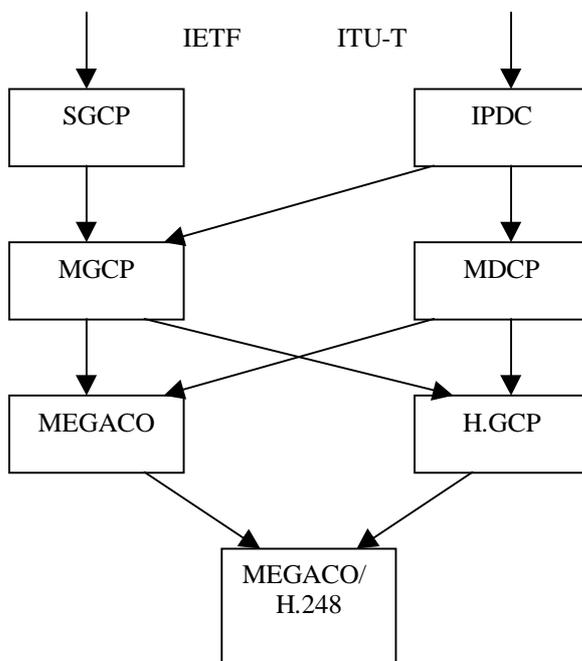


Figure 4: History of Gateway Control Protocols.

It is the opinion of the author that the specification of MEGACO took too long and the industry unfortunately started adopting the previous protocols.

The author has a belief that if an implementation of MEGACO or MGCP should be done now, year 2001, the most convenient solution would be implementation which would be configurable in the installation time to behave according to the needs of the installation environment. It is very probable that there will be both types of devices (MGCP and MEGACO) in the future and so it would be very convenient if the same controller could control the both types of gateways.

4.3 Network architecture

There are multiple alternative scenarios where MEGACO can be utilized. In small size gateways, it is cost-efficient to dismiss MEGACO altogether and combine the functionalities of MG and MGC in the same node. Small deployment contains up to a couple ISDN PRI type lines (up to maybe 60 voice channels)

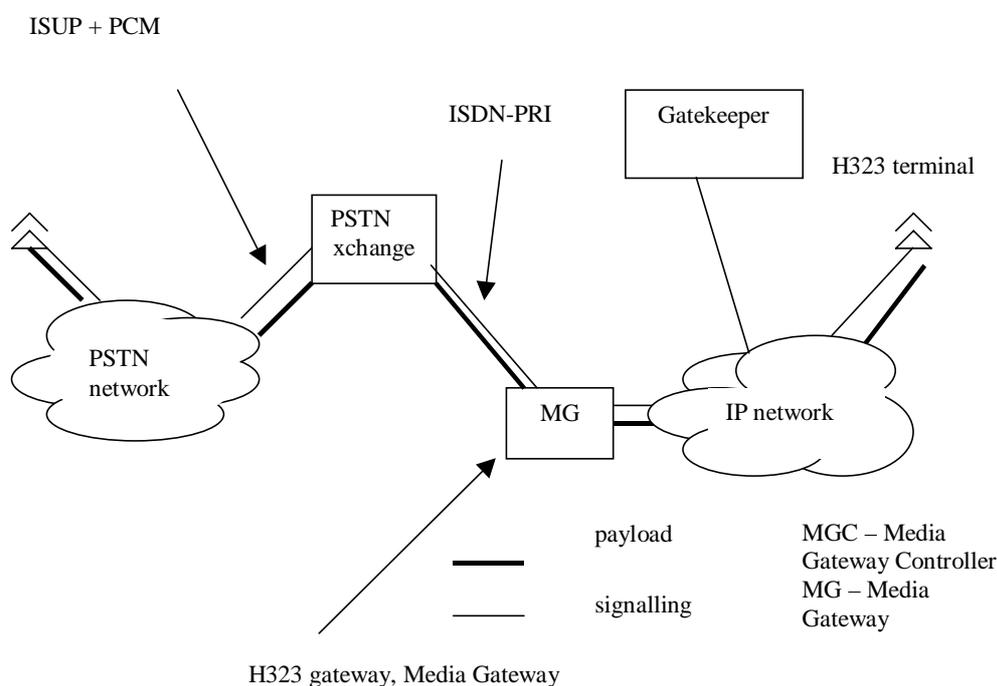


Figure 5: Small deployment

In the mid-range environment, where several ISDN PRIary lines are used, it is possible to choose from stand-alone or MEGACO based solution. Please keep in mind that MGCP does not support multiple gateways in one domain.

When considering a larger gateway, ISUP is generally used for multiple reasons for connecting MGC(s) to PSTN network. Builder of the large gateway system might be a telecom operator operating with the backbone of the network and not some other company that may be a “leaf node” of the PSTN network. For these companies, ISUP is readily available and no special arrangements are needed. From the network

perspective, the introduction of the VoIP network may seem like adding a telephone exchange to existing network.

MEGACO is primarily suitable for large scenarios, where MGs can span to many nodes and contain many types of functionality. It must be kept in mind, that addressing and routing schemes are very flexible in the PSTN exchanges; the same voice trunks can be divided for use for multiple phone numbers and the same called numbers can span multiple voice trunks. This distinction in routing can many times be based even on the type of call, whether it is all digital or analogue voice call.

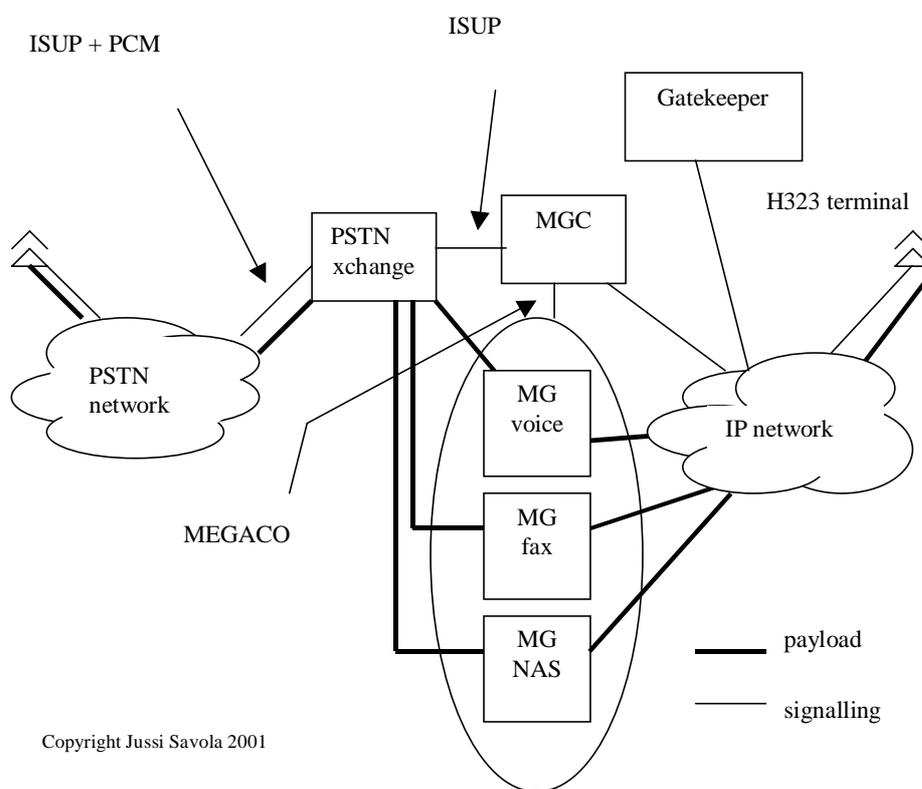


Figure 6: Multi-MG deployment

It is possible to separate different functionalities to different Media Gateways as the picture above illustrates. One interesting aspect for using MEGACO is in the network access servers. MEGACO has support for dial-up network access e.g. for the Internet or company intranet access.

ISUP as a protocol is quite suitable for maintaining the circuit switched network and establishing and tearing down the calls in the network. ISUP, however, is symmetric by nature and expects the underlying network to behave in certain way. ISUP bears historical load and has no concepts or mechanisms for handling the addressing, data transport mechanisms, QoS mechanisms or voice encodings of the packet networks. The conference calls and multimedia messaging are both outside the scope of ISUP. Extending ISUP to cover these purposes is probably not a good idea.

ISUP is a peer-to-peer type protocol where MEGACO defines a master-slave relationship between the network entities. Using ISUP for signaling in between the MGs and MGC is not practical for many reasons which are outside the scope of this thesis.

4.4 Usage scenarios

Even though building a packet based voice transmission network is a quite costly investment, there are several scenarios, where e.g. the cost issues are a good reason to think about packet based network instead of circuit based one.

Running voice over IP network in UMTS environment will possibly employ MEGACO signaling in between the corresponding network elements [2].

Connecting Digital Subscriber Line (DSL) or cable network or some other IP-network to PSTN might also be interesting scenario, where IP and PSTN telephony functionalities might be involved. “Traditional” Voice over DSL (VoDSL) is not necessarily suitable directly for IP-based telephony as the DSL line only replaces the local loop part of the connection, not the entire functionality.

4.5 Description of the protocol

MEGACO protocol is a freely usable standard, which can be downloaded from the IETF network servers. ITU-T has its own document distribution mechanisms. This thesis concentrates on the IETF document, known as RFC 3015.

The RFC contains 179 pages, and relies heavily on several other RFCs, namely Session Description Protocol (SDP) which is defined by RFC 2327 [11].

MEGACO is modular in a sense that functionality is divided into so called packages. Different scenarios use different packages and so the network elements do not need to implement the whole protocol. For example, a fax gateway does not need the functionality of the Network Access Server (NAS) and vice versa.

The packages are listed in appendix 1. Additional packages defined by IETF are to be published in separate RFCs. A mechanism for publishing packages published by ITU-T is also specified.

