A STUDY ON VOIP

BY

MD HASAN
ID: 061-19-333

AND

MD. ABDUR RAHMAN

ID: 061-19-377

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Electronics and Telecommunication Engineering

Supervised By

Dr. MD Golam Mowla Chowdhuri

Professor and Head

Department of ETE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

APPROVAL

This project report title "A Study On VoIP" Submitted by Md Hasan, ID: 061-19-333 and Md. Abdur Rahman, ID: 061-19-377 Department of Electronics and Telecommunication Engineering Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Electronics and Telecommunication Engineering and approved as to its style and contents. The presentation has been held on February 2011.

Board of Examiners

1. ……..

Dr. Md. Golam Mowla Chowdhury **Chairman**

Professor and Head, Department of Electronics and Telecommunication Engineering

Daffodil International University

2. ……..

A.K.M Fazlul Haque **Internal**

Assistant Professor, Department of Electronics and Telecommunication Engineering,

Daffodil International University

3. ……..

M M G Golam Rashed **Internal**

Assistant Professor, Department of Electronics and Telecommunication Engineering,

Daffodil International University

4. ……..

Dr. Subrata Kumar Aditya **External**

Professor & Chairman,

Department of Applied Physics, Electronics & communication Engineering

University of Dhaka

DECLARATION

We do, declare that the Project work presented in this Report is done by us under the supervision of **Dr. Md. Golam Mowla Chowdhury** ,Department of Electronics and Telecommunication Engineering. We also declare that neither this report nor any part there of has been submitted elsewhere for the award of any Degree or Diploma.

Submitted by:

……

(Candidate)

Md Hasan

ID no: 061-19-333

……

(Candidate)

Md. Abdur Rahman

ID no: 061-19-377

Department of Electronics and Telecommunication Engineering

Countersigned:

……

(Supervisor)

Dr. Md. Golam Mowla Chowdhury

Professor and Head

Department of Electronics and Telecommunication Engineering

Daffodil International University

ACKNOWLEDGEMENTS

At the beginning we remember Allah the merciful, the beneficent since, but for His grace it would not been possible on our part to complete this project. Next we would like to thank our parents for their unconditional support and care during our whole educational period.

We would like to express our deep sense of gratitude to our supervisor, **Dr. Md. Golam Mowla Chowdhury** for eoposing this interesting and widespread area of Voice Over Internet Protocol and int us how to inform research works. Our project works couldn't be accomplished without his invaluable help guidance during the course of the wok. We are highly indebted to him for constantly encouraging us by giving his critical opinion on our work. We are grateful to all of for having given us the support and confidence.

ABSTRACT

For many years, voice over internet protocol (VoIP) has held the promise of enabling the next generation of voice communication within the enterprise. In this project paper we discuss about "The Study of VOIP ". The study of voice over internet protocol includes the fundamentals of VoIP, including two techniques of voip that is H.323 and SIP. This two standards currently complete for the domains of IP telephony signaling: the H.323 protocol suite by ITU-T, and the Session Initiation Protocol (SIP) by IETF. Both of this signaling protocol provides mechanisms for call establishment and teardown, call control and supplementary services, and capability exchange. We also study the comparisons of these two protocols in terms of Functionality, Quality of Service (QoS), Scalability, Flexibility, Interoperability, and Ease of Implementation. We also discussed briefly on two gateway control protocol, one is MGCP and another is H.248. We highlighted about the voice over internet protocol in Bangladesh. Finally we consider the best protocol on voice over internet protocol is session initiation protocol in terms of ease of customization, protocol encoding and ease of installation as companied to other protocol.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ACF	Admission Confirm Message
ACS	Admission confirm sequence
AUEP	Audit Endpoint
AUCX	Audit Connection
ABNF	Augmented Backus-Naur Form
ARx	Admission request, reject, and confirm messages
BTCL	Bangladesh Telecommunications Company Ltd
BTRC	Bangladesh Telecommunication Regulatory Commission
BRx	Bandwidth request, reject, and confirm message
CODECs	Coder/decoder
CC	Country Code
CRCX	Create Connection
DSP	Digital Signal Processor
DLCX	Delete Connection
DUNDi	Distributed Universal Number Discovery
DRx	Disengage request, reject, and confirm
EN	End Number
EP	End Point
GK	Gatekeeper
GDS	Global Dialing Scheme
GRx	Gatekeeper request, reject, and confirm messages
GCF	Gatekeeper Confirm
HTTP	Hyper Text Transport Protocol
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol

IPv6	Internet Protocol Version 6
IPTSP	Internet Protocol Telephony Service Provider
ISP	Internet Service Provider
IAC	International Access Code
ITU	International Telecommunication Union
IMS	IP Multimedia Subsystem
IETF	Internet Engineering Task Force
IPDC	Internet Protocol Device Control
IRx	Info request, ack, nack, and response
ILDTS	International Long Distance Telecommunication Services
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
LAN	Local Area Network
LRx	Location request, reject, and confirm messages
LRQ	location requests
MOS	Mean Opinion Score
MCU	Multipoint Control Unit
MSD	Master/Slave Determination
MDCX	Modify Connection
MSRP	Message Session Relay Protocol
MGCP	Media Gateway Control Protocol
MG	Media Gateway
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OP	Organizational prefix
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
PER	Packed Encoding Rules

RAS	Registration Administration Status
RTP	Real-Time Transport Protocol
RSIP	Restart In Progress
RQNT	Request Notification
RTCP	Real-time Transport Control Protocol
RACs	Request for Comments
RRx	Registration request, reject, and confirm messages
RIP	Request in progress
RAx	Resource availability indication and confirm
RCF	Registration Confirm
RSVP	Resource Reservation Protocol
SS-CCBS	Supplementary Service Call Completion on Busy Subscriber
SS-CW	Supplementary Service-Call Waiting
SS-HOLD	Supplementary Service HOLD
SIP	Session Initiation Protocol
SDP	Session Description Protocol
SS7	Signaling System 7
SIMPLE	Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions
SMTP	Simple Mail Transfer Protocol
SCTP	Stream Control Transmission Protocol
SBC	Session border controllers
SGCP	Simple Gateway Control Protocol
SCN	Switched Circuit Network
SP	Signaling Protocol
SG	Signaling Gateway
SCx	Service control indication and response
TCP	Transmission Control Protocol
TCS	Terminal Capability Set
TDM	Time Division Multiplexing

TLS	Transport Layer Security
TELCOS	Traditional Telecommunication Companies
VOIP	Voice Over Internet Protocol
URL	Universal Resource Identifier
URx	Unregister request, reject, and confirm messages
VoBB	Voice Over Broadband
VTC	videoteleconference
WAN	Wide Area Network
UDP	User Datagram Protocol

URL	Uniform Resource Locator
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
URI	Uniform Resource Identifier

CHAPTER 1
INTRODUCTION

1.1 What is VOIP?

Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. Other terms frequently encountered and synonymous with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, and broadband phone.

Internet telephony refers to communications services — voice, facsimile, and/or voice-messaging applications — that are transported via the Internet, rather than the public switched telephone network (PSTN). The basic steps involved in originating an Internet telephone call are conversion of the analog voice signal to digital format and compression/translation of the signal into Internet protocol (IP) packets for transmission over the Internet; the process is reversed at the receiving end. VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs which encode speech allowing transmission over an IP network as digital audio via an audio stream. Codec use is varied between different implementations of VoIP (and often a range of codecs are used); some implementations rely on narrowband and compressed speech, while others support high fidelity stereo codecs [4].

1.2 What is IP?

The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP.IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagram's (packets) from the source host to the destination host solely based on their addresses. For this purpose the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4) is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPV6) is being deployed actively worldwide [5].

1.3 Benefits of VoIP

Voice over Internet Protocol (VoIP) is a technology that enables the users to make voice calls, using a broadband Internet connection. Voice over Internet Protocol (VoIP), refers to a collection of transmission technologies, which make voice communications possible over the Internet. It is also known as Internet telephony and helps the conversion of voice into a digital signal that can be sent over the Internet. These signals are then compressed and translated to IP (Internet Protocol) packets for transmission. They are converted to a regular telephone signal, if the user is calling on a normal phone. VoIP gives the provision of making calls directly from a desktop computer and uses a special VoIP phone for the purpose. The services and benefits offered by Internet telephony feature the ones which are not available with a traditional phone. Here are some of the benefits of VoIP. VoIP can be a benefit for reducing communication and infrastructure costs. Examples include: Routing phone calls over existing data networks to avoid the need for separate voice and data networks .Conference calling, IVR, call forwarding, automatic redial, and caller ID features that traditional telecommunication companies (telcos) normally charge extra for are available free of charge from open source VoIP implementations. Costs are lower, mainly because of the way Internet access is billed compared to regular telephone calls. While regular telephone calls are billed by the minute or second, VoIP calls are billed per megabyte (MB). In other words, VoIP calls are billed per amount of information (data) sent over the *Internet* and not according to the time connected to the telephone network. In practice the amount charged for the data transferred in a given period is far less than that charged for the amount of time connected on a regular telephone line [7].

1.3.1 Flexibility

VoIP can facilitate tasks and provide services that may be more difficult to implement using the PSTN. Examples include:

The ability to transmit more than one telephone call over a single broadband connection without the need to add extra lines [8].

Secure calls using standardized protocols (such as Secure Real-time Transport Protocol). Most of the difficulties of creating a secure telephone connection over traditional phone lines, such as digitizing and digital transmission, are already in place with VoIP. It is only necessary to encrypt and authenticate the existing data stream. Location independence. Only a sufficiently fast and stable Internet connection is needed to get a connection from anywhere to a VoIP provider. Integration with other services available over the Internet, including video conversation, message or data file exchange during the conversation, audio conferencing, managing address books, and passing information about whether other people are available to interested parties [9].

1.3.2 Cost Efficiency

The most important benefit of VoIP technology is its cost efficiency, which in turn adds to the savings of consumers and companies using it. Generally, it saves around 30% to 50% of the traditional phone bills, and sometimes more. It may not sound as lucrative for individuals, but if large organizations are considered, the savings can be in the millions.

1.3.3 Improved Productivity

Installation of Internet telephony ensures improved productivity of an organization. As the technology is cost-efficient, the money thus saved can be utilized for various other purposes. VoIP technology treats services on the phone like any other kind of data, enabling the users to attach documents to voice messages, or participate in virtual meetings with the help of shared data and video conferencing. The clarity of voice over phone is also an added feature of the technology. Earlier, talking through VoIP phones often led to calls which were distorted, lagging and many a times, dropped. With the change in technology, the sound clarity is better than ever, and rarely the calls get dropped.

1.3.4 Simple and Scalable Infrastructure

The installation process for VoIP phones is very simple, and once done, high mobility of the system is an added advantage. The hassles of separate cabling for telephone systems

can also be avoided by using this technology. The infrastructure of the whole system is very scalable and new components can be added easily without much difficulty. As the transfer of voice, which is converted into signals is based on software, rather than hardware, it is easier to alter and maintain the whole system. All these attributes makes VoIP more popular, as one does not have to be very good at computers. In order to availites facilities, IP Telephony combines voice and data networks onto a single network, creating a more manageable, cost-efficient, and productive solution for business communications. In addition to the above-mentioned advantages, wireless VoIP enables the user to make low cost calls from any place and also facilitates WiFi. These WiFi spots may include airports, cafeterias, hotels, and various other locations.

Chapter 2

How VOIP works?

2.1 How VOIP Process a Typical call

A voice signal from a Voice over IP phone (or an older phone connected through a suitable VoIP adapter) is passed through a VoIP device that converts the regular telephone voice signal to a digital one so it can use a broadband internet connection where it travels to the destination equipment. The digital signal is then converted back to the original voice call. In other words, when the originator calls a number the Voice over IP (VoIP) phone logs on to the routing server - which looks up the destination IP number that's associated with the dialled phone number - and it makes the connection. If the destination number isn't using VoIP, and doesn't have the phone number tied in with an IP number, then it is recognised that the destination number is a Public Switched Telephone Network (PSTN) phone and the call is routed through the PSTN [10].

2.2 Numbering Scheme:

The most common addressing systems are:

- E.164: The ITU-T recommendation used in PSTN
- URI: Universal resource identifier, used in internet
- ENUM: E.164 addressing plan based NUMber
- GDS: Global Dialing Scheme
- DUNDi: Distributed Universal Number Discovery

2.2.1 ENUM

ENUM is a protocol defined by IETF that facilities resolving of E.164 telephone numbers into Other resources or services on the internet. E.g.:%204689761234 3: 4.3.2.1.6.7.9.8.6.4.e164.arpa

2.2.2 GDS

GDS, Global Dialing Scheme, is a dialling scheme for enabling global number recognition for H323. the structure of GDS is:

- < IAC>
- The International Access Code (IAC)
- Country Code (CC)
- Organisational Prefix (OP)
- Endpoint Number (EN)
- E.g.: 00(IAC) 1(CC) 189(OP) 7201234(EN): 0011897201234

2.2.3 DUNDi

Opposed to ENUM and GDS which are based on servers for resolving addresses the DUNDi is a p2p standard (one can say p2p version of ENUM). DUNDi is not a numbering standard but an implementation standard. Instead of DNS server registration a client has a record of all nodes connected to it. When a client needs to look up for a number it will contact all connected nodes to find the address, they in turn ask the nodes they are connected to for finally to find the destination [10].

2.3 Codecs:

There are many codecs for audio, video, fax and text. Below is a list of the most common codecs for VoIP [11]

Table 1. List Of Codec

Codec	Bandwidth/kbps	Comments
G.711	64	Delivers precise speech transmission. Very low processor requirements. Needs at least 128 kbps for two-way.
G.722	48/56/64	Adapts to varying compressions and bandwidth is conserved with network congestion.

G.723.1	5.3/6.3	High compression with high quality audio. Can use with dial-up. Lot of processor power.
G.726	16/24/32/40	An improved version of G.721 and G.723 (different from G.723.1)
G.729	8	Excellent bandwidth utilization. Error tolerant. License required.
GSM	13	High compression ratio. Free and available in many hardware and software platforms. Same encoding is used in GSM cellphones (improved versions are often used nowadays).
iLBC	15	Robust to packet loss.

2.4 Mean opinion Score:

The mean opinion score (MOS) of a VoIP call is a subjective measurement of the call's quality. Specified in ITU-T Recommendation P.800, MOS values range from 1-5, with 1 being bad and 5 excellent. There are several factors that can affect the quality of a VoIP call, such as packet loss, latency, and jitter. A MOS value is derived from a pool of individuals listening to recordings over the system being tested. The indivuals rate the quality of the recording from 1-5. The mean score of those values is the MOS of the VoIP call [12].

Table 2. Rating system used to obtain a MOS

Listening Quality Scale	
Quality of Speech	**Score**
Excellent	5
Good	4
Fair	3
Poor	2
Bad	1

The table above depicts the rating system used to obtain a MOS

2.5 Delay/Latency:

VoIP delay or latency is characterized as the amount of time it takes for speech to exit the speaker's mouth and reach the listener's ear. Three types of delay are inherent in today's telephony networks: propagation delay, serialization delay, and handling delay. Propagation delay is caused by the length a signal must travel via light in fiber or electrical impulse in copper-based networks. Handling delay also called processing delay defines many different causes of delay (actual packetization, compression, and packet switching) and is caused by devices that forward the frame through the network. Serialization delay is the amount of time it takes to actually place a bit or byte onto an interface. Serialization delay is not covered in depth in this book because its influence on delay is relatively minimal [1].

2.5.1 Propagation Delay

Light travels through a vacuum at a speed of 186, 000 miles per second, and electrons travel through copper or fiber at approximately 125, 000 miles per second. A fiber network stretching halfway around the world (13, 000 miles) induces a one-way delay of about 70 milliseconds (70 ms). Although this delay is almost imperceptible to the human ear, propagation delays in conjunction with handling delays can cause noticeable speech degradation [1].

2.5.2 Handling Delay

As mentioned previously, devices that forward the frame through the network cause handling delay. Handling delays can impact traditional phone networks, but these delays are a larger issue in packetized environments. The following paragraphs discuss the different handling delays and how they affect voice quality.

In the Cisco IOS VoIP product, the Digital Signal Processor (DSP) generates a speech sample every 10 ms when using G.729. Two of these speech samples (both with 10 ms of delay) are then placed within one packet. The packet delay is, therefore, 20 ms. An initial look-ahead of 5 ms occurs when using G.729, giving an initial delay of 25 ms for the first speech frame. Vendors can decide how many speech samples they want to send in one

packet. Because G.729 uses 10 ms speech samples, each increase in samples per frame raises the delay by 10 ms. In fact, Cisco IOS enables users to choose how many samples to put into each frame. Cisco gave DSP much of the responsibility for framing and forming packets to keep router/ gateway overhead low. The Real-Time Transport Protocol (RTP) header, for example, is placed on the frame in the DSP instead of giving the router that task [1].

2.5.3 Queuing Delay

A packet-based network experiences delay for other reasons. Two of these are the time necessary to move the actual packet to the output queue (packet switching) and queuing delay. When packets are held in a queue because of congestion on an outbound interface, the result is queuing delay. Queuing delay occurs when more packets are sent out than the interface can handle at a given interval. The actual queuing delay of the output queue is another cause of delay. You should keep this factor to less than 10 ms whenever you can by using whatever queuing methods are optimal for your network. The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) G.114 recommendation specifies that for good voice quality, no more than 150 ms of one-way, end-to-end delay should occur, as shown in Figure 2.1. With the Cisco VoIP implementation, two routers with minimal network delay (back to back) use only about 60 ms of end-to-end delay. This leaves up to 90 ms of network delay to move the IP packet from source to destination.

