Winter 1-2014

Analyzing Implementation of IP Telephony solutions

Erkan Ramadani
University for Business and Technology - UBT

University for Business and Technology

Faculty of Computer Science and Engineering

Analyzing Implementation of IP Telephony solutions

Student: Erkan Ramadani

January 2014

Pristina

University for Business and Technology
Faculty of Computer Science and Engineering

Bachelor Thesis

Academic Years 2010-2013

Erkan Ramadani

Analyzing Implementation of IP Telephony solutions

Mentor:

MSc. Selman Haxhijaha

January / 2014

This Thesis was prepared and submitted in partial fulfillment of the requirements for the Bachelor Degree

Abstract

In this thesis, Voice over Internet Protocol (VoIP) technology will be explored and a recommendation of the operational benefit of VoIP will be provided. A network model will be used to demonstrate improvement of voice End-to-End delay by implementing quality of service (QoS) controls. An overview of VoIP requirements will be covered and recommended standards will be reviewed.

Take some time-off from your busy schedules and have a look at what I have to say. I guarantee that you will change your mind.

In the near future, if you make a telephone call, it is more than likely that it would be over the Internet or some other packet network. But, what is it that would make this possible? It is a bunch of protocols and standards; and years of research done by organizations all over the world that would bring about this revolution.

They call it ‘VOICE OVER IP’, ‘INTERNET TELEPHONY’ & a host of other names.

The next few chapters of this project report will discuss this phenomenon in detail.

Acknowledgement

I take this opportunity to offer my gratitude to my mentor prof. Selman Haxhijaha for his support and guidance. He allowed me a great deal of freedom in choosing our topics for study and also provided me encouragement throughout this venture.

I also wish to thank him who took time off from their busy schedules to help me with the project. I will also have to show appreciation to the management of the department of Computer Science for the period of my bachelor studies here at University of Business and Technology – UBT in Pristina.

Lastly, I am very grateful to my family, my who always expressed full hope and encouragement toward me. While writing this I had an opportunity to seek help from some very fine colleagues and without their support, this thesis would prove unsuccessful.

This thesis would have been incomplete without the contributions of the following people.

Pristina, January 2013

Erkan Ramadani

Table of Contents

1. Introduction 7

1.2 Research Questions 8

1.3. What is Voice Over IP? 9

2. Literature Review 11

2.1. IP Telephony Overview 11

2.1.1. Telephony Standardization 11

2.1.2. H.323 11

2.1.3. H.323 Components 12

2.1.4. H.323 Specification 15

2.1.5. Protocol Stack 16

2.1.6. Call Sequence 17

2.1.7. VoIP Implementation 18

2.1.8. IP Telephony Deployment Models 20

2.1.9. Single Site Deployment 21

2.1.10. Multisite with Centralized Call Processing 22

2.1.11. Multisite with Distributed Call Processing 25

2.2. PSTN Overview 28

2.2.1. PSTN 28

2.2.2. SS7 29

2.2.3. PSTN Security 30

3. Methodology 31

4. Case Study 32

4.1. Traditional and IP Telephony Comparison 32

4.2. Methods for comparison 32

4.3. General aspects 32

4.3.1. Packet switched / Circuit switched 32

4.3.2. Transport of information 33

4.3.3. Quality of service 33

4.4. Security aspects 34

4.4.1. Security services 34

4.4.2. Security vulnerabilities 36

4.5. Results 37

4.5.1. General aspects 37

4.5.2. Security aspects 38
5. References 42

List of figures

Figure 1. H.323 Terminals on Packet Network. (From: Ref. 4)..... 10
Figure 2. H.323 Components (From: Ref 4) 11
Figure 3. Gateway (From: Ref 4)..... 11
Figure 4. H.323 interoperates with other H.32X Networks (From: Ref 4) 12
Figure 5. H.323 Call Sequence (From: Ref 5) 15
Figure 6. VoIP Implementation (From: Ref 6)..... 18
Figure 7. Interoffice Trunking (From: Ref 5)..... 19
Figure 8. VoIP with cellular networks (From: Ref 5) 19
Figure 9. Single Site Deployment (From: Ref 7) 22
Figure 10. Multisite Deployment with Centralized Call Processing (From: Ref 7)……..... 23
Figure 11. Multisite Deployment with Distributed Call Processing (From: Ref 7) 26

List of Abbreviations

ATM - Asynchronous Transfer Mode
CIA - Confidentiality, Integrity and Authentication
DSP - Digital Signal Processor
IETF - Internet Engineering Task Force
IEC - International Engineering Consortium
IP - Internet Protocol
IPX - Internet Packet Exchange
ISDN - Integrated Services Digital Network
IT - Information Technology
LAN - Local Area Network
MAN - Metropolitan Area Network
MCU - Multipoint Control Unit
PBX - Private Branch Exchange
PCM - Pulse Code Modulation
PSTN - Public Switching Telephone Network
RAS - Registration, Admission, and Status
RAS - Remote Authentication Service
RSVP - Resource Reservation Protocol
RTCP - Real-time Transport Control Protocol
RTP - Real-time Transport Protocol
SIP - Session Initiation Protocol
SNTP - Simple Network Time Protocol
SS7 - Signalling System No. 7
TCP - Transmission Control Protocol
UDP - User Datagram Protocol
VAD - Voice Activity Detector
VoIP - Voice over Internet Protocol
VPN - Virtual Private Network
VQ - Voice Quality
WAN - Wide Area Network
WEP - Wired Equivalent Privacy
WFQ - Weighted Fair Queuing

1. Introduction

The global communications transformation is in full swing. Packet-switched technology has moved from data-only applications into the heart of the network to take up the functions of traditional circuit-switched equipment. While the lower cost of packet-switched networks initially drove this change, the improving quality and reliability of voice over these networks is speeding integration of voice and data services. Consequently, the overwhelming majority of voice networks in service today will be replaced by packet infrastructure within the next decade. Service providers and corporate organizations, therefore, must develop a plan to migrate their voice services from circuit-switched networks to packet-switched networks to ensure their future success and survival.

1.2 Research Questions

To get a clear understanding of what has to be researched and analyzed in the thesis we have defined two research questions:

a) What is the challenge for implementing VoIP network for a small to medium size enterprise
b) Describe and compare VoIP and PSTN technologies and protocols.

1.3. What is Voice Over IP?

Voice over IP (VOIP) uses the Internet Protocol (IP) to transmit voice as packets over an IP network. So VOIP can be achieved on any data network that uses IP, like Internet, Intranets and Local Area Networks (LAN). Here the voice signal is digitized, compressed and converted to IP packets and then transmitted over the IP network. Signaling protocols are used to set up and tear down calls, carry information required to locate users and negotiate capabilities. One of the main motivations for Internet telephony is the very low cost involved.

There are four different types of connections for setting up the call. In all of the cases of VoIP, the Internet Protocol (IP) is used. This means that the service is best effort i.e. the application handles the end-to-end communication without any guarantees from the net.

The four different types are: [1]

1. PC to PC
2. PC to Telephone
3. Telephone to PC
4. Telephone to Telephone
5. Regular phones connected to PSTN
6. IP-telephones connected to a data net

Most of the focus on VoIP is currently centered on two key applications.

The first is private business network applications. Businesses with remotely located branch offices which are already connected together via a corporate intranet for data services can take advantage of the existing intranet by adding voice and fax services using VoIP technologies. Businesses are driving the demand for VoIP solutions primarily because of the incredible cost savings that can be realized by reducing the operating costs of managing one network for both voice and data and by avoiding access charges and settlement fees, which are particularly expensive for corporations with multi-international sites. Managed corporate intranets do not have the QOS issues which currently plague the Internet; thus voice quality approaches toll quality. [1]

The second key application is VoIP over public networks. This application involves the use of voice gateway devices designed to carry voice to Internet Service Providers, now known as Internet Telephony Service Providers, or to the emerging Next Generation Carriers which are developing IP networks specifically to carry multimedia traffic such as VoIP. ISPs are interested in VoIP as a way of offering new value-added services to increase their revenue stream and break out of the low monthly fixed fee structure currently in place for data services. VoIP also allows them to improve their network utilization. These new services include voice and fax on a per-minute usage basis at

rates significantly less than prevailing voice and fax rates for service through the PSTN. The sustainability of this price advantage may be short term, and is dependent on whether the FCC and foreign regulatory agencies will require ISPs to pay the same access charges and settlement fees PSTN carriers are obligated to pay. In the long term, IP networks are more efficient for a wide range of new applications, particularly multimedia applications enabling convergence of voice, video, data, and fax. Carriers, too, are interested in VoIP, primarily for competitive reasons. Although VoIP will cannibalize some of their POTS services, they have wisely determined that they too must compete in this rapidly growing marketplace. The market projections are too staggering to be ignored: according to a survey, 10% of the world's fax market could be on the internet in 2 - 3 years, and by 2002, the Internet could carry 11% of US and international long distance traffic. [1]

In this project report we discuss VoIP in both contexts.

