MINISTERE DE L'ENSEIGNEMENT SUPERIEURE

UNIVERSITE DE YAOUNDE I

ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE

DEPARTEMENT DES GENIES ELECTRIQUE ET DES TELECOMMUNICATIONS

MINISTRY OF HIGHER EDUCATION

THE UNIVERSITY OF YAOUNDE I

NATIONAL ADVANCED SCHOOL OF ENGINEERING

DEPARTMENT OF ELECTRICAL AND TELECOMMUNICATIONS ENGINEERING

DESIGN OF A VIDEO CONFERENCING NETWORK AT THE NATIONAL HYDROCARBONS CORPORATION (SNH), Case Study: Headquarter Extension Building Project

END OF COURSE DISSERTATION

Presented and defended by**:**

EPIE ETONE KINGSLEY

In partial fulfilment of the requirements for the award of a

Master's Degree in Telecommunications Engineering

UNDER THE SUPERVISION OF**:**

TALLA TANKAM Narcisse, Lecturer, E.N.S.P

Before the Jury composed of**:**

- **President: BOUETOU Thomas, MC, ENSP**
- **Academic Supervisor: TALLA TANKAM Narcisse, Lecturer, ENSP**
- **Examiner: LELE Chrislin, Lecturer, ENSP**
- **Professional Supervisor: SANGO Paul Roger, Engineer, SNH**

Defended on July 25th, 2016

2015-2016 ACADEMIC YEAR

DEDICATION

I thank

The LORD JESUS CHRIST in whom I have life, strength, and wisdom, for making the achievement of this work possible.

I dedicate this work:

To my late father Mark ETONE and my mother ETONE Loveline; this is the result of their efforts and relentless sacrifices made for my education.

To my Pastor Bishop FON S.M.M GHOGOMU,

To my brothers: NGWESE ETONE Edmond and ECUBE Wilslow ETONE

And my sister Campbell ETONE NGOMUSI for their advice, support and attention.

To all my coaches, friends and acquaintances

ACKNOWLEDGEMENTS

This document is the fruit of the combined efforts of several individuals who contributed either directly or indirectly to its elaboration. It's therefore with sincere and heartfelt gratitude that I thank:

- **Pr. Martin KOM**, Head of Department of electrical and telecommunications engineer department, for his efforts in maintaining the quality of teaching in this department.
- **Pr. BOUETOU Thomas**, for kindly accepting to preside the jury of this defence. I also thank him for his patience and goodwill in transmitting his knowledge
- **Dr TALLA TANKAM Narcisse**, my academic supervisor and teacher for accepting to oversee my end of course project. I equally thank him for constantly encouraging and boosting me.
- **Dr LELE Chrislin**, lecturer at the National Advanced School of Engineering, Yaoundé, for accepting to be a member of the jury of this defence.
- **Engineer SANGO Paul Roger** my professional Supervisor, for all the help and contributions he made to make of this work a success.
- **Engineer NJOCK Séverin** executive at SNH, for his endless support throughout my internship. Not forgetting the entire SNH staff for their support.
- The entire CFAO TECHNOLOGIES staff and particularly Mr. Jonathan Roger TENE for his enormous help during my internship.
- The entire ENGIE (GDF SUEZ) CAMEROON staff and particularly **Dr. NOLABI Raoul** for his enormous help during my internship.
- All my Aunties and Uncles for the wonderful support they gave me.
- All my "long time" friends: F. Amstrong, Talla N. Yannick, Nchanji Joshua, Ndongo Daniel, N. Godlove, S. Nancy, Ndongo. Ida. Having you is a plus.
- All the leaders of the United Crusade Team for Jesus Christ (UNITEJC). I think of Rev. Annick Ghogomu, Rev. Nforgwei D., Mr. EPEH Moses, E. Dolly and Pastor Odile.

- My fellow UNITEJC youths and the entire congregation.
- All my classmates and friends of the 2015 batch of Polytechnique. Gwagsi B., Manior W., Nganyu D., Kongnso W., Fonyuy Cedric, Nfongang G. etc. it was a nice time spent together.

GLOSSARY

Abbreviation	Meaning
3G	Third Generation
4G	Fourth Generation
ADSL	Asynchronous Digital Subscriber Line
AES	Advanced Encryption Standard
AGC	Automatic Gain Control
a.k.a	Also Known As
API	Application Programming Interface
AVC	Advanced Video Coding
B2B	Business to Business
BE6K	Business Edition 6000
BFCP	Binary Flow Control Protocol
BYOD	Bring Your Own Device
CAPEX	Capital Expenditure
CIF	Common Intermediate Format
CODEC	Compression/Decompression
DGA	Division of General Affairs
DiffServ	Differentiated Services
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Server
DVD	Digital Versatile Disc
DVI	Digital Visual Interface
EITI	Extracted Industries Transparency Initiative
Gbps	Gigabit per second
GUI	Graphical User Interface
HD	High Definition or High Density
HDMI	High-Definition Multimedia Interface
HTML	HyperText Markup Language

HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
HVAC	Heating, Ventilation and Air Conditioning
IEEE	Institute of Electrical and Electronics Engineering
IM	Instant Messaging
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISDN	Integrated Digital Services Network
ISO	International Standardization Organisation
ITU	International Telecommunications Union
Kbps	Kilobit per second
LAN	Local Area Network
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
M2M	Machine to machine
MACD	Moves, Adds, Changes, and Deletions
Mbps	Megabit per second
MCU	Multipoint Control Unit
MD	Medium Density
MPEG4	Moving Picture Experts Group version 4
NAT	Network Address Translation
PBX	Private Automatic Branch eXchange
PC	Personal Computer
PCM	Pulse Code Modulation
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
PTZ	Pan, Tilt, and Zoom
QCIF	Quarter Common Intermediate Format
QoS	Quality of Service
QVGA	Quarter Video Graphics Array
RJ45	Registered Jack 45

RH	Relative Humidity
RTCP	Real-time Transmission Control Protocol
RTP	Real-time Transmission Protocol
SCP	Secure Copy
SD	Standard Definition
SDP	Session Description Protocol
SDSL	Symmetric Digital Subscriber Line
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SQCIF	Semi Quarter Common Intermediate Format
SSH	Secure Shell
SVC	Scalable Video Coding
TAC	Technical Assistance Center
TCP	Transmission Control Protocol
ToS	Type of Service
TV	Television
UC	Unified communications
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UMTS	Universal Mobile Telecommunications System
URI	Universal Resource Identifier
US	United States
VC	Video Conference
VHF	Very High Frequency
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
XML	eXtensible Markup Language

ABSTRACT

In today's complex economic environment, many companies especially the National Hydrocarbons Corporation (best known in French as SNH) are under extreme pressure and must optimize their employee's productivity, maximize their revenue and forge very close relationships within their organization and with business partners.