The protocol employs the following terms:

- Stream – Bi-directional flow of media or control data (e.g. RTP stream in IP network) received or sent by media gateway as part of a call or conference. Identified by StreamId.
- Termination – A termination sources and / or sinks one or more streams. Special case is “root termination” which refers to entire gateway.
- Context – A context is an association between a collection of terminations. There also exists a special case, “null context”, for those terminations which are not in some other context (i.e. “idle terminations”).
- Message – Single bulk of data transferred between MG and MGC.
- Command – One of [add, modify, subtract, move, auditvalue, auditcapabilities, notify, servicechange]. Commands are applied to terminations or give information regarding the terminations.
- Action – Action consists of a series of commands, which are limited to operating with a single ContextId. May also contain context manipulation or auditing instructions.
- Transaction – Commands between the entities are grouped into transactions, each of which is identified by a transactionId. A transaction consists of one or many Actions.

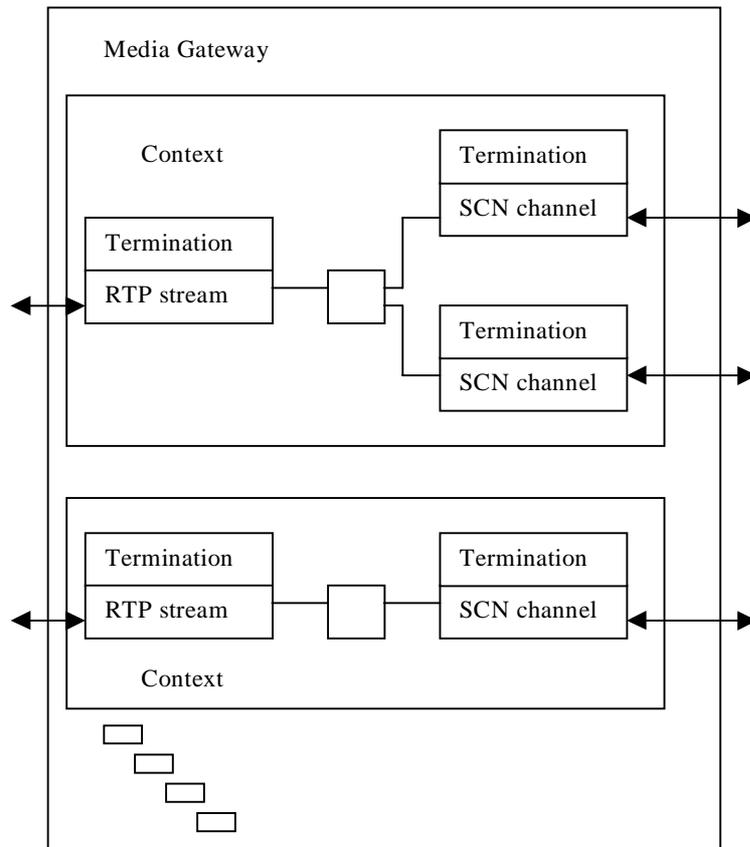


Figure 7 Context, termination, stream, and channel

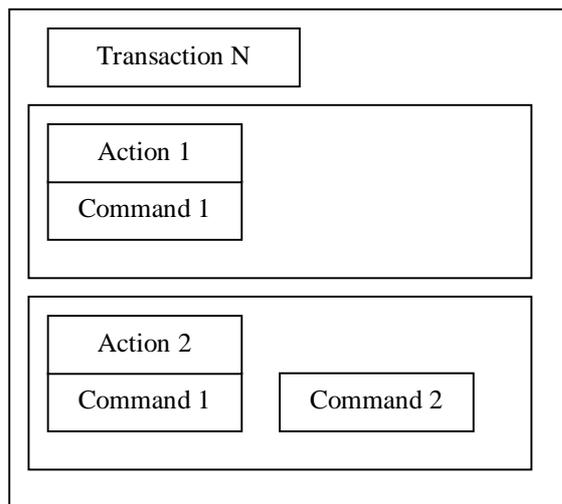


Figure 8 Transactions, Actions and Commands

4.5.1 Functionality

The MEGACO protocol looks quite simple; it consists only of eight commands.

The commands are explained here:

1. The **Add** command is used to add a termination to a context. The first "add" regarding an empty context implicitly creates the context.
2. The **Modify** command modifies the properties, events and signals of a termination.
3. The **Subtract** command takes a Termination away from corresponding Context. The Subtract command on the last Termination in a Context deletes the Context.
4. The **Move** command moves a Termination to another context.
5. The **AuditValue** command returns the current parameters regarding the corresponding Terminations.
6. The **AuditCapabilities** command is used by the MGC to query the features of an MG.
7. The **Notify** command is sent by the MG when predefined events occur.
8. The **ServiceChange** Command is used by MG to notify MGC when it's coming to service or going off of service. The command is used by the MGC to notify MGs in handover (changing the active MGC) situations.

4.5.2 Encoding

There are two alternative encoding schemes for MEGACO. The MEGACO RFC gives alternatives for textual and binary encoding.

Binary description of the protocol is given as ASN.1 [12]. The Basic Encoding Rules are to be applied, when coding the messages to be transferred over the transport medium [13].

Textual encoding is given as ABNF [14]. MGC should support both encoding formats; MG may support both formats.

Even though the machine processable (binary) encoding may provide slight performance advantage, the development phase of the product might be shorter when using the textual encoding.

4.5.3 Transfer

MEGACO specification states that the MEGACO messages can be transferred over User Datagram Protocol (UDP) over Internet Protocol (IP) or over Transmission Control Protocol (TCP) connection.

The transport mechanism for the protocol should allow the reliable transport of the transactions not depending on the actual transport mechanism used between the communicating entities. The MEGACO RFC defines a couple of transport mechanisms and a mechanism for adding new transport mechanisms is also defined.

The location of the entities is defined either by Domain Name Service (DNS) or numeric IP address. Both TCP and UDP default port numbers are also given, the textually encoded messages should be sent to port number 2944 whereas binary

encoded messages are to be sent to port 2945. These numbers are valid for both TCP and UDP.

MGs are to be configured with information on the location of the primary (and secondary) MGC. Upon startup and subsequent changes, the MGs inform the MGC(s) about their existence.

For guaranteeing the authenticity and validity of the messages, IPSec (RFC 2401 and many others) security scheme is to be used. For system environments, where IPSec is not available, additional headers ("AH" as defined in the RFC 2402) to MEGACO protocol are used to ensure the authenticity and integrity of the protocol messages.

For coping with network congestion and MG restart avalanche, several mechanisms have been defined, namely dynamic retransmission timers and addition of random component to retransmissions and initialization messages. When a large number of MGs are to be restarted simultaneously, it could otherwise create resource congestion in the MG and possibly in the communication network. Coping with avalanche may seem like a trivial problem, but not all installations consist of one MGC and "a couple" MGs, as residential gateways may also be controlled by MEGACO under the supervision of one MGC. Thus there may be thousands, even tens of thousands, of MGs to be taken care of e.g. after large area blackout.

TCP over IP is a practical protocol for many types of applications, but it has some shortcomings. A new protocol, Stream Control Transport Protocol (SCTP) has been designed with signaling transport in mind. SCTP can be run over redundant routes and it has packet oriented nature. These features make it an interesting candidate for future evaluation. SCTP has also other good features for using it in communication in between MG and MGC. [15]

For now, messages (signaling, network maintenance) which need to be transferred reliably but which are not timing critical are run over TCP. Not so critically

important data packets (media data transfer) which require precise timing are run over UDP.

4.5.3.1 Transport over TCP

Transmission Control Protocol is a reliable, stream oriented protocol quite suitable for MEGACO despite the fact that TCP is octet oriented and MEGACO message oriented.

Even though TCP should be reliable enough, the MEGACO protocol envisages the use of application level timers, which take care of resending the messages in case of packet failure. Mechanisms for preventing duplicates are also presented.

4.5.3.2 Transport over UDP

User Datagram Protocol is message oriented and as such, quite suitable for transporting MEGACO traffic. Unfortunately, the network may impose maximum size for the message and so Application Level Framing (ALF) must be utilized.

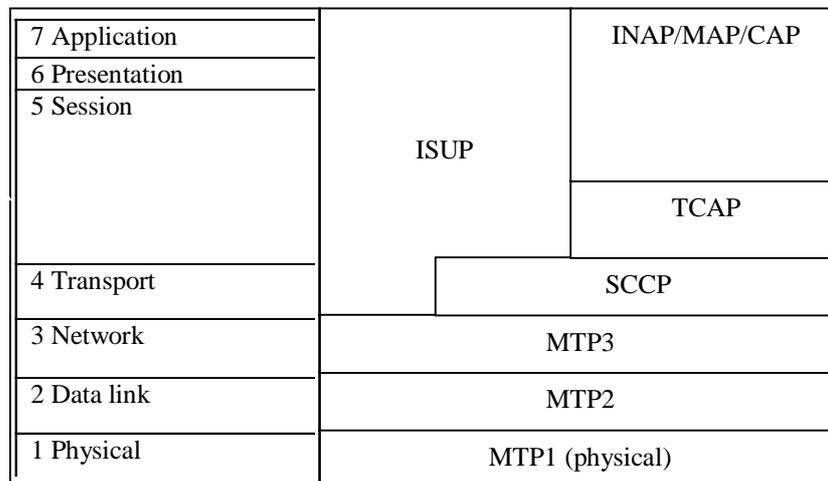
UDP messages may be lost and so the communicating entities must store the messages they have sent and resend them in case of lost message. Upon acknowledgement, they are destroyed from the sender's memory. Timer mechanisms are encouraged for ensuring the reliable communication.

5 ISUP and other SS7 protocols

Earlier analogue telephone signaling systems carried the signaling information on the same circuit as the voice traffic. The newer signaling systems, e.g. SS7, reserve a separate data transfer channel for signaling information. These systems are often called Common Channel Signaling, as a separate but common channel is used for signaling related to multiple voice circuits.

Even though SS7 is tightly standardized, there are multiple versions, mainly in different countries and continents. American networks are based on ANSI standards, whereas European networks use standards written by European Telecommunication Standards Institute (ETSI) enriched with national add-ons and modifications. Japan and other Far East countries have their own standards as well. This multitude of standards gives network equipment manufacturers additional work.

SS7 is layered set of protocols, in many ways similar than OSI protocol stack.



OSI model

SS7 stack

Figure 9: Comparing the OSI model and SS7 stack

5.1 MTP

Message Transfer Part (MTP) consists of three separate layers. The lowest layer, MTP1, defines the physical characteristics of the signaling link. It corresponds to the physical layer of the OSI-model.