We now discuss the switching technology that differentiates Voice over an IP network from the traditional circuit switched technology.

2. Literature Review

2.1. IP Telephony Overview

The primary function of IP Telephony is to record and packetize speech into series of voice packets, then transmit them through the networks and release the entire speech to the listener with acceptable delays. This chapter explains the architecture of this technology and the relevant technical standards.

2.1.1. Telephony Standardization

As previously mentioned, IP telephony technology is still immature. Several organizations are developing their own standards to serve the industry requirements and some vendors are still using their proprietary design. However, most vendors tend to support the approved standards to allow interoperability.

Currently, the first and most commonly-adopted standard of telephony is the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) Recommendation H.323 [Ref 2].This standard is designed for multimedia communication systems including voice applications. This standard of telephony, H.323, was originally created in 1996, and the complete standard on version 4 was released in November 2000. The advantages of this standard are that it is now completely open source with GUI and that it can operate on any operating systems. [3]

A standard developed by the Internet Engineering Task Force (IETF) is the Session Initiation Protocol (SIP). It addresses some drawbacks ofH.323. The SIP offers less complexity and provides more flexibility. The latest SIP standard is released in RFC 3261 posted in July, 2002. All new VoIP application designs support H.323 or both H.323 and SIP. As SIP is a relatively new standard, in this chapter, H.323 is presented as the main telephony architecture. [3]

2.1.2. H.323

The ITU- T designed H.323 to be part of the H.32X recommendation family, so it can work with other standards for different networks as following: [4]

- H.324 over switched circuit network (SCN) and wireless network
- H.320 over integrated services digital networks (ISDN)
- H.321 and H.310 over broadband ISDN (B-ISDN)
- H.322 over LAN with guaranteed QoS

The H.323 standard specifies the technical requirements - such as components, protocols, and procedures - for packet-based multimedia communication systems, including real-time audio, video, and data communications. It covers all applications deployed on IP-based and IPX-based (Internet packet exchange networks, i.e., local area networks (LAN), enterprise networks (EN), wide area networks (WAN), metropolitan area networks (MAN), and Internets. The H.323 is designed for different mixes of data types: audio only (IP telephony), audio-video (video-telephony), audio-data, and audio video- data. This design also supports multipoint multimedia communications. [4]

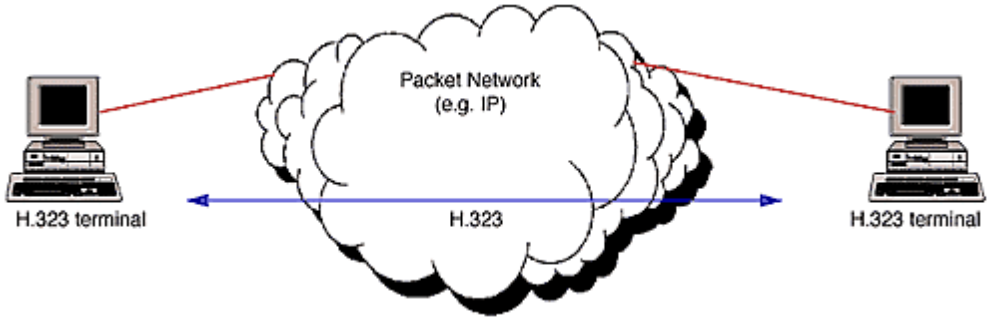

Figure 1 H.323 Terminals on Packet Network. [4]

2.1.3. H.323 Components

The H.323 incorporates four main components: terminal, gateway, gatekeeper, and a multipoint control unit (MCU) [Ref 8]. Their interaction is illustrated in Figure 2. If all components are located in the same area, with only one gatekeeper, they are considered to be in the same H.323 zone.

1. **Terminal**

An H.323 terminal can be either a personal computer or any standalone device running an H.323 protocol stack and multimedia applications. The required basic service is audio communications, while video or data service is optional. Since the primary goal of this

standard is to interoperate with other multimedia terminals, the H.323 terminal can talk to all terminals in the H.32X family. The terminal also supports multipoint conferences. [4]

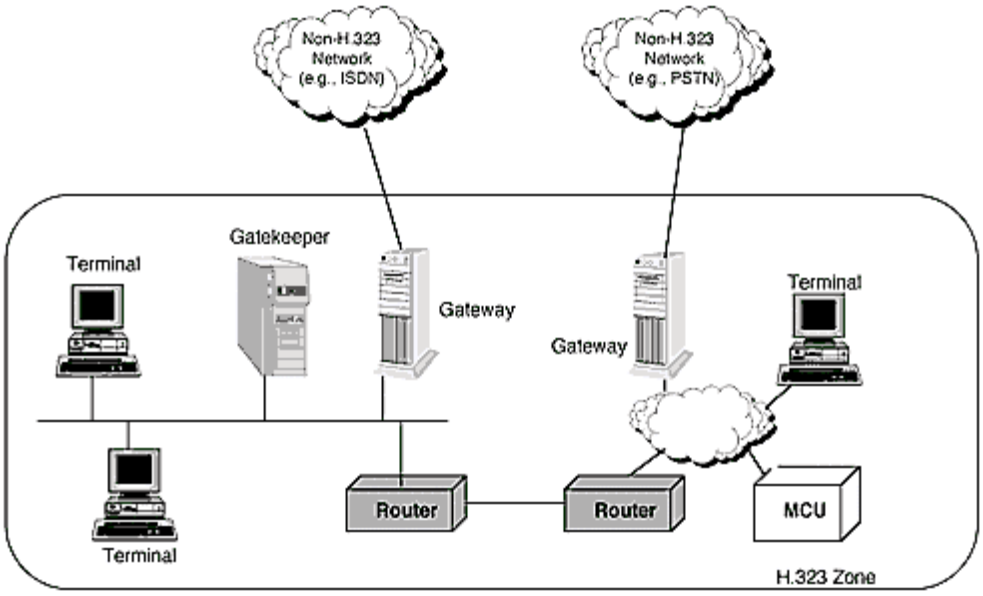

Figure 2. H.323 Components [4]

2. **Gateway**

To interconnect heterogeneous systems, a gateway is introduced for binding H.323 networks and non-H.323 networks. Normally the gateway is used to link H.323 terminals to PSTN. It also provides translating protocols for call setup and release, converts media format, and transfers information. However, a gateway is not always required within an H.323 region. [4]

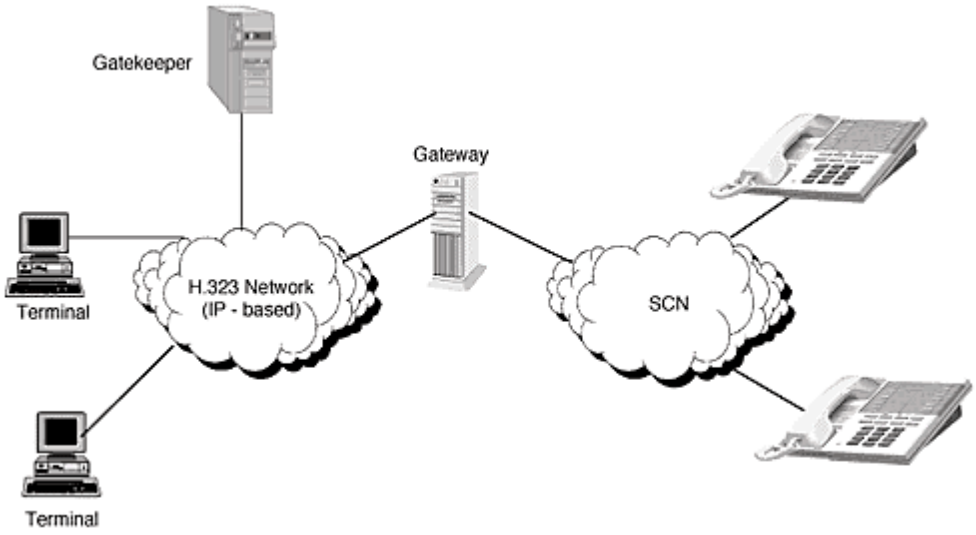

Figure 3. Gateway [4]

3. **Gatekeeper**

The gatekeeper is designed to be a control center of all calls in an H.323 network. It performs many important tasks such as addressing, authorizing and authenticating of terminals and gateways, bandwidth management, accounting, billing, charging, and callrouting services. A gatekeeper is not required if these services are not needed.