Because expenditures are always a sensitive issue and SNH constantly seeks to optimize technology used in order to meet budgets while giving their employees the means to do more with fewer resources, SNH is thus faced with the problem of not only connecting their different branches and both local like international partners together but equally reduce the cost of doing so. This with objective to reduce the risk especially of accidents employees take each time they leave for missions to different work sites, expenditures (fuel, car used, trainings, flight tickets, hotel and restaurant bills, missions fees for staff, drivers) on mission orders each time technicians have to be displaced to the various sites even for minute problems, to protect the environment since a reduction in employee displacement, reduces the emission pollutant from vehicles, planes etc. and finally to be in constant and direct link with partners without the need to pass through a third party like is presently the case.

To respond to these pre-occupations we first assessed the present state of the network infrastructure and then proposed solutions with some recommendations on how to proceed with setting up a VC network. Nevertheless, this proposal wasn't enough for immediate implementation. We therefore had to proceed with the "**DESIGN OF A VIDEO CONFERENCING NETWORK AT THE NATIONAL HYDROCARBONS CORPORATION (SNH), Case Study: SNH Headquarter Extension Building Project**". We attempted to present a topological design of the network.

We concluded the first part by evaluating the network requirements and equipment needed per site to have an overall estimate of the cost of implementing the project. In the second part of our work we therefore examined the security risks and threats and proposed measures to combat these threats. We then defined the security policies aimed at ensuring smooth streaming with integrity.

RESUME

Dans l'environnement économique complexe d'aujourd'hui, de nombreuses entreprises en particulier la Société nationale des hydrocarbures (SNH) sont sous une pression extrême et doivent optimiser la productivité de leurs employés, maximiser leurs revenus et de forger des relations très étroites au sein de leur organisation et avec les partenaires commerciaux.

Parce que les dépenses sont toujours une question sensible et la SNH cherche constamment à optimiser les technologies afin de répondre aux budgets tout en donnant à leurs employés les moyens de faire plus avec moins de ressources, la SNH fait face à un problème majeur qui est celui non seulement de connecté ses différentes sites entre eux et avec ses partenaire mais aussi de réduire le budget actuellement alloué pour cela. Ceci avec l'objectif de réduire le risque particulier d'accidents que prennent les employés chaque fois qu'ils sortent pour des missions sur différents sites de travail, les dépenses (carburant, voiture utilisés, formations, billets d'avion, factures d'hôtels et restaurants, frais de missions pour le personnel) sur les ordres de mission chaque fois que des techniciens doivent se déplacés vers les différents sites même pour des légers problèmes, pour protéger l'environnement car une réduction des déplacements des employés va réduire les polluant émit par des véhicules, des avions, etc., et enfin d'être en lien direct et constant avec les partenaires sans passer par un intermédiaire comme ce le cas actuellement.

Pour répondre à ces préoccupations nous avons d'abord évalué l'état actuel du réseau, puis proposé des solutions avec des recommandations sur la façon de procéder à la mise en place d'un réseau de VC. Néanmoins, cette proposition n'a pas été suffisante pour permettre la mise en œuvre immédiate de ce réseau. Il a donc fallu procéder à la **"Conception d'un Réseau de Vidéoconférence à la SOCIETE NATIONALE des HYDROCARBURES (SNH), Étude de cas: Projet d'Extension de l'Immeuble Siège de la SNH** ". Nous avons essayé de présenter une conception topologique du réseau.

Nous avons conclu la première partie en évaluant les besoins du réseau et d'équipement nécessaires par site pour avoir une estimation globale du coût de la mise en œuvre du projet. Dans la deuxième partie de notre travail, nous avons examiné les risques et les menaces pour la sécurité et proposées des mesures pour lutter contre ces menaces. Nous avons ensuite défini les politiques de sécurité visant à assurer la diffusion en douceur et de l'intégrité

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENT

INTRODUCTION

We see work sites more and more located not only in different cities and across the national territory but equally international thus creating an increase in the acquisition and use of various transport means to that these are always linked to each other while staying in contact with partners equally. This in bid to try and make decision making faster. But in so doing, many companies and more precisely the National Hydrocarbons Corporation (better known in French as SNH) have seen their expenditures tremendously increase. With the advent of the internet known as a network of networks, video conference (VC) has received a new push standing at the juncture between the telecommunications world and computer networks. VC *per se* is not a recent invention – it was already envisioned by the inventor of the telephone, Alexander Graham Bell, who was quoted in a 1924 article in the New York Times as saying "*the day would come when the man at the telephone would be able to see the distant person to whom he was speaking" [4]*.

Despite its seemingly long history, video conferencing has only recently become increasingly popular and disperse in the wake of faster and cheaper connections with better technologies. Modern standalone video conferencing units provide advanced video and audio quality due to more efficient compression and can function over normal broadband internet connections [4]. Growing processing power and cheaper accessories, such as webcams, have also made it possible to participate into a video conference using dedicated software on a normal personal computer without any expensive special hardware. In short, the quality has gone up and the price has come down and the number of different technologies has multiplied. Thus, in the last decade, there has been a noticeable growth in both the number of people and institutions using video conferencing and the software and hardware solutions available to bridge geographical barriers and enhance decision making.

The aim of this dissertation**: "Design of a Video Conference Network at the National Hydrocarbons Corporation (SNH), Case Study: Headquarter Extension Building Project"**, gives everyone a broad view on different aspects related to the video conferencing techniques and their importance in choosing and operating a video conferencing solution. In this dissertation, the term video conferencing is recognized in a broad sense, encompassing, standalone video conferencing units and related infrastructure equipment, software based

desktop conferencing systems, web conferencing systems with video and audio functionality, and video calls from mobile phones.

The remaining part of the document is organized as follows:

Chapter 1 presents the context and Problem statement, describes the relevant concepts to the project for clear understanding after presenting the structure of the company in which our work is carried out. Equally, it covers a theoretical review and definition of key aspects and finally the problem at hand is described with all details as well as the project objectives and expected results.

Chapter 2 talks on the methodology used in carrying out the work assigned to us and

Chapter 3 present the main commented results obtained. It also gives the financial cost of the implementation of the work so as to draw out the huge benefit the company stands to enjoy after the deployment of the system.

The document ends with the conclusion and perspectives.