The next layer, MTP2, provides services for the network layer (MTP3) by using the services of the MTP1 layer. MTP2 corresponds to link layer of the OSI model [15].

The highest layer of Message Transfer Part, MTP3, provides some features of the OSI models network layer. MTP3 provides reliable network wide message transfer to its users, usually ISUP and SCCP. Network entities are known by their Signaling Point Code addresses in the MTP3 level. [16]

5.2 SCCP

Signaling Connection Control Part (SCCP) uses the reliable message transfer provided by the MTP3 layer. SCCP enhances the addressing mechanisms of the SS7 network by providing message routing to various User Parts by the SubSystemNumber addresses. Well known SS7 services are located in the network entities in established Sub Systems and are addressed by their SSNs. SCCP also provides enhanced addressing mechanism on top of the Point Code based addressing, Global Title (GT) addressing. In some ways GT addressing vs. Point Code addressing can be compared to Domain Name Service (DNS) and numeric IP-codes of the IP-network.

5.3 TCAP

Transaction Capabilities Application Part (TCAP) is a protocol layer, which resides on the OSI Session, Presentation and Application layer. It provides reliable dialogue and remote operation services to its users, INAP, CAP, MAP, to name a few. There are several remote operation classes that TCAP provides its users. TCAP can inform the corresponding user about success and failure of operation execution.

TCAP always resides on top of SCCP and uses its connectionless services.

There are a couple of versions of TCAP defined by ITU-T. The most commonly used in Finland nowadays is so called “white book” version of the protocol, specified in 1992.

5.4 MAP, INAP, CAMEL

These protocols provide features on top of TCAP. TCAP does not provide any semantics or meaning for the remote operations that the network entities invoke in other network elements. Mobile Application Part (MAP), Intelligent Network Application Part (INAP) and Customized Application for Mobile networks Enhanced Logic (CAMEL) are examples of protocols, which utilize the transport and session mechanisms provided by TCAP.

5.5 ISUP

ISUP is a NNI, which operates in between the nodes in the telephone network. The protocol is defined by ITU-T (Q.76X) and consists of group of messages and corresponding activities. ISUP specifies both the protocol and the functionality of the network elements. The functionality consists of Call Control specifications for different types of exchanges, maintenance procedures and many other issues.

ISUP is nowadays the omnipresent glue that ties together PSTN switches from different vendors. ISUP is run on Signaling System #7 network as defined in the following protocol figure.

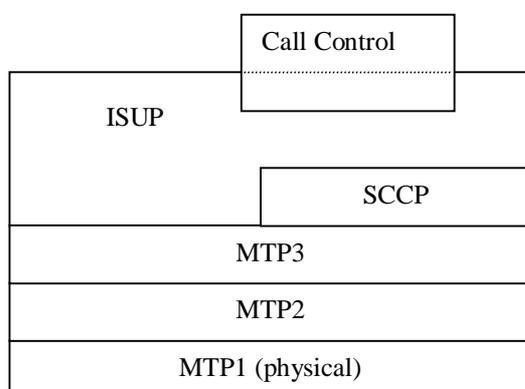


Figure 10: ISUP Protocol Stack

ISUP contains two types of functionalities: Non Call related and Call Related. The NonCall related features are mostly used in relation to network maintenance.

The call related functionalities are needed on the setup and teardown of the call. In addition, mechanisms have been defined to transport call related (“User”) data during the call.

5.5.1 History

The SS7 ISUP protocol was created after other digital signaling protocols had already been in use for several years. Telephone User Part (TUP) is a direct predecessor. By year 2001 there has not been TUP based telephone traffic in Finland for several years.

5.5.2 Network architecture

There are several different types of network elements (in addition to terminals) which have to be considered when examining the route of the call.

- Originating Exchange - The exchange which the calling party is connected to
- Terminating Exchange - The exchange which the called party is connected to
- Transit Exchange – An exchange that just passes the call towards final destination (not on the picture below)
- Signaling Transfer Point – Network device that routes the SS7 messages towards the final destination

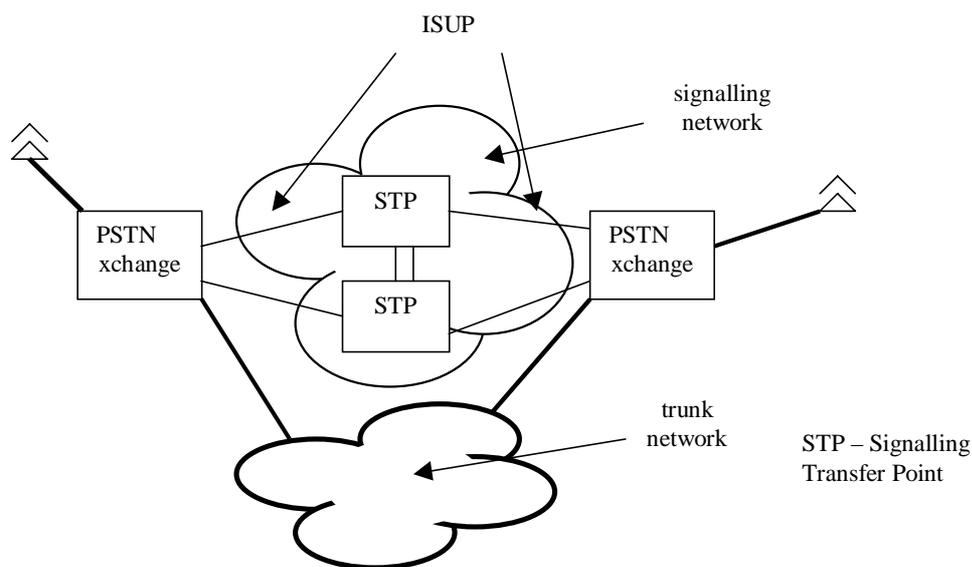


Figure 11: Heavily simplified structure of PSTN

5.5.3 Usage scenarios

On the left side, the calling party is using DSS1 (ISDN PRI) signaling for communicating with the Local Exchange. ISUP is used in between the exchanges along the path of the call. It is possible that there are intermediate (transit) exchanges along the path of the call. For the purposes of this thesis, the transit exchanges simply relay the call related messages towards the final destination exchange and so are not active participants in the message transfer. The signalling transfer point functionality is not relevant either when considering the functionality of the Media Gateway Controllers or the Media Gateways.

For correlating the messages, which are related to a specific call, a Circuit Identification Code (CIC) number is used. A CIC has significance only in between two exchanges (so the information bundle of “time”, Point Codes of both exchanges and CIC is used to identify a single call). One call can be referred with many different CICs along its way, if transit exchanges are present in the route of the call.

ISUP can segment and reassemble messages that are too long for underlying protocol layers to handle. This, however, is quite a rare situation; normally the messages are passed on in one piece. Maximum length of MTP3 message is 273 octets and usually it is more than enough for ISUP. Especially the Initial Address Message (IAM) may need segmenting, if many of the optional parameters are present.

6 H.323 and SIP

MEGACO is of local significance only; it provides communication mechanism in between MG(s) and MGC(s). Protocols and mechanisms have to be introduced to be used in end-to-end call setup, maintaining and teardown.

ISUP is traditionally used in the PSTN for these purposes in NNI, and analogue DTMF signaling is used for signaling from the non-ISDN terminals to the Local Exchange (LE). DSS1 protocol is used in between the local exchange and ISDN terminal (be it computer with ISDN adapter card, ISDN-fax or ISDN-telephone).

In the media over packet network - world, similar issues have to be solved. The protocol H.320 was introduced by the year 1990. H.320 is an umbrella standard for other recommendations that defined video telephony over switched digital telephone networks [17]. The current H.323 v 2 is a derivative of the original H.320 standard.

Later, the Internet Engineering Task Force (IETF) introduced lighter alternative, Session Initiation Protocol (SIP). Where H.323 is heavily and tightly standardized in

“telecommunication way”, SIP is developed in the Internet community and defined as RFC 2543 and is based on intuitive textual representation of the protocol elements, much like the well known SMTP, HTTP and similar protocols.

SIP	H.323
"New World" - a relative of Internet protocols - simple, open and horizontal	"Old World" - complex, deterministic and vertical
IETF	ITU
Carrier-class solution addressing the wide area	Borne of the LAN - focusing on enterprise conferencing priorities
A simple toolkit upon which smart clients and applications can be built. It re-uses Net elements (URLs, MIME and DNS)	H.323 specifies everything including the codec for the media and how you carry the packets in RTP
Leaves issues of reliability to underlying network	Assumes fallibility of network - an unnecessary overhead
SIP messages are formatted as text.	Binary format doesn't sit well with the internet – this adds complexity
SIP allows for standards-based extensions to perform specific functions	Extensions are added by using vendor-specific non-standard elements
Hierarchical URL style addressing scheme that scales	Addressing scheme doesn't scale well
Minimal delay - simplified signaling scheme makes it faster	Possibilities of delay (up to 7 or 8 seconds!)
Slim and Pragmatic	The suite is too cumbersome to deploy easily

Table 1: Differences in between SIP and H.323 [18]

6.1 H.323 architecture

H.323 has its roots in the International Telecommunications Union (ITU) and has gone through several evolutionary cycles. The H.323 as such is an umbrella for other standards. H.323 is aimed to packet networks, which do not provide Quality of Service (QoS).

The H.323 standard provides a foundation for audio, video and data communications across IP-based networks, including the Internet. Compliance with H.323 guarantees that multimedia products and applications from different vendors can interoperate. This allows the users to communicate without concern for compatibility.

H.323 mandates some intercommunication standards and codecs. Some of the codecs are optional, while others are mandatory (e.g. G.711 in audio compression).

The ITU's Study Group 16 approved the H.323 specification in 1996. Version 2 was approved in January 1998.

The H.323 architecture defines four major components for a network-based communications system: Terminals, Gateways, Gatekeepers and Multipoint Control Units.

Terminals are the client endpoints on an IP network, commonly LAN that provide real-time, two-way communications. All terminals must support voice communications; video and data features are optional. All terminals are obliged to support **H.245**, a standard that is used for negotiating the channel usage and capabilities. In addition, **Q.931** is needed for call signaling, a component called **Registration/Admission/Status (RAS)**, which is a protocol used to communicate with a Gatekeeper and support for **RTP / RTCP** which is the actual transport media for media streams.