4. Multipoint Control Unit (MCU)

For multi-party communication with at least three terminals, the MCU is required.
All terminals connect with the MCU, which serves as a central point of the conference. It checks and manages the conference resources, negotiates between terminals to determine codec type, and handles the media streams.

All four components are logically separate, but they can be implemented on the same device. [4]

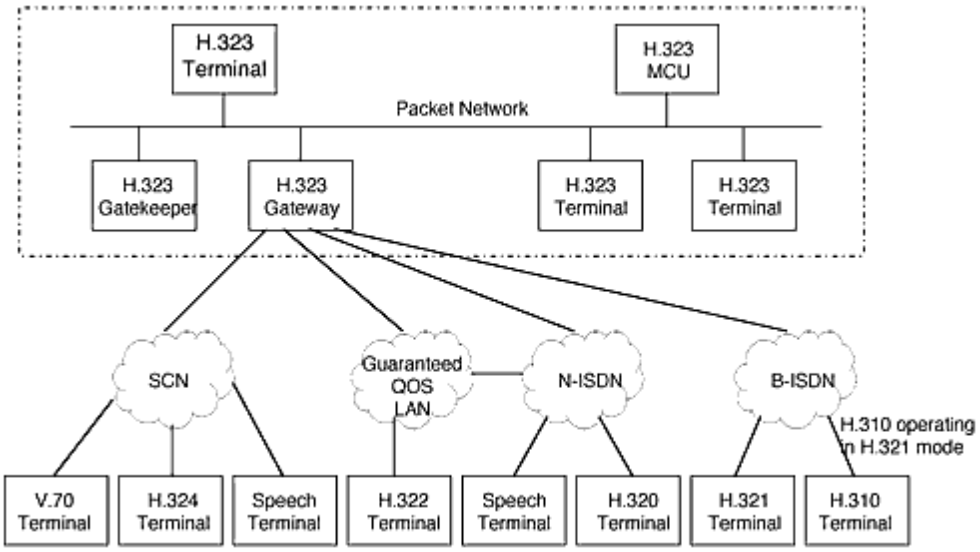

Figure 4. H.323 interoperates with other H.32X Networks [4]

2.1.4. H.323 Specification

The H.323 recommendation specifies several protocols for multimedia communication processing and controlling. [4]

1. **Audio Codec**

The audio codec encodes voice signals from the sender's microphone into packets and at the receiver decodes these packets to reproduce the voice signals for playout by the receiver's speakers. Each terminal must support at least one default audio codec, G.711. Additional codecs like G.722, G.723.1, G.728, and G.729 may be provided. [4]

2. **Video Codec**

The video codec encodes video signals from the sender's camera into packets and at the receiver decodes these packets to reproduce the video signals for display on the receiver's monitor. In H.323, this codec is optional. The video codec specification is defined in the H.261 recommendation. [4]

3. H.225 Registration, Admission, and Status (RAS)

In H.225, RAS is used to establish some management functions between endpoints (terminals and gateways). Its responsibilities include registration, admission control, bandwidth change, status, and a disengage procedure between endpoints and gatekeepers. The messages of RAS are exchanged via an RAS channel which is the signaling channel connecting between endpoints. [4]

4. H.225 Call Signaling

A connection between two H.323 endpoints is established by exchanging H.225 messages on the call signaling channel. This channel is opened between an endpoint and the gatekeeper. [4]

5. H.245 Control Signaling

The end-to-end control messages managing the operation of all endpoints are exchanged with H.245 control signaling. The control messages encapsulate the information on capability exchange, logical channel opening and closing, flow control, and command and indication. [4]

2.1.5. Protocol Stack

The voice protocol suit is designed to support packet transmission behavior requirement. Since VoIP tries to emulate regular speech communication on PSTN, the interactive communication quality is the key consideration that distinguishes voice from data packet. On a traditional data network, data packets are loss-sensitive and delaytolerant.
On the other hand, voice packets are loss-tolerant and delay-sensitive. As a result, the transport layer in the VoIP protocol stack is implemented with UDP to carry voice instead of TCP. However, TCP is still used to carry signaling messages, such as call establishment and capability exchange. [5]

Moreover, as voice communication requires real-time interactions, RTP is used on top of UDP to deliver end-to-end services. The RTP is designed for real-time applications and to provide payload type identification, sequence numbering, timestamp, and delivery monitoring.

Real-time Transport Control Protocol (RTCP) serves as a control counterpart of the RTP operation. This protocol reports the data distribution quality periodically in the form of sender and receiver reports. The RTP source can also use RTCP to help its receiver synchronize audio and video input.

In addition, Resource reSerVation Protocol (RSVP) is implemented in routing devices to set up and maintain a suitable transmission path for each communication. This can improve the transmission quality by avoiding congested links. [5]

2.1.6. Call Sequence

The ITU incorporates H.323 with its T.120 data-conferencing standard. The call sequence consists of three steps and messages that are delivered over two transport layer protocols. The TCP is first used to setup call establishment with Q.931 and to exchange capability with H.245 messages. Then UDP is used to carry RTP and RTCP payloads after the communication pipeline is opened between the endpoints. The call sequence is illustrated in the following figure. [5]

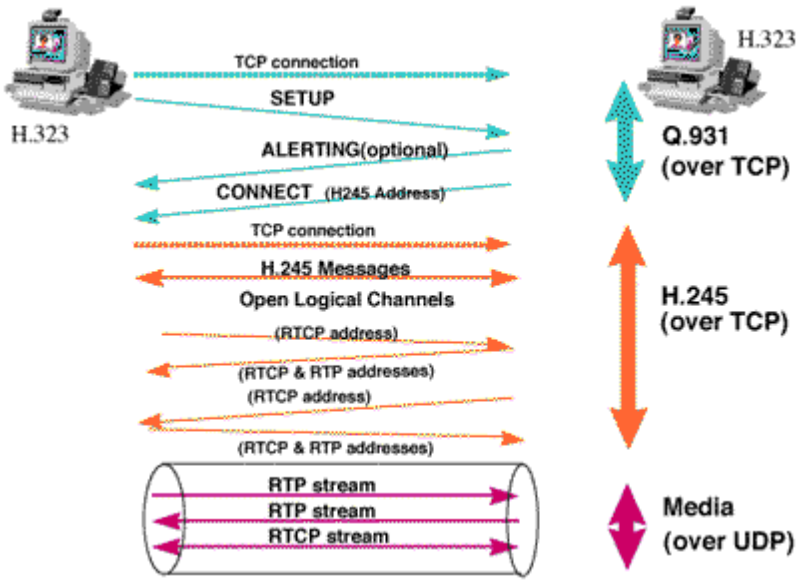

Figure 5. H.323 Call Sequence [5]

2.1.7. VoIP Implementation

A wide variety of IP Telephony applications used in the corporate networks is normally called VoIP. Some of these applications are discussed here to give a general idea of how voice packets practically move around corporate units located in different areas. [Ref 10]

The first application is for large companies with many branch offices. The packet network used for standard data transmission is enhanced to carry voice traffic along with data. Voice traffic should be compressed to save bandwidth. The inter-working function (IWF), which is the physical implementation of hardware and software, allows the mixed voice-data traffic to access the packet network. In this case, the IWF must support analog interfaces that directly connect to telephones. The IWF has two responsibilities; it works as a private branch exchange (PBX) at branches and it behaves like a telephony terminal at home office as demonstrated in this architecture. [6]

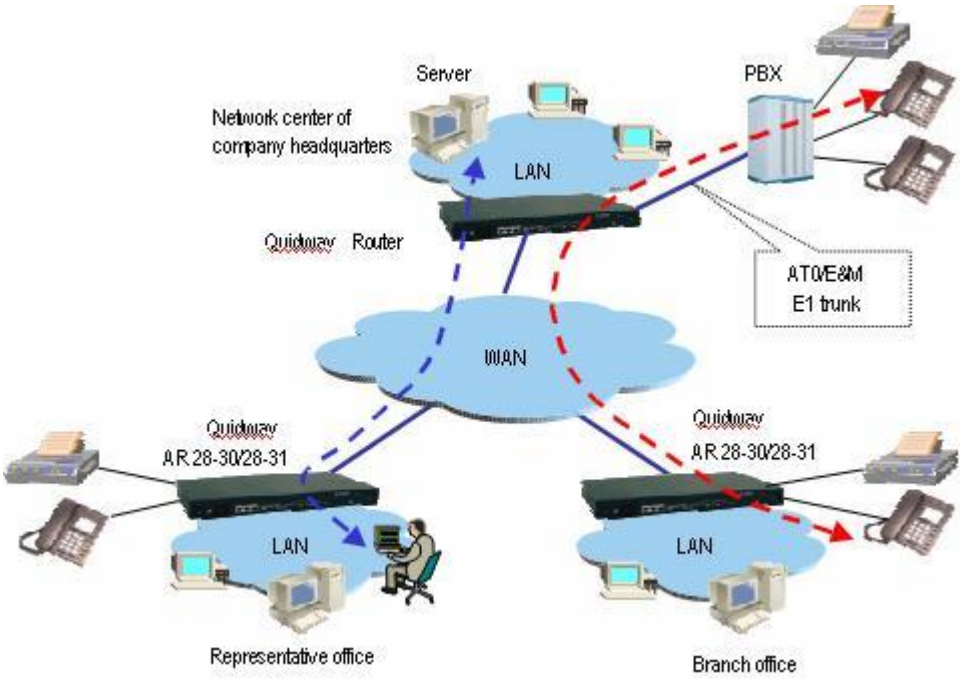

Figure 6. VoIP Implementation [6]

The next usage of VoIP is a trunking application. The packet network, installed between remote offices, completely replaces the original telephone lines being used to link the PBXs. Voice and data traffic volume is higher than the branch office scenario; therefore,

the IWF must support a larger capacity digital channel, such as T1/E1 interfaces. The IWF also emulates the PBX signaling responsibilities. Figure 7 displays this scenario.