CHAPTER 1: CONTEXT AND PROBLEM STATEMENT

1.1) CONTEXT

1.1.1) History and Missions

National Hydrocarbons Corporation (best known by its French acronym as SNH) is a state funded industrial and commercial company which has financial autonomy. Created on March 12th, 1980 with a capital of CFA Francs 8 billion.

SNH has as missions:

- To promote and develop liquid hydrocarbons and natural gas
- To manage the State's interest in these areas.

SNH manages State's interest in the petroleum and gas sectors and as part of this:

- It seeks for partners who have a proven experience in the hydrocarbons sector and signs contracts with them to carry out possible exploration activities of deposit of hydrocarbons (crude oil and natural gas) in subsoil or sea bottom of the Cameroon mining domain.
- These activities take place within the framework of associations constituted by SNH and these partners. Daily management of activities is entrusted to one of them called operator.
- SNH then receives the share of national crude oil or gas production accruing to the State, in the share provided for in the contract signed with its partners and commercializes it on the international market.
- SNH transfers to the public treasury revenues from these sales after deducing production expenses. In fact, following the Cameroon petroleum Code, the State takes no financial risk during the exploration phase. The risk is borne by the petroleum

companies concerned. In the event of discovery, the State can decide to go into petroleum operations, during the development phase and take participation through SNH. It repays then exploration expenses to the tune of the participation subscribed.

1.1.2) Petroleum Activities

Petroleum activities are carried out in the Rio de Rey (producer since 1997), Douala/Kribi-Campo (producer since 1997) and Logone Birni (not yet producer) basins. As of 1st January 2010, the mining domain consecrated to exploration and development of hydrocarbons has more than 15 permits and exploration licenses, for an area of more than 27 424.18 km^2; and more than 16 concessions and mining permits, for an area of more than 2 954.09 km^2.

Currently, Cameroon produces four types of crude oil, referred to as Kole, Lokele, Moudi and Ebome. Gas production should have started with the gas supply from the Kribi thermal station.

1.1.3) Portfolio and Partners

1.1.3.1) Portfolio

SNH is truly a group, for it withholds shares in thirteen Cameroonian companies commonly called SNH portfolio companies.

Company	Area of Activity	SNH share
Hydrocarbons Analysis Control (HYDRAC)	Quality control	97.10%
TRADEX	Commercializing crude oil and petroleum products	54%
International Business Corporation (IBC)	Metallurgy	51%
Cameroon Industrial Shipyard Company (CNIC)	Naval constructions and repairs	41.50%
National Refining Company (SONARA)	Hydrocarbons refining	29.91%
Total E&P Cameroon	Hydrocarbons exploration/production	20%
Mobile Producing Cameroon Inc.	Hydrocarbons exploration/production	20%
Perenco Cameroon	Hydrocarbons exploration/production	20%

Pectin Cameroon	Hydrocarbons exploration/production	20%
Chanas Assurance S.A	Insurance	20%
Cameroon Petroleum Deports Company (SCDP)	Storage of petroleum products	15%
Cameroon Hotels Corporation (Hilton)	Hotelier	6.21%
Cameroon Oil Transportation Company (COTCO)	Pipeline crude oil transportation	5.17%

Table 1: SNH Portfolio

1.1.3.2) Partners

Glencore, Murphy, EurOil (filiale de Bowleven), Noble Energy, Dana Petroleum, Addax Petroleum, Kosmos Energy, Yang Chang, Gaz du Cameroun (filiale de Victoria Oil & Gas) Amongst others.

1.1.4) Organizational Chart

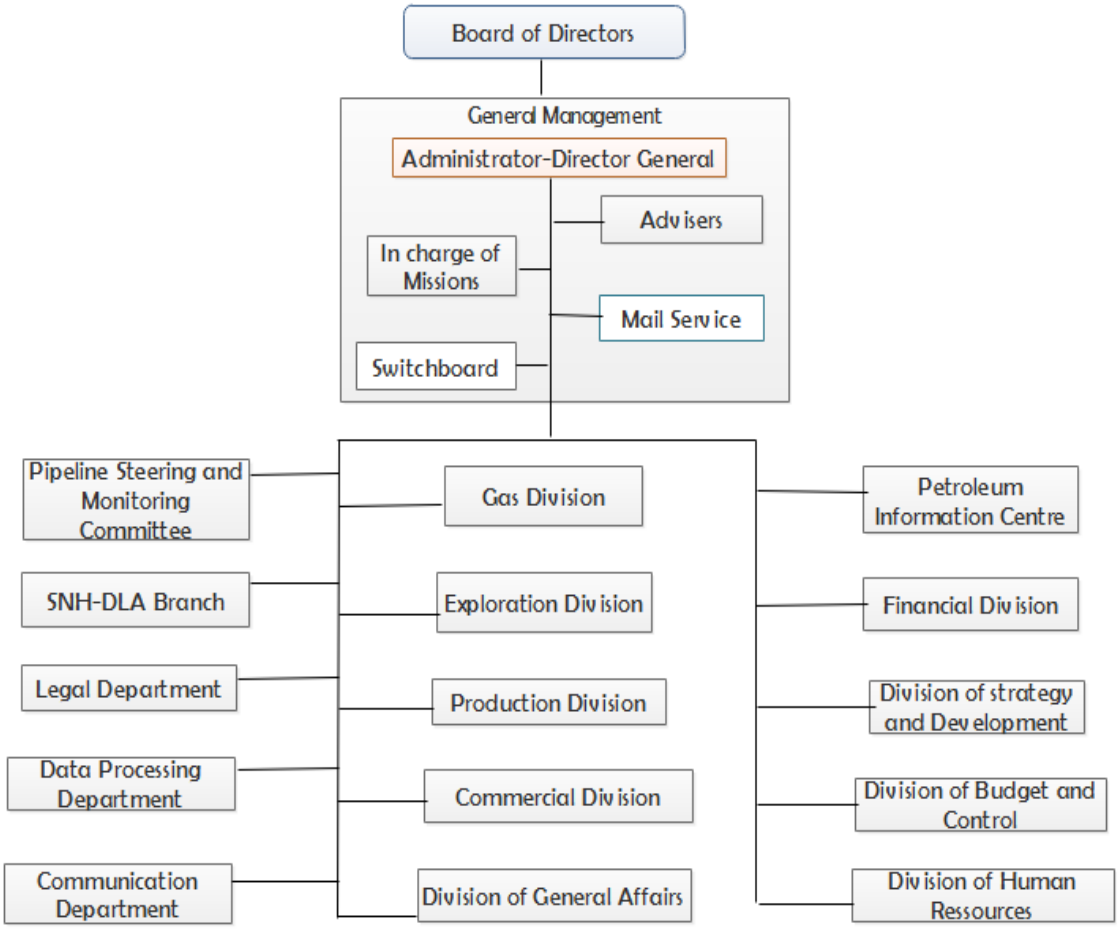

Figure 1: SNH organisational chart

1.1.5) Management

SNH defined and implemented a human resource management policy based mainly on the recruitment of competent staff and management per objective. The target is set through a five year development plan, where the unit's actions plans and declination stem, at the individual level, of set objectives. This declination, which is elaborated in a participative manner, shows each employee's actions to be carried out during the year. It permits a better follow up of activities embarked on, and an objective assessment of the performances of agents.