Gateways are optional elements in the H.323 architecture. They are needed when some kind of media conversion is needed, e.g. when connecting LAN to PSTN. The terminals communicate with the Gateways using H.245 and modified Q.931 protocols. With appropriate codecs, the Gateways can communicate with terminals, which support H.310, H.321, H.322 and V.70.

Gatekeeper acts as a central point for all calls within its zone and provides call control services to registered endpoints. Gatekeeper takes care of naming and addressing of the terminals as well as bandwidth management. All H.323 components in a network including Terminals, Gateways and Multipoint Control Units controlled by a single Gatekeeper are collectively known as H.323 **zone**. Gatekeeper is able to route the calls to and from its zone. This provides mechanisms for e.g. billing services. If Gatekeeper is present in the network, terminals are mandated to make use of the services of it. Gatekeeper is also capable of providing routing of calls which use E.164 based numbering

Multipoint Control Units and corresponding **Multipoint Processors** are entities responsible for conference type media streams.

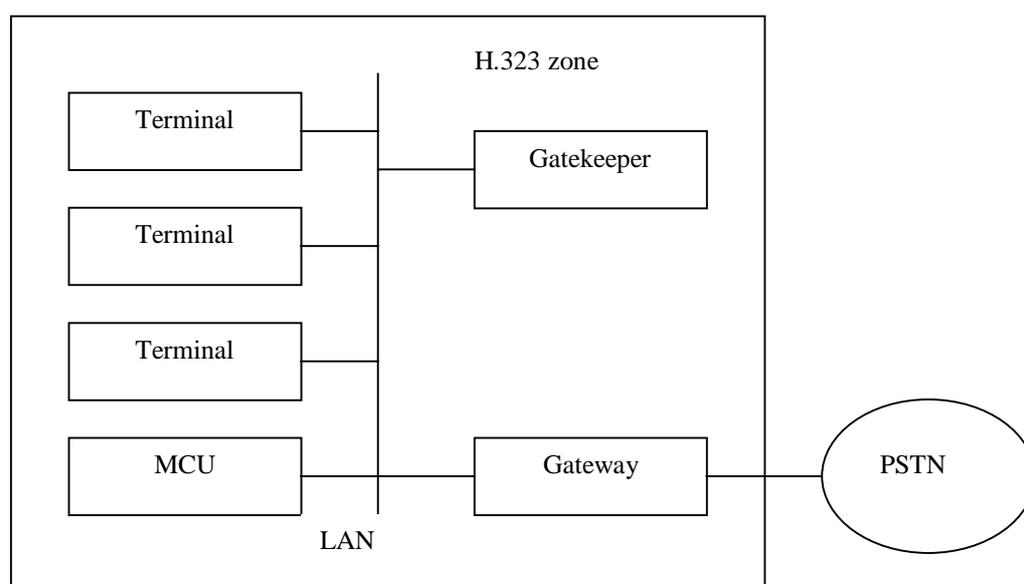


Figure 13: H.323 zone and components

6.2 SIP

Session Initiation Protocol (SIP) is a light weight alternative to relatively widely deployed H.323 protocol family. Whereas H.323 tightly requires certain codecs, SIP gives the implementers of the terminals and other equipment much more free hands.

Where H.323 is difficult to parse by hand, SIP is human readable, formed according to the same principles as HTTP, NNTP, SMTP and other Internet related protocols. SIP offers functionality similar to H.225.0/Q.931/RAS, H.245 and H.450. More detailed comparison can be found on the Internet [19].

SIP was developed within the IETF MMUSIC (Multiparty Multimedia Session Control) working group, with work proceeding since September 1999 in the IETF SIP working group [20]. SIP reached Proposed Standard stage by March 17, 1999 when it was published as RFC 2543.

Considering the future, the author is inclined to believe that there will be room for both SIP and H.323. SIP could be adopted for ISP – type companies (for selling to end users), other companies for building Intranets etc and new telcos whereas H.323 and related standards might get future in old telco environment. This thesis, however, concentrates on the "big iron environment", thus selection of H.323.

The tables may turn, as SIP seems to scale better upwards as it has not so tight centralized control. SIP has also other advantages over H.323, as it is simpler and more extendable. [2]

7 ISUP / MEGACO Interconnection

The primary focus of this thesis is to examine mechanisms to provide interworking for IP based telephony systems and PSTN. Scenarios are considered for both from CSN to packet network calls as well as for from packet network to CSN calls.

H.323 has been chosen as the reference internet signaling due to its relatively wide deployment. H.323 is already standardized, while the alternative, Session Initiation Protocol (SIP), is still developing and getting maturer.

Crucial H.323 network component is the gatekeeper (GK), which is responsible for routing the calls to correct destinations. Gateway (GW) is the entity responsible for converting PSTN circuit switched voice to IP networks RTP carried voice stream and vice versa.

H.323 GK can forward the H.225 call setup messages on behalf of the Terminal. This forwarding mechanism can be used to convey the signaling information to Media Gateway (MG or GW). In this scenario, the H.323 MG corresponds directly to combined MEGACO MGC and MEGACO MG.

This thesis takes somewhat unorthodox approach to connecting of ISUP and H.323 networks, as the Signaling Gateway and Media Gateway Controller are seen as different devices as depicted in the figure 14.

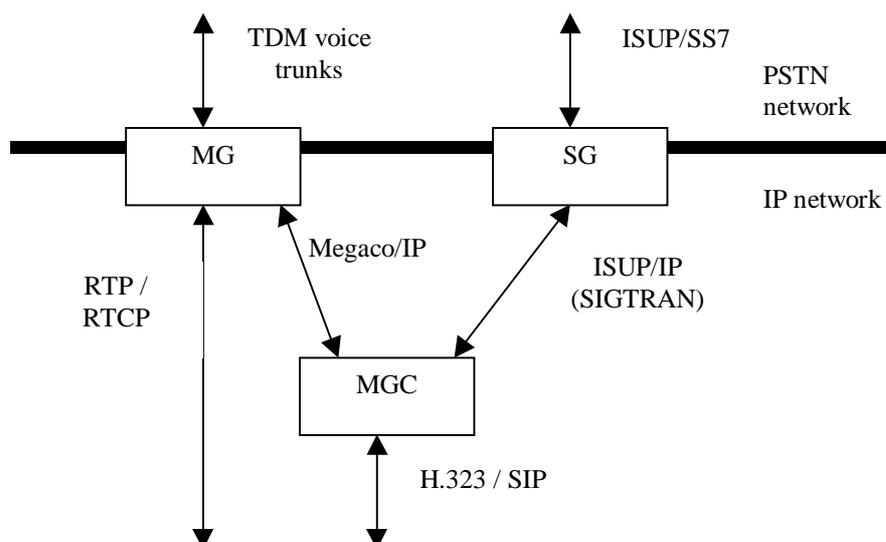


Figure 14: traditional view of gateway composition

Quite often MGC is separated from PSTN network, as MGC manufacturers not necessarily are familiar with PSTN signaling. This approach is quite natural, but in this work, the functionalities of SG and MGC are combined, as suitable PSTN protocols are already available.

7.1 Applications

When operator wants e.g. to offload calls from PSTN to IP network, some interworking functionality has to be introduced into the network. In addition, when company wide telephony based networks are to be connected to PSTN, the signaling and the payload must be interfaced.

Future Public Land Mobile Telephone Networks (FPLMTN) may also introduce VoIP functionality in the large scale. The emerging UMTS networks may even introduce end-to-end all-IP infrastructure. [2]

7.2 Benefits

Although Voice over IP is a nice thing in itself, the pros and cons have to be weighed. There are some easily seen benefits which are listed below.

- If a large company has IP-based internal telephone network, it is quite beneficial to connect it to external world, PSTN
- Residential ISP operators who operate on DSL or cable or similar networks may provide telephone service over their IP-infrastructure.
- Consistency with other future networks (UMTS, CAMEL) is a good thing. [2], [21]
- People entering the business are more familiar with IP technology, it is easier to find competent personnel for planning and operating the networks.
- IP technology usually is cheaper to obtain and administer than traditional telco equipment. The difference in prices shall be greater in future. Currently (year 2001), however, the price is not a remarkable driving force for VoIP.

7.3 Technical requirements

Traditionally the devices related to handling the IP traffic have been not highly available or fault tolerant. The growth of Internet has shown that a single fault somewhere in the network can result in massive malfunction in the availability of IP based services.

It is clear that the reliability and fault tolerance levels of the hybrid network must meet the requirements of the PSTN [22].

Telephone network switches have extremely high requirements for uptime and availability. In contrast, it is not uncommon to note company email server to be down

or Intranet services to be unavailable. This type of unavailability is unacceptable for telephony traffic.

Redundancy has been a key word in PSTN signaling; there is always a spare communication channel for the unfortunate failure case. Internet, as a technology also provides means for alternate routing of data packets. Redundancy costs money, and quite often the alternate routes have been neglected in the competed field of data communication. Customers accept the poor quality of the networks, as they are often not knowledgeable enough to demand better technical solutions.

7.4 Normal call, message sequence and events

The following message sequence charts depict only the simplest cases, where a calling party tries to reach called party and succeeds. The call goes on for some time and is eventually hung up. No erroneous situations have been considered.

Possibilities for call failing are numerous: Invalid called party number, network connectivity failure (in signaling or payload handling), network device outage, call restrictions, called party busy, to name just a few.

7.4.1 From H.323 to PSTN

Monolithic gateway

The message sequence chart in figure 16 below depicts a normal voice call setup from H.323 terminal to PSTN terminal. The details of the PSTN side have purposefully been left out. The scenario in figure 16 is constructed using monolithic gateway.