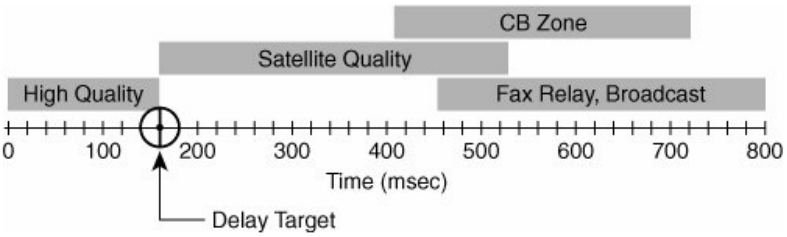

Figure 2.1. End-to-End Delay

As shown in Figure 2.1, some forms of delay are longer, although accepted, because no other alternatives exist. In satellite transmission, for example, it takes approximately 250 ms for a transmission to reach the satellite, and another 250 ms for it to come back down

to Earth. This results in a total delay of 500 ms. Although the ITU-T recommendation notes that this is outside the acceptable range of voice quality, many conversations occur every day over satellite links. As such, voice quality is often defined as what users will accept and use.

In an unmanaged, congested network, queuing delay can add up to two seconds of delay (or result in the packet being dropped). This lengthy period of delay is unacceptable in almost any voice network. Queuing delay is only one component of end-to-end delay. Another way end-to-end delay is affected is through jitter [1].

2.6 Jitter:

Jitter is a variable-length delay that can cause a conversation to break and become unintelligible. Jitter is a variation in the delay of received packets. At the sending side, packets are sent in a continuous stream with the packets evenly spaced apart. As a result of network congestion, improper queuing, or configuration errors, this steady stream can become fragmented, causing the delay between each packet to vary instead of remaining constant. In VoIP networks which existing data traffic might be bursty, jitter can occur [1].

2.7 Echo:

Echo is annoying effect that we experience over a phone call when you hear your own voice back after some milliseconds (one millisecond is one thousandth of a second). The amount of time after which we hear the echo varies depending on the factors that are causing the echo. An echo of a few milliseconds is bearable; we only feel as if you are speaking in an empty room. An echo of a few hundred milliseconds can be extremely annoying and can affect the call completely .For echo to be noticeable, it has to be loud and delayed. Delay already exists in PSTN, but it is more noticeable in VoIP because the latter has more delay. PSTN phone calls function with a delay of no more than 10 milliseconds, while VoIP can have up to 400 milliseconds of delay. We can bear with a little echo is you are benefiting from a free service, but will be very much annoyed if the service is one you are paying for [13].

CHAPTER 3

SIGNALLING PROTOCOL

In VoIP communication, the signaling that controls the conversation is distinct from the actual stream of data carrying the voice content of the conversation. VoIP signaling protocols are described briefly below.

3.1 H.323

H.323 is an umbrella Recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences. The first version of H.323 was published by the ITU in November 1996[2] with an emphasis of enabling videoconferencing capabilities over a Local Area Network (LAN), but was quickly adopted by the industry as a means of transmitting voice communication over a variety of IP networks, including WANs and the Internet [14] .

Over the years, H.323 has been revised and re-published with enhancements necessary to better-enable both voice and video functionality over Packet-switched networks, with each version being backward-compatible with the previous version [15], Recognizing that H.323 was being used for communication, not only on LANs, but over WANs and within large carrier networks, the title of H.323 was changed when published in 1998.[4] The title, which has since remained unchanged, is "Packet-Based Multimedia Communications Systems." The current version of H.323, commonly referred to as "H.323v6", was published in 2006 [16].

3.1.1 Protocols

- H.323 is a system specification that describes the use of several ITU-T and IETF protocols. The protocols that comprise the core of almost any H.323 system are:

H.225.0 Registration, Admission and Status (RAS), which is used between an H.323 endpoint and a Gatekeeper to provide address resolution and admission control services.

- H.225.0 Call Signaling, which is used between any two H.323 entities in order to establish communication.
- H.245 control protocol for multimedia communication, which describes the messages and procedures used for capability exchange, opening and closing logical channels for audio, video and data, control and indications.
- Real-time Transport Protocol (RTP), which is used for sending or receiving multimedia information (voice, video, or text) between any two entities.

Many H.323 systems also implement other protocols that are defined in various ITU-T Recommendations to provide supplementary services support or deliver other functionality to the user. Some of those Recommendations are [17].

- H.235 series describes security within H.323, including security for both signaling and media.
- H.239 describes dual stream use in videoconferencing, usually one for live video, the other for still images.
- H.450 series describes various supplementary services.
- H.460 series defines optional extensions that might be implemented by an endpoint or a Gatekeeper, including ITU-T

In addition to those ITU-T Recommendations, H.323 utilizes various IETF Request for Comments (RFCs) for media transport and media packetization, including the Real-time Transport Protocol (RTP) [16].

3.1.2 Codecs:

H.323 utilizes both ITU-defined codecs and codecs defined outside the ITU. Codecs that are widely implemented by H.323 equipment include:

- Audio

codecs: G.711, G.729 (including G.729a), G.723.1, G.726, G.722, G.728, Speex

- Text codecs: T.140
- Video codecs: H.261, H.263, H.264

All H.323 terminals providing video communications shall be capable of encoding and decoding video according to H.261 QCIF. All H.323 terminals shall have an audio codec and shall be capable of encoding and decoding speech according to ITU-T Rec. G.711. All terminals shall be capable of transmitting and receiving A-lawand μ-law. Support for other audio and video codecs is optional [18].

3.1.3 H.323 Architecture

The H.323 system defines several network elements that work together in order to deliver rich multimedia communication capabilities. Those elements are Terminals, Multipoint (MCUs), Gateways, Gatekeepers, and Border Elements. Collectively, terminals, multipoint control units and gateways are often referred to as endpoints. While not all elements are required, at least two terminals are required in order to enable communication between two people. In most H.323 deployments, a gatekeeper is employed in order to, among other things, facilitate address resolution.

3.1.4 H.323 Elements

Figure 3.1 illustrates the elements of an H.323 system. These elements include terminals, gateways, gatekeepers, and multipoint control units (MCU).

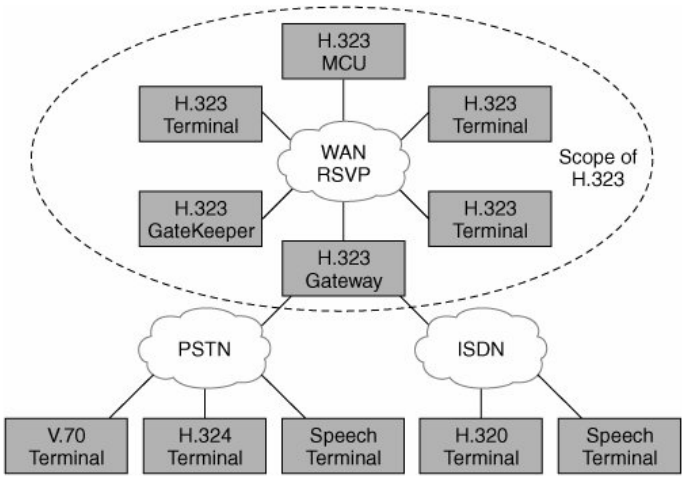

Figure 3-1 Elements of H.323 Networking

Often referred to as endpoints, terminals provide point-to-point and multipoint conferencing for audio and, optionally, video and data. Gateways interconnect to Public Switched Telephone Network (PSTN) or ISDN networks for H.323 endpoint interworking. Gatekeepers provide admission control and address translation services for terminals or gateways. MCUs are devices that allow two or more terminals or gateways to conference with either audio and/or video sessions.

3.1.5 Terminal

The network element illustrated in Figure 3-2 is defined in H.323 as a terminal. H.323 terminals must have a system control unit, media transmission, audio codec, and packet-based network interface. Optional requirements include a video codec and user data applications.

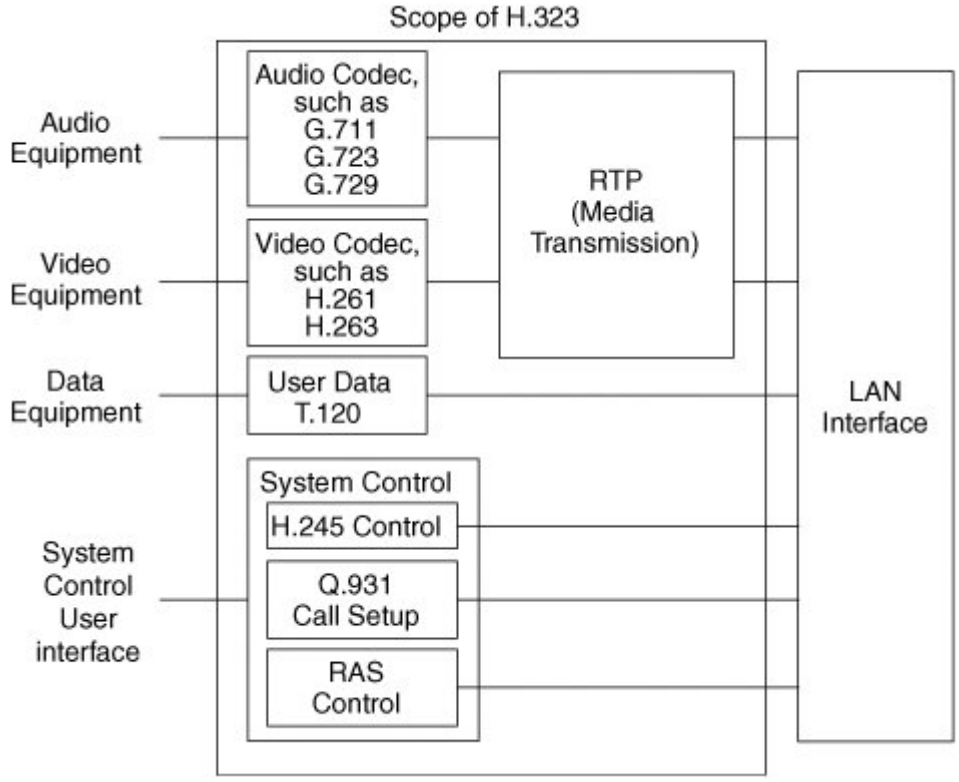

Figure 3-2. Relationships of H.323 Components

The following functions and capabilities are within the scope of the H.323 terminal:

System Control Unit Provides H.225 and H.245 call control, capability exchange, messaging, and signaling of commands for proper operation of the terminal.

Media Transmission Formats the transmitted audio, video, data, control streams, and messages onto network interface. Media transmission also receives the audio, video, data, control streams, and messages from the network interface.

Audio Codec Encodes the signal from the audio equipment for transmission and decodes the incoming audio code. Required functions include encoding and decoding G.711 speech and transmitting and receiving a-law and μ-law formats. Optionally, G.722, G.723.1, G.728, and G.729 encoding and decoding can be supported. Network Interface A packet-based interface capable of end-to-end Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) unicast and multicast services. Video Codec Optional, but if provided, must be capable of encoding and decoding video according to H.261/H.263 standards. Data Channel Supports applications such as database access, file transfer, and audio graphics conferencing (the capability to modify a common image over multiple users' computers simultaneously), as specified in Recommendation T.120.

3.1.6 H.323 Gateway:

An H.323Gateway is an optional type of end point that provides interoperability between H.323 end points and endpoints located on a switched-circuit network (SCN), such as the PSTN or an enterprise voice network, as a depicted in figure. Ideally, the gateway is transparent to both the H.323 endpoint and the SCN-based endpoint [2].

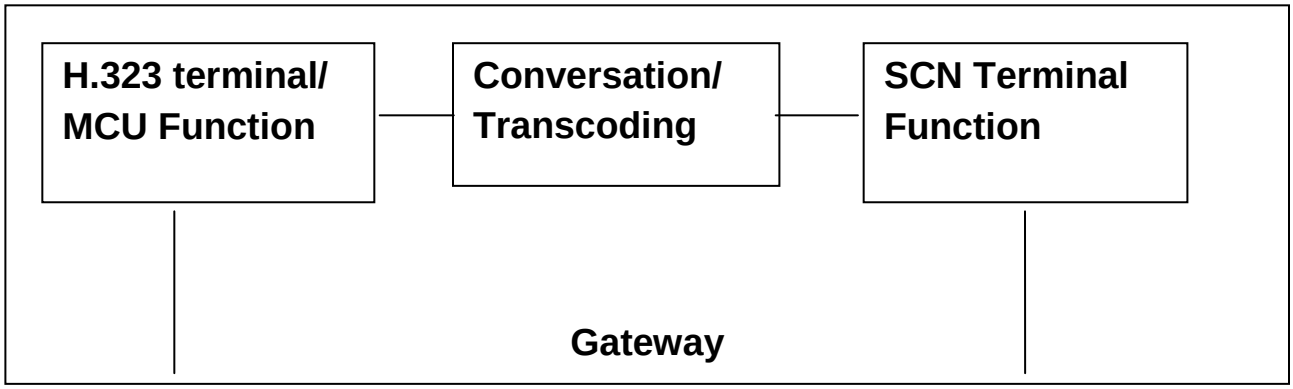

Figure 3.3: Element of an H.323 Gateway

An H3.323 gateway performs the following services:

1. Translation between audio, video, and data formats
2. conversation between call setup signals and procedures
3. Conversation between communication control signals and procedures

3.1.7 Gatekeepers

A Gatekeeper is an optional component in the H.323 network that provides a number of services to terminals, gateways, and MCU devices. Those services include endpoint registration, address resolution, admission control, user authentication, and so forth. Of the various functions performed by the gatekeeper, address resolution is the most important as it enables two endpoints to contact each other without either endpoint having to know the IP address of the other endpoint. Gatekeepers may be designed to operate in one of two signaling modes, namely "direct routed" and "gatekeeper routed" mode. Direct routed mode is the most efficient and most widely deployed mode. In this mode, endpoints utilize the RAS protocol in order to learn the IP address of the remote endpoint and a call is established directly with the remote device. In the gatekeeper routed mode, call signaling always passes through the gatekeeper. While the latter requires the gatekeeper to have more processing power, it also gives the gatekeeper complete control over the call and the ability to provide supplementary services on behalf of the endpoints. H.323 endpoints use the RAS protocol to communicate with a

gatekeeper. Likewise, gatekeepers use RAS to communicate with other gatekeepers. A collection of endpoints that are registered to a single Gatekeeper in H.323 is referred to as a “zone”. This collection of devices does not necessarily have to have an associated physical topology. Rather, a zone may be entirely logical and is arbitrarily defined by the network administrator. Gatekeepers have the ability to neighbor together so that call resolution can happen between zones. Neighboring facilitates the use of dial plans such as the Global Dialing Scheme. Dial plans facilitate “inter-zone” dialing so that two endpoints in separate zones can still communicate with each other. An H.323 Gatekeeper serves the purpose of Call Admission Control and translation services from E.164 IDs (commonly a phone number) to IP addresses in an H.323 telephony network. Gatekeepers can be combined with a gateway function to proxy H.323 calls and are sometimes referred to as Session Border Controllers. A gatekeeper can also deny access or limit the number of simultaneous connections to prevent network congestion. H.323 endpoints are not required to register with a gatekeeper to be able to place point to point calls, but they are essential for any serious H.323 network to control call prefix routing and link capacities among other functions [19].

A typical H323 Gatekeeper call flow for a successful call may look like:

3.1.8 Border Elements and Peer Elements

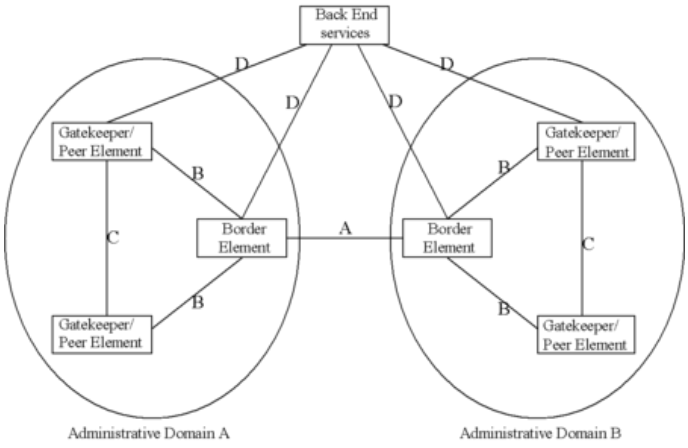

Fig 3.4: Border elements and peer elements

Figure 3.4 - An illustration of an administrative domain with border elements, peer elements, and gatekeepers. Border Elements and Peer Elements are optional entities similar to a Gatekeeper, but that do not manage endpoints directly and provide some

services that are not described in the RAS protocol. The role of a border or peer element is understood via the definition of an "domain”. An administrative domain is the collection of all zones that are under the control of a single person or organization, such as a service provider. Within a service provider network there may be hundreds or thousands of gateway devices, telephones, video terminals, or other H.323 network elements. The service provider might arrange devices into "zones" that enable the service provider to best manage all of the devices under its control, such as logical arrangement by city. Taken together, all of the zones within the service provider network would appear to another service provider as an "administrative domain”. The border element is a signaling entity that generally sits at the edge of the administrative domain and communicates with another administrative domain. This communication might include such things as access authorization information; call pricing information; or other important data necessary to enable communication between the two administrative domains. Peer elements are entities with the administrative domain that, more or less, help to propagate information learned from the border elements throughout the administrative domain. Such architecture is intended to enable large-scale deployments within carrier networks and to enable services such as clearinghouses.