SNH is a modern and structured company, at the forefront as far as management is concerned, and owing to the codification of administrative, accounting and financial procedures, which respect international standards as far as good governance is concerned. Company accounts of the corporation are regularly audited by renowned national and international firms, and oil operations are published regularly, notably on the corporation's website (www.snh.cm). This approach embarked by SNH since the mid-90s is saluted by Extracted Industrial for Transparency Initiative (EITI), where Cameroon joined in March 2005. This international forum which was launched by former British Prime Minister Tony Blair, prescribed notably to oil companies to publish their balance sheet and amount they transfer to States which they exploit natural resources.

1.1.6) The Division of General Affairs (DGA)

The Division of General Affairs (DGA) was our home unit throughout our internship.

1.1.7.1) Missions

Under the responsibility of a Director assisted by a Deputy, the General Affairs Division is responsible for:

- ✓ Providing, implementing and managing the material resources required for SNH's proper functioning;
- ✓ Assist all business units in the management of material resources;
- ✓ Organize and manage the logistics necessary for the proper functioning of SNH;
- ✓ Inventory of furniture and non-furniture as well as maintain the company's mobile and immobile equipment;
- ✓ Management and exploitation operations of the automobile park.

1.2) PROBLEM STATEMENT

1.2.1) Problem Description

Looking at sections 1.2) to 1.4) above, SNH in accomplishing its missions has not only recruited competent and qualified staff, but to increase efficiency has created a branch in Douala with two other sites at Mvia, and Bipaga. With local and foreign partners often needed for expertize and exploration experience, there has been a serious problem of connecting the headquarter to the various branches and both local like international partners this in view of meeting up with set objectives as employees are constantly displacing themselves to various exploration sites to resolve problems no matter how minute they are.

Not only that but they displace themselves locally like internationally for business-to-business meetings, professional training, internal meetings and presentations thus causing a steady increase at the level of expenditure to an extend where annually the 2000 mission order mark has been reached.

1.2.2) Objectives

This project has as overall objective to design a reliable, secured, scalable, manageable and highly available video conferencing system for SNH to permit them be in constant link with their branches and their partners (locally like internationally). But more specifically our project has as objective:

- To reduce the risk especially of accidents employees take each time they leave for missions to these different sites,
- To reduce expenditures (fuel, car used, trainings, flight tickets, hotel and restaurant bills, missions fees for staff, drivers) on mission orders each time technicians have to be displaced to the various even for minute problems,
- To protect the environment since a reduction in employee displacement, reduces the emission pollutant from vehicles, planes etc.

1.2.3) Expected results

At the end of this internship we have to present a technical document showing the new architecture to be implemented with a detailed list of all equipment (hardware and/or software with technical details of their implementation) needed for immediate implementation of this system as well as an estimate of its implementation cost. The designed system shall provide the following services:

- Video and audio calls with branches in Cameroon and both local and international partners.
- Redundant routes or fail over routes
- Rapid decision making through guarantee of a good quality of service (QoS)
- Secured access to the information database as well as the entire system.

1.2.4) State of the Art

Presently at SNH, the company's global architecture looks like:

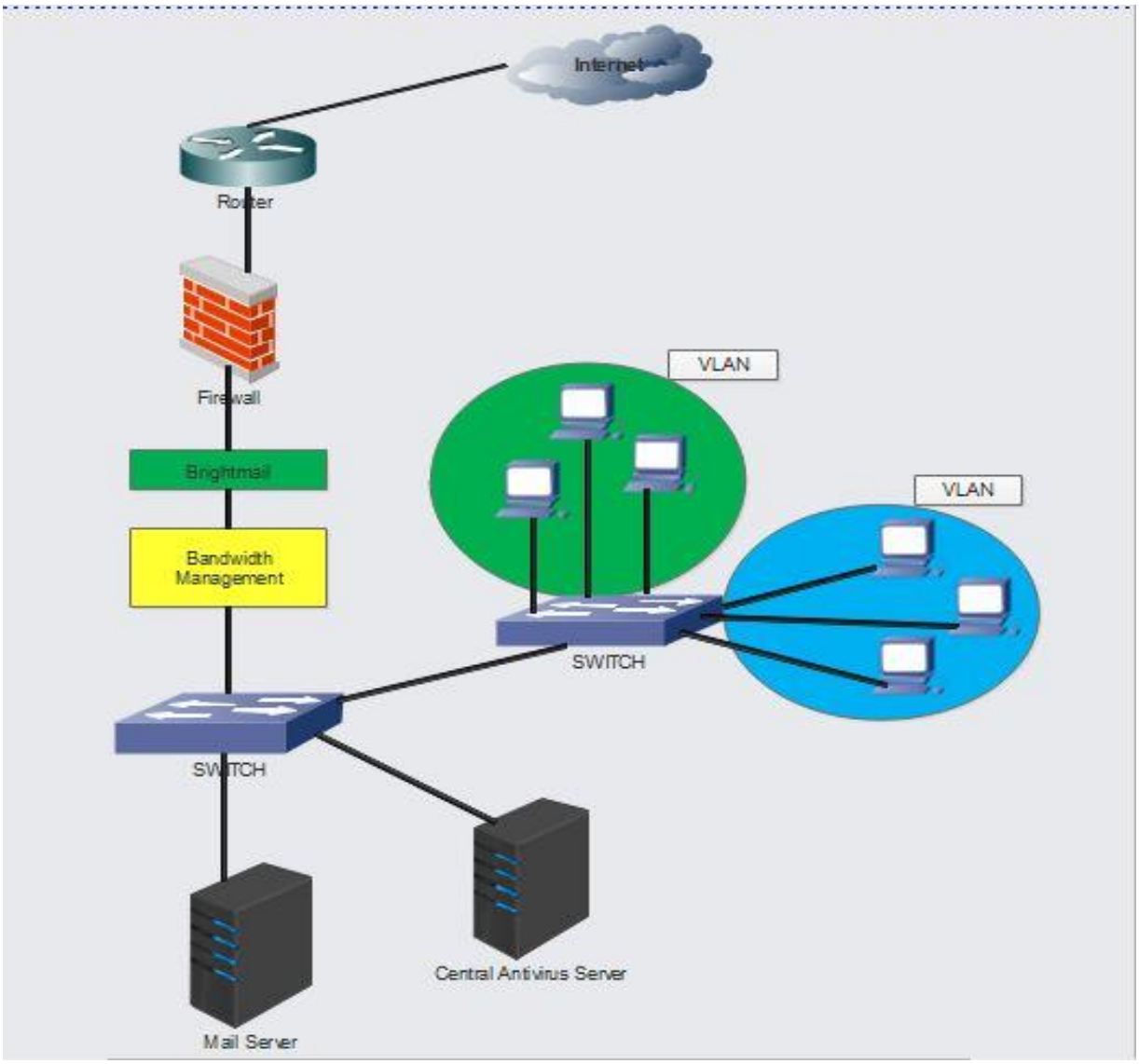

Figure 2: Global SNH architecture view [7]

From the simplified architecture above and looking at the present day functioning of the company, we realize such a system has never been implemented there. A number of companies have worked on this same topic notably ENGIE CAMEROON (representative of GDF SUEZ) who's IT Specialist served as adviser to this project.

1.3) VIDEO CONFERENCING OVERVIEW

1.3.1) Video Conferencing

Video conferencing in its most basic form is the transmission of image (video) and speech (audio) back and forth between two or more physically separate locations. This is accomplished through the use of cameras (to capture and send video from your local endpoint), video displays (to display video received from remote endpoints), microphones (to capture and send audio from your local endpoint), and speakers (to play audio received from remote endpoints). Although there are many factors that serve to modify or increase the complexity of this basic definition, it is useful to keep the concept simple in the beginning when deciding why or how we may be able to use video conferencing for ourselves or our organization.

Figure 3: Video Conference room

In understanding the role that video conferencing could play, consider two general situations: a) those where you are already able to communicate with someone who is not physically nearby, but you wish that communication could be richer, and b) those where you wish to access or communicate to a location that may or may not be nearby but is limited by situational or physical constraints. Distance education often comes to mind first when considering the former situation, but several other existing types of communications can also be enhanced or extended. These include organizational and cross-organizational meetings,

counseling, foreign language and cultural exchanges, and telecommuting. Communication is already occurring in each of these applications, but they could be made more compelling, more effective, or less expensive via video conferencing. (Imagine a telephone call where you can see the speaker, or a television through which you can talk.) For the latter situation, the introduction of video conferencing has enabled communication to restricted areas such as clean rooms, nuclear facilities, operating rooms, and the space shuttle. It has been used to observe wildlife in their natural habitat, to establish interactive surveillance and security, and, combined with micro-instrumentation, to observe inside the human body. This side of video conferencing may not come to mind as readily as the enhancement of simple communication but it can be quite powerful. Simply imagine situations where you might like to be a "fly on the wall", with the ability to interact if desired. To imagine even further, consider that video conferencing can be point-to-point (between two endpoints), or multi-point (combining two or more endpoints into the same "conversation"). When you begin to combine diverse endpoints into one setting where audio and video from each can be shared in real-time, whole new levels of interaction are enabled and entirely new ideas for communication can result.

1.3.2) Why use video conferencing?

Video conferencing can help businesses to save significantly - travel reduction, reduce carbon emissions and improved productivity are usually the top of the list of benefits. Video communications can also create values to your businesses through:

1.3.2.1) Improved employee satisfaction:

Video conferencing allows staff in different locations to see each other on a regular basis, which enables them to become better acquainted and helps to improve interactions, job satisfaction levels and overall morale.

1.3.2.2) Improved work/life balance:

Less business travels mean employees will spend less time away from their family and personal interests, and in doing so they could be happier and more productive.

1.3.2.3) Cultivate business relationships:

More face-to-face meetings can be conducted over video and at lower costs to help you to build better relationship with your customers and business partners.

1.3.2.4) Faster decision making

Video conferencing enables data, documents and images to be shared instantly. With today's high definition video equipment, materials and designs can be observed in great detail with instant feedback from stakeholders, to speed up decision making. This in turn speeds up products or services to market, and can even help to solve customer service issues.

1.3.2.5) Immediate access to remote experts:

The entire organization can gain access to remote experts without paying for travel costs. For example, any incident on the production floor can be inspected by experts in real time even if they are on different continents.

Some special applications of Video conferencing include:

- Telemedicine,
- Telecommuting,
- Judiciary system,
- Laboratories,
- Campus surveillance and security by selectively muting audio and/or video on one side or the other location.

1.3.3) Update on where we are today

The speed and worldwide availability of **Asynchronous Digital Subscriber Line *(*ADSL)** and the **Internet** along with the national telephone companies has virtually stopped the availability and use of **Plain Old Telephone Service (POTS)** as a direct means of connecting video conferencing systems. In its place we now have **Fast ADSL** (Fiber), **Cable** (Optic Fiber) and the forthcoming media-enabled **3G/4G** (Third Generation/Fourth Generation) smartphones and tablets as well as next generation of Codecs and Gateways to transcode the new protocols.

We also need to be aware of new and emerging standards that might have an impact on what we purchase. The latest video compression used by video conferencing systems is **H.264** and its derivatives **H.264 High-Profile** and **H.264 SVC** (Scalable Video Coding). As a guideline, basic **H.264** offers twice the quality over its predecessor **H.263** at the same bandwidth, or the same quality at half the bandwidth. **H.264 High-Profile** has even higher

performance and the latest **H.264 SVC** is scalable and more flexible across networks. So if you are restricted in the available bandwidth, take a look at systems that support the latest video compressions.

There's also been changes in the way data collaboration is achieved; with the development of the **H.239** (Dual Video) standard and 'data-showing' being favoured and replacing the old and now obsolete **T.120** 'data sharing' standard. **H.239** defines how additional media channels are used and managed by video conferencing systems. It introduces the concept of 'data-showing', whereby the Personal Computer (PC) desktop is digitized and converted into a separate video stream and transmitted in parallel with the main 'talking heads' video stream - hence the term Dual Video. Endpoints that support **H.239** will receive the dual streams and display the desktop graphics and far-end video in separate windows. Endpoints that don't support **H.239** will display the shared desktop graphics instead of the far-end video.