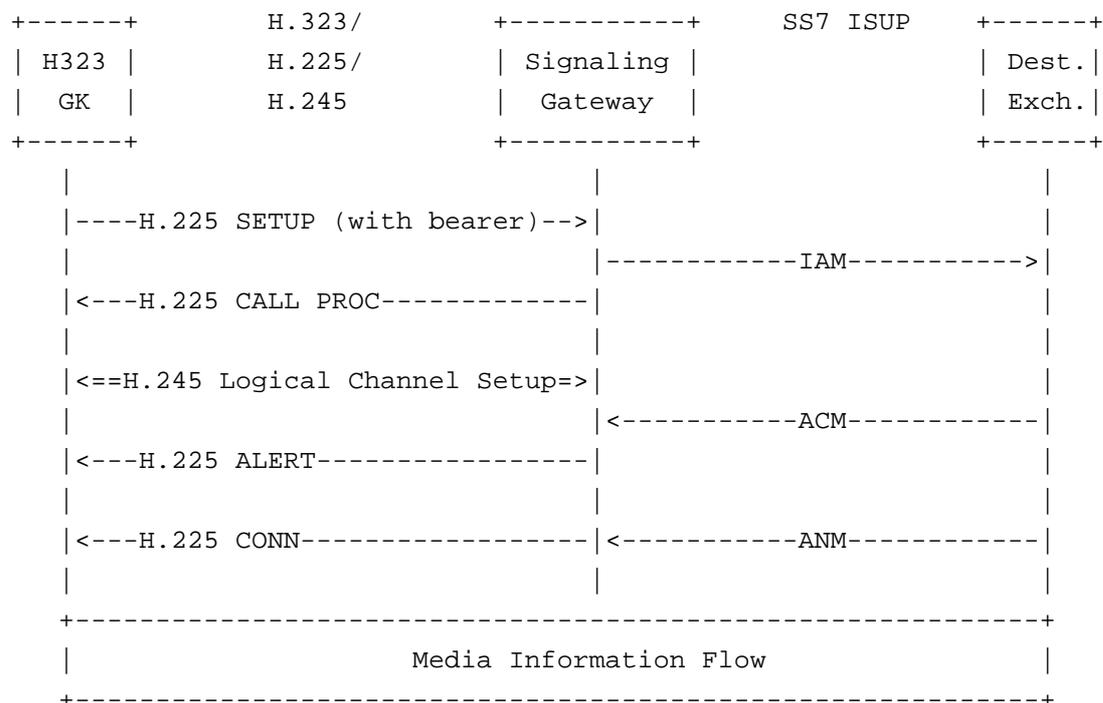


Figure 16: Voice call set up from H.323 to PSTN

Distributed gateway

Normal call events and messages using distributed gateway

- ❑ H.323 terminal starts up
- ❑ Terminal sends a message “Gatekeeper Request” (GRQ)
- ❑ Gatekeeper responds with “Gatekeeper Announce” (CGA)
- ❑ Terminal sends Registration Request (RRQ) message to Gatekeeper
- ❑ Terminal wants to start a call, it uses H.225 to send Admission Request (ARQ) to GK
- ❑ GK answers with Admission Confirmation (ACF), if bandwidth is available
- ❑ Terminal starts a H.225 (with inbuild Q931) dialogue with GK “Setup”
- ❑ GK analyzes the Setup and notes that GW is needed. GK forwards the Setup message to MGC

- ❑ MGC sends an IAM to PSTN and “Add” message to MG, a new context is created implicitly
- ❑ MGC sends “Proceeding” to GK, which forwards it to Terminal
- ❑ MGC and Terminal negotiate a H.245 logical channel
- ❑ MGC receives ACM from PSTN
- ❑ MGC sends H.225 “Proceeding” to Terminal via GK
- ❑ MGC receives ANM from PSTN
- ❑ MGC sends H.225 “Connect” to Terminal via GK. The Connect message carries the IP-address and RTP port number located in the GW, which is reserved for this call.
- ❑ MG now has clear speech channel as indicated by ANM, MGC instructs the MG to Add in to newly created context.
- ❑ Terminal connects to RTP port in the GW
- ❑ MGC issues a Modify command to open two-way speech path between the terminals

The following figure estimates the message sequence in a situation, where Media Gateway and Media Gateway Controller functionalities are distributed and MEGACO protocol is used in between. The call is originated from H.323 terminal.

It should be noted that these charts are not exact representations of all the traffic in between the entities but more like descriptions of major events.

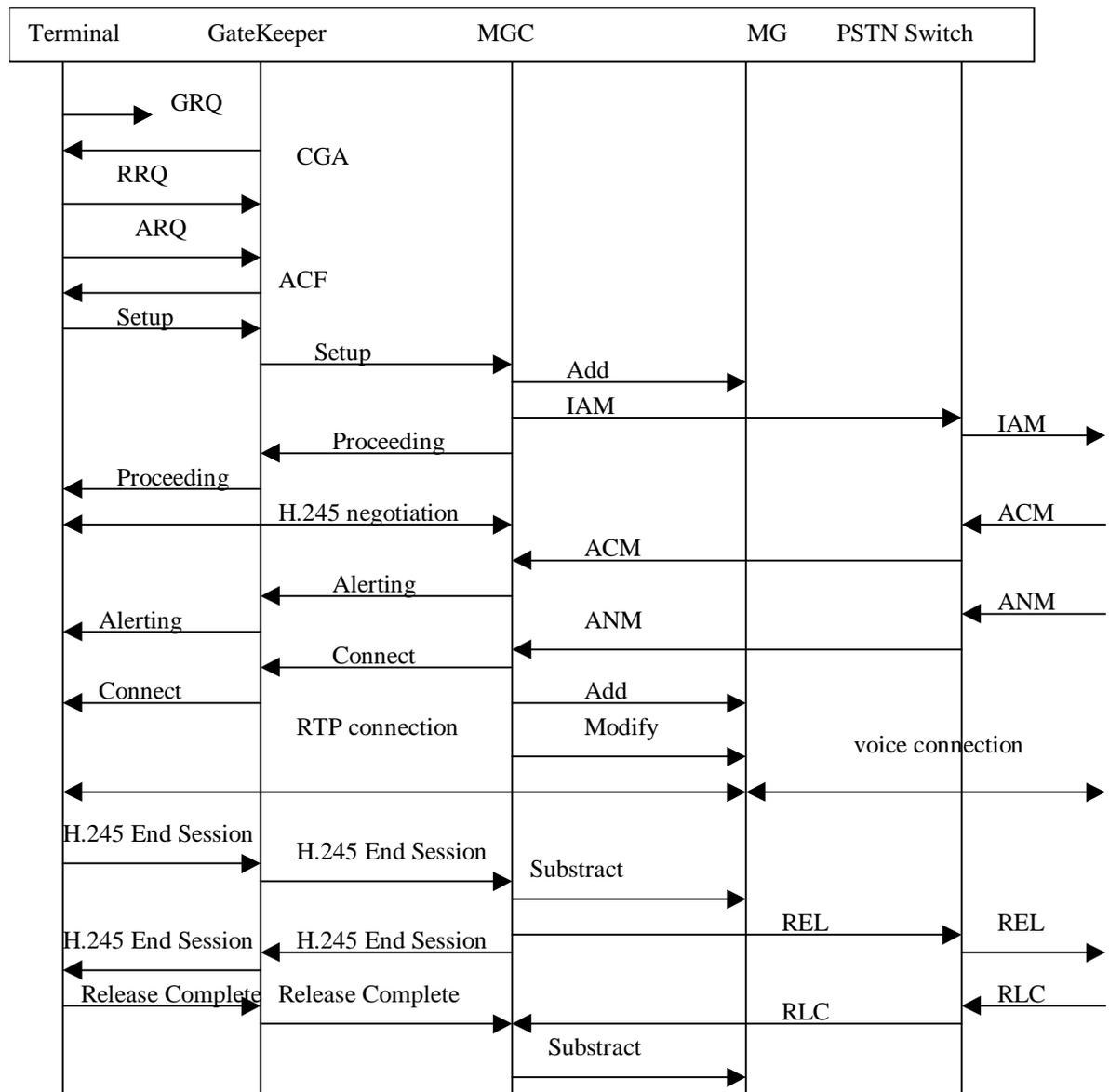


Figure 17: Message Sequence Chart, call from H.323 to PSTN using distributed gateway

7.4.2 From PSTN to H.323

In a comparison to the figure above, the following figure contains estimate of message sequence in a situation, where GateWay is monolithic (signaling and payload handling in a same entity). The call originates from the PSTN.

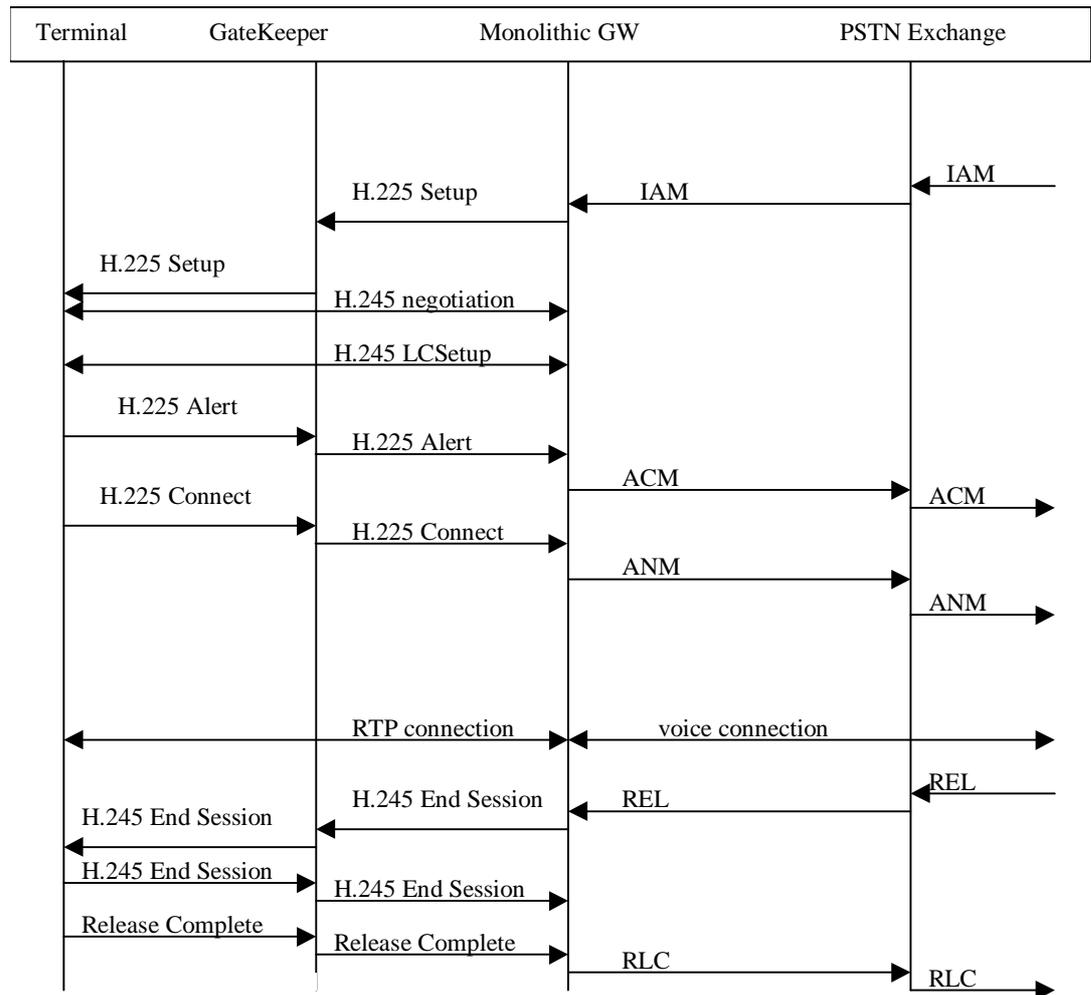


Figure 18: Successful call setup from PSTN terminal to H.323 terminal using monolithic gateway

The following figure (fig.19) sums up of the above figures, employing a distributed GW and a situation where call comes from the PSTN.