3.1.9 H.323 Network Signaling

H.323 is defined as a binary protocol, which allows for efficient message processing in network elements. The syntax of the protocol is defined in ASN.1 and uses the Packed Encoding Rules (PER) form of message encoding for efficient message encoding on the wire. Below is an overview of the various communication flows in H.323 systems.

3.1.10 H.225.0 Call Signaling

Once the address of the remote endpoint is resolved, the endpoint will use H.225.0 Call Signaling in order to establish communication with the remote entity. H.225.0 messages are:

- Setup and Setup acknowledge
- Call Proceeding
- Connect

- Alerting
- Information
- Release Complete
- Facility
- Progress
- Status and Status Inquiry
- Notify

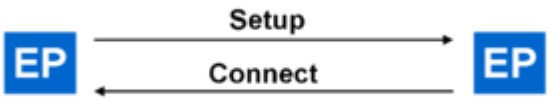

Figure 3.5 - A high-level communication exchange between two endpoints (EP)

In the simplest form, an H.323 call may be established as follows :

In this example, the endpoint (EP) on the left initiated communication with the gateway on the right and the gateway connected the call with the called party. In reality, call flows are often more complex than the one shown, but most calls that utilize the Fast Connect procedures defined within H.323 can be established with as few as 2 or 3 messages. Endpoints must notify their gatekeeper (if gatekeepers are used) that they are in a call. Once a call has concluded, a device will send a Release Complete message. Endpoints are then required to notify their gatekeeper (if gatekeepers are used) that the call has ended.

3.1.11 RAS Signaling

Endpoints use the RAS protocol in order to communicate with a gatekeeper. Likewise, gatekeepers use RAS to communicate with peer gatekeepers. RAS is a fairly simple protocol composed of just a few messages. Namely:

- Gatekeeper request, reject, and confirm messages (GRx)
- Registration request, reject, and confirm messages (RRx)
- Unregister request, reject, and confirm messages (URx)
- Admission request, reject, and confirm messages (ARx)
- Bandwidth request, reject, and confirm message (BRx)

- Disengage request, reject, and confirm (DRx)
- Location request, reject, and confirm messages (LRx)
- Info request, ack, nack, and response (IRx)
- Nonstandard message
- Unknown message response
- Request in progress (RIP)
- Resource availability indication and confirm (RAx)
- Service control indication and response (SCx)
- Admission confirm sequence (ACS)

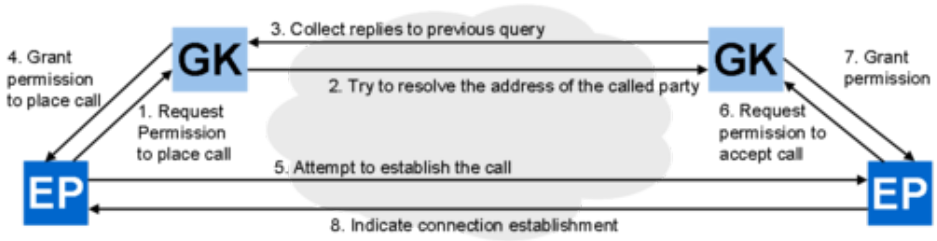

Figure 3.6 - A high-level communication exchange between two endpoints (EP) and two gatekeepers (GK)

When an endpoint is powered on, it will generally send either a gatekeeper request (GRQ) message to "discover" gatekeepers that are willing to provide service or will send a registration request (RRQ) to a gatekeeper that is predefined in the system's administrative setup. Gatekeepers will then respond with a gatekeeper confirm (GCF). If a GRQ has been sent the endpoint will then select a gatekeeper with which to register by sending a registration request (RRQ), to which the gatekeeper responds with a registration confirm (RCF). At this point, the endpoint is known to the network and can make and place calls.

When an endpoint wishes to place a call, it will send an admission request (ARQ) to the gatekeeper. The gatekeeper will then resolve the address (either locally, by consulting another gatekeeper, or by querying some other network service) and return the address of

the remote endpoint in the admission confirm message (ACF). The endpoint can then place the call. Upon receiving a call, a remote endpoint will also send an ARQ and receive an ACF in order to get permission to accept the incoming call. This is necessary, for example, to authenticate the calling device or to ensure that there is available bandwidth for the call [16].

Figure 3.6 depicts a high-level communication exchange between two endpoints (EP) and two gatekeepers (GK).

3.1.12 H.245 Call Control

Once a call has initiated (but not necessarily fully connected) endpoints may initiate H.245 call control signaling in order to provide more extensive control over the conference. H.245 is a rather voluminous specification with many procedures that fully enable multipoint communication, though in practice most implementations only implement the minimum necessary in order to enable point-to-point voice and video communication.H.245 provides capabilities such as capability negotiation, master/slave determination, opening and closing of "logical channels" (i.e., audio and video flows), flow control, and conference control. It has support for both unicast and multicast communication, allowing the size of a conference to theoretically grow without bound [19].

3.1.13 Capability Negotiation

Of the functionality provided by H.245, capability negotiation is arguably the most important, as it enables devices to communicate without having prior knowledge of the capabilities of the remote entity. H.245 enables rich multimedia capabilities, including audio, video, text, and data communication. For transmission of audio, video, or text, H.323 devices utilize both ITU-defined codecs and codecs defined outside the ITU. Codecs that are widely implemented by H.323 equipment include:

- Video codecs: H.261, H.263, H.264
- Audio codecs: G.711, G.729, G.729a, G.723.1, G.726
- Text codecs: T.140

H.245 also enables real-time data conferencing capability through protocols like T.120. T.120-based applications generally operate in parallel with the H.323 system, but are integrated to provide the user with a seamless multimedia experience. T.120 provides such capabilities as application sharing T.128, electronic whiteboardT.126, file transfer T.127, and text chat T.134 within the context of the conference.

When an H.323 device initiates communication with a remote H.323 device and when H.245 communication is established between the two entities, the Terminal Capability Set (TCS) message is the first message transmitted to the other side [19].

3.1.14 Master/Slave Determination

After sending a TCS message, H.323 entities (through H.245 exchanges) will attempt to determine which device is the "master" and which is the "slave." This process, referred to as Master/Slave Determination (MSD), is important, as the master in a call settles all "disputes" between the two devices. For example, if both endpoints attempt to open incompatible media flows, it is the master who takes the action to reject the incompatible flow.

3.1.15 H.323 and Voice over IP services

Voice over Internet Protocol (VoIP) describes the transmission of voice using the Internet or other packet switched networks. ITU-T Recommendation H.323 is one of the standards used in VoIP. VoIP requires a connection to the Internet or another packet switched network, a subscription to a VoIP service provider and a client (an analogue (ATA), VoIP Phone or "soft phone"). The service provider offers the connection to other VoIP services or to the PSTN. Most service providers charge a monthly fee, then additional costs when calls are made. Using VoIP between two enterprise locations would not necessarily require a VoIP service provider, for example. H.323 has been widely deployed by companies who wish to interconnect remote locations over IP using a number of various wired and wireless technologies [20].

3.1.16 H.323 and Videoconference services

A videoconference of videoteleconference (VTC) is a set of telecommunication technologies allowing two or more locations to interact via two-way video and audio

transmissions simultaneously. There are basically two types of videoconferencing; dedicated VTC systems have all required components packaged into a single piece of equipment while desktop VTC systems are add-ons to normal PC's, transforming them into VTC devices. Simultaneous videoconferencing among three or more remote points is possible by means of a Multipoint Control Unit (MCU). There are MCU bridges for IP and ISDN-based videoconferencing. Due to the price point and proliferation of the Internet, and broadband in particular, there has been a strong spurt of growth and use of H.323-based IP videoconferencing. H.323 is accessible to anyone with a high speed Internet connection, such as DSL. Videoconferencing is utilized in various situations, for International Conferences.

H.323 has been used in the industry to enable large-scale international video conferences that are significantly larger than the typical video conference. One of the most widely attended is an annual event called Megaconference [20].

3.2 Session Initiation Protocol

The Session Initiation Protocol (SIP) is a signaling protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. The modification can involve changing addresses or ports, inviting more participants, adding or deleting media streams, etc. Other feasible application examples include video conferencing, streaming multimedia distribution, instant messaging, presence information and online games.SIP was originally designed by Henning Schulzrinne and Mark Handley starting in 1996. The latest version of the specification is RFC 3261from the IETF Network Working Group. In November 2000, SIP was accepted as a 3GPP signaling protocol and permanent element of the IP Multimedia Subsystem (IMS) architecture for IP-based streaming multimedia services in systems. The SIP protocol is a TCP/IP-based Application Layer protocol. SIP is designed to be independent of the underlying transport layer; it can run on Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or Stream Control Transmission Protocol (SCTP). It is a text-based protocol, incorporating many elements of

the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP), allowing for direct inspection by administrators [21].

3.2.1 Protocol design

SIP employs design elements similar to the HTTP request/response transaction model.[5] Each transaction consists of a client request that invokes a particular method or function on the server and at least one response. SIP reuses most of the header fields, encoding rules and status codes of HTTP, providing a readable text-based format.

SIP works in concert with several other protocols and is only involved in the signaling portion of a communication session. SIP clients typically use TCP or UDP on port numbers 5060 and/or 5061 to connect to SIP servers and other SIP endpoints. Port 5060 is commonly used for non-encrypted signaling traffic whereas port 5061 is typically used for traffic encrypted with Transport Layer Security (TLS). SIP is primarily used in setting up and tearing down voice or video calls. It has also found applications in messaging applications, such as instant messaging, and event subscription and notification. There are a large number of SIP-related Internet Engineering Task Force (IETF) documents (Request for Comments) that define behavior for such applications. The voice and video stream communications in SIP applications are carried over another application protocol, the Real-time Transport Protocol (RTP). Parameters (port numbers, protocols, codecs) for these media streams are defined and negotiated using the Session Description Protocol (SDP) which is transported in the SIP packet body.

A motivating goal for SIP was to provide a signaling and call setup protocol for IP-based communications that can support a superset of the call processing functions and features present in the public switched telephone network (PSTN). SIP by itself does not define these features; rather, its focus is call-setup and signaling. However, it was designed to enable the construction of functionalities of network elements designated proxy servers and user agents. These are features that permit familiar telephone-like operations: dialing a number, causing a phone to ring, hearing ringback tones or a busy signal. Implementation and terminology are different in the SIP world but to the end-user, the behavior is similar. SIP-enabled telephony networks can also implement many of the more advanced call processing features present in Signaling System 7 (SS7), though the two protocols themselves are very different. SS7 is a centralized protocol, characterized

by a complex central network architecture and dumb endpoints (traditional telephone handsets). SIP is a peer-to-peer protocol, thus it requires only a simple (and thus scalable) core network with intelligence distributed to the network edge, embedded in endpoints (terminating devices built in either hardware or software). SIP features are implemented in the communicating endpoints (i.e. at the edge of the network) contrary to traditional SS7 features, which are implemented in the network. Although several other VoIP signaling protocols exist, SIP is distinguished by its proponents for having roots in the IP community rather than the telecommunications industry. SIP has been standardized and governed primarily by the IETF, while other protocols, such as H.323, have traditionally been associated with the International Telecommunication Union (ITU).The first proposed standard version (SIP 2.0) was defined by RFC 2543. This version of the protocol was further refined and clarified in RFC 3261, although some implementations are still relying on the older definitions [21].

3.2.2 SIP network elements

A SIP user agent (UA) is a logical network end-point used to create or receive SIP messages and thereby manage a SIP session. A SIP UA can perform the role of a User Agent Client (UAC), which sends SIP requests, and the User Agent Server (UAS), which receives the requests and returns a SIP response. These roles of UAC and UAS only last for the duration of a SIP transaction.

A SIP phone is a hardware-based or software-based SIP user agent that provides call functions such as dial, answer, reject, hold/unhold, and call transfer. Examples include soft phones such as Ekiga, K Phone, Twinkle, Windows Live Messenger, X-Lite, and hardware phones from vendors such as Avaya, Cisco, Leadtek,Polycom, Snom, and Nokia. Each resource of a SIP network, such as a User Agent or a voicemail box, is identified by a Uniform Resource Identifier (URI), based on the general standard syntax also used in Web services and e-mail. A typical SIP URI is of the form: sip:username:password@host:port. The URI scheme used for SIP is *sip.* If secure transmission is required, the scheme *sips:* is used and SIP messages must be transported over Transport Layer Security (TLS). In SIP, as in HTTP, the User Agent may identify itself using a message header field 'User-Agent', containing a text description of the software/hardware/product involved. The User-Agent field is sent in request messages,

which means that the receiving SIP server can see this information. SIP network elements sometimes store this information, and it can be useful in diagnosing SIP compatibility problems. SIP also defines server network elements. Although two SIP endpoints can communicate without any intervening SIP infrastructure, which is why the protocol is described as peer-to-peer, this approach is often impractical for a public service.RFC 3261 defines these server elements:

A proxy server “is an intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity "closer" to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it."

"A registrar is a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles."

"A redirect *server* is a user agent server that generates 3xx responses to requests it receives, directing the client to contact an alternate set of URIs. The redirect server allows SIP Proxy Servers to direct SIP session invitations to external domains."

The RFC specifies: "It is an important concept that the distinction between types of SIP servers is logical, not physical."

Other SIP related network elements are:

Session border controllers (SBC), they serve as "man in the middle" between UA and SIP server, see the article SBC for a detailed description [18].

3.2.3 SIP Messages

SIP is a text-based protocol with syntax similar to that of HTTP. There are two different types of SIP messages: requests and responses. The first line of a request has a *method*, defining the nature of the request, and a Request-URI, indicating where the request should be sent.[10] The first line of a response has a *response code*.

For SIP requests, RFC 3261 defines the following methods:

1. REGISTER: Used by a UA to notify its current IP address and the URLs for which it would like to receive calls.

2. INVITE: Used to establish a media session between user agents.

3. ACK: Confirms reliable message exchanges.

4. CANCEL: Terminates a pending request.

5 BYE: Terminates a session between two users in a conference.

6. OPTIONS: Requests information about the capabilities of a caller, without setting up a call.

The SIP response types defined in RFC 3261 fall in one of the following categories:

1. Provisional (1xx): Request received and being processed.

2. Success (2xx): The action was successfully received, understood, and accepted.

3. Redirection (3xx): Further action needs to be taken (typically by sender) to complete the request.

4. Client Error (4xx): The request contains bad syntax or cannot be fulfilled at the server.

5. Server Error (5xx): The server failed to fulfill an apparently valid request.

6. Global Failure (6xx): The request cannot be fulfilled at any server.

3.2.4 Instant messaging (IM) and presence:

The Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) is the SIP-based suite of standards for instant messaging and presence information. During an instant message session, files can be transferred using, for example, MSRP (Message Session Relay Protocol).

Some efforts have been made to integrate SIP-based VoIP with the XMPP specification. Most notably Google Talk, which extends XMPP to support voice, plans to integrate SIP. Google's XMPP extension is called Jingle and, like SIP, it acts as a Session Description Protocol carrier[18].

3.2.5 Conformance testing

TTCN-3 test specification language is used for the purposes of specifying conformance tests for SIP implementations. SIP test suite is developed by a Specialist Task Force at ETSI (STF 196).

3.2.6 Applications

Many VoIP phone companies allow customers to bring their own SIP devices, as SIP-capable telephone sets, or softphones. The market for consumer SIP devices continues to expand; there are many devices such as SIP Terminal Adapters, SIP Gateways etc.

The free software community started to provide more and more of the SIP technology required to build both end points as well as proxy and registrar servers leading to a commodification of the technology, which accelerates global adoption. As an example, the open source community at SIP foundry actively develops a variety of SIP stacks, client applications and SDKs, in addition to entire IP PBX solutions that compete in the market against mostly proprietary IP PBX implementations from established vendors.

The National Institute of Standards and Technology (NIST), Advanced Networking Technologies Division provides a public domain implementation of the JAVA Standard for SIP JAIN-SIP which serves as a reference implementation for the standard. The stack can work in proxy server or user agent scenarios and has been used in numerous commercial and research projects. It supports RFC 3261 in full and a number of extension RFCs including RFC 3265 (Subscribe / Notify) and RFC 3262 (Provisional Reliable Responses) etc [19].

3.2.7 SIP-ISUP interworking

SIP-I, or the Session Initiation Protocol with encapsulated ISUP, is a protocol used to create, modify, and terminate communication sessions based on ISUP using SIP and IP networks. Services using SIP-I include voice, video telephony, fax and data. SIP-I and SIP-T are two protocols with similar features, notably to allow ISUP messages to be transported over SIP networks. This preserves all of the detail available in the ISUP header, which is important as there are many country-specific variants of ISUP that have been implemented over the last 30 years, and it is not always possible to express all of the same detail using a native SIP message. SIP-I was defined by the ITU-T, where SIP-T was defined via the IETF RFC route.

CHAPTER 4

COMPARISON OF H.323 AND SIP

This Chapter includes the comparisons two protocols in terms of Functionality, Quality of Service (QoS), Scalability, Flexibility, Interoperability, and Ease of Implementation.

4.1. INTRODUCTION

Telephony service is provided for the most part over circuit-switched networks, which are referred to as Public Switched Telephone Networks (PSTN). This service is known as Plain Old Telephone Service (POTS). A new trend that is beginning to emerge is to provide telephony service over IP networks, known as IP telephony, or Voice over IP. An important driving force behind IP Telephony is cost savings, especially for corporations with large data networks. The high cost of long-distance and international voice calls – thanks to layers of local and international carriers – is the crux of the issue. A significant portion of this cost originates from regulatory taxes imposed on long-distance voice calls. Such surcharges are not applicable to long-distance circuits carrying data traffic; thus, for a given bandwidth, making a data call is much less expensive than making a voice call. In addition to the cost savings for long-distance voice calls, carrying voice traffic on the data network within a business building or campus also can achieve substantial cost savings, since the operation of PBX setups is relatively cost-inefficient. There are other very significant motivating factors for carrying voice traffic over data networks as well. A very important benefit of IP Telephony is the integration of voice and data applications, which can result in more effective business processes. Examples of such applications are integrated voice mail and e-mail, teleconferencing, computer supported collaborative work and automated and intelligent call distribution. Another benefit is the enabling of many new services both for businesses and for customers. The flexibility offered by IP Telephony by moving the intelligence from the network to the end stations, as well as the open nature of IP networks, are the factors that enable new services.