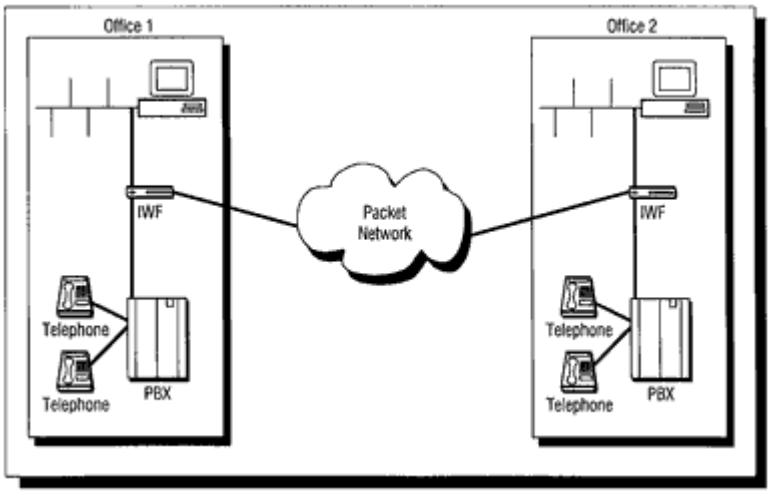

Figure 7. Interoffice Trunking [6]

Furthermore, VoIP can interoperate with cellular networks as shown in Figure 8. In a digital cellular network, voice is already compressed and packetized by the cellular phones. The voice network then transmits these packets to destinations. Finally, IWF performs the transcoding to convert the cellular voice data to PSTN voice format.

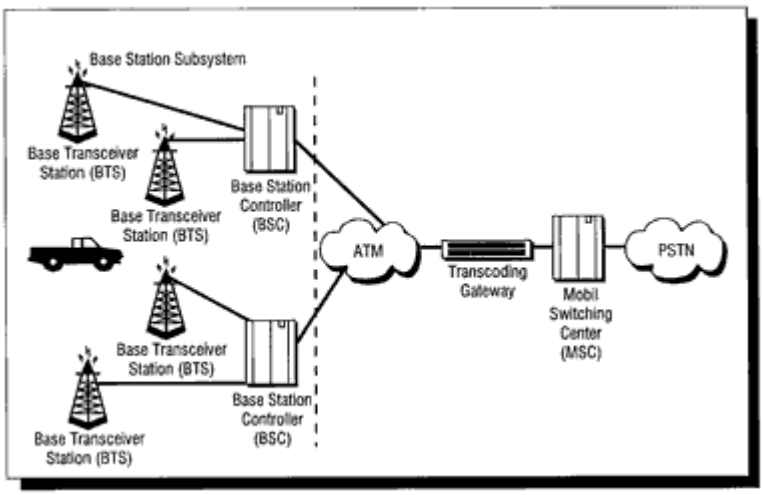

Figure 8. VoIP with cellular networks [6]

2.1.8. IP Telephony Deployment Models

Because many organizations have multiple locations, their IP telephony networks might span those locations. Therefore, there are three deployment models depending on a company size: single-site deployment, multisite WAN with centralized call processing deployment, multisite WAN with distributed call processing deployment, and a clustering over the WAN deployment. [14]

Bellow we will explain each solution that is based on a Unified CM deployment model, and the type of deployment model is based on one or more of the following factors: [14]

- Number of call processing agent clusters
- Number of IP phones
- Locations of the call processing agent cluster(s) and IP phones

2.1.9. Single Site Deployment

The single-site model for Unified Communications consists of a call processing agent cluster located at a single site, or campus, with no telephony services provided over an IP WAN. An enterprise would typically deploy the single-site model over a LAN or metropolitan area network (MAN), which carries the voice traffic within the site. In this model, calls beyond the LAN or MAN use the public switched telephone network (PSTN).

Provide a highly available, fault-tolerant infrastructure based on a common infrastructure philosophy. A sound infrastructure is essential for easier migration to Unified Communications, integration with applications such as video streaming and video conferencing, and expansion of Unified Communications deployment across the WAN or to multiple Unified CM clusters. [15]

The single-site model has the following design characteristics:

- Single Unified CM cluster.
- Maximum of 30,000 configured and registered Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP) IP phones or SCCP video endpoints per cluster.
- Maximum of 2,100 gateways and trunks (that is, the total number of H.323 gateways, H.323 trunks, digital MGCP devices, and SIP trunks) per Unified CM cluster.
- PSTN for all calls outside the site.
- Digital signal processor (DSP) resources for conferencing, transcoding, and media termination point (MTP).
- Voicemail, unified messaging, Unified Presence, audio and video components.
- Capability to integrate with legacy private branch exchange (PBX) and voicemail systems.
- H.323 clients, MCUs, and H.323/H.320 gateways that require a gatekeeper to place calls must register with a IOS Gatekeeper (IOS Release 12.3(8)T or greater). Unified CM then uses an H.323 trunk to integrate with the gatekeeper and provide call routing and bandwidth management services for the H.323 devices registered to it. Multiple IOS Gatekeepers may be used to provide redundancy.
- MCU resources are required for multipoint video conferencing. Depending on conferencing requirements, these resources may be either SCCP or H.323, or both.
- H.323/H.320 video gateways are needed to communicate with H.320 videoconferencing devices on the public ISDN network.

- High-bandwidth audio (for example, G.711, G.722, or Wideband Audio) between devices within the site.
- High-bandwidth video (for example, 384 kbps or greater) between devices within the site. The Unified Video Advantage Wideband Codec, operating at 7 Mbps, is also supported. [7]

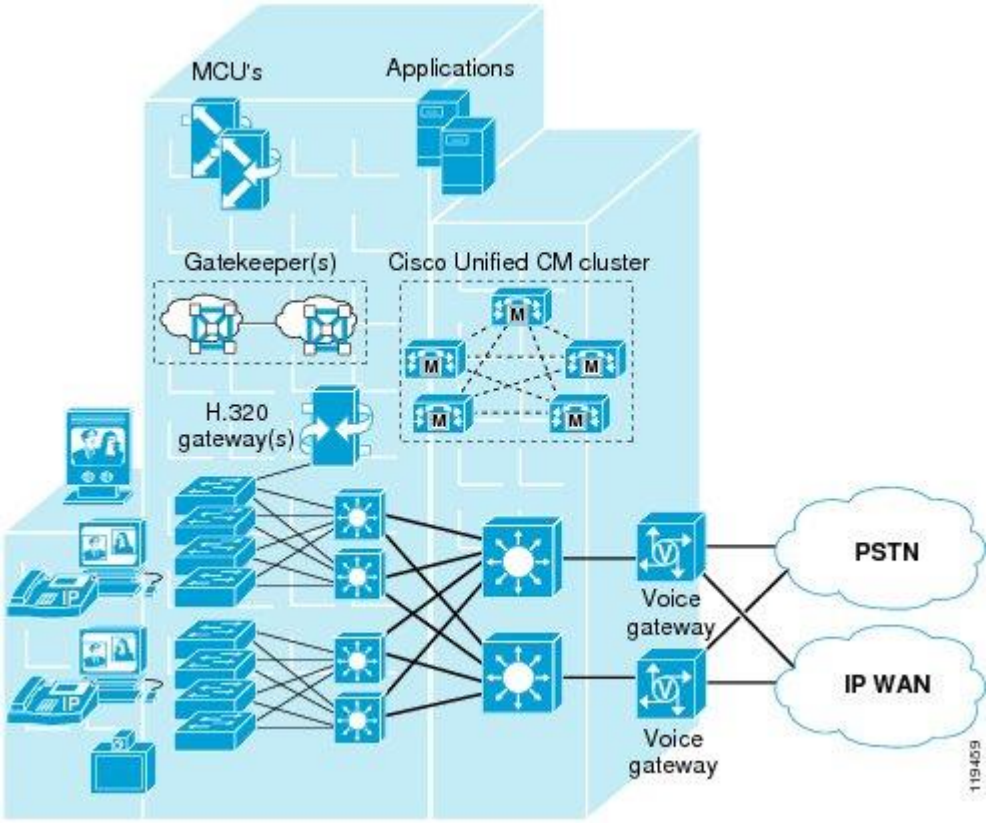

Figure 9. Single Site Deployment [7]