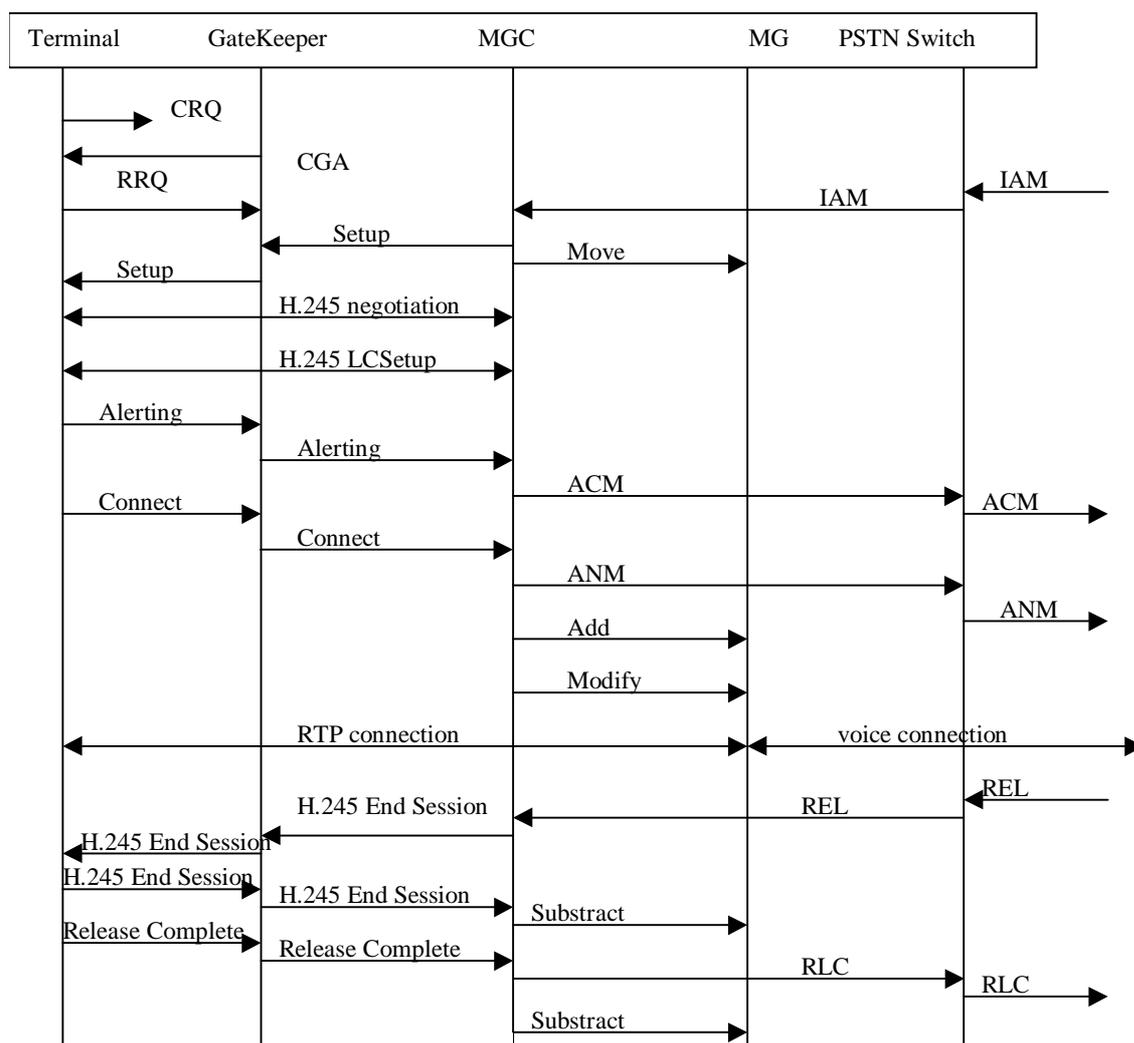


Figure 19: Successful call setup from PSTN terminal to H.323 terminal using distributed gateway

The goal of the implementation is successful handling of the scenarios described in figures 17 and 19. In addition to handling the scenarios, much more must be done to provide a functional multinetwork gateway.

Requirements for the gateway:

- Handling of calls originating from H.323 network
- Handling of calls originating from PSTN network
- Handling of conference calls
- MG “farm” management

- Interfaces to charging and billing systems
- Interfaces to operations & maintenance systems
- Robustness, no single points of failure

8 Technical implementation

This chapter considers the actual implementation; what kind of devices are needed for the installation and especially, what is the structure and functionality of the software.

8.1 Network architecture

The figure below gives an example of a possible scenario where distributed Media GateWay farm is deployed in real network. The MGC nodes back up each other performing no load sharing. MG nodes are all active and not dependent on each other. It is possible to group the MGs to same logical group so they ensure connectivity at all times even though some of the MGs might be not available at some moment.

In reality, the telephone exchange in the figure 20 is possibly substituted with access to STP-nodes and trunking network unless the exchange in question has other functionality as well.

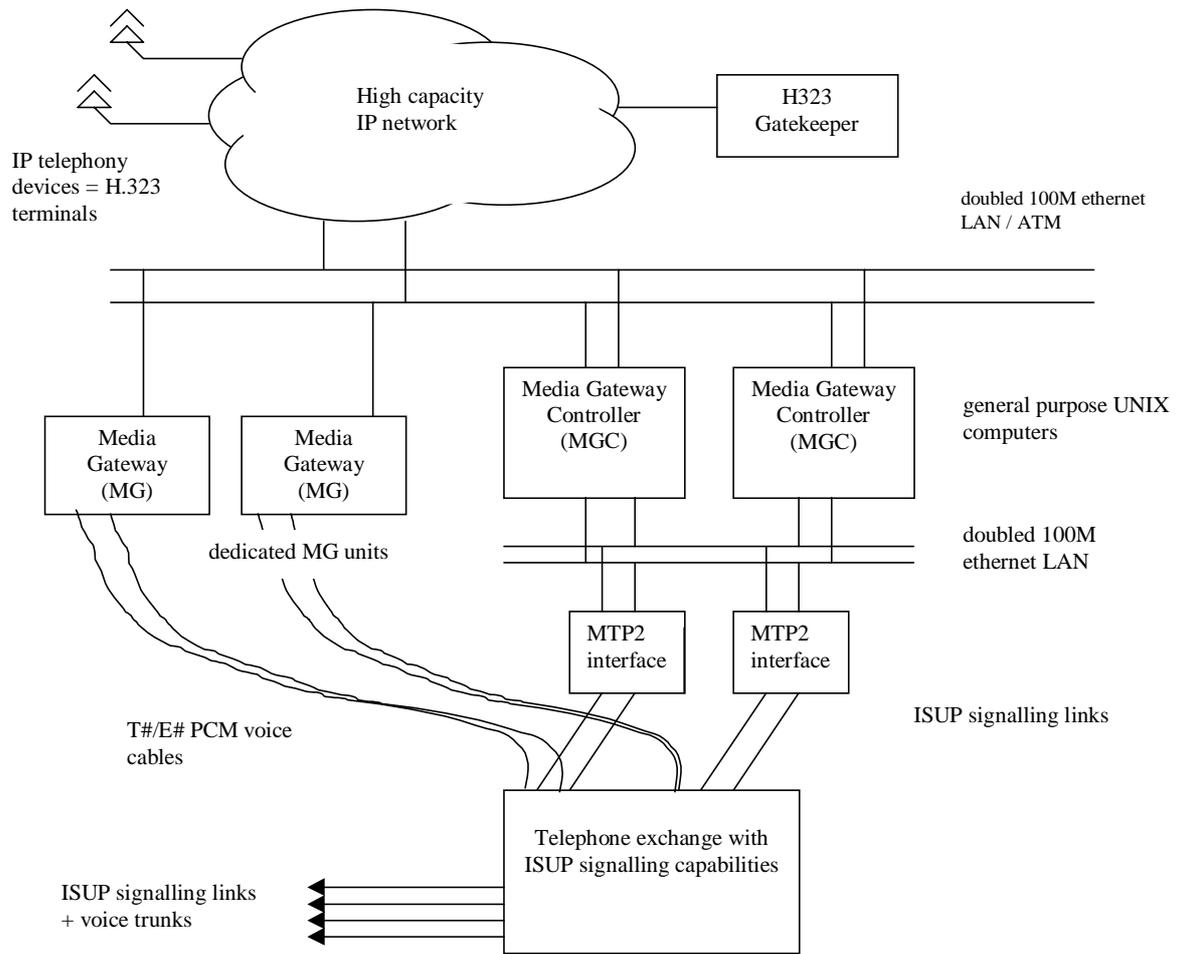


Figure 20: Example network configuration

8.2 Hardware architecture

Suitable choices for the hardware could be:

Media Gateway

Any GateWay which has support for the following:

- Raw voice trunk interface (E1, E3,..)
- MEGACO/H.248 control interface
- RTP/RTCP interface
- high speed IP-interface

The author is not familiar with exact models from hardware vendors.