Furthermore, many of the existing services such as caller-id, call-forwarding, and multi-line presence become trivial to implement; therefore, such services are likely to be offered for free for competitive reasons. In order for IP Telephony to gain mainstream acceptance and ultimately replace traditional Plain Old Telephone Service (POTS), two conditions have to be met. First, the quality of the voice communication must be at least

at the same level as POTS. The two primary aspects of voice quality are the end-to-end delay, and the voice clarity (which depends on many factors, including the voice digitization and compression scheme used, and the amount of lost or late-arrived packets). Therefore, the IP network must be designed such that it can meet the delay and packet loss requirements of the telephony application. The second condition for the acceptance of IP Telephony is the ease of operation and functionality offered to the end user at least at the same level as in PSTN. This requires the IP Telephony architecture to provide a signaling infrastructure that offers at least the same capabilities and features as the Signaling System 7 (SS7) architecture in PSTN [35]. More specifically, the signaling infrastructure must:

· provide the functionality required to set up, manage, and tear down calls and connections;

· be scalable to support a very large number of registered endpoints (in the order of billions worldwide), and a very large number of simultaneous calls (in the order of millions worldwide);

· support *network management* features for policy control, accounting, billing, etc;

· provide a mechanism to communicate and set up the Quality of Service requested by the end points;

· be extensible to help with adding new features easily;

· support interoperability among different vendors' implementations, among different versions of the signaling protocol, and with different signaling protocols.

Two standards compete for IP Telephony signaling. The older and currently more widely accepted standard is the ITUT recommendation H.323 [36], which defines a multimedia communications system over packet-switched networks, including IP networks. The other standard, Session Initiation Protocol (SIP), comes from the IETF MMUSIC working group [37].

4.2. OVERVIEW OF H.323 AND SIP

4.2.1. H.323 Overview

Name	The description of protocols
H.323	Specification of the system
H.225.0	Call control (RAS), call setup (Q.931-like protocol), and packetization and synchronization of media stream
H.235	Security protocol for authentication, integrity, privacy, etc.

H.245	Capability exchange communication and mode switching
H.450	Supplementary services including call holding, transfer, forwarding, etc
H.246	Interoperability with circuit-switched services
H.332	For large size conferencing
H.26x	Video codecs including H.261 and H.263
G.7xx	Audio codecs including G.711, G.723, G.729, G.728, etc

Table -3: ITU-T recommendations that are part of the H.323 specification.

H.323 is an umbrella specification, and various aspects of H.323 are specified in different ITU-T recommendations. Table 4.1 shows the recommendations that are part of the H.323 specification [38].

4.2.2 H.323 Endpoint Types

H.323 defines four major components for a network-based communication system: Terminals, Gateways, Gatekeepers and Multipoint Control Units (MCUs). (See Figure 4.1.)

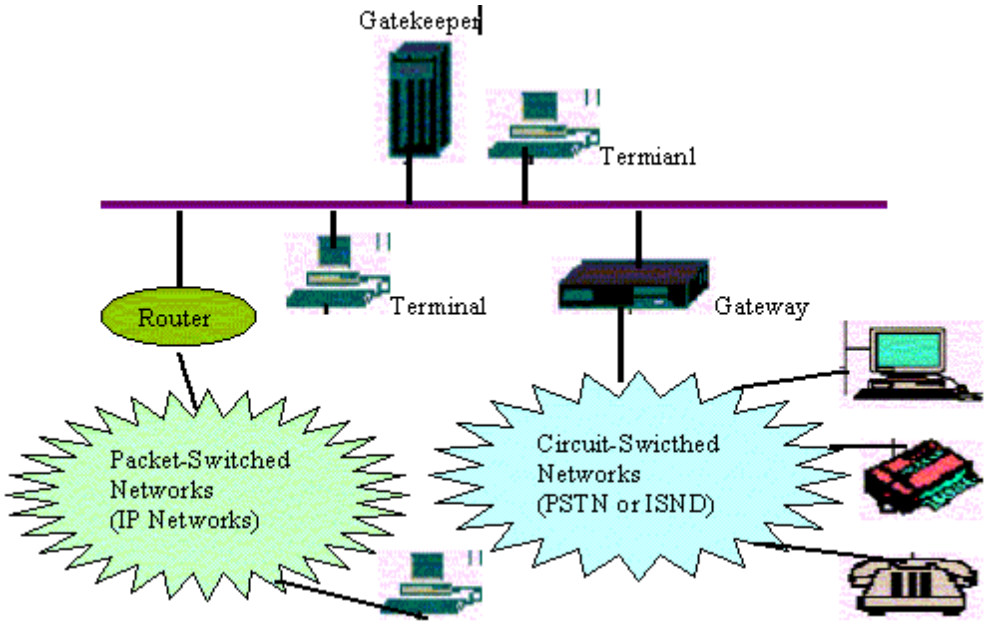

Figure 4.1: H.323 endpoint types.

Terminals are client endpoints on IP-based networks that provide real-time, two-way communications with other H.323 entities. H.323 terminals are required to support the following three functional parts:

Signaling and Control: H.323 must support H.245, a complex standard for channel usage and capabilities, in addition to a Q.931-like protocol defined in H.225 for call signaling and establishment, as well as Registration/Administration/Status (RAS) protocol defined in H.225 for communication with gatekeepers. All of these protocols use ASN.1 encoding for their messages.

Real-time communication: H.323 terminals must support RTP/RTCP, a protocol for sequencing audio and video packets.

Codecs: Codecs are pieces of software that compress audio/video before transmission and decompress them back after receiving compressed packets. For interoperability purposes, every H.323 terminal is required to support the G.711 audio codec. Other audio and video codecs are optional.

Gateways provide the connection path between the packet-switched network and the Switched Circuit Network (SCN, which can be either public or private). The gateway is not required when there is no connection to other networks. In general, a gateway deflects the characteristics of a LAN endpoint to a SCN endpoint, and vice-versa. Gateways perform call setup and control on both the packet-switched network and on the SCN, and they translate between transmission formats and between communication procedures. Some gateways can also translate between different codec standards Terminal for audio and/or video (referred to as transcoding), with the purpose of reducing the bandwidth of the audio/video flow if the SCN bandwidth is limited.

Gatekeepers are optional on an H.323 system, but they have certain mandatory functions if they are present. Gatekeepers perform four required functions: Address Translation (from alias addresses or phone numbers to transport addresses*), Admission Control, Bandwidth Control and Zone Management. Gatekeepers can also support four optional functions: Call Control Signaling, Call Authorization, Bandwidth Management and Call Management. When a gatekeeper is present on an H.323 system, all other types of endpoints are required to register with the gatekeeper and receive its permission prior to making a call.

Multipoint Control Units (MCU) support conferencing between three or more endpoints. The MCU typically consists of a Multipoint Controller (MC) and zero or more Multipoint Processors (MP). MC provides the control functions such as negotiation between terminals and determination of common capabilities for processing audio and video. MP performs the necessary processing on the media streams for a conference. Such processing typically involves audio mixing and audio/video switching.

4.2.3. Channels Defined in H.323

H.323 uses the concept of channels to structure the information exchange between communication entities. A channel is a transport-layer connection, which can be either unidirectional or bi-directional. In particular, H.323 defines the following types of channels:

RAS Channel: This channel provides a mechanism for communication between an endpoint and its gatekeeper. The RAS (Registration, Admission, and Status) protocol is specified in H.225.0. Through the RAS channel, an endpoint registers with the gatekeeper, and requests permission to place a call to another endpoint. If permission is granted, the gatekeeper returns the transport address for the call signaling channel of the called endpoint.

Call Signaling Channel: This channel carries information for call control and supplementary service control. The Q.931-like protocol used over this channel is specified in H.225.0 and H.450.x. When the call is established, the transport address for H.245 Control Channel is indicated on this channel.

H.245 Control Channel: This channel carries the H.245 protocol messages for media control with capability exchange support. After the call participants exchange their capabilities, logical channels for media are opened through the H.245 control channel.

Logical Channel for Media: These channels carry the audio, video, and other media information. Each media type is carried in a separate pair of uni-directional channels, one for each direction, using RTP and RTCP.H.323 specifies that the RAS channel and the logical channels for media are carried over an unreliable transport protocol, such as UDP. The H.245 control channel is specified to be carried over a reliable transport protocol, such as TCP. H.323 versions 1 and 2 specify that the call signaling channel is carried

over a reliable transport protocol. In version 3, this channel can optionally be carried over an unreliable transport protocol.

4.3. SIP Overview

IETF has also specified a multimedia communications protocol suite. In the IETF architecture, the media flows are carried using RTP, just like in H.323. Therefore, the main difference between H.323 and IETF specifications is how the call signaling and control is achieved.

The primary protocol that handles call signaling and control in the IETF specification is SIP. SIP is an application layer control protocol that can establish, modify and terminate multimedia sessions or calls. There are two major architectural elements to SIP: the user agent (UA), and the network server. The UA resides at the SIP end stations, and contains two components: a user agent client (UAC) which is responsible for issuing SIP requests, and a user agent server (UAS), which responds to such requests. There are three different network server types, a redirect server, a proxy server, and a registrar. A basic SIP call does not need servers, but some of the more powerful features depend upon them. To the first degree of approximation, the SIP User Agent is equivalent to a H.323 terminal (or the packet-network side of a gateway), and the SIP network servers are equivalent to a H.323 gatekeeper.

The most generic SIP operation involves a SIP UAC issuing a request, a SIP proxy server acting as end-user location discovery agent and a SIP UAS accepting the call. A successful SIP invitation consists of two requests: INVITE followed by ACK. The INVITE message contains session description that informs the called party what type of media the caller can accept and where it wishes the media data to be sent. SIP addresses are referred to as SIP Uniform Resource Locators (SIP-URLs), which are of the form sip:user@host.domain. SIP message format is based on the Hyper Text Transport Protocol (HTTP) message format, which uses a human-readable, text-based encoding. Redirect servers process an INVITE message by sending back the SIP-URL where the callee is reachable. Proxy servers perform application layer routing of the SIP requests and responses. A proxy server can either be stateful or stateless. A stateful proxy holds information about the call during the entire time the call is up, while a stateless proxy processes a message and then forgets everything about the call until the next message

arrives. Furthermore, proxies can either be forking or non-forking. A forking proxy can, for example, ring several phones at once until somebody takes the call. Registrar servers are used to record the SIP address (called a SIP URL) and the associated IP address. The most common use of a registrar server is to register after start-up, so that when an INVITE request arrives for the SIP URL used in the REGISTER message, the proxy or redirect server forwards the request correctly. Note that usually a SIP network server implements a combination of different types of servers.

SIP is used to establish, modify, and terminate multimedia sessions. However, it only handles the communication between the caller and the callee, the endpoint addressing, and user location. There needs to be a description about a multimedia session within a SIP request and response message, as well as an announcement for a session. IETF Session Description Protocol (SDP) is used together with SIP to accomplish all the call signaling functions in IP telephony. Roughly speaking, SIP is the equivalent of RAS and the Q.931-like protocol in H.323. SDP is the equivalent of H.245[39].

4.4. COMPARISON OF H.323 AND SIP FOR IP TELEPHONY SIGNALING

We compare H.323 and SIP in terms of Functionality, Quality of Service (QoS), Scalability, Flexibility, Interoperability, Security, and Ease of Implementation. For fairness of comparison, we consider similar scenarios for both protocols. In particular, we focus on scenarios that involve a gatekeeper for H.323, and a Proxy/Registrar server for SIP. The reason is that medium-to-large IP Telephony systems are not manageable without a gatekeeper or a proxy server.

4.4.1 Functionality

In addition to the basic telephone call service, both SIP and H.323 support some call control services, advanced features, and capability exchange. Roughly, the services they provide are similar but with different approaches. We will discuss the detailed signaling procedure for some services, then summarize their characteristics.

4.4.2Basic Call Setup and Tear Down

H.323 v2 call setup is based on reliable transport protocol. Therefore, the call setup needs a two-phase connection: TCP connection and call connection. H.323 v3 supports both TCP and UDP, which simplifies the call setup procedure. (See Figures 4.2, and 4.3 for call setup in H.323 v2 and v3, respectively.) SIP call setup procedure is similar to H.323 v3. (See Figure 4.4 for Call setup in SIP.)

The tear down procedure is a reverse of the call setup. Either caller or callee can terminate a call by RELEASE COMPLETE (in H.323) or BYE (in SIP) message.

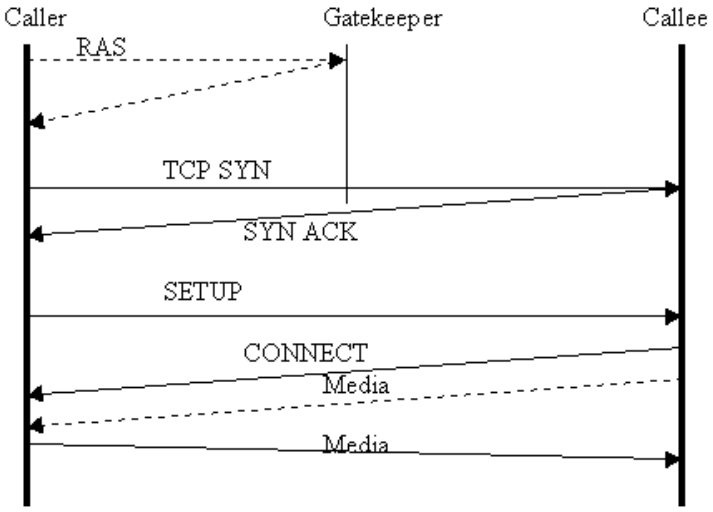

Figure 4.2: Call Setup in H.323 v2

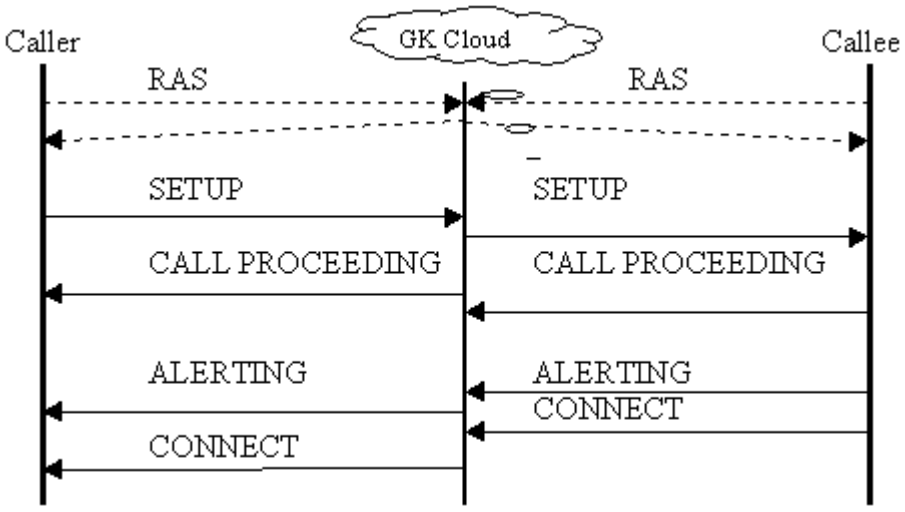

Figure 4.3: Call Setup, H.323 v3 using UDP (both Endpoints registered, Gatekeeper routed call setup)

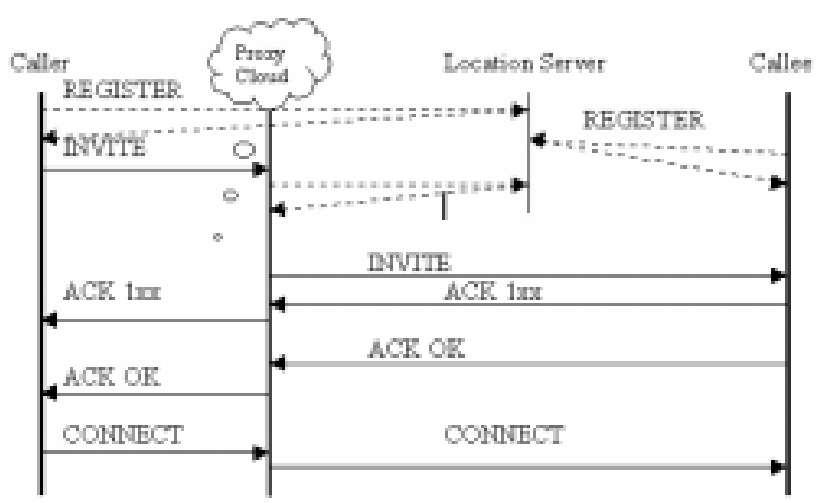

Figure 4.4: Call Setup with SIP (both endpoints registered, proxy routed call setup)

4.4.3. Call control services

SIP and H.323 both support call hold, call transfer, call forwarding, call waiting, conferencing, and some other supplementary services. In the following, some example supplementary services, namely, call hold, call transfer, call forwarding, and call waiting.

Call Hold

Call Hold is defined as one call party disconnecting the voice communication without terminating the call, with the ability to reestablish the voice communication at a later time. When the call is on hold, optionally some music can be played, so that the party on hold knows that the call is still active.