1.3.4) Network Concerns for Video Conferencing

Before we look deeper, it is useful to understand what types of networks are available and used by video conferencing systems. The following are popular media transport networks used in video conferencing:-

- **ISDN** - Integrated Service Digital Network
- **LAN** - Local Area Network
- **WAN** - Wide Area Network
- **VPN** - Virtual Private Network
- **802.11 a/b/g/n** - Wireless Network
- **POTS** - Plain Old Telephone Service
- **ADSL** - Asynchronous Digital Subscriber Lines
- **SDSL** - Synchronous Digital Subscriber Lines
- **3G/4G** - Mobile Network

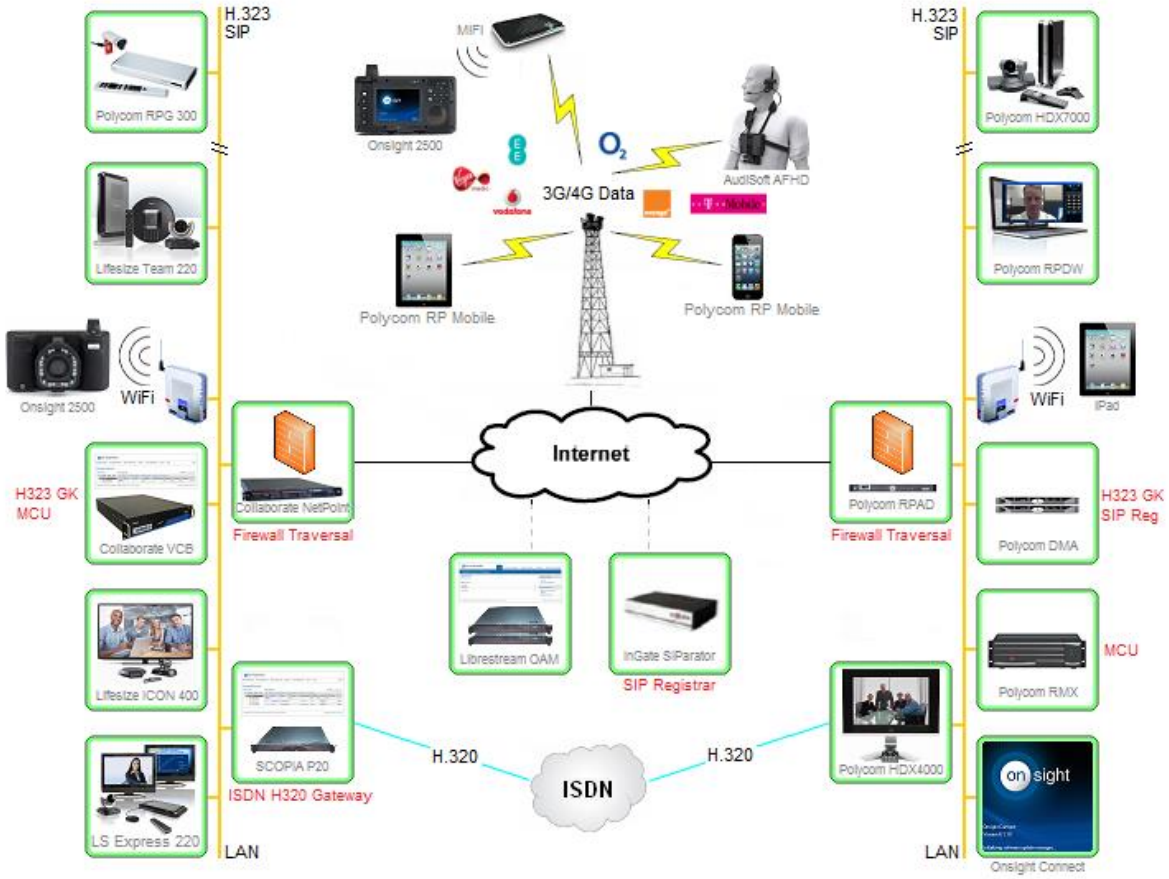

Figure 4: Network concerns [12]

The success of any VC depends on the "end-to-end" bandwidth available and the quality of service characteristics of all network components along the way. By "end-to-end" one includes the hardware and software of the sending device, all of the communications devices between that device and the building connection to the company network, the company network itself, all other connections (when applicable) and all of the above components back to the receiving device.

The **bandwidth** needed for one video conferencing stream typically ranges from 384 to 768 Kbps. Adding network overhead of about 20%, you are looking at 461 to 922 Kbps. If a video conferencing device is sending one video conferencing stream (actually one audio and one video stream) to and receiving video conferencing streams from three other sources, the total bandwidth needed will be two times the amount needed for one stream.

Video conferencing devices send out data at regular intervals and the receiving device expects to get the data at the same regular intervals. As the data passes through each network device from sender to receiver, a minimum amount of **delay (or latency)** is introduced. If

there are a number of devices between sender and receiver, the latency increases. If the latency exceeds **150 milliseconds**, there is a possibility that people may be speaking over one another. Also, the latency for the audio stream may differ from the video stream which means that the sound coming from a person's voice won't match what his/her lips are doing.

Another potential problem is **packet loss**, which is typically due to a communication device that has become congested with too much network traffic. Under this condition, the communication device starts dropping packets, either equally among competing networked devices or in a prioritized manner if quality of service capabilities have been enabled (see below).

Jitter, which is the variation in latency, can also ruin a video conferencing session. This is typically caused by networked devices competing for the uplink connection on a communications device whether it is an Ethernet switch or a router to the company or wide-area network. This situation can be mitigated at the Ethernet switch level by recognizing video and audio stream traffic on a port and marking the Ethernet frames with **Institute of Electrical and Electronics Engineers 802 .1p** (IEEE 802 .1p) prioritization at a high level. (Note: All of the switches in the network, and the router to which they connect, have to recognize and support 802.1p for Ethernet prioritization to work.) At the router level, it must be able to support either Differentiated Services (DiffServ) or Type of Service (ToS) or even quality of service (QoS) markings so they can prioritize the timing sensitive traffic. (Note: All of the routers between the sender and receiver must support one of these two QoS mechanisms to maximize the probability of having a successful videoconference.)

So, what does all this mean in terms of one's video conferencing needs? First, one has to look at the amount of bandwidth needed. If one wishes to have a VC with more than one remote location, the amount of bandwidth needed will be multiples of the amount needed for one remote location. For example, if one wants a four-way videoconference (which requires a device called a multi-point control unit or MCU), one will need anywhere from 2.766 to 5.532 Mbps of end-to-end bandwidth available at all times during the videoconference.