2.1.10. Multisite with Centralized Call Processing

The model for a multisite deployment with centralized call processing consists of a single call processing agent cluster that provides services for many remote sites and uses the IP WAN to transport Unified Communications traffic between the sites. The IP WAN also carries call control signaling between the central site and the remote sites. Figure 10 illustrates a typical centralized call processing deployment, with a Unified CM cluster as the call processing agent at the central site and an IP WAN with QoS enabled to connect all

the sites. The remote sites rely on the centralized Unified CM cluster to handle their call processing. Applications such as voicemail, presence servers, interactive voice response (IVR) systems, and so forth, are typically centralized as well to reduce the overall costs of administration and maintenance.

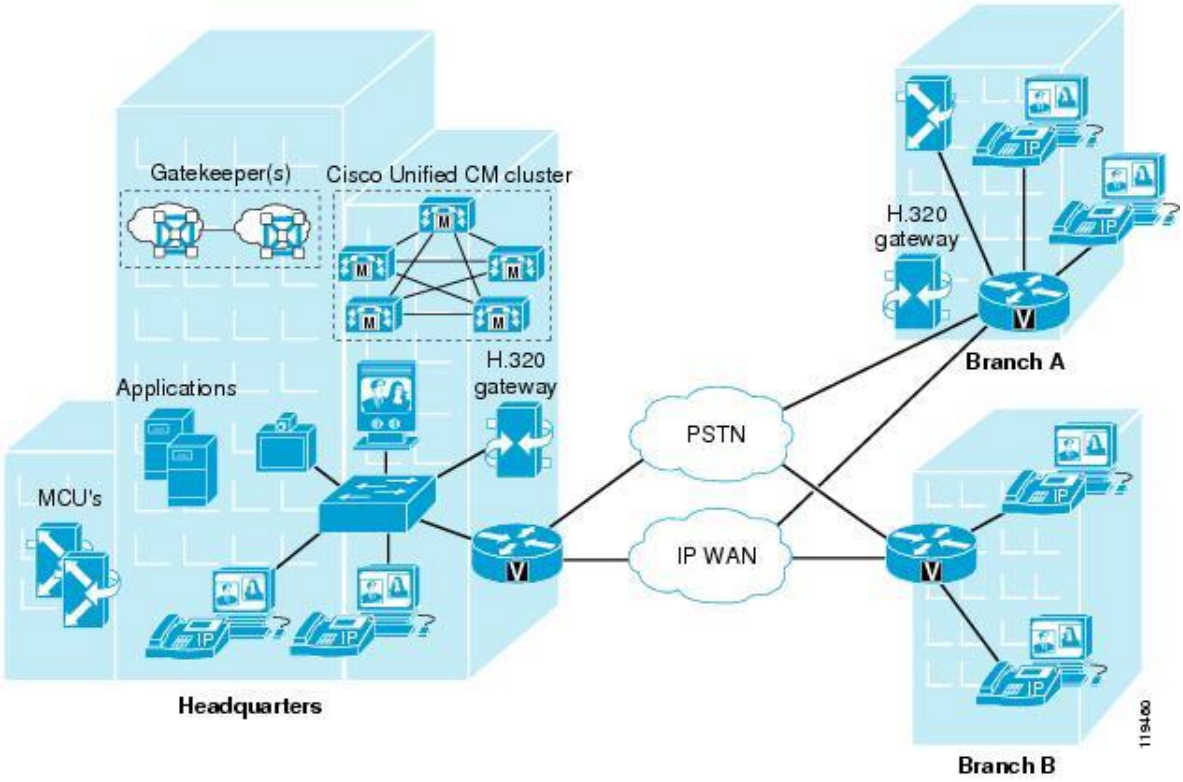

Figure 10. Multisite Deployment with Centralized Call Processing [7]

Routers that reside at the WAN edges require quality of service (QoS) mechanisms, such as priority queuing and traffic shaping, to protect the voice traffic from the data traffic across the WAN, where bandwidth is typically scarce. In addition, a call admission control scheme is needed to avoid oversubscribing the WAN links with voice traffic and deteriorating the quality of established calls. For centralized call processing deployments, locations (static or RSVP-enabled) configured within Unified CM provide call admission control. [7]

The multisite model with centralized call processing has the following design characteristics: [7]

- Single Unified CM cluster.

- Maximum of 30,000 configured and registered Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP) IP phones or SCCP video endpoints per cluster.
- Maximum of 2000 locations or branch sites per Unified CM cluster.
- Maximum of 2,100 gateways and trunks (that is, the total number of H.323 gateways, H.323 trunks, digital MGCP devices, and SIP trunks) per Unified CM cluster.
- PSTN for all external calls.
- Digital signal processor (DSP) resources for conferencing, transcoding, and media termination point (MTP).
- Voicemail, unified messaging, Cisco Unified Presence, audio and video components.
- Capability to integrate with legacy private branch exchange (PBX) and voicemail systems.
- H.323 clients, MCUs, and H.323/H.320 gateways that require a gatekeeper to place calls must register with a Cisco IOS Gatekeeper (Cisco IOS Release 12.3(8)T or greater). Unified CM then uses an H.323 trunk to integrate with the gatekeeper and provide call routing and bandwidth management services for the H.323 devices registered to it. Multiple Cisco IOS Gatekeepers may be used to provide redundancy.
- MCU resources are required for multipoint video conferencing. Depending on conferencing requirements, these resources may be either SCCP or H.323, or both, and may all be located at the central site or may be distributed to the remote sites if local conferencing resources are required.
- H.323/H.320 video gateways are needed to communicate with H.320 videoconferencing devices on the public ISDN network. These gateways may all be located at the central site or may be distributed to the remote sites if local ISDN access is required.
- High-bandwidth audio (for example, G.711, G.722, or Cisco Wideband Audio) between devices in the same site, and low-bandwidth audio (for example, G.729 or G.728) between devices in different sites.
- High-bandwidth video (for example, 384 kbps or greater) between devices in the same site, and low-bandwidth video (for example, 128 kbps) between devices at different sites. The Cisco Unified Video Advantage Wideband Codec, operating at 7 Mbps, is recommended only for calls between devices at the same site.
- Minimum of 768 kbps or greater WAN link speeds. Video is not recommended on WAN connections that operate at speeds lower than 768 kbps.

- Unified CM locations (static or RSVP-enabled) provide call admission control, and automated alternate routing (AAR) is also supported for video calls.
- Survivable Remote Site Telephony (SRST) versions 4.0 and higher support video. However, versions of SRST prior to 4.0 do not support video, and SCCP video endpoints located at remote sites become audio-only devices if the WAN connection fails.

2.1.11. Multisite with Distributed Call Processing

The model for a multisite deployment with distributed call processing consists of multiple independent sites, each with its own call processing agent cluster connected to an IP WAN that carries voice traffic between the distributed sites. Figure 11 illustrates a typical distributed call processing deployment.

A multisite deployment with distributed call processing has many of the same requirements as a single site or a multisite deployment with centralized call processing. Follow the best practices from these other models in addition to the ones listed here for the distributed call processing model. (See Single Site, and Multisite with Centralized Call Processing.)

Gatekeeper or Session Initiation Protocol (SIP) proxy servers are among the key elements in multisite distributed call processing deployments. They each provide dial plan resolution, with the gatekeeper also providing call admission control. A gatekeeper is an H.323 device that provides call admission control and E.164 dial plan resolution.