Gatekeeper

Any Gatekeeper which supports H.323

The author is not familiar with exact models from hardware vendors.

Media Gateway Controller

Pair of general purpose UNIX computers. It is also possible to cope with a single computer system if it is fully redundant (Power supply, CPU, I/O, storage media, etc.)

SS7 network interface unit

G.704 compliant interface towards SS7 network

Ethernet interface for IP traffic to gateway

Example: Nethawk MTP2 server

H.323 Terminal

No specific requirements

8.3 Software architecture

The hardware of the solution is naturally relevant when deploying solution, but much more is needed to build a functional solution. In addition to the Operating System, lots of protocol engines and other application software are needed.

8.3.1 Host software

Operating System (e.g. HP-UX 11.0 or RedHat Linux 6.2) is naturally needed for the basis of the gateway. In addition, a generic application software framework eases the implementation. Instead of building “once and for all” monolithic application, which solves the particular problem in hand, a modular “Lego brick” type of approach has proven successful.

This paper is written for Intellitel Communications Ltd., telecommunications software house.

All Intellitel's solutions are based on the Intellitel™ ONE networking engine, consisting of:

- signaling interfaces (per application)
- Customer Care and Billing System (CCBS) interfaces
- Operating and Maintenance Center (OMC) interfaces and system management
- service programming environment
- core system with high availability service
- optional redundant database component (Oracle and others)

The essential strengths of the ONE networking engine as a basis for the gateway can be seen as follows: [23]

- ONE runs on standard hardware.
- ONE has multiprotocol support by nature

- In-house SS7 stack
- ONE has advanced and flexible database access - can access any internal or external data storage and share its data with other systems.
- True high availability, no single point of failure - built-in carefree hot standby.
- Mass-customizable services - many services or flavors of the same service can share logic and data.
- Clean equipment vendor interfaces - enables operation in multi-vendor environment, easy porting to new environments
- Standard network interfaces.
- Carefree management and clear interfaces – decreases operational costs and makes system integration easier and quicker.

At the market, Intellitel is positioned as a provider of Network Intelligence Middleware for telecom operators and similar companies.

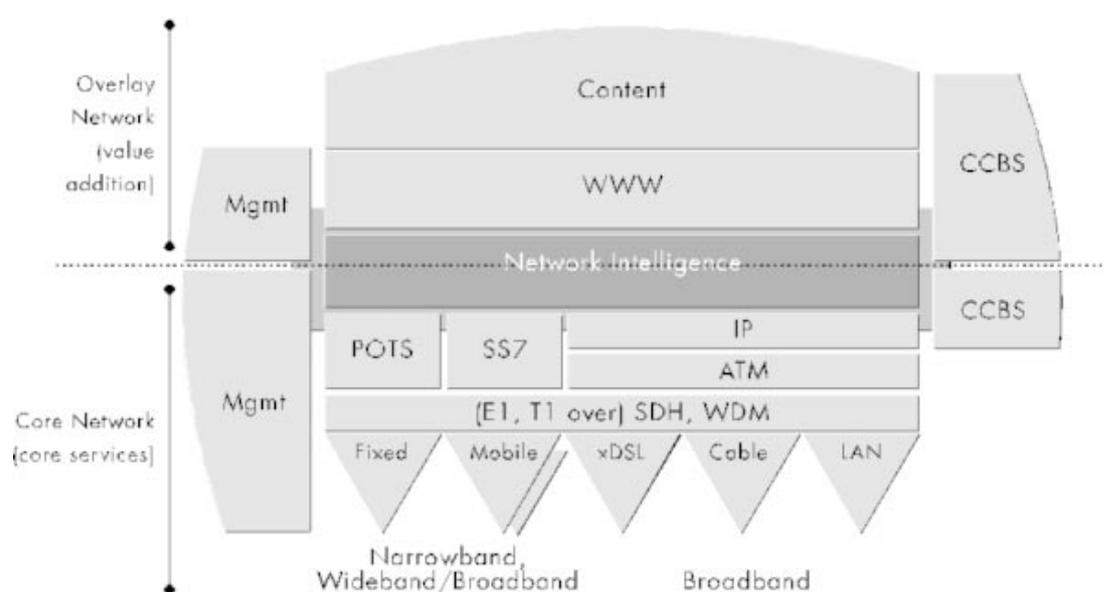


Figure 21: Network Intelligence Middleware

The internals of a host running ONE software consist of multiple OS-level processes depending on a particular application. The following figure depicts the process structure of the signaling gateway between PSTN and VoIP networks.

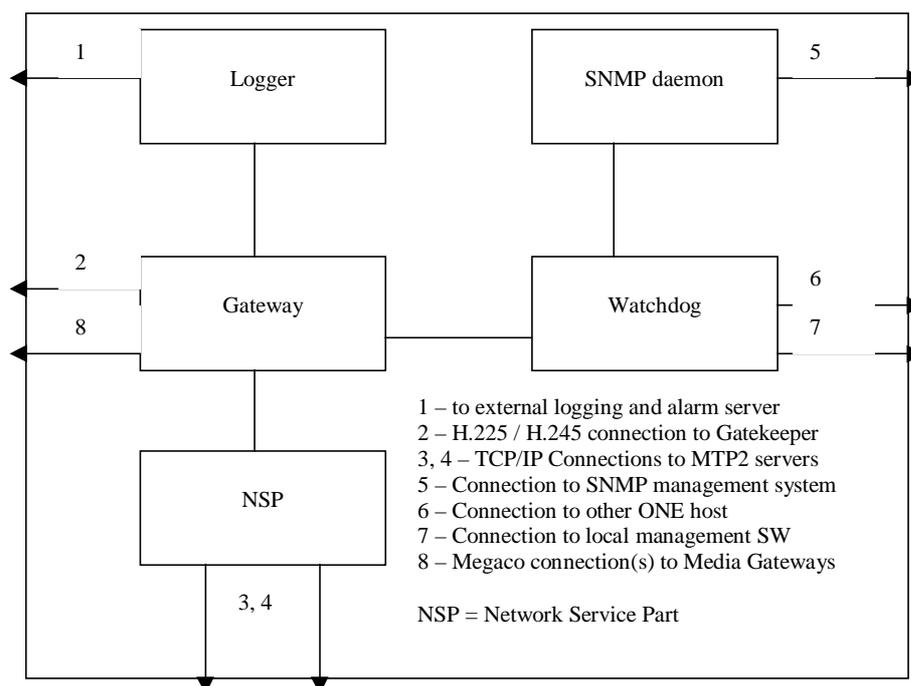


Figure 22: Process structure

The processes in the Figure 22 explained:

- **Logger** - Process collecting the various log messages system wide. Takes also care of alarm messages that are to be delivered to external OMC systems.
- **Gateway** - The actual business logic. Contains call control and the protocol stacks towards SS7 (ISUP) and H.323 network. Codecs, where ASN.1 encoding is needed, are built with CASN-compiler (CASN is product of Nokia Research Center).
- **NSP** - Process containing mainly the MTP3 protocol implementation. Process takes also care of the welfare of the SS7 connectivity, provides reliable transfer of SS7 messages.
- **SNMP Daemon** - Provides management and monitoring interface to external OSS systems. Contains generic and proprietary MIBs.
- **Watchdog** - Takes care of starting (and stopping) of other processes. Provides communication facilities to all other processes and management gateway to external systems. Also responsible for managing the switchover situations.

In addition to processes listed above the system contains software to monitor the well being of the host itself (CPU-load, memory) and network interfaces. The system may also contain internal database for e.g. customer specific services.

Other host is active and other a “lukewarm” standby. The standby ONE host contains the same processes as the active ONE. The hosts monitor each other’s welfare by proprietary management protocol run over TCP/IP in between the watchdog processes.

In case of failure of hot node, the passive node warms itself (engages the active mode) and starts handling the payload. The failure of the passive node is not visible to external systems and payload handling. It is possible to maintain the state of the calls during switchover.

The hosts are connected to each other with two LANs to prevent cable, network card or hub failure cause installation to fail. Switching from primary LAN to backup or the other way around is completely automated and takes less than one second to accomplish.

8.3.2 Application software

The Operating System and the host software as defined above take care of the welfare of the actual application software, which runs the actual “business logic”. The actual functionality of the system is to connect calls in between the different networks.

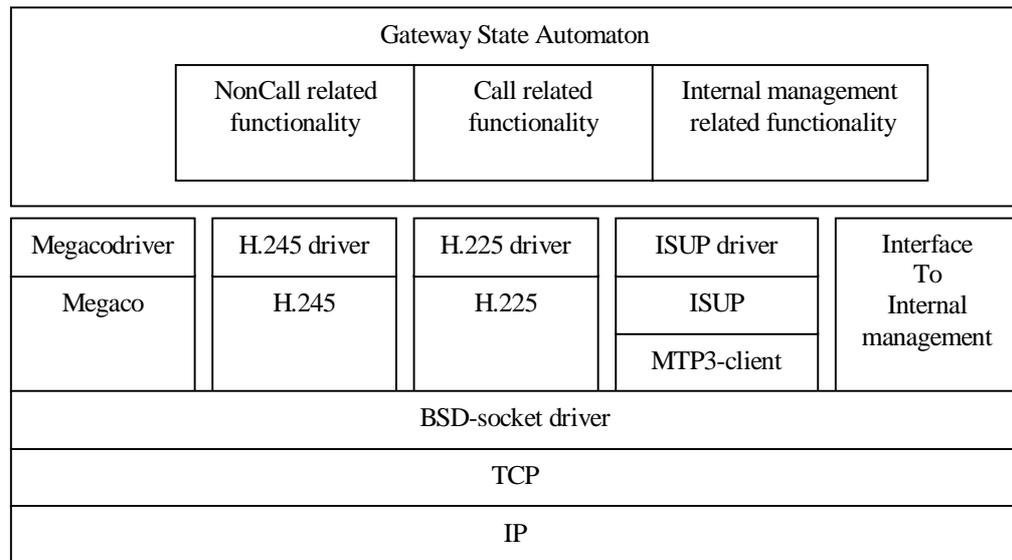


Figure 23: Application software architecture

The protocol engines (MEGACO, H.245, H.225 and ISUP) are conveniently built on CVOPS protocol development and runtime environment. CVOPS provides timers, message transfer mechanisms as well as framework for concurrent tasks and state automaton. [24]

By utilizing Intellitel™ ONE networking engine, the solution is robust, modular, easily manageable and maintainable and it scales nicely. In addition, every protocol component, which is built during the implementation, can be re-used in the future in other projects. There are no Single Points Of Failure (SPOF) in the installed production system, as all the components are (at least) doubled and their welfare is continuously monitored. A replacement component activates automatically if and when the primary fails.