Second, the QoS capabilities of all communications devices between sender and receiver need to be addressed.

Once all of these issues have been adequately addressed, however, one can feel fairly confident that everything possible has been done to make video conferencing successful.

1.3.5) Location and Number of participants

H.323 (IP) and H.320 (ISDN) systems can interoperate with the use of gateways for example the **H.320 Gateway**. Essentially, the **H.320 Gateway** provides translation and transcoding between different circuit-switched networks (ISDN) and packet-based networks (LAN, ASDL, SDSL, Wireless, 3G/4G), enabling the endpoints to communicate. Most **H.320 Gateways** can support several conferences simultaneously in different locations. Most **H.320 Gateways** work in conjunction with and include a basic **H.323 Gatekeeper** functionality.

Figure 5: H.320 Gateway <> H.323 (IP) Gatekeeper [12]

If there will be more than two participants in a video call then there are two choices for handling the interaction: using an MCU or using multicast.

Figure 6: Multisite meeting [6]

ISDN based H.320 conferences typically use a point-to-point connection and need to use some form of Multipoint Control Unit (**MCU**) to link and manage all the ISDN lines in order to hold a conference with three or more participants. The MCU's basic function is to maintain the communications between all the participants in the conference. **H.320 MCU's** are usually a separate piece of hardware dedicated to their function as they need to connect to all of the ISDN lines from each participant.

Figure 7: H.320 (ISDN) Multipoint Conference [12]

Most H.323 systems support IP multicast and use this to send just one audio and one video stream to the other participants when in a broadcast. However, to allow three or more participants into a conference, most H.323 systems usually require a Multipoint Control Unit (**H.323 MCU**). This is not the same as an H.320 MCU; hence it is important to be clear about what you mean when using the term MCU.

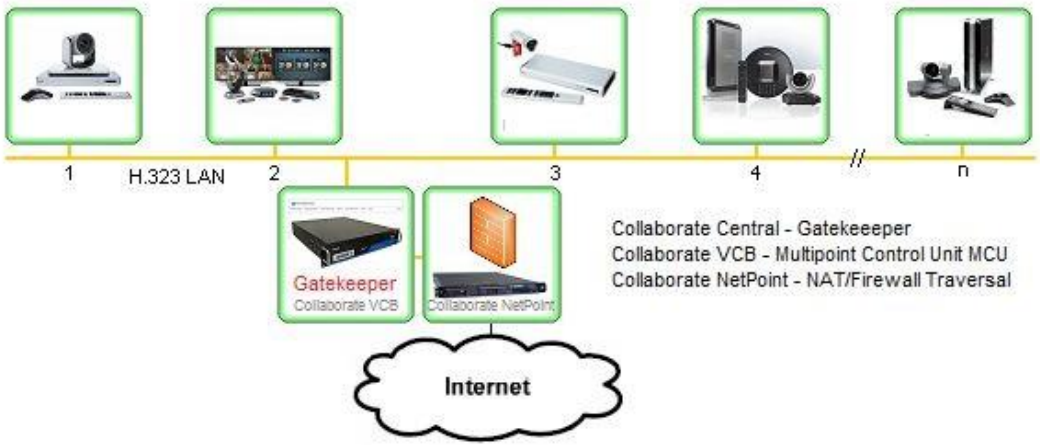

Figure 8: H.323 (IP) Multipoint conference using H.323 Gatekeeper, MCU, and NAT/Firewall transversal. [12]

The **H.323 MCU's** basic function is to maintain all the audio, video, data and control streams between all the participants in the conference and hence most **H.323 MCU's** use propriety or dedicated hardware. ClearOne's **Video Conference Bridge, Collaborate VCB**, is an all-in-one solution that includes an embedded ClearOne Collaborate Central Gatekeeper and a high-definition MCU capable of allowing Ad-Hoc Conferencing in either Continuous Presence or Voice-Activated Switching modes.

1.3.6) Equipment Requirement

As discussed in the beginning of this chapter precisely under the section; **what is Video Conferencing,** any video conferencing terminal must have a few basic components to "get the job done": a camera (to capture local video), a video display (to display remote video), a microphone (to capture local audio), and speakers (to play remote audio). In addition to these more obvious components, a video conferencing terminal also includes among others a CODEC ("COmpressor/DECompressor"), a user interface, a computer system to run on, and a network connection. Each of these components plays a key role in determining the quality, reliability, and user-friendliness of the video conferencing experience as well as any given video conferencing terminal's suitability to particular purposes. A basic understanding of each of these component's roles will help us map video conferencing technology capabilities to our specific application needs.

Figure 9: The figure includes a setup codec, camera, dual monitors and stand, table top microphone [12]

1.3.6.1) Main Camera

By nature of the general definition of video conferencing, at least one video source is typically present at each endpoint. The most common video source is a single main camera that captures live movement occurring images at one end so that it may be sent to the other end in near real-time. ("Near real-time" is an important concept in the success of a VC and is covered more in the sections below on the codec.)

Figure 10: 2.0 Megapixel 20x optical zoom video conferencing equipment for conference room

When selecting a camera for video conferencing, it is important to understand that the quality of your camera heavily determines how your video will appear to the receiving end. It is often our first reaction to attribute video quality to the receiving system. Yet, if you cannot see the other site clearly, their camera is quite often the culprit. In addition to image quality, cameras vary in terms of other features that will affect both their usefulness and their cost. Among these are: the ability to pan, tilt, and zoom, wide angle versus narrow angle lens, manual focus versus auto-focus, manual iris versus auto-iris, auto-tracking, remote control, and/or RS-232 control. Naturally, as features are added, cost goes up.

1.3.6.2) Video Display

In addition to capturing local video, a video conferencing solution must include the ability to display the remote video that is being received. This incoming video is displayed on a monitor, most often a computer monitor, which influences how clearly the remote site can be seen and also how many people at the receiving site can easily see it. "Typical" display monitor quality considerations such as screen size and resolution affect the size and clarity of the incoming video window and also the integration of the incoming video window with the application interface that surrounds it. In some cases, an entire display monitor can be

dedicated to displaying incoming video (a "full screen" conference) while a second monitor is added for call control and data sharing.

Figure 11: video display

A final note: Video resolutions supported by H.323 are CIF (352 X 288 pixels) and QCIF (176 by 44 pixels) amongst others. Since these resolutions are fixed, increasing the network bandwidth of a call beyond a certain point will not show an appreciable difference in video quality within any given video frame. However, additional bandwidth enables higher frame rates (i.e., the sending of additional video frames per second) which can have dramatic improvements on the smoothness and video quality of motion.