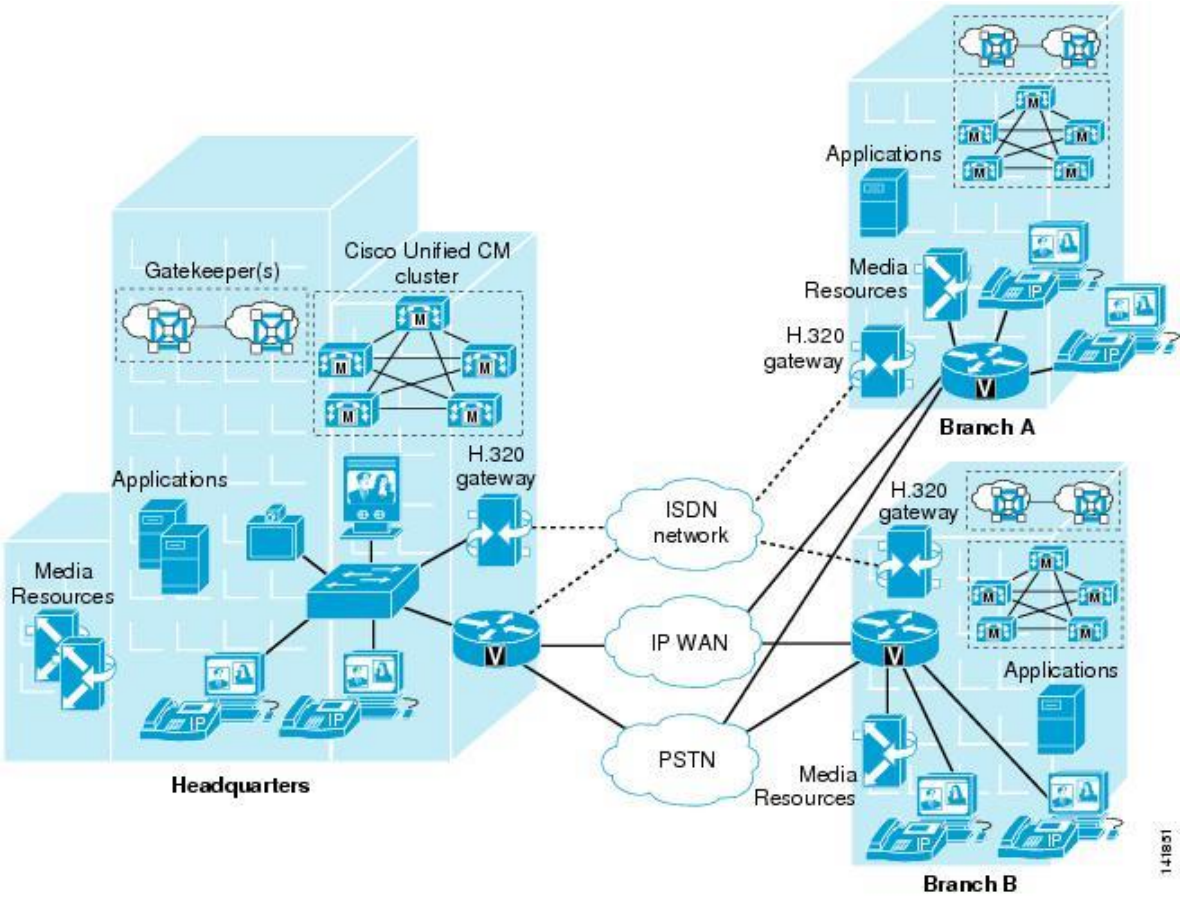

Figure 11. Multisite Deployment with Distributed Call Processing [7]

The multisite model with distributed call processing has the following design characteristics: [7]

- Maximum of 30,000 configured and registered Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP) IP phones or SCCP video endpoints per cluster.
- Maximum of 2,100 gateways and trunks (that is, the total number of H.323 gateways, H.323 trunks, digital MGCP devices, and SIP trunks) per Unified CM cluster.
- PSTN for all external calls.
- Digital signal processor (DSP) resources for conferencing, transcoding, and media termination point (MTP).
- Voicemail, unified messaging, and Cisco Unified Presence components.

- Capability to integrate with legacy private branch exchange (PBX) and voicemail systems.
- H.323 clients, MCUs, and H.323/H.320 gateways that require a gatekeeper to place calls must register with a Cisco IOS Gatekeeper (Cisco IOS Release 12.3(8)T or greater). Unified CM then uses an H.323 trunk to integrate with the gatekeeper and provide call routing and bandwidth management services for the H.323 devices registered to it. Multiple Cisco IOS Gatekeepers may be used to provide redundancy. Cisco IOS Gatekeepers may also be used to provide call routing and bandwidth management between the distributed Unified CM clusters. In most situations, Cisco recommends that each Unified CM cluster have its own set of endpoint gatekeepers and that a separate set of gatekeepers be used to manage the intercluster calls. It is possible in some circumstances to use the same set of gatekeepers for both functions, depending on the size of the network, complexity of the dial plan, and so forth. (For details, see Gatekeepers.)
- MCU resources are required in each cluster for multipoint video conferencing. Depending on conferencing requirements, these resources may be either SCCP or H.323, or both, and may all be located at the regional sites or may be distributed to the remote sites of each cluster if local conferencing resources are required.
- H.323/H.320 video gateways are needed to communicate with H.320 videoconferencing devices on the public ISDN network. These gateways may all be located at the regional sites or may be distributed to the remote sites of each cluster if local ISDN access is required.
- High-bandwidth audio (for example, G.711, G.722, or Cisco Wideband Audio) between devices in the same site, but low-bandwidth audio (for example, G.729 or G.728) between devices in different sites.
- High-bandwidth video (for example, 384 kbps or greater) between devices in the same site, but low-bandwidth video (for example, 128 kbps) between devices at different sites. The Cisco Unified Video Advantage Wideband Codec, operating at 7 Mbps, is recommended only for calls between devices at the same site. Note that the Cisco VT Camera Wideband Video Codec is not supported over intercluster trunks.
- Minimum of 768 kbps or greater WAN link speeds. Video is not recommended on WAN connections that operate at speeds lower than 768 kbps.
- Call admission control is provided by Unified CM locations for calls between sites controlled by the same Unified CM cluster, and by the Cisco IOS Gatekeeper for calls between Unified CM clusters (that is, intercluster trunks). Automated alternate routing (AAR) is also supported for both intra-cluster and inter-cluster video calls.

An IP WAN interconnects all the distributed call processing sites. Typically, the PSTN serves as a backup connection between the sites in case the IP WAN connection fails or does not have any more available bandwidth. A site connected only through the PSTN is a standalone site and is not covered by the distributed call processing model.

Connectivity options for the IP WAN include: [7]

- Leased lines
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- ATM and Frame Relay Service Inter-Working (SIW)
- Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN)
- Voice and Video Enabled IP Security Protocol (IPSec) VPN (V3PN) [Ref 7]

2.2. PSTN Overview

2.2.1. PSTN

The PSTN is the oldest and hitherto largest telecommunications network in existence. For years, the PSTN has been the only network available for telephony, but newer technologies allow people to communicate via mobile and IP telephony networks.

The PSTN has a few characteristics: [11]

- Analog access, 300-400 Hz.
- Circuit-switched duplex connection.
- Switched bandwidth, 64 Kbit/s or 300-3400 Hz for analog exchanges.
- Immobility (very limited mobility).
- Many functions in common with another bearer network, N-ISDN.

Started in 1876, the PSTN has undergone a complete technical transformation. Even factors such as network structure and network utilization have changed completely. The most significant difference between the PSTN that exist today and the PSTN before 1960's is that current network is digital, which has been an ongoing process for years in the majority

of today's countries. Before when conversions between analog and digital were performed, it could result in problems with set-up time and irregular transmission quality. The limited bandwidth of the PSTN is a bottleneck when it comes to video and multimedia services. [11]

Switching

PSTN nodes can be subdivided into three main categories: local exchanges, transit exchanges, international exchanges. Local exchanges are used for the connection of subscribers. Transit exchanges switch traffic within and between different geographical areas. International exchanges, and other gateway-type exchanges, switch traffic to telecommunications networks that belong to other operators.