H.323 defines two scenarios in call hold service: Near-end Call Holding and Remote-end Call Holding. Both can work with or without a gatekeeper. Gatekeepers only pass SS-HOLD (Supplementary Service-HOLD) operation transparently. (Thus, we illustrate the signaling message flow without gatekeepers for simplicity.)

Near-end Call Hold: Hold is invoked at the holding endpoint as a local procedure. (See Figure 4.5)

Remote-end Call Hold: The holding endpoint sends a hold request to the remote endpoint requiring the held endpoint to provide Music on Hold (MOH) to the held user. (See Figure 4.6)

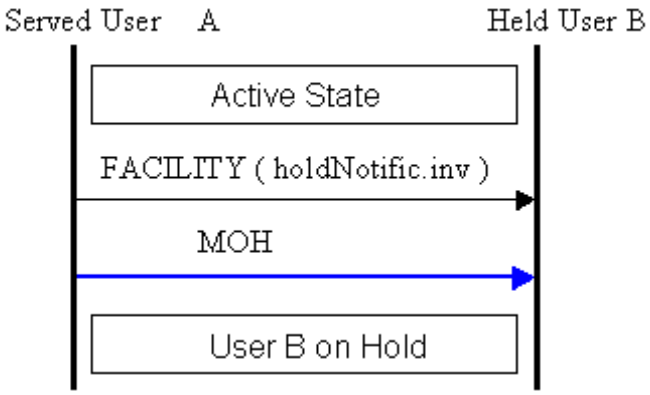

Figure 4.5: Signaling flow for Near-end call hold without a gatekeeper in H.323

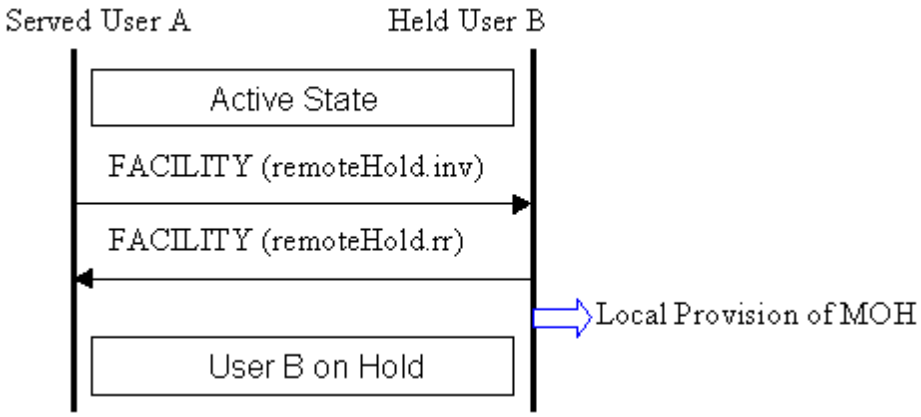

Figure 4.6: Signaling Flow for Remote-End Call Hold without a gatekeeper in H.323

SIP uses a simpler approach to achieve the same call hold functionality as H.323. For a Near-end Call Hold, no protocol assistance is needed. The client just continually receives media stream from a server but does not generate any response. (See Figure 4.7.) To achieve Remote-end Call Hold, the holding side needs to send an INVITE message to other side, indicating a NULL set of receiving capability for any kind of media (See Figure 4.8.) MOH can be implemented by asking an RTSP server to play to the IP address or phone number provided in the RTSP SETUP request.

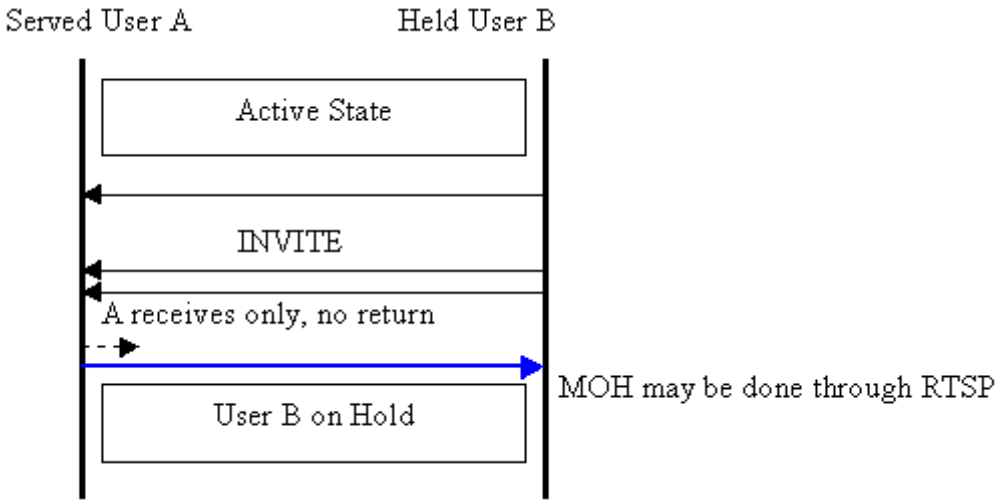

Figure 7: Near-end Call Hold in SIP

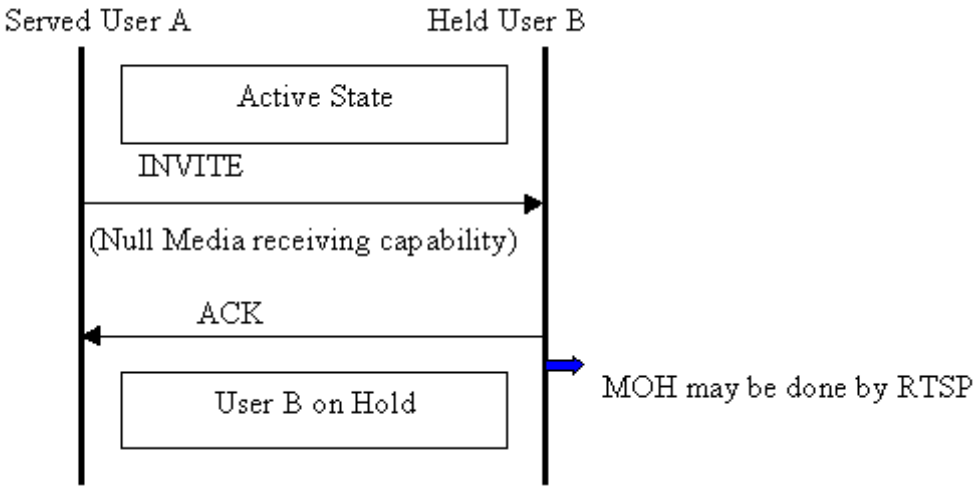

Figure 4.8: Remote-end Call Hold in SIP

Call Transfer

Call Transfer enables a user to transfer an established call to a third party. Both H.323 and SIP support three types of Call Transfer: Blind Transfer, Alternative Transfer, and Operator-Assisted Transfer. The signaling flow diagrams of Blind Transfer and Operator-Assisted Transfer for both H.323 v3 and SIP are provided in Figures 4.9, 4.10, and 4.11.

Blind Transfer works as follows:

Originator A connects with B

A asks B to connect with C

A simply disconnects with B without any acknowledgement of connection between B and C

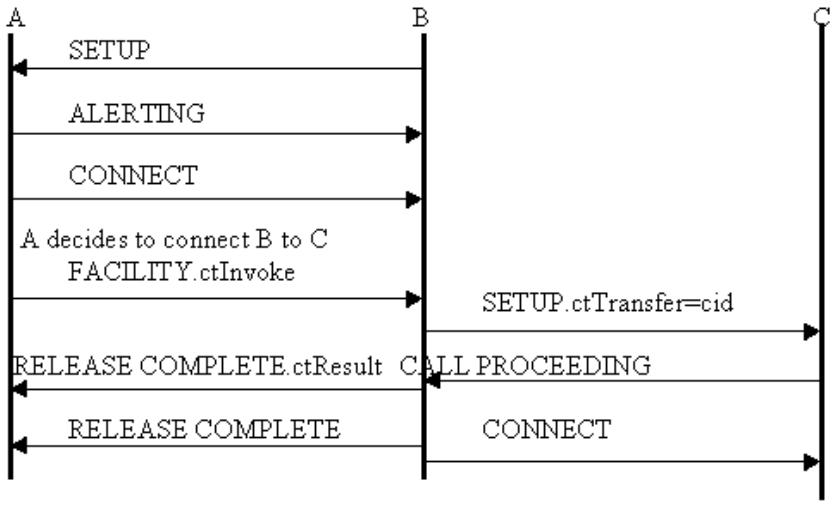

Figure 4.9: Signaling Flow for Blind Call Transfer in H.323

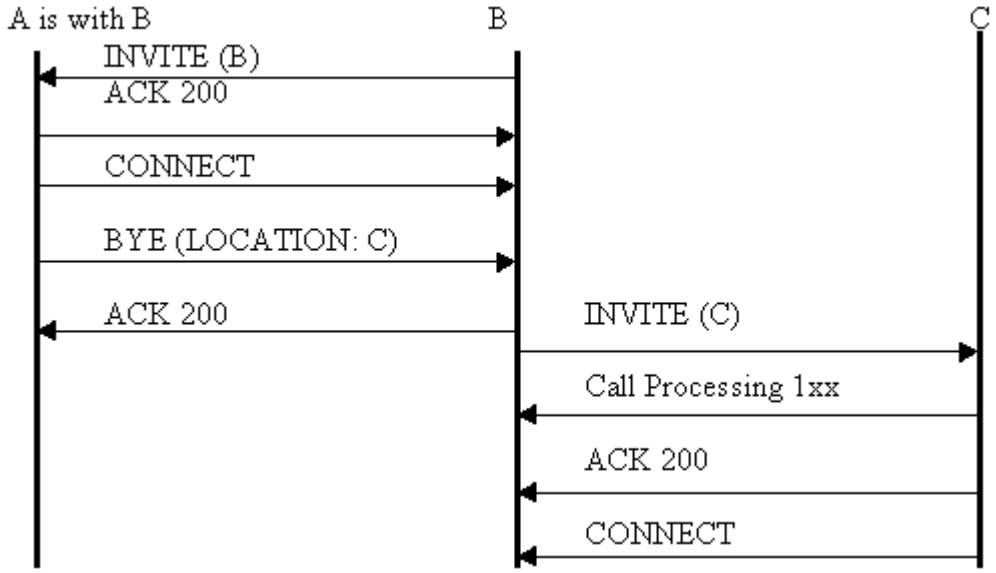

Figure 4.10: Signaling Flow for Blind Call Transfer in SIP

Operator-Assisted Transfer works as follows:

Originator B sets up a connection with the operator A

A puts B on HOLD, then sets up another connection with C

B and C set up the connection between them

A releases the connection with B

A releases the connection with C

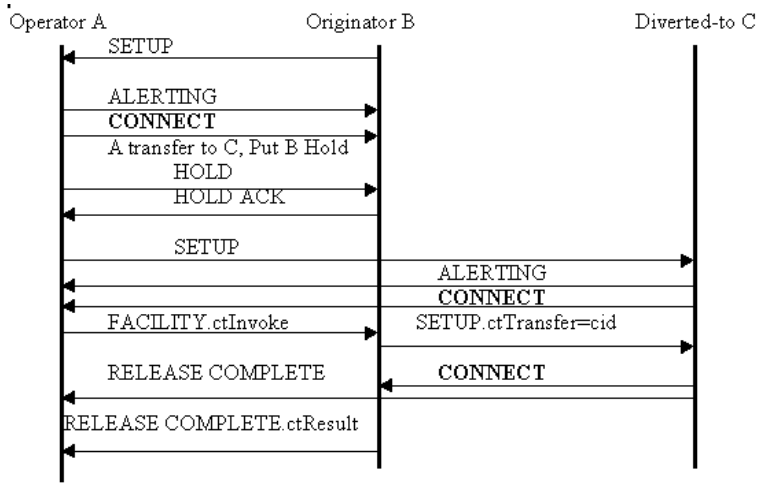

Figure 4.11: Operator-Assisted Call Transfer in H.323

The procedure of Operator-Assisted Call Transfer in SIP is very similar to that in H.323, except that the equivalent SIP messages are sent out.

Call Forwarding

Call Forwarding permits the called party to forward particular pre-selected calls to other addresses. H.323 defines the following operation models for call forwarding: Call Forwarding immediate/delayed with rerouting, Call Forwarding partial rerouting in gatekeeper, CFU/CFB invoked by the gatekeeper, and CFNR invoked by the gatekeeper.

Call Forwarding services provided by SIP are usually instantiated with the LOCATION header fields, which contain the forwarding destination. SIP supports Call Forwarding Busy, Call Forwarding no Response, and Selective Call Forwarding.

A more general model, Call forwarding partial rerouting in gatekeeper/proxy is chosen as an example. (See Figures 4.12 and 4.13) The messages used for call forwarding are different in H.323 and in SIP. However, the call flows are very similar.

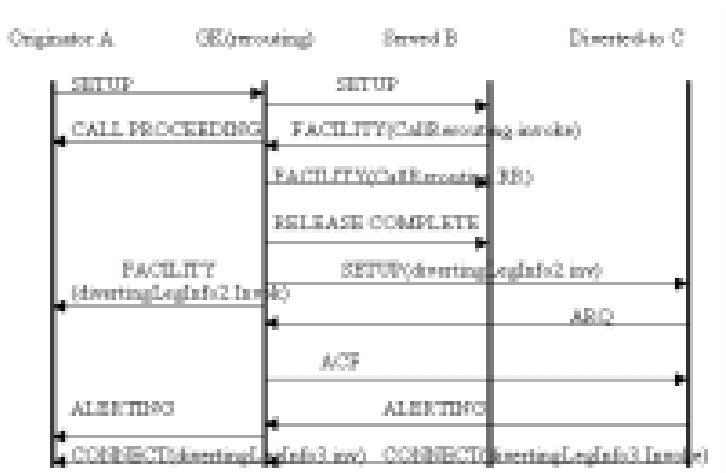

Figure 4.12: Signaling Flow for Call Forwarding partial rerouting in GK (H.323)

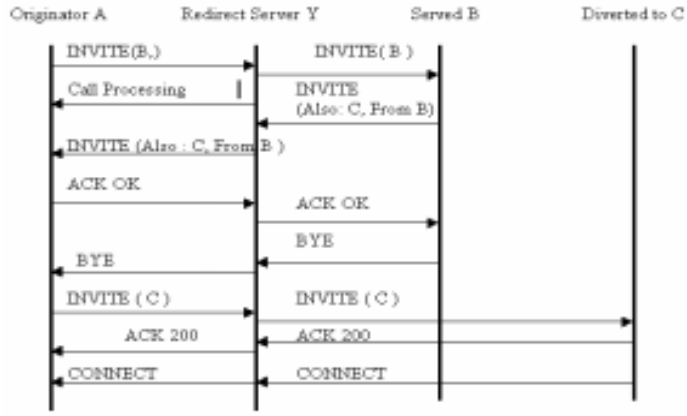

Figure 4.13: Signaling Flow for Call Forwarding with redirect server (SIP)

Call Waiting

Call Waiting allows the called party to receive a notification that a new party is trying to reach it while it is busy talking to another party.

In Figure 4.14 we illustrate the call waiting signaling flow for H.323. Gatekeepers only pass on SS-CW (Supplementary Service-Call Waiting) operations transparently. We consider that party C calls the party B while B is in another call with A.

Actions at the served endpoint B: B returns an ALERTING message to C. B also optionally starts a timer, and locally provides a call indication to the user. If the served user B likes to accept the waiting call, B stops the timer, and sends a CONNECT message to the calling point.

Action at the calling endpoint C: On receipt of an ALERTING message, the calling endpoint may indicate call waiting to the calling user. Then the calling user may wait until the waiting call gets accepted, release the call, or choose other supplementary services.

SIP can provide call waiting service using the Call-Disposition header field, which allows the UAC to indicate how the server is to handle the call. The following is an example of Call Waiting Service provided by SIP.

The called party B is temporarily unreachable (e.g. it is in another call).

The caller indicates that it wants to have its call queued rather than rejected immediately via a "Call-Disposition: Queue" header field.

If the call is queued, the server returns "181 Queued"

When the callee becomes available, it will return the appropriate status response.

A pending call can be terminated by a SIP BYE request.

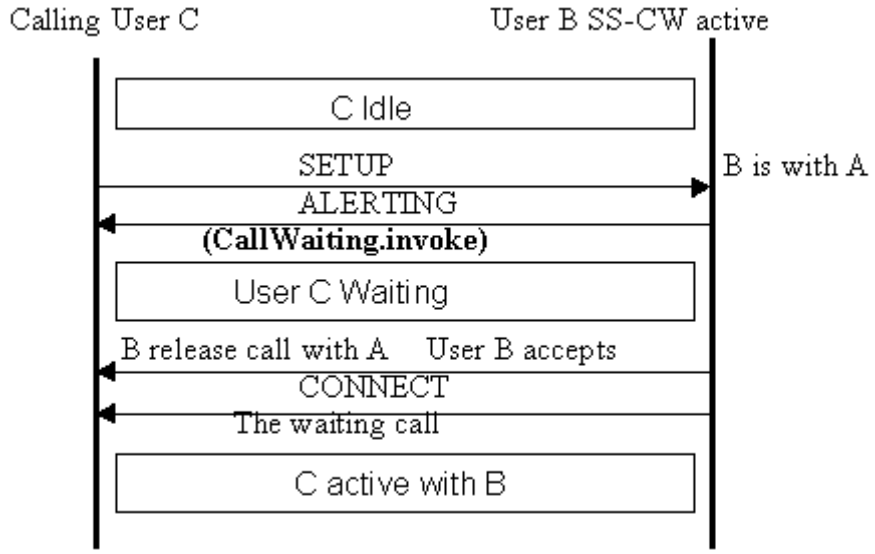

Figure 14: Signaling Flow for Call Waiting (H.323)

Other Supplementary Services

Other supplementary call control services supported by both H.323 and SIP are Call Park and Call Pickup, Call Completion on Busy Subscriber (SS-CCBS) or Camp-on, and Call Identification (Call Screening). H.323 and SIP signaling flow diagrams for those services are very similar. Table 4 lists all the supplementary services supported in H.323 along

with the H.450 specification where the service is defined. The third column of the table indicates whether or not SIP supports the same service.