9 Conclusion

The world is changing. The speed of the change seems to be accelerating. When this piece of work started, SIP was still far in the horizon and H.323 was strong.

H.323 is still strong and it is not disappearing anywhere soon. The author believes that the players in the industry who have their network components built around H.323 architecture will continue with it for many years to come. These players, however, cannot ignore the IETF-based SIP forever.

H.323 protocol stacks with relevant Application Programming Interfaces (API) are available from numerous vendors. These stacks, however, are often costly and a serious barrier for companies which are starting on the field. Often the licensing issues of the implementations can pose a problem for building a commercially successful solution.

Intellitel Communications Ltd., the company that pays the author's salary, is not a new player in the market. Intellitel has the capability to either obtain the stacks from another party or build them by itself. Still, aiming towards the future, instead of the present day, the SIP is probably a more future-proof choice. The solution drafted in this paper might possibly never be productized, at least by Intellitel. The same solution but with SIP is a completely different matter.

SIGNaling TRANSport (SIGTRAN) team from IETF has gotten several documents and protocols to RFC stage while this thesis is being written. Implementing a signaling gateway should rely on the support for standard Stream Control Transmission Protocol (SCTP) family of protocols. By utilizing a set of widely known standards, the system integrators are freer to select from different products from different vendors.

No matter what the technologies behind the commercial networks are, be them Digital Television, DSL, ATM, SDH, UMTS, GPRS, W-LAN and what ever the bit rates are, 10, 100 or 1000 kilobytes per second, one thing remains the same. There are sources and sinks of media. There is and there will be a data transport mechanisms in between the source and sink. These mechanisms shall be controlled,

if not for any other purpose, for billing. For the control, building blocks (protocol stacks, special software applications) are needed.

Newcomers in the industry and the vendors who are just starting to provide software and integrated solutions for this highly challenging field of technology, may be better off with SIP and forget H.323 from the day one.

Even though the product drafted in this thesis may never realize, the amount of know-how (VoIP in general, MEGACO and H.323 in particular) gained during the writing of this thesis is significant, and what's equally important, it is relevant.

REFERENCES

- [1] Black, U. ISDN and SS7 Architectures for Digital Signaling Networks
Prentice Hall, 1997

- [2] EURESCOM. Project P920-GI, UMTS Network Aspects,
Deliverable 2, Investigation of architectures and protocols for
UMTS network evolution. October 2000

- [3] Harju, Jarmo. Siirto- ja välitystekniikan perusteet. ISBN
951-763-667-9, Lappeenrannan teknillinen korkeakoulu 1991

- [4] Stallings, William. IPv6: The New Internet Protocol
Referenced: 28.05.2001 Available:
<http://www.cs-ipv6.lancs.ac.uk/ipv6/documents/papers/stallings/>

- [5] Information Sciences Institute, University of Southern
California. Internet Protocol. RFC 791, September 1981. Referenced:
04.06.2001. Available: <http://www.ietf.org/rfc/rfc0791.txt>

- [6] Postel, J. Address Mappings. RFC 796, September 1981.
Referenced 04.06.2001
Available: <http://www.ietf.org/rfc/rfc0796.txt>

- [7] Information Sciences Institute, University of Southern
California. Transmission Control Protocol. RFC 793, September
1981.
Referenced 04.06.2001. Available: <http://www.ietf.org/rfc/rfc0793.txt>

- [8] VoIP-perusteet, copyright Relevantum Oy 2000

- [9] H. Schulzrinne et al. RTP: A Transport Protocol for Real-Time Applications. RFC 1889, January 1996. Referenced 04.06.2001.
Available: <http://www.ietf.org/rfc/rfc1889.txt>
- [10] Cuervo F. et al. MEGACO Protocol Version 1.0. RFC 3015, November 2000. Referenced 04.06.2001.
Available: <http://www.ietf.org/rfc/rfc3015.txt>
- [11] Handley, M. and V. Jacobson. SDP: Session Description Protocol. RFC 2327, April 1998. Referenced 04.06.2001.
Available: <http://www.ietf.org/rfc/rfc2327.txt>
- [12] ITU-T Recommendation X.680 (1997): "Information technology-Abstract Syntax Notation One (ASN.1): Specification of basic notation".
- [13] ITU-T Recommendation X.690 : "Information technology – ASN.1 Encoding rules: Specification of the Basic Encoding Rules (BER)"
- [14] Crocker, D. and P. Overell. Augmented BNF for Syntax Specifications: ABNF RFC., RFC 2234, November 1997.
Available: <http://www.ietf.org/rfc/rfc2234.txt>
- [15] R. Stewart et al. Stream Control Transmission Protocol. RFC 2960, October 2000. Referenced: 04.06.2001.
Available: <http://www.ietf.org/rfc/rfc2960.txt>
- [16] Idman, J. Digitaalisen matkapuhelinverkon MAP-matkapuhelinosaan tarjoamat palvelut. Diplomityö. Lappeenrannan teknillinen

korkeakoulu. 1997

- [17] Databeam. Primer on the H.323 Series Standard. May 15, 1998

- [18] SipCenter. SIP and H.323 Referenced: 28.05.2001
Available: <http://www.sipcenter.com/aboutsip/siph323/h323sip.htm>

- [19] Schulzrinne, H. Comparison of H.323 and SIP.
Referenced: 30.05.2001 Available:
<http://www.cs.columbia.edu/~hgs/sip/h323-comparison.html>

- [20] Schulzrinne, H. Session Initiation Protocol (SIP). Referenced:
30.05.2001 Available: <http://www.cs.columbia.edu/~hgs/sip/>

- [21] 3G.IP. 3G.IP: Our Mission: Referenced: 28.05.2001
Available: <http://www.3gip.org/>

- [22] Telehallintokeskus. Määräys televerkon suorituskyvystä.
THK 29A/97M. 1997.

- [23] Pasi Kemppainen. White Paper, Network Intelligence Middleware.
2001

- [24] Celtius. CVOPS - for implementing portable communications
software Referenced: 30.05.2001 Available:
http://www.celtius.com/cpfpage_811.htm

- [25] Sipcenter. MGCP/Megaco Background. Referenced: 28.05.2001
Available: <http://www.sipcenter.com/aboutsip/siph323/mgcpback.htm>

APPENDICES

Appendix 1: MEGACO Packages

Appendix 2: ISUP Messages

Appendix 1: MEGACO Packages

1 Generic

Generic package for commonly encountered items.

2 Base Root Package

This package defines Gateway wide properties.

3 Tone Generator Package

This package defines signals to generate audio tones. This package does not specify parameter values. It is intended to be extendable. Generally, tones are defined as an individual signal with a parameter, ind, representing "interdigit" time delay, and a tone id to be used with playtones. A tone id should be kept consistent with any tone generation for the same tone. MGs are expected to be provisioned with the characteristics of appropriate tones for the country in which the MG is located.

4 Tone Detection Package

This Package defines events for audio tone detection. Tones are selected by name (tone id). MGs are expected to be provisioned with the characteristics of appropriate tones for the country in which the MG is located.

5 Basic DTMF Generator Package

This package defines the basic DTMF tones as signals and extends the allowed values of parameter tl of playtone in tonegen.

6 DTMF detection Package

This package defines the basic DTMF tones detection. This Package extends the possible values of tone id in the "start tone detected" "end tone detected" and "long tone detected" events.

7 Call Progress Tones Generator Package

This package defines the basic call progress tones as signals and extends the allowed values of the tl parameter of playtone in tonegen

8 Call Progress Tones Detection Package

This package defines the basic call progress detection tones. This Package extends the possible values of tone id in the "start tone detected", "end tone detected" and "long tone detected" events.

9 Analog Line Supervision Package

This package defines events and signals for an analog line.

10 Basic Continuity Package

This package defines events and signals for continuity test. The continuity test includes provision of either a loopback or transceiver functionality.

11 Network Package

This package defines properties of network terminations independent of network type.

12 RTP Package

This package is used to support packet based multimedia data transfer by means of the Real-time Transport Protocol (RTP) [RFC 1889].

13 TDM Circuit Package

This package is used to support TDM circuit terminations.

Appendix 2: ISUP messages

The most common ISUP messages explained briefly

IAM Initial Address Message. Used to reserve the path for the call through the PSTN network.

ACM Address Complete Message. The final exchange, where the call is being routed, sends ACM when it has received IAM and has knowledge to what subscriber line the call is to be made.

ANM ANswer Message. When the called subscriber answers the call, the nearest exchange to her sends this message to backward direction, towards caller.

REL RElease. When the call is released for any reason, this message is transported through the call path.

RLC ReRelease Complete. When an exchange has received REL message and freed the relevant CICs, it answers to the exchange which sent the REL with RLC.

BLO BLOcking. This message is used for blocking out a group of CICs from the exchange which has issued the BLO message. Used for maintenance purposes (e.g. when MG is temporarily out of service the trunks terminated to it are BLOcked)

BLA BLocking Acknowledge. When an exchange receives a BLO message, it responds with BLA to inform that it has received BLO, processed it and wont send new calls to blocked CICs.

UBL UnBLOckin. When the set of CICs that have been BLOcked earlier, are to be unblocked, this message is sent by the exchange that sent the BLO message earlier.

UBA UnBlocking Acknowledge. When an exchange receives a UBL message, it responds with UBA to inform that it has received UBL, processed it and will use the unblocked CICs for new calls.

RSC ReSet Circuit. If a circuit needs to be resetted, this message is used by either end of the circuit. The other end responds with RLC.

There are lots more ISUP messages and even more parameters, but these are most often seen in the live network.