The primary task for a local exchange is to switch call from one subscriber to another in the same exchange, to switch calls to subscribers outside the local exchange and to charge for calls and services that are performed within the local exchange. [11]

In the traditional PSTN exchange hierarchy, traffic has been routed to direct links (highcongestion routes) and if these links have been busy, the next higher level in the hierarchy (low-congestion routes) has been used. New routing functions are now available thanks to SS7 and the Telephone User Part (TUP) protocol. One example is the possibility of preventing rerouting further on in the network and instead trying an alternative route all the way from the originating exchange. Another example is placing subscribers in different categories, emergency services, could have access to a number of alternative routes or even routes designated for their exclusive use. [11]

2.2.2. SS7

Signaling refers to the exchange of information between call components required to provide and maintain service [5]. Dialing digits, providing dial tone, sending a call-waiting tone are examples of signaling between a caller and the telephony network. SS7 is a protocol that helps telephone networks exchange information and it uses out-of-band signaling, which refers to signaling that does not take place over the same path as the conversation. Out-ofband signaling creates a separate digital channel for exchanging signaling information, which is called a signaling link. This link is used to transport all

necessary signaling messages between nodes. When a call is made the dialed digits, trunk selected, and other significant information are sent between switches using their signaling links, rather than the trunks which will ultimately carry the conversation. [12]

The SS7 is held together by a digital switch known as a Signaling Transfer Point (STP), and the main tasks of the STP are to examine the destination of the messages it receives, check with a routing table, and send the messages on their way by using the links that are determined in the routing tables. STP may have a number of different links to an end user of the network therefore it is necessary with routing, because the preferred way of routing is declared in the routing tables. [12]

2.2.3. PSTN Security

The PSTN network does not provide any cryptographic mechanisms to protect the speech channels from intruders. Physical access is needed to perform intrusion attempts. For intruders that possess specific resources can have the possibility to gain access to the physical lines, for example in cross-connects or concentrators. [13]

When the PSTN was developed there were no thoughts of end-to-end user data security. The authentication of the subscribers is based on physical wiring, resulting in that no authentication, integrity or confidentiality exists for voice, data or signaling. However, availability and non-repudiation are guaranteed. It would require physical resources to prevent authorized users from gaining access to the network and non-repudiation is provided through the statistical information held by the supplier. There are vulnerabilities with the network, but since the physical security is good and the operators are trustworthy organizations, the threats are disregarded. [13]

3. Methodology

For the research of this thesis, the case study methodology is most suited methodology. The information gathering phase of the case studies will be completed through document study and a literature review.

The main part of the research for the thesis will be based on the Case Study. In the thesis we have also used comparatives methodology for the purpose of analyzing various technologies and techniques for IP Telephony.

Extensive secondary research will be conducted. Acknowledged texts, standards documents, industry periodicals and white papers, analysts' reports and conference journals will be referenced. A critical analysis of the secondary research is applied in the formulation of the roadmap and framework proposed.

The data for this research will be collected from statements about privacy policy, acceptable use policy, terms of use and service level agreements available from the websites of the equipment vendors. In case of any such information missing from the websites, similar information will be sought via internet research of whitepapers, press releases and news articles of IP Telephony in different IT magazines and Journals.

4. Case Study

4.1. Traditional and IP Telephony Comparison

This The comparison consists of a qualitative theoretical analysis that compares IP telephony with traditional telephony (PSTN) to evaluate the stated hypothesis. The comparison will be divided into two different areas, general and security aspects. The first area will describe the differences from a general approach of the two technologies, IP telephony and PSTN. The second area, the security aspects is the essential part of the comparison. The security aspects are divided into two sub areas, security services and security vulnerabilities. [8]

4.2. Methods for comparison

The authors of this thesis have analyzed collected information from literature and articles in order to distinguish the criteria relevant for this comparison. The reason for dividing the comparison into two different areas is the evaluation between the two technologies becomes more perspicuous. [8]

4.3. General aspects

The general aspects will describe the basic differences between a PSTN and an IP network.

4.3.1. Packet switched / Circuit switched

The PSTN is a circuit-switched network that communicates via a two-way channel. The channel is open in both directions during the entire phone call. Packet-switching is used by networks based on the destination addresses that all packets contain. The advantage with packet-switching is that the packets can transfer both data and multimedia, such as voice. This type of communication between sender and receiver is known as connectionless, i.e. one-way channel, which is the type that is used in IP networks. [8]

4.3.2. Transport of information

The PSTN is a closed network that uses the protocol SS7 to transfer voice. The IP network is open and uses protocols, like TCP and UDP that are built on the IP technology to transfer voice packets. Both the protocols H.323 and SIP can use TCP or UDP, but H.323 prefers TCP and UDP is preferred by SIP. The IP telephony technology is able to adapt to the bandwidth when either voice, data or video are transferred. The PSTN network does not have this ability, the bandwidth is fixed, i.e. 64kbit/s. [8]

4.3.3. Quality of service

In circuit switched networks QoS refers to the ability to initiate a call to another party. This is guaranteed with the PSTN. QoS in a packet-switched network refers to the probability of a packet passing between two nodes in the network. IP telephony has to deal with problems such as delay, packet loss and bandwidth, since IP networks are developed for data transfers and not voice transfers. Therefore, IP telephony does not ensure that the packets are delivered in a sequential order and this may cause problems like buffer overflows because the router is waiting for lost packets and the other packets have to wait. This causes the router to be over loaded. [8]

General Aspects

	PSTN	**H.323**	**SIP**
Packet/Circuit switched	Circuit-switched	Packet-switched	Packet-switched
Transport of Information	SS7	Mostly TCP	Mostly UDP
Quality of Service	Guaranteed	Not Guaranteed	Not Guaranteed

4.4. Security aspects

The security area is split into two parts, security services and security vulnerabilities. The security services consist of five terms, which are defined in the section 2.2 in this thesis. These five terms are essential for the basis of security in IP telephony. The security vulnerabilities describe the threats that exist when transmitting voice over IP networks and the threats against traditional telephone networks. [9]

4.4.1. Security services

Authentication

The SS7 protocol which PSTN uses has no authentication, it is based on physical wiring, i.e. it only checks if the phone number called from and the number that the caller wants to contact are accepted. For VoIP the authentication procedure for H.323 and SIP are similar. H.323 uses either symmetric encryption or subscription based authentication, which uses either symmetric or asymmetric encryption. When using the first type for authentication no previous communications between two entities are needed, but the subscription based requires key exchange before the actual authentication can be performed. The SIP protocol can use three types for authentication, basic, digest or PGP (Pretty Good Privacy) authentication. Basic authentication involves username and password for authentication and the digest is checksum based. The last type for authentication, PGP requires the exchange of digital certificates. [9]

Integrity

The integrity check in PSTN and the SS7 protocol consists of a physical control or a digital signal to assure that the phone number (userID) and the phone jack concur. In VoIP, the protocols H.323 and SIP use a Message Authentication Check (MAC) to ensure that the messages have not been modified during the transfer. The integrity checksums are encrypted to protect the packet's payload, the content of the message (voice). It is only the header of the packet, or parts of header, that needs to be encrypted and this reduces the transfer process. Voice is transmitted in real-time and since only the header is encrypted, the delay and jitter problems decreases. [9]

Confidentiality

The PSTN do not have any encryption for the transferred voice messages, but since the network is closed, there is no need for encrypting the voice traffic and confidentiality is

provided because of this. The two protocols for IP telephony use different encryption techniques to ensure that if the data are intercepted, it cannot be viewed by unauthorized users that do not have the appropriate key to decrypt the intercepted data. The protocols H.323 and SIP use different kinds of asymmetric or symmetric ciphers to encrypt the voice messages, for example H.323 can use the Diffie -Hellman algorithm and SIP has usually the DES algorithm as default, but both can use IPSec. [9]

Non-repudiation

The non-repudiation service in the PSTN is provided through phone call specification from the vendor, e.g. Telia, and this is a proof of that the call to the recipient was performed from the sender. Since H.323 and SIP use public -private key encryption methods, these can be used to proof that the message was actually sent by the proposed sender. The caller has to encrypt and verify the call with his/her private key and the public key of the intended recipient. [9]

Availability

Since the PSTN is less dependent on electricity, there should not be any problems for user to be guaranteed availability, the only thing that could prevent authorized users from accessing the network would be someone directly cutting the wires connected to the user's phone or misuse of the signaling. The existence of IP telephony is dependent on electricity to be able to function, if a power failure occurs the users of the IP telephony network are not guaranteed availability. [9]

Security Services

	PSTN	**H.323**	**SIP**
Authentication	Physical	Symmetric Encryption	Basic
		Subscription Based	Digest
			PGP
Integrity	Physical	Msg Authentication Check	Msg Authentication Check
Confidentiality	Closed Network	Encryption	Encryption
Non-repudiation	Call Specification	e.g PKI	e.g PKI
Availability	Not electricity dependent	Electricity dependent	Electricity dependent

4.4.2. Security vulnerabilities

Eavesdropping

The PSTN is protected from these kinds of attacks and the integrity and confidentiality of the phone conversation by physical separation (isolation) between the data network and the voice network. There are possibilities for malicious parties to decode and eavesdrop on conversations, but it would require specific resources. Eavesdropping is a threat to VoIP, because the technology uses the IP protocol and the format of the packets are well-known. This can result in that the packets are targets for manipulation. H.323 and SIP uses the Real Time Protocol (RTP) for voice transmission and this protocol does not provide any form of confidentiality. Anyone that are able to intercept unencrypted RTP packets between two communicating end-point can eavesdrop on the conversations. [10]

Theft of service

Masquerade and free calls are theft of services types that exists in the PSTN network. Masquerading refers to that the caller or the called party may not be who he/she claims to be. It is also possible with the right resources to hack the signaling system, to be able to perform phone calls by using another person's identity. When using VoIP it is easy to impersonate an authorized user, i.e. masquerading. The reason for this is that user identities can be authenticated via MAC addresses and IP number and MAC addresses are known to be targets of spoofing. It is the transportation protocols TCP, UDP and RTP that control if the voice packets are transferred or not. Either H.323 or SIP can influence this control. [10]

Denial of service

The PSTN is protected against Denial of Service (DoS) attacks, because to be able to perform this kind of attack you need to physically remove the telephony from the wall jack or damage the wire connecting the telephone from the server. The protocols H.323 and SIP are vulnerable for denial of service attacks because they use the IP network, which means that voice and data are transmitted via the same network and are therefore sensitive for the same type of attacks. [10]

Security vulnerabilities

	PSTN	**H.323**	**SIP**
Eavesdropping	Physical access	Possible	Possible
Theft of service	Hack signaling system	Spoofing MAC addresses	Spoofing MAC addresses
Denial of Service	Physical access	Vulnerable	Vulnerable

4.5. Results

The results from the performed comparison between traditional (PSTN) and IP telephony are stated in this chapter, the aspects are divided into the same areas as in the comparison, general and security. This chapter will end with a table to give the reader an overview of the results.