Service Name	H.323	SIP
Call Transfer Supplementary Service for H.323	H.450.2	Yes
Call Diversion Supplementary Service for H.323	H.450.3	Yes
Call Hold Supplementary Service for H.323	H.450.4	Yes
Call Park and Call Pickup Supplementary Services for H.323	H.450.5	Yes
Call Waiting Supplementary Service for H.323	H.450.6	Yes
Massage Waiting Indication Supplementary service for H.323	H.450.7	No
Conference out of Consultation Supplementary Service for H.323	H.450.8	No
Call Completion on Busy Subscriber for H.323	H.450.9	Yes

Table 4: Supplementary services in H.323 and SIP.

4.4.4. Third-Party Control in SIP

Third-Party control is defined as the ability for a party to set up a call between two other parties without necessarily participating in the call. This feature is currently available only in SIP, although work is in progress to add the same functionality to H.323. The flexible and powerful SIP headers, which are very similar to those used in the Hyper-Text Transfer Protocol (HTTP) make the implementation simple. Third-party control is useful for many scenarios, including:

• A secretary dials for a manager

• Auto-dialer hands call to a telemarketer

• Attended call transfer

• Operator service

4.4.5. Capability Exchange

The capability exchange procedures are intended to ensure that multimedia signals that are transmitted can be received and processed appropriately by the receiving terminal.

H.323 uses the H.245 protocol for exchanging capabilities. The complete set of what a terminal can receive and decode is made known to the other terminal by transmission of its capability set. The terminal's total capabilities are described by a set of Capability Descriptor structures, each of which is a single Simultaneous Capabilities structure and a capability Descriptor Number[40]. With this structure, very precise information about each terminal's capabilities can be expressed in a relatively compact structure.

SIP uses SDP for capability exchange. The caller can use an OPTION request to find out the capability of the callee. Currently, SIP does not have the full negotiation flexibility of H.245, due to the limited expressiveness of SDP. For example, SIP does not support asymmetric capabilities (receive or transmit only) and simultaneous capabilities of audio & video encoding.

4.5. Quality of Service (QoS)

Quality of Service is a term that encompasses many different aspects. The relevant QoS parameters for multimedia flows are the bandwidth, maximum delay, delay jitter, and packet loss rate. It is important for the call signaling and control protocols to provide support for communicating the required QoS parameters with the goal of meeting the required QoS levels. In addition to the above QoS parameters, call setup delay is another parameter that affects the perceived QoS, and it is highly dependent on the particular signaling protocol used. Call setup delay is also dependent on the transport protocol that is used to carry the signaling messages, in particular when some signaling messages are lost, and need to be retransmitted.

Therefore, here we first consider the QoS support by the signaling protocols for the multimedia flows. Then, we examine the call setup delay. Since the call setup delay is affected by error detection and error correction mechanisms, we then describe such mechanisms in H.323 and SIP.

4.5.1 QoS Support for Multimedia Flows

Gatekeepers in H.323 provide a rich set of control and management functions, including address translation, admission control, bandwidth control, and zone management. Some optional functions inside gatekeeper are call control signaling, call authorization, bandwidth management and call management. By contrast, SIP does not supply the management or control functions by itself but relies on other protocols.

Admission Control determines whether the network has sufficient resources to support the QoS required for a call, and accepts or rejects the call accordingly. In order to do admission control, the protocol must handle bandwidth management, call management, and bandwidth control. These are supported by H.323 but not by SIP.

In their current stages, neither H.323 nor SIP supports resource reservation by itself. Both of them recommend using external means for resource reservation, such as the Resource

Reservation Protocol (RSVP) by the IETF IntServ working group [41]. RSVP addresses the needs of applications that require QoS, promising per-flow service. The reliance of IntServ on Per-flow State and per-flow processing is an impediment to its deployment in the Internet at large networks [42].

Recently, a new Differentiated Services architecture has drawn more attention. Unlike the IntServ model, in which applications explicitly request QoS reservations, Differentiated Services provides a simpler model: Network providers define a set of service levels that is general, simple and application independent. The applications and the users match their needs to specific service levels based on their performance and policy constrains [43].

H.323 v3 can offer some Differentiated Services based on QoS parameter negotiation (Bit rate, delay, and jitter)[44].Upon initiation of a call, a terminal may request one of three service classes defined: "Guaranteed Service," "Controlled Service," and "Unspecified Service." Neither SIP nor the older versions of H.323 support a similar functionality.

4.5.2. Call Setup Delay

We define call setup delay as the number of round trips needed for establishing audio communication between the call participants. Call setup delay is very large in H.323 v1; it has been reduced significantly with the fast call setup procedure in H.323 v2. SIP and H.323 v3 both have a significantly more efficient call setup, resulting in relatively small delays.

H.323 uses H.225/Q931 signaling procedures to establish a connection between caller and callee. Depending on whether a gatekeeper is being used or not, a H.323 v1 call can take about 6 to 7 round-trip times, including setting up the Q.931 and H.245 TCP connections.

The fast call setup method is an option specified in H.323 v2 that reduces the number of delays up to three roundtrips involved in establishing a call and initial media streams by including H.245 logical channel information in the SETUP and CONNECT messages. With the fast call setup method, only G.711-based voice communication can be established between the two call parties, since the capabilities are not exchanged. If the parties wish to establish other types of media channels, they can optionally perform the H.245 capability exchange procedures after the G.711 channel is established.

In H.323 v3, either UDP or TCP can be used to carry call setup messages. Using UDP has the advantage that there is no roundtrip delay associated with establishing a transport-layer connection. When UDP is used, the call setup delay can be 1.5 or 2.5 round trips, depending on whether or not a gatekeeper is involved.

SIP call setup is very similar to the one in H.323 v3. However, if the UDP call setup fails, H.323 v3 has some advantages over SIP. H.323 v3 sets up a UDP connection and a TCP connection almost simultaneously, and provides an efficient mechanism to close the TCP connection if the UDP set up is successful. If the UDP setup fails, TCP can take over immediately. SIP operates UDP and TCP sequentially. This increases the call setup delay if the UDP connection is not available.

4.5.3. Error detection and correction Packet Loss

H.323 v1 and v2 are based on the reliable transport protocol. They achieve the reliability based on transport protocol. The use of TCP would simplify the state machine for the call control protocol, since it has its own flow control, window control, and retransmission mechanisms to ensure the reliability.

H.323 v3 specifies its own retransmission policies for both sender and receiver for support TCP and UDP[45]. The sender starts two timers, T1 and T4, after it sends call setup PDU. If T1 expires before the caller received a response from the callee or GK, the sender retransmits the SETUP packet and starts a timer T3. If T3 expires, another retransmission is performed, and T3 is restarted. After a total of N1 transmission, the caller stops retransmission and reverts to the use of TCP call signaling instead of UDP.

With the first transmission of response, the receiver starts a timer T1. If T1 expires, the callee retransmits the packet and restarts a timer T3. If T3 expires, the callee sends another transmission of response and restarts T3. After the response message has been sent for a total N1 times, the callee stops re-transmitting and starts a timer T5. After T5 expires, the callee discards the conference/call identification information and associated state, and regards the setup of this session as failed.

The reliability of SIP is messages is achieved by having the client retransmit requests every 0.5 seconds until either a progress report (1xx) or final status (>200) response has been received. The server simply retransmits the original final response until an ACK is received. The client retransmits an ACK for every final message.

Loop Detection

Another common type of error is call forwarding loops, which may occur especially when multiple gatekeepers or SIP network servers are involved in setting up a call. There is no provision to prevent loops in H.323 v1 and v2. H.323 v3 defines a PathValue field to indicate the maximum number of gatekeepers that signaling message should traverse before being discarded. Using the PathValue field can reduce the rate of loop occurrence, but not as efficiently as the loop detection algorithm used in SIP. When a loop occurs without knowing the names of gatekeepers, the signaling messages will not be stopped until reaching the PathValue. Thus how to define a proper value for PathValue becomes a critical

issue. Furthermore, when the network configuration changes, the PathValue may possibly need to be changed.

SIP provides loop detection algorithms similar to the one used in BGP (Border Gateway Protocol) to prevent searching loop [37]. It works through the *via* header field. Before a proxy server redirects any request, it checks the via field. If its own name is already in there, then a loop must have occurred. If its name is not on the list of via field, then the proxy server posts its name on the list, then transmits the request to another proxy server or endpoint.

Fault Tolerance

Errors happen in networks for a variety of reasons. The signaling protocol should have the capability to bypass network faults and provide a normal service whenever possible. A client should not notice the error during the services. This capability is called Fault Tolerance.

H.323 v3 provides better fault tolerance than SIP by redundant gatekeepers and endpoints. During registration, a gatekeeper may indicate alternate gatekeepers to the registering endpoint, which may be used in the event of a primary gatekeeper failure. Likewise, an endpoint may indicate a backup, redundant or alternate Transport Address. This allows an endpoint to have a secondary network interface or a secondary H.323 endpoint as a backup.

4.6. Scalability

In a fully operational system, it should be possible for every Internet host to act as an IP telephony client (albeit not all of them participating in a call simultaneously). It is estimated that the worldwide number of Internet users will reach 500 million by the year 2000, with the number increasing exponentially. Therefore, scalability of the current signaling protocols is extremely important. Many different aspects affect a system's scalability. We compare the scalability of H.323 and SIP in terms of their Complexity, Endpoint Location, Server Processing, Inter-Server Communication, Global Addressing, and Multipoint Communication.

4.6.1. Complexity

H.323 is a rather complex protocol. It includes H.225 for call signaling, H.245 for call control, H.332 for large conferences, H.450.x (x=1,2,…9) for supplementary services, H.235 for security and encryption, and H.246 for interoperability with circuit-switched services. Many services require interactions between those sub-protocols, which increases the complexity but decreases the scalability.

On the other hand, SIP and SDP are less complicated. A basic SIP Internet Telephony implementation can be done using four headers (To, From, Call-ID, and Cseq) and three request types (INVITE, ACK, and BYE). This simplifies programming and maintenance, and better scalability is a consequence.

4.6.2. Server Processing

No connection states are required in UDP. Therefore, large backbone servers based on UDP can operate in a stateless manner. This significantly reduces the memory requirements and improves the scalability.

In SIP, a transaction through servers and gateways can be either stateful or stateless. The stateless model simplifies the memory management, and the stateful model provides the sufficient information to forward the response correctly. H.323 v1 and v2 server processing is stateful, in which TCP was chosen as the transport protocol. Gatekeepers must hold the call states, as well as the TCP connections for the duration of a call. H.323 v3 supports the stateless processing model just as in SIP.

4.6.3. Endpoint Location

The current mechanism for logical addressing and addressing resolution in H.323 standard is to utilize aliases (E.164 or H323ID) and a mapping mechanism supported by gatekeepers. When a client likes to make a connection, the gatekeeper may either return the endpoint's address to the client (in direct call model) or route the SETUP message to the called endpoint (in GK routed model). H.323 v3 defines a mechanism for inter-gatekeeper communication, which aids in locating an endpoint registered in a different zone or administrative domain.

SIP chooses an e-mail-like address, referred to as a SIP URL. When a client wishes to send a request, it either sends it to a locally configured SIP proxy server or a SIP redirect server, independent of the Request-URL, or sends it to the IP address and port corresponding to the Request-URL. In the former case, SIP redirect or proxy server obtains information about a callee's possible location(s) from SIP location servers. SIP does not specify a means to locate endpoints registered in other administrative domains, and suggests the use of external mechanisms such as DNS.

4.7. Flexibility

A well-defined protocol should have the capability to extend the current functionality for further development, and should allow implementers to customize sub-components depending on individual interest. In this section, H.323 and SIP will be evaluated in terms of those aspects.

4.7.1. Extensibility of Functionality

IP telephony technology is not yet mature. It is likely that new signaling capabilities and functionality need to be added. Also, different vendors may want to support additional features.

H.323 chooses vendor-defined NonStandardParam field in ASN.1 as its extension mechanism. NonStandardParam consists of vendor codes and an opaque code for that particular vendor. This approach has some limitations, as only the NonStandardParam field can be extended. SIP offers a more flexible mechanism by providing a hierarchical namespace of feature names and hierarchically organized numerical error codes. The client inputs feature information in a SIP Require header. If there are some required features that the server does not support, the server sends back a hierarchical error code to

the client. New features can either be registered with Internet Assigned Numbers Authority (IANA) or hierarchically derived from the feature owner's Internet domain name depending on whether the new feature can be derived directly.

4.7.2. Ease of customization

To customize the services, H.323 requires more interactions between its sub-protocols. For example, if the conference size changes from small to big, then a different protocol, H.332, has to be used. Also, since H.323 requires the full compatibility between each version, the customization will definitely increase the size of code. SIP uses its relatively simple header fields to handle those interactions. The text-based encoding makes the customization in SIP much easier than that in H.323.

4.8. Interoperability

An IP Telephony signaling protocol needs to cooperate with different versions, implementations, and other signaling protocols crossing worldwide networks. This capability is defined as interoperability.

4.8.1. Interoperability among Versions

The fully backward compatibility in H.323 enables all implementations based on different H.323 versions to be seamlessly integrated. This is important for customers. If a customer has bought client side products implemented by H.323 v2, he or she does not have to change anything when server side is upgraded to H.323 v3. The new server supports every function the customer had before with the older server.

In SIP, a newer version may discard some old features that are not expected to be implemented any more. This approach saves code size and reduces protocol complexity, but loses some compatibility between different versions. Some products implemented on the older version may not be supported in the new version.

4.8.2. Interoperability among Implementations

Different vendors on the market may implement the same protocol with different approaches. It is possible that endpoints in a large-scale system use different vendors' products, and simply complying with the standard does not guarantee interoperability among the different products.

H.323 provides an implementers' guide, which clarifies the standard and helps towards interoperability among different implementations. Furthermore, International Multimedia

Teleconferencing Consortium (IMTC) iNOW! Activity Group defined an interoperability profile, which combines, clarifies and complements existing standards to provide a complete IP telephony interoperability protocol12. IMTC also organizes interoperability events, where different vendors can test their implementations against each other.

SIP, being in an earlier stage of development, thus far has not provided an implementation agreement. The

Interoperability between different implementations is still uncertain, although the first interoperability tests began recently.

4.8.3. Interoperability with Other Signaling Protocols

To support traditional telephony services, the VoIP signaling protocols have to support ISDN Signaling System 7 (SS7). SS7 performs out-of-band signaling in support of the call-establishment, billing, routing, and information-exchange functions of the public switched telephone networks (PSTN). There are two signaling specifications available in SS7 for different interfaces: Q.931 used for User-to-Network Interface (UNI) and ISUP used for Network-to-Network Interface (NNI).

H.323 embraces the more traditional circuit-switched approach based on the ISDN/Q.931 protocols. Q.931-like signaling messages are used in H.323 procedures,which makes it easier to interoperate with ISDN/Q.931. However, the call setup messages of H.323 are only a subset of those in SS7/ISUP. Because there is no established standard for relaying of SS7/ISUP messages over an H.323 network, H.323 can only translate a portion of SS7 messages in the conversion.

The H.32x family of recommendations offers specific standards to interoperate with other circuit-switched networks; for example, H.320 for ISDN and B-ISDN, H.324 for GSTN. Within those standards, the interoperability by gateways is well defined.

For SIP, no translation function for SS7 signaling messages is provided. Although there is an Internet draft on the subject, "A Functional Description of SIP-PSTN Gateway," the detailed information about signaling information transportation is not yet worked out[47].

3.6. Ease of Implementation

H.323 signaling messages are binary encoded using ASN.1 PER (Packet Encoding Rules)[48]. Within a system, the information represented using an abstract syntax must be mapped into some form for presentation to human users. Similarly, this abstract syntax

must be mapped into some local format for storage. Such mappings require a special parser, which makes implementation and debugging more complicated.

SIP messages are text-based, using ISO 10646 in UTF-8 encoding[49]. Text-based encoding allows easy implementation in languages such as JAVA, Tcl and Perl, and easy debugging.