4.5.1. General aspects

- **Packet switched/circuit switched –** Packet switched is preferred since the packets are compressed to decrease the use of bandwidth. The bandwidths for circuit switched networks are always fixed and do not have the possibility to adapt the bandwidth after what type of transfers, i.e. voice, data or video. The communication channel for circuit switched is open during the entire call, which results in that the bandwidth resources are occupied even when no voice transfers are made.
- **Transport protocols** – SS7 more complex than TCP/UDP. The SS7 protocol is developed for PSTN to transfer voice and signals. The transportation protocols used for IP networks TCP and UDP were originally developed for data transfers, the signaling is handled by the protocols SIP and H.323. Since the SS7 protocol is used for both voice and signaling transfers the complexity increases, in comparison to TCP and UDP that only need to handle the voice transfers.
- **Quality of Service** – The quality of service for PSTN is guaranteed, but not for IP telephony since it is dependent on bandwidth, delay and packet loss. Since these factors may cause problems it will therefore impact the quality of service.

4.5.2. Security aspects

Security services

- **Authentication** – Better authentication for IP networks, since the subscriber needs to authenticate him/her for access to the network and when placing calls. The subscribers of a PSTN only have to authenticate themselves via their phone numbers (UserIDs).
- **Integrity** – Advantage IP telephony, because it encrypts the integrity checksums to protect the packets payload from modification. PSTN does not provide for any encryption, which may result in modified voice transfers.
- **Confidentiality** – IP Telephony uses encryption techniques to prevent from intrusion attempts to the network. Since the PSTN do not use any encryption techniques, no confidentiality is provided.
- **Non-repudiation** – This security service is provided by the PSTN, because the suppliers keep statistics for all subscribers. For IP telephony the risks for theft of service attacks and denia l of service attacks can cause problems with modified or lost audits.
- **Availability** – Advantage PSTN because physical access is needed and there is a low dependence on electricity. The downtime for the PSTN is of no significance and the availability for authenticated subscribers is almost guaranteed, as long as no natural disasters occur.

Security vulnerabilities

- **Eavesdropping –** It easier to eavesdrop on IP telephony networks, but it is more difficult to retrieve the actual payload. Gaining access to the PSTN network requires special resources, but one's you are in everything can be eavesdropped in clear.
- **Theft of Service** – This vulnerability causes more problems due to IP telephony networks because it is easier to gain access by sniffing/spoofing.
- **Denial of Service (DoS)** – IP telephony networks are more vulnerable for denial of service attacks, because the two protocols SIP and H.323 have weaknesses. To be able to perform denial of service against PSTN networks it would require physical access.

General comments on the security aspects

- More threats against IP networks, because it's use of the IP protocol. The IP protocol is "open" and the vulnerabilities related to the network are several [See 4.4.2 Security vulnerabilities].

- PSTN is more "secure" because it is a closed network. The belief that the network can be secure as long as no unauthorized are allowed to find out anything about its internal mechanisms, this is referred to as security by obscurity.

Results from the comparison

	IP Telephony	**PSTN**
General Aspects		
Packet switched or circuit switched	Packet switched are preferred	Circuit switched
Transport protocols	TCP, UDP	SS7 more complex
Quality of service	Not guaranteed	Guaranteed
Security aspects		
Authentication	Provided by H.323 and SIP	Physical authentication
Integrity	Uses encryption	No use of encryption
Confidentiality	Uses encryption	No use of encryption
Non-repudiation	Provided through RTCP	Provided
Availability	Electricity and functioning computer environment dependent	Always guaranteed
Security vulnerabilities		

Eavesdropping	High risk factor	Risk factor
Theft of Service	Risk factor	High risk factor
Denial of Service	High risk factor	Low risk factor

CONCLUSION

The stated hypothesis that was evaluated in the thesis has been found verified. The reason for this is that IP telephony maintains the same standard as PSTN. IP telephony fulfills the requirements for the security services through authentication, integrity and confidentiality.

There are number of authentication methods that can be used to access to the network and for voice transfers. Integrity and confidentiality is provided for the IP telephony network by usage of encryption techniques to protect the voice packets from being modified or intercepted.

There are problems when it comes to the security services non-repudiation and availability due to the integration of several IP telephony networks that are provided by different suppliers, the technology's dependence on electricity and a functioning computer environment for authorized subscribers.

The traditional telephony network PSTN does not deal with problems concerning non-repudiation and availability. The other security services that IP telephony provides for are not fulfilled by the PSTN, but since the network is closed the security services are of no concern. Numbers of requirements for security services that are fulfilled by the IP telephony technology outweigh the services that are not. This point out the advantages for IP telephony compared to the PSTN, since the protocols H.323 and SIP can provide encryption of voice and stronger authentication than PSTN.

Although there are more risk factors related to IP telephony. The risks are also of concern for PSTN but it requires more resources for gaining access to perform various attacks. The IP telephony network may be a pleasant target for malicious parties, but the use of encryption makes it more difficult to eavesdrop on conversations. Eavesdropping and denial of service are problems that are connected to transfers in the IP network. By applying a certain level of security throughout the entire IP network and take precautions against possible threats, the security for IP telephony services will be included.

To conclude the thesis, IP telephony can be a valuable future investment especially for organizations with a large number of employees, because the administration costs will decrease when integrating the IP telephony technology with IP networks and the charging of phone calls will also decrease.

5. References

[1] *IP telephony design & implementation Issues- William E. Witowsky (2004) date accessed (September 2013).*

[2] *Voice over IP: Protocols & Standards- Rakesh Arora, date accessed (September 2013).*

[3] *H.323 Tutorial- Trillium Digital Systems, date accessed (September 2013).*

[4] *ITU-T Recommendation H.323, Packet-Based Multimedia Communication Systems, date accessed (September 2013).*

[5] *Migrating Corporate voice traffic to the Data network- Quintum Technologies Inc, date accessed (September 2013).*

[6] *Cisco Voice over IP Third Edition – Kevin Wallace, date accessed (June 2013).*

[7] *Unified Communication Deployment Models - http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/models.html#wp1043564 , date accessed (September 2013).*

[8] *Huovinen, Niu, "IP Telephony" http://www.tml.hut.fi/Opinnot/Tik-110.551/1999/papers/04IPTelephony/voip.html, date accessed (July 2013).*

[9] *Newman, TMCnet.com, "Security for H.323-based Telephony" ,May 1998 http://www.tmcnet.com/articles/ctimag/0598/nettelephony001.htm, date accessed (July 2013).*

[10] *Klein, "Security Analysis: Traditional Telephony and IP telephony", 2003, http://www.giac.org/practical/GSEC/Alan_Klein_GSEC.pdf , date accessed (July 2013).*

[11] *Ericsson & Telia, "Understanding Tele communication 2", Studentlitteratur, Lund, Sweden, date accessed (July 2013).*

[12] *International Engingeering Concortium, "Signaling System 7 (SS7)", http://www.iec.org/online/tutorials/ss7/, date accessed (September 2013).*

[13] *Isomaki, "Security in the Traditional Telecommunications Networks and in the Internet", November 1999, http://www.tml.hut.fi/Opinnot/Tik- , date accessed (September 2013).*

[14] *IP Telephony Deployment models http://www.cisco.com/cisco/web/docs/iam/unified/ipt611/IP_Telephony_Deployment_Models.html , date accessed (July 2013).*

[15] *CUCM 6.1 SRND http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/srnd/design/guide/models.html date accessed (September 2013).*