	H.323 v1	**H.323 v2**	**H.323 v3**	**SIP**
FUNCTIONALITY				
Call Holding	No	Yes	Yes	Yes
Call Transfer	No	Yes	Yes	Yes
Call Forwarding	No	Yes	Yes	Yes
ADVANCED FEATURES:				
Third Party Control	No	No	No	Yes
Conference	Yes	Yes	Yes	Yes
Click-for-Dial	Yes	Yes	Yes	Yes
Capability Exchange	Yes &Better	Yes &Better	Yes &Better	Yes
QUALITY OF SERVICE				
Call Setup Delay	6~7 RT	3~4 RT	2~3 RT	2~3 RT
RELIABILITY:				
Packet Loss Recovery	Through TCP	Through TCP	Better	Better
Fault Detection	Yes	Yes	Yes	Yes
Fault Tolerance	N/A	N/A	Better	Good
MANAGEABILITY				
Admission Control	Yes	Yes	Yes	No
Policy Control	Yes	Yes	Yes	No
Resource Reservation	No	No	No	No
SCALABILITY				
Complexity	More	More	More	Less
Server Processing	Stateful	Stateful	Stateful or Stateless	Stateful or Stateless
Inter-Server Communication	No	No	Yes	Yes
FLEXIBILITY				
Transport Protocol Neutrality	TCP	TCP	TCP/UDP	TCP/UDP
Extensibility of Functionality	Vendor Specified			Yes, IANA

Ease of Customization	Harder	Harder	Harder	Easier
INTEROPERABILITY				
Version Compatibility	N/A	Yes	Yes	Unknown
SCN Signaling Interoperability	Better	Better	Better	Worse
EASE OF IMPLEMENTATION				
Protocol Encoding	Binary	Binary	Binary	Text

Table 5: Comparison summary

We can consider SIP is much better then H.323 in terms of above categories and two main thing is that the installation procedure of session initiation protocol is very easy than H.323 and also encoding procedure is simple.

CHAPTER 5

GATEWAY CONTROL PROTOCOL

This chapter covers two Internet Engineering Task Force (IETF) gateway control protocols that control Voice over IP (VoIP) gateways from external call-control elements: Media Gateway Control Protocol (MGCP) and H.248/MEGACO.

5.1 MGCP Overview

MGCP is a protocol used by media gateway controllers (MGC, also known as call agents) to control media gateways (MG). MGCP is based on a master/slave paradigm in which MGC is the master that issues commands to the MG (slave). The MG acknowledges the command, executes it, and notifies the MGC of the outcome (successful or not). In this architecture, the MG handles the media functions, such as conversion of time-division multiplexing (TDM)/ analog signals into Real-time Transport Protocol (RTP)/Real-time Transport Control Protocol (RTCP) streams. MGC handles the call-signaling functions. In this model, the call-control intelligence resides in the MGC, and the MG is a "dumb" entity that acts on the commands of the MGC. MGCP messages are carried over User Datagram Protocol (UDP). Because UDP does not guarantee message delivery, messages are retransmitted, if needed. MGCP has its historic roots in two other earlier protocols: Simple Gateway Control Protocol (SGCP) and Internet Protocol Device Control (IPDC). This chapter covers MGCP version 1.0 as described in RFC 2705 and does not go into the details of SGCP, IPDC, or earlier versions of MGCP. MGCP uses Session Description Protocol (SDP) to describe the media sessions. SDP describes session parameters of the media flow between the MGs such as IP addresses, the UDP port, RTP profiles, and multimedia conference capabilities. MGCP follows the conventions of SDP as defined in RFC 2327, and implementations are expected to conform. The SDP specification defines several media types; MGCP, however, limits the usage of SDP to two media types: audio circuits and data access circuits [20].

Call agents use the following SDP parameters to provision telephony gateways:

1. IP addresses Use remote gateway, local gateway, or multicast audio conference addresses to exchange RTP packets

2. UDP port Indicates the transport port used to receive RTP packets from the remote gateway
3. Audio media Specify audio media, including codec.

5.1.1 MGCP Commands

MGC --> MG	Create Connection: Creates a connection between two endpoints; uses SDP to define the receive capabilities of the participating endpoints.
MGC --> MG	Modify Connection: Modifies the properties of a connection; has nearly the same parameters as the Create Connection command.
MGC <--> MG	Delete Connection: Terminates a connection and collects statistics on the execution of the connection.
MGC --> MG	Notification Request: Requests the media gateway to send notifications on the occurrence of specified events in an endpoint.
MGC <-- MG	Notify: Informs the media gateway controller when observed events occur.
MGC --> MG	Audit Endpoint: Determines the status of an endpoint.
MGC --> MG	Audit Connection: Retrieves the parameters related to a connection.
MGC <-- MG	Restart In Progress: Signals that an endpoint or group of endpoints is take in or out of service.

MGC= Media Gateway Controller

MG=Media Gateway

- Create Connection.
- Modify Connection.
- Delete Connection.
- Notification Request.
- Notify.
- Audit Endpoint.
- Audit Connection.
- Restart In Progress.

The first four commands are sent by the Call Agent to a gateway. The Notify command is sent by the gateway to the Call Agent. The gateway may also send a Delete Connection. The Call Agent may send either of the Audit commands to the gateway. The Gateway may send a Restart In Progress command to the Call Agent. All commands are composed of a command header, optionally followed by a session description. All responses are composed of a response header, optionally followed by a session description. Headers and session descriptions are encoded as a set of text lines, separated by a carriage return and line feed character (or, optionally, a single line-feed character). The headers are separated from the session description by an empty line. MGCP uses a transaction identifier to correlate commands and responses. Transaction identifiers have values between 1 and 999999999. An MGCP entity cannot reuse a transaction identifier sooner than 3 minutes after completion of the previous command in which the identifier was used.

The command header is composed of:

- A command line, identifying the requested action or verb, the transaction identifier, the endpoint towards which the action is requested, and the MGCP protocol version,
- A set of parameter lines, composed of a parameter name followed by a parameter value.

The command line is composed of:

- Name of the requested verb.
- Transaction identifier correlates commands and responses. Values may be between 1 and 999999999. An MGCP entity cannot reuse a transaction identifier sooner than 3 minutes after completion of the previous command in which the identifier was used.
- Name of the endpoint that should execute the command (in notifications, the name of the endpoint that is issuing the notification).
- Protocol version.

These four items are encoded as strings of printable ASCII characters, separated by white spaces, i.e., the ASCII space (0x20) or tabulation (0x09) characters. It is recommended to use exactly one ASCII space separator [24].

5.1.2 Call Generation

Call Generation function allows to send call control messages to the MG with proper usage of scripts and respective profiles. Call generation provides various options to create and operate on the call instances and the window displays Script Name, Profile, Call Info, Status, Events, Results and Iterations statistics along with call flow details for easy monitoring of the scripts being executed. The Call Generation interpretation of establishing call is to invoke the required scripts for call.

Call Receive Script Configuration

The Call Reception function focuses on the MGC (MAPS) receiving signaling information/requests from the MG (MAPS) during Media Gateway testing. The Call Reception operation is triggered on reception of proper messages for the corresponding messages are pre-loaded in the Script configuration window.

The script configuration option is used to preset the script required to handle all possible signaling and call processing messages for responding to the call requests in Call Receive part of the MAPS [23].

Message Sequence

Message Sequence pane gives the ladder diagram of the messages flowing between the MAPS (MGC) and the DUT (MG). Each message sequence can be highlighted to observe the corresponding script execution results as shown in the screen below [23].

MGCP Call Flow

Diagram below depicts MAPS-MGCP simulating the Call flow scenario which is placed from one PSTN interface to another PSTN interface between two Media Gateways through IP Network [25].

- Media Gateway indicates to MGC that it is in the process of restarting with Restart In Progress (RSIP) command Media Gateway informs MGC with RSIP command about rebooting of the Gateway, and it also indicates the resources available in the Gateway to place a Call.

- To request notification of events and to apply signal on the Media Gateway, MGC programs Endpoint using Request Notification (RQNT) command.

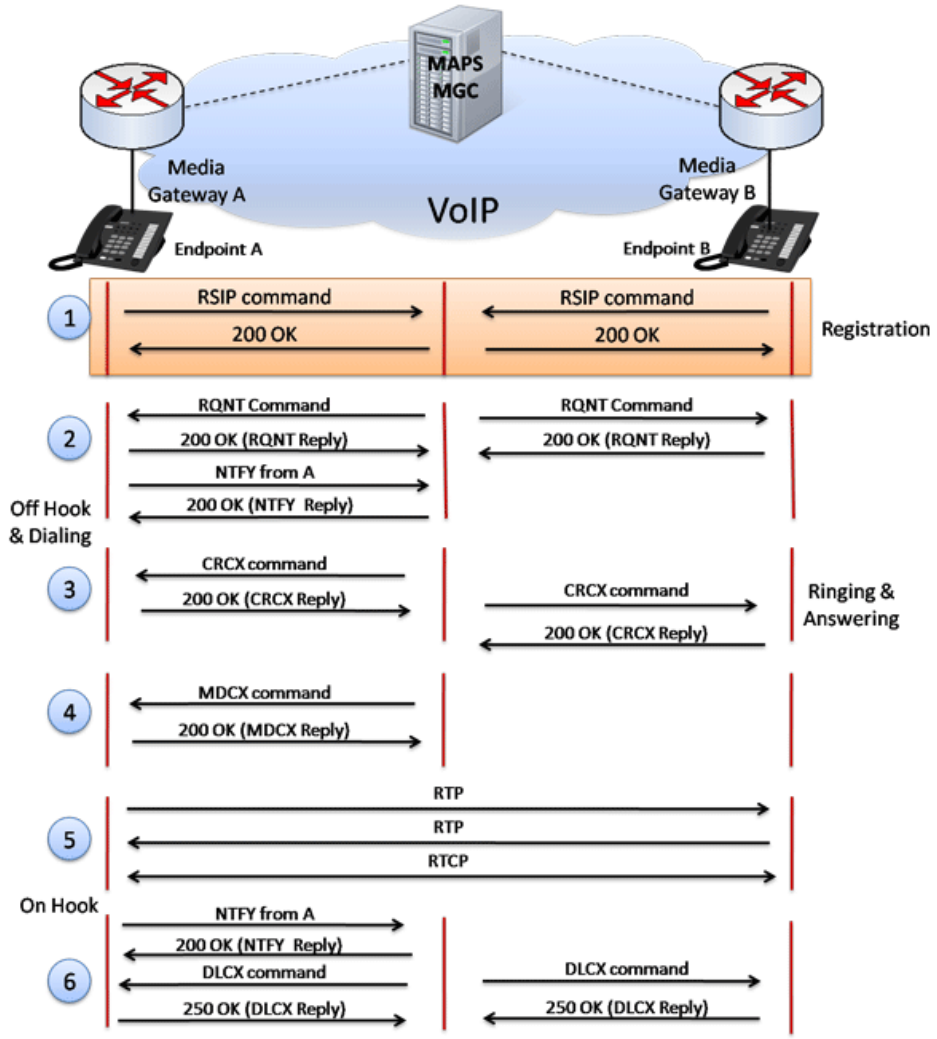

Figure 5.1: MGCP Call Flow

- Media Gateway responds NTFY command to MGC indicating that it has detected an event for the previously requested notification (via the RQNT command)

- To manage the connection on a Media Gateway, MGC uses Create Connection (CRCX) command to create the connection. Now the two-way call is established to exchange the media.

- MGC queries (the state of) a Media Gateway using Audit Endpoint (AUEP) and Audit Connection (AUCX) commands to get the statistics of the Endpoint and Connection.

- Media Gateway sends a Delete Connection (DLCX) command to delete the connection for its self-management.

- With the appropriate responses for the above set of commands, the call flow is completed.

Protocol Overview:

- MGCP packets are unlike those generated by many other protocols. Usually wrapped in UDP port 2427, the MGCP datagrams are formatted with whitespace, much like you would expect to find in TCP protocols. An MGCP packet is either a command or a response.
- Commands begin with a four-letter verb. Responses begin with a three number response code.
- There are nine (9) command verbs:
- AUEP, AUCX, CRCX, DLCX, EPCF, MDCX, NTFY, RQNT, RSIP
- Two verbs are used by a Call Agent to query (the state of) a Media Gateway:
- AUEP - Audit Endpoint
- AUCX - Audit Connection
- Three verbs are used by a Call Agent to manage an RTP connection on a Media Gateway (a Media Gateway can also send a DLCX when it needs to delete a connection for its self-management):
- CRCX - Create Connection
- DLCX - Delete Connection
- MDCX - Modify Connection
- One verb is used by a Call Agent to request notification of events on the Media Gateway, and to request a Media Gateway to apply signals:
- RQNT - Request for Notification
- One verb is used by a Call Agent to modify coding characteristics expected by the "line-side" on the Media Gateway:
- EPCF - Endpoint Configuration

- One verb is used by a Media Gateway to indicate to the Call Agent that it has detected an event for which the Call Agent had previously requested notification of (via the RQNT command verb):
- NTFY - Notify
- One verb is used by a Media Gateway to indicate to the Call Agent that it is in the process of restarting:
- RSIP - Restart In Progress
- The distributed system is composed of a Call Agent (or Media Gateway Controller), at least one Media Gateway (MG) that performs the conversion of media signals between circuits and packets, and at least one Signaling gateway (SG) when connected to the PSTN.
- The Call Agent uses MGCP to tell the Media Gateway:
- what events should be reported to the Call Agent
- how endpoints should be connected together
- What signals should be played on endpoints.
- MGCP also allows the Call Agent to audit the current state of endpoints on a Media Gateway.
- The Media Gateway uses MGCP to report events (such as off-hook, or dialed digits) to the Call Agent.
- (While any Signaling Gateway is usually on the same physical switch as a Media Gateway, this needn't be so. The Call Agent does not use MGCP to control the Signaling Gateway; rather, SIGTRAN protocols are used to backhaul signaling between the Signaling Gateway and Call Agent).
- Every issued MGCP command has a transaction ID and receives a response.
- Typically, a Media Gateway is configured with a list of Call Agents from which it may accept programming (where that list normally comprises only one or two Call Agents). In principle, event notifications may be sent to different Call Agents for each endpoint on the gateway (as programmed by the Call Agents, by setting the Notified Entity parameter). In practice, however, it is usually desirable that at any given moment all endpoints on a gateway should be controlled by the same Call Agent; other Call Agents are available only to provide redundancy in the

event that the primary Call Agent fails, or loses contact with the Media Gateway. In the event of such a failure it is the backup Call Agent's responsibility to reprogram the MG so that the gateway comes under the control of the backup Call Agent. Care is needed in such cases; two Call Agents may know that they have lost contact with one another, but this does not guarantee that they are not both attempting to control the same gateway. The ability to audit the gateway to determine which Call Agent is currently controlling can be used to resolve such conflicts.

- MGCP assumes that the multiple Call Agents will maintain knowledge of device state among themselves (presumably with an unspecified protocol) or rebuild it if necessary (in the face of catastrophic failure). Its failover features take into account both planned and unplanned outages [26].

5.2 Megaco/H.248: Media Gateway Control Protocol

Megaco/H.248, the Media Gateway Control Protocol, is for control of elements in a physically decomposed multimedia gateway, which enables separation of call control from media conversion. The Media Gateway Control Protocol (Megaco) is a result of joint efforts of the IETF and the ITU-T Study Group 16. Therefore, the IETF defined Megaco is the same as ITU-T Recommendation H.248 [27].

Megaco/H.248 addresses the relationship between the Media Gateway (MG), which converts circuit-switched voice to packet-based traffic, and the Media Gateway Controller (MGC, sometimes called a call agent or softswitch, which dictates the service logic of that traffic). Megaco/H.248 instructs an MG to connect streams coming from outside a packet or cell data network onto a packet or cell stream such as the Real-Time Transport Protocol (RTP). Megaco/H.248 is essentially quite similar to MGCP from an architectural standpoint and the controller-to-gateway relationship, but Megaco/H.248 supports a broader range of networks, such as ATM. There are two basic components in Megaco/H.248: terminations and contexts. Terminations represent streams entering or leaving the MG (for example, analog telephone lines, RTP streams, or MP3 streams). Terminations have properties, such as the maximum size of a jitter buffer, which can be

inspected and modified by the MGC. Terminations may be placed into contexts, which are defined as when two or more termination streams are mixed and connected together. The normal, "active" context might have a physical termination (say, one DS0 in a DS3) and one ephemeral one (the RTP stream connecting the gateway to the network). Contexts are created and released by the MG under command of the MGC. A context is created by adding the first termination, and it is released by removing (subtracting) the last termination [27].

A termination may have more than one stream, and therefore a context may be a multi stream context. Audio, video, and data streams may exist in a context among sevProtocol Structure - Megaco/H.248 (Media Gateway Control Protocol)

All Megaco/H.248 messages are in the format of ASN.1 text messages. Megaco/H.248 uses a series of commands to manipulate terminations, contexts, events, and signals. The following is a list of the commands:

1. Add. - The Add command adds a termination to a context. The Add command on the first Termination in a Context is used to create a Context.
2. Modify - The Modify command modifies the properties, events and signals of a termination.
3. Subtract - The Subtract command disconnects a Termination from its Context and returns statistics on the Termination's participation in the Context. The Subtract command on the last Termination in a Context deletes the Context.
4. Move - The Move command atomically moves a Termination to another context.
5. Audit Value - The Audit Value command returns the current state of properties, events, signals and statistics of Terminations.
6. Audit Capabilities - The Audit Capabilities command returns all the possible values for Termination properties, events and signals allowed by the Media Gateway.
7. Notify - The Notify command allows the Media Gateway to inform the Media Gateway Controller of the occurrence of events in the Media Gateway.

8. Service Change - The Service Change Command allows the Media Gateway to notify the Media Gateway Controller that a Termination or group of Terminations is about to be taken out of service or has just been returned to service. Service Change is also used by the MG to announce its availability to an MGC (registration), and to notify the MGC of impending or completed restart of the MG. The MGC may announce a handover to the MG by sending it Service Change command. The MGC may also use Service Change to instruct the MG to take a Termination or group of Terminations in or out of service.

All of these commands are sent from the MGC to the MG, although Service Change can also be sent by the MG. The Notify command, with which the MG informs the MGC that one of the events the MGC was interested in has occurred, is sent by the MG to the MGC. eral terminations [27].

CHAPTER 6

VoIP IN BANGLADESH

A move is underway to bring illegal VoIP (voice over internet protocol) under a legal framework by renting out E1 connections to the operators. E1 is an all-digital communications line that allows transmission of voice, data, video, and graphics at high speed compared to standard communication lines. Illegal VoIP operators handle international calls through the E1 devices.The parliamentary standing committee on the post and telecommunication ministry asked state-run Bangladesh Telecommunications Company Ltd (BTCL), the distributor of E1, to make a report on whether the government's earnings will increase or decrease if VoIP operators use the line. BTCL charges Tk 1.2 lakh for each E1 connection that can rout 30 calls at a time. The parliamentary body is looking for a suitable way to legalise international call termination through VoIP. Earlier, the government had decided in principle to issue more international gateway licences for handling international calls to trigger a price war and bring illegal VoIP operators under a legal framework. Around 60 million minutes of international calls are made in and out of Bangladesh a day. Illegal VoIP handlers rout around 40 percent calls of the total volume. Presently, BTCL rents out E1 connections to the licensed telecom operators. According to the Telecoms ministry Officials, the VoIP operators will still remain illegal as they will have to take licences for both E1 connection and for routing international calls. However, if the government wants to bring VoIP operators under a legal framework, the recently amended international long distance telecommunication services (ILDTS) policy will require a further modification. "A major policy improvement is required, if the government goes for renting out E1 to the VoIP operators," Currently, illegal VoIP operators charge around 1.75 cents per minute for an international call whereas legal call handlers charge 3 cents. Bangladesh Telecommunication Regulatory Commission has decided to activate the private land phone connections, which were switched off over allegation against the operators of having involvement with illegal call termination. "BTRC officials will visit the offices of accused landline operators and only the subscribers having valid documents will get connections," "No illegal connection will be restored," according to the law of BTRC. The telecommunication regulator has suspended operations of RanksTel, Dhaka Phone,

PeoplesTel and WorldTel on charge of being involved in illegal call termination through voice over internet protocol. The companies have more than 5.5 lakh subscribers BTRC will continue. The its investigation of illegal VoIP activities by any telephone operator or Internet service provider and shut them down, if found guilty, as it did in cases of three private landline companies and 18 ISPs recently. Bangladesh Telecommunication Regulatory Commission is ignoring the plights of around 4,00,000 subscribers of the three phone companies, saying it does not want any citizen to use telecom services of companies involved in illegal activities. Some clients of these three landline operators–RanksTel, Dhaka Phone and WorldTel–have accused the BTRC of not having considered their rights while shutting down operations of these telecom service providers. The BTRC will serve show-cause notices on operators already accused of conducting illegal VoIP business. If they fail to give satisfactory reply, the commission will go for tougher actions like canceling licences or imposing penalty or both. Industry insiders said the VoIP-based call termination business has already captured over 40 percent of the market of incoming and outgoing international calls. This has tremendously affected telecom companies licensed to handle international calls while the government is being deprived of huge revenue. Illegal VoIP operation has been thriving in Bangladesh since the late 1990s amid the authorities' silence. At one point in 2006-07, such operators were taking away around Tk 15,000 crore annually, the money too being illegally transacted internationally. During the last caretaker government rule the BTRC fined five mobile phone operators and a few landline service providers for their involvement in the illegal business. It realised around Tk 650 crore in fines from them. By 2008, illegal VoIP business shrank amid strong drives spearheaded by the Rapid Action Battalion and the BTRC. Soon after the political government came to power, the VoIP business reappeared on the scene. The prime minister in a decisive move recently directed the telecom ministry and BTRC to take steps against illegal VoIP operation. Twelve landline operators and six mobile phone operators have more than 56 million customers in Bangladesh with mobile operators serving around 54 million. More than one crore non-resident Bangladeshis generate over three crore minutes' calls to Bangladesh every day. After the recent drive international call termination through legal channels jumped over 4.5 crore minutes a day as of yesterday from 3 crore a week ago. In two recent raids, the

BTRC seized huge VoIP equipment from Dhaka Phone and WorldTel on March 14 and March 16. Dhaka Phone's five top officials were arrested and sent to jail. With 2,88,272 subscribers throughout Bangladesh, Ranks Telecom Ltd is the largest private fixed line operator. Dhaka Phone has 75,000 customers while WorldTel has 14,000. BTRC is set to take legal action against the private land phone operator WorldTel Bangladesh for its alleged involvement in illegal VoIP business. BTRC seized different equipment, including two multiplexers used for VoIP (voice over Internet protocol) calls from the office of WorldTel. So, a team of BTRC visited the office and found no official there and the switch room remained locked down. Since then BTRC could not contact any responsible officials of WorldTel over phone as all their cell numbers remained off. Bangladesh Telecommunications Company Ltd (BTCL) urged a cut in international incoming call charge, which it said will help check illegal call termination through VoIP (voice over internet protocol) technology. The state-run telecom operator sought a call charge at 1.5 cents, down from existing three cents per minute. "Price reduction can be one of the best ways to control illegal call termination business," Landline business apart, BTCL owns an international gateway (IGW) to handle overseas calls. Three other IGWs from private sector are also running IGW business. In contrast such call charge ranges from three cents to 10 cents in Pakistan where illegal VoIP business is rampant. Presently, illegal VoIP operators charge 1.5 cents to 2.5 cents for handling international incoming calls. Bangladesh's telecom market receives more than three crore minutes' calls a day. E1 is an all-digital communications line that allows transmission of voice, data, video, and graphics at higher speed compared to standard communication lines. Illegal VoIP operators handle international calls through E1 devices. However, private IGW operators earlier opposed the move to cut international call charge, which they said would harm their business. According to BTRC report such a price cut always increases call volume. After the government decision to reduce international incoming call charge from six cents to three cents, incoming international calls went up significantly. The users connected to the internet through local internet service providers (ISPs) can now talk to each other and telecom subscribers, as the telecom regulator made a tariff directive to commercially launch IP telephony services. Under the tariff plan, 33 licensees, known as internet protocol telephony service providers (IPTSPs), can now sell voice services.

Service providers can charge a maximum of Tk 0.20 a minute for domestic IPTSP to IPTSP calls and a maximum of Tk 2 for a call from IPTSP to any mobile or landline operator, in line with a Bangladesh Telecommunication Regulatory Commission (BTRC) directive. However, the minimum airtime charge for calls from IPTSP to any mobile or landline operator will not be below Tk 0.65 a minute, according to the BTRC. For international outgoing calls, IPTSP will have to follow the rates for international calls, as issued earlier by BTRC. However, the new tariff directive frustrates IP telephony licence holders; as such charges will not be financially viable. Different telecom operators are charging lower than the tariff set for IPTSP. “If we offer IPTSP to IPTSP calls almost free of cost, it will help boost internet penetration,” said the president of Internet Service Providers Bangladesh. In addition, other IP-based voice services to other operators will not be viable due to the uncompetitive tariff directive, he said. “It’s not a very good proposition in terms of tariff.” It would have been better if the per minute charge was fixed between Tk 0.30 to Tk 0.60, The services are to be value-added services at low costs, it will gain popularity in some areas such as intra-company communication. IP telephony licence owners can provide PC (personal computer) to phone, phone to PC, phone to phone or any other use to subscribers, based on the IP telephony voice service. From a technical point of view, experts said, the voice over internet protocol (VoIP) is set to open through legal channels as IP and VoIP technologies have nearly the same features. BTRC last year made a guideline to award IP telephony licences exclusively to local ISPs. Customers now can talk by using their internet connection just after installing a modem for voice transmission. Presently, more than five lakh internet users are connected through local ISPs. On the other hand, mobile operators claimed more than 40 lakh are connected via mobile internet. Bangladesh’s internet penetration rate is only 4 percent. The government has decided in principle to issue more VoIP licences for handling international calls to trigger a price war and bring illegal VoIP operators under a legal framework. As per an amended policy, illegal VoIP (voice over internet protocol) operators will get a chance to make their business legal by routing calls through legal exchanges. Earlier, international calls through VoIP were completely prohibited under the International Long Distance Telecommunications Service Policy. The government did not legalise the existing illegal VoIP business. However, it expects that when more

exchanges are launched, VoIP calls will be routed through legal channels due to competitive pricing. Currently, illegal VoIP operators on an average charge 1.75 cent per minute for an international call whereas legal call handlers charge 3 cents. The policy recommends issuing more licences for international call handling to encourage existing VoIP businesses that operate outside the law to be under a legal framework. Sources in Bangladesh Telecom Regulatory Commission (BTRC) said 10 more licences would be given by March. As per the amended policy, all call handlers will be responsible for compelling illegal calls go through their channels and make them legal. Among the existing six call handlers, three international gateways are mainly responsible for handling international voice calls along with the state-run BTCL. Two other legal interconnection exchanges transmit the calls between the gateways and telecom operators, while the lone private international internet gateway is responsible for handling data traffic. Around 60 million minutes of international calls are made to and from Bangladesh a day. In Bangladesh, VoIP has become a lucrative business as the technology offers international calls at charges much lower than that of the legal calls. Hundreds of people have been engaged in this business. More individuals and companies will be involved in international call termination to stop the illegal VoIP business. People of Bangladesh will remember him with gratitude for his contribution in getting the equal share of water of the Ganges through the signing of the Ganges water-sharing treaty. NEW technologies require new laws and regulations. But these regulations must be sensible and they have to be enforced uniformly. The tragedy in Bangladesh is that we make senseless regulations and do not enforce the sensible ones. As a result, businesses get destroyed, our workers migrate and then we highlight “record remittances” to console ourselves. To illustrate, let us focus on recent events in the telecommunications and internet sector. It is hard to find a better example of senseless regulation than Voice over Internet Protocol (VoIP). VoIP is much maligned by the Bangladesh Telecom Regulatory Commission (BTRC) and the media because it is “illegal.” But nobody explains the rationale behind making VoIP illegal. Unlike cars, firearms or alcohol, all of which require licenses in Bangladesh, VoIP does not carry with it the possibility of harming another individual. Why should VoIP operators need a license? VoIP hurts the companies that have invested heavily in traditional telephony systems by providing the same

services to customers more cost-effectively. In Bangladesh, the state-owned Bangladesh Telecommunications Company Ltd (BTCL, formerly BTTB), is the only company that has invested heavily in the traditional system and therefore is the only one who stands to lose if VoIP technology is widely adopted. Naturally the question arises: if this were not a government monopoly, would it be given such protection from cheaper technologies through regulations? After all, the government is not moving to protect handloom weavers from machine-looms or the ayurvedic medicine industry from big pharmaceuticals, both instances where a new technology undercut an established one. We keep hearing the refrain that BTRC's strict enforcement of this senseless regulation brought more money into the government coffers. Yes, it did, by ensuring that a government monopoly could charge the consumer (you and me) more than their more efficient competitors. The strange phenomenon of our tax money going to bureaucrats enforcing regulation that deprives us of a cheaper way of calling our loved ones in distant lands perfectly encapsulates the dysfunction of present-day Bangladesh. Of course making VoIP illegal has not stopped it from spreading. Rather, it has enabled political patronage, which thrives when governments hold too much power over the citizens' ability to earn a living. Ironically, the very media that was instrumental in bringing to light the corruption under the last elected government seems to have taken hold of the wrong end of the stick on this issue. Instead of asking for greater liberalization of VoIP to prevent further government corruption in this sector, they have decided to stigmatize this technology altogether. And the mainstream media's silence — for whatever reasons — over the last minute changes of a very sensible rule, regarding eligibility of bidding for Wimax licenses, that might have long-term consequences, is very puzzling. No major print media outlet has reported the irregularities surrounding the post-auction complications of the Wimax licenses. There linger questions as to whether one of the companies set to get a Wimax license, Mango Teleservices, was eligible to enter the bidding in the first place. Mango Teleservices won the license after 4 other companies were unable or unwilling to acquire them [34].

CHAPTER 7

CONCLUSION

In this project paper ,we present a summary of the comparison presented in above table. In terms of functionality and services that can be supported, H.323 version 2 and SIP are very similar. However, supplementary services in H.323 are more rigorously defined. Therefore, fewer interoperability issues are expected among its implementations. Furthermore, H.323 has better compatibility among its different versions and better interoperability with PSTN. The two protocols are comparable in their QoS support (similar call setup delays, no support for resource reservation or class of service (QoS) setting), but H.323 version 3 will allow signaling of the requested QoS. SIP's primary advantages are its flexibility to add new features and its relative ease of implementation and debugging. Finally, we note that H.323 and SIP are improving themselves by learning from the other side, and the differences between them are diminishing with each new version.

Every technology has several advantages and limitations also. If we can overcome these limitations that help them to develop new VoIP protocol and also consider the efficient implementations which would be cost effective. We must not ignore the security impact that relies on how we tackle the situation in handling the security issues. Government should take necessary initials to legalize VoIP licenses in low cost. So that VoIP can be use by the operators to offer telephony (voice), broadband internet access and service such as TV video. And if VoIP is open, it ensures improved productivity of an organization.

REFERENCES

1. Jonathan Davidson, James Peters, Manoj Bhatia, Satish Kalidindi, Sudipto Mukherjee Voice over IP Fundamentals, Second Edition

2. Kevin Wallace, Authorized Self Study Guide Cisco Voice over IP (CVoice)

3. Jeffrey G. Andrews, Arunabha Ghosh, Rias Muhamed; Fundamental Of WiMAX Understanding Broadband Wireless Network

4. http://www.iec.org/online/tutorials/int_tele/index.asp. Retrieved 2009-04-27.

5. wikipedia.org/wiki/***ip***

6. http://www.ieee802.org/16/docs/06/C80216-06_007r1.pdf. Retrieved 2008-03-12.

7. FCC.gov, What are some advantages of VoIP?

8. FCC.gov, If I have VoIP service, who can I call?

9.Creating a secure and reliable VoIP solution (section: Protecting VoIP at the application layer) — ZDnet Asia]

10. http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=1966

11. http://voip.about.com/od/voipbasics/a/voipcodecs.htm

12. http://www.hill2dot0.com/wiki/index.php?title=MOS

13. http://voip.about.com/od/glossary/g/echo.htm

14. Davidson, Jonathan; James Peters, Jim Peters, Brian Gracely. "H.323". Voice over IP fundamentals. Cisco Press. pp. 229–230.]

15. ITU-T Recommendation H.323

16. ITU-T Recommendation H.323 (06/2006), Packet-based multimedia communications systems.]

17. See ITU-T Recommendations of the H.323 System for a detailed list.

18. ITU-T Recommendation H.323 (06/2006), *Packet-based multimedia communications systems*.

19. thttp://en.wikipedia.org/wiki/H.323_Gatekeeper

20. en.wikipedia.org/wiki/H.323

21. en.wikipedia.org/wiki/Session_Initiation_Protocol

22. en.wikipedia.org/wiki/Session_Initiation_Protocol/Application

23. en.wikipedia.org/wiki/MGCP

24. http://www.protocols.com/pbook/VoIPFamily.htm

25. http://www.gl.com/mapsmgcp.html

26. http://en.wikipedia.org/wiki/MGCP

27. http://www.javvin.com/protocolMegaco.html

28. file://X:\www-docs\cse574-06\ftp\wimax_voip\index.html

29. http://www.wimaxforum.org/kshowcase/view

30. http://doc.trolltech.com/qtopia4.3/syscust-voip.html

31. http://doc.trolltech.com/qtopia4.3/qtelephonyservice.html

32. http://doc.trolltech.com/qtopia4.3/qphonecallprovider.html

33. http://doc.trolltech.com/qtopia4.3/qphonecallprovider.html#endStateTransaction

34. http://www.btrc.com

35. Bell Atlantic, "Signaling System 7 (SS7) Tutorial",
http://www.webproforum.com/bellatlantic2/topic01.html

36. ITU-T Recommendation H.323, "Packet-Based Multimedia Communications Systems", February 1998.

37. M. Handley, H. Schulzrinne, E. Scholler, J. Rosenberg, " SIP: Session Initiation Protocol", RFC2543, IETF, March
1999.

38. H. Schulzrinne, J. Rosenberg, "A Comparison of SIP and H.323 for Internet Telephony", Network and Operating

System Support for Digital Audio and Video (NOSSDAV), Cambridge, England, July 1998.

39. V. Jacobson and M. Handley," SDP: Session Description Protocol", RFC2327, IETF, April 1998, work in process.

40. ITU-T Recommendation H.245, "Control protocol for multimedia communication," February 1998.

41. Braden, R., Zhang, L., Berson, S., herzog, S. And Jamin, S.," Resource Reservation Protocol (RSVP) - version 1
Functional Specification," RFC 2205, proposed standard, September 1997.

42. Y. Bernet, R.Yavatkar, P. Ford, F. Baker, L, Zhang, “A Framework for End-to-End QoS Combining RSVP/Intserv
and Differentiated Services ," Internet Draft, March, 1998.

43. S. Blake, et. al, "An Architecture for Differentiated Services," RFC 2475, December 1998.

44. "H.323 Differentiated Services and Their Protocol Architectures," ITU Telecommunication Standardization Sector,
APC-1492, February, 1999

45. ITU-T Standardization Sector, "H.323 Annex E: call signaling over UDP", APC 1441, September, 1998

46. International Multimedia Teleconferencing Consortium, “iNOW!™ Standards-Based IP Telephony Interoperability
Profile,” February 23, 1999

47. Steve Donovan, Mattew Cannon, "A Functional Description of SIP-PSTN Gateway", Internet Draft, IETF, November 1998.

48. ITU-T Recommendation X.691, “Information Technology - ASN.1 encoding rules – Specification of Packed Encoding Rules (PER),” Dec. 1997.

49. ISO/IEC 10646-1:1993, “Information technology -- Universal Multiple-Octet Coded Character Set (UCS) -- Part 1: Architecture and Basic Multilingual Plane”, 1993.