1.3.6.3) Audio Components

Within a video conference, audio is as important, and often considered more important, than video. If we lose video or experience poor video quality in a conference but audio remains intact, we can still accomplish many of our communication objectives. The conference would simply become a teleconference rather than a video conference.

Figure 12: Cisco table microphone

In contrast, poor or disrupted audio quality effectively shuts down a video conference. In light of this, the devices that capture local audio (microphones) and those that reproduce remote audio (speakers) are critical conference components. Coupled with this are characteristics associated with comprehensible full duplex (simultaneous two-way) transmission of audio, such as echo cancellation, noise suppression, and audio mixing. These features are influenced by a combination of the microphones, speakers, and codecs. One key to ensuring audio that supports conference requirement and expectations is to examine the location, quantity, and quality of microphones and speakers to be used.

1.3.6.4) The codec

It has been mentioned above as affecting both the video and audio within a video conference. Indeed, the codec actually forms the heart of any video conferencing terminal and is the main enabler of wide-scale video conferencing. The word "codec" is a shortened version of "compressor/de-compressor" and is specifically applied to the wide variety of algorithms used for actually compressing or decompressing audio and/or video information. This compression has historically been necessary to make the audio/video data "small enough" to be practical for sending over expensive network connections. In this sense, there are many audio and video "codecs" (particular compression/decompression methodologies) that are supported as part of the H.323 video conferencing standard. For the purposes of this section, we are considering a broader meaning for codec: the codec as the portion of the video conferencing terminal that is responsible for whatever compression/decompression of the audio/video signals is taking place.

Though we think of the conference as a real-time conversation, the real-time feeling is a function of how fast each of the codecs are compressing/decompressing the data, and how fast and reliably the compressed data is travelling back and forth across the network. In light of this, some factors to consider when evaluating codecs are:

- *Is the codec a software or hardware component?*

Hardware codecs are generally faster in completing their compression/decompression task, making near real-time communication more likely. Hardware codecs also often carry their own processing power "on-board" such that they do not rely on the resources of the

underlying system. For instance, in the case of a desktop system, using a hardware codec may mean that you don't need a "souped-up" PC, or that you will be able to run other applications on your PC while simultaneously participating in a video conference. On the other hand, software codecs are generally less expensive and easier to install (no special hardware required), but they tend to produce lower quality ("casual") conferencing with very low frame rates. In H.323 desktop video conferencing systems, the codec typically resides on an interface board or in a software application.

- *What actual audio and video codecs (compression/decompression methodologies) does the more broadly defined "codec" support?*

In order for a successful video conference to take place, endpoints must be able to negotiate a common methodology for both audio and video exchange. Any given video terminal/codec (using the broader definition) may support a number of audio/video codecs (the narrower definition), some of which must be supported for a video conferencing terminal to be considered "H.323 compliant". A video terminal/codec may also support proprietary audio or video codecs of the system developer's own design. When two of these video terminals are in the same video conference, they may have access to improved functionality, quality, or reliability between them because they can each understand and use the proprietary features. When selecting a video conferencing terminal, you should be aware of its range of support for various types of audio/video compression. You then need to consider whether or not this range covers the range you are most likely to encounter in your video conferences.

1.3.7) System Type - Personal or Room.

There is a major difference in the usage concept between Personal and Group video conferencing systems. Group systems are usually in a specific room that has to be reserved in order to schedule when they can be used. This can be restrictive and takes away the spontaneity of using video conferencing. Furthermore, Group systems usually have a PTZ (Pan, Tile & Zoom) camera with remote controller and their own specific Graphical User Interface that needs to be learnt and navigated, hence they tend to be used by only a select number of people.

On the other hand, Personal video conferencing systems are both PC based and use the familiar Windows GUI, or available as 'apps' for Smartphones and Tablets. However, neither are usually left running in the background in an ***always-on*** mode. If there is going to be a

large uptake of video conferencing, then it must be always available and easy to use. You need to exploit the spontaneity of the occasion in order to get the most from video conferencing. The concept is like that of using the telephone. It's always there and easy to use. Likewise, video conferencing systems should be configured to be 'always-on' and answerable. The availability of video conferencing 'apps' on Smartphones and Tablets should help on a personal level in BYOD (bring your own device) situations.

1.3.8) Acceptable Quality.

There are several steps that can be taken to reduce the amount of data that has to be transmitted when conferencing. The obvious combination is to use the smallest acceptable resolution (window size) with the minimum acceptable frame rate. This determines the 'raw' volume of data before applying any compression to further reduce the overall amount of data; but these have a crucial effect on quality.

Resolution & Frame Rate	H.264 Baseline Bitrate (kbps)	H.264 High Profile Bitrate (kbps)
1080p30	2048	1024
720p60	1512	832
720p30	1024	512
4CIF30	256	128
CIF30	128	64

Required bitrate for H.264 Baseline and H.264 High Profile at various video resolutions and frame rates

Figure 13: Some required bitrate

Limiting the actual video resolution (number of pixels) has a direct impact on the graininess and hence quality of the video. And reducing the number of frames per second has a direct effect on the smoothness and hence quality of the video. So there are compromises to be had when setting the minimum resolution and minimum frame rate to be used. Once these are set, it depends on the efficiency of the video compression algorithm used that will determine the required bandwidth. But which compression algorithm used is determined by

the video conferencing systems when they do the initial 'handshake' or Capability Exchange. You might have the latest and greatest system that supports H.264 High Profile, but if the other system only supports H.264 Baseline, then they will use H.264 Baseline.

1.3.9) Required versus Available Bandwidth.

Video conferencing is a form of communications involving the transfer of information between two or more locations. The connection between these locations is the communications channel and is called the network. It is the network loading in terms of required bandwidth that needs to be considered. Bandwidth is the resource of a network. It is the term given to the rate of transfer of information, usually in kilobits per second (kbps); it is like the speed limit of the network and cannot be exceeded.

Available bandwidth is a limiting factor with conferencing and sending video creates lots of data. Consider a typical 720p video image size of 1280x720 pixels; then this represents 921600 pixels of information per single frame. Now consider how the color of each pixel is represented; this typically uses the 4:2:0 format. Finally, consider how many frames per second that you want to see; this is called frame rate. The human eye perceives 25 frames per second as continuous motion, but HD 720p video typically uses 60 frames per second.

The diagram below gives an indication of just how much more data is required to be sent (bigger area) per frame depending upon the resolution of the video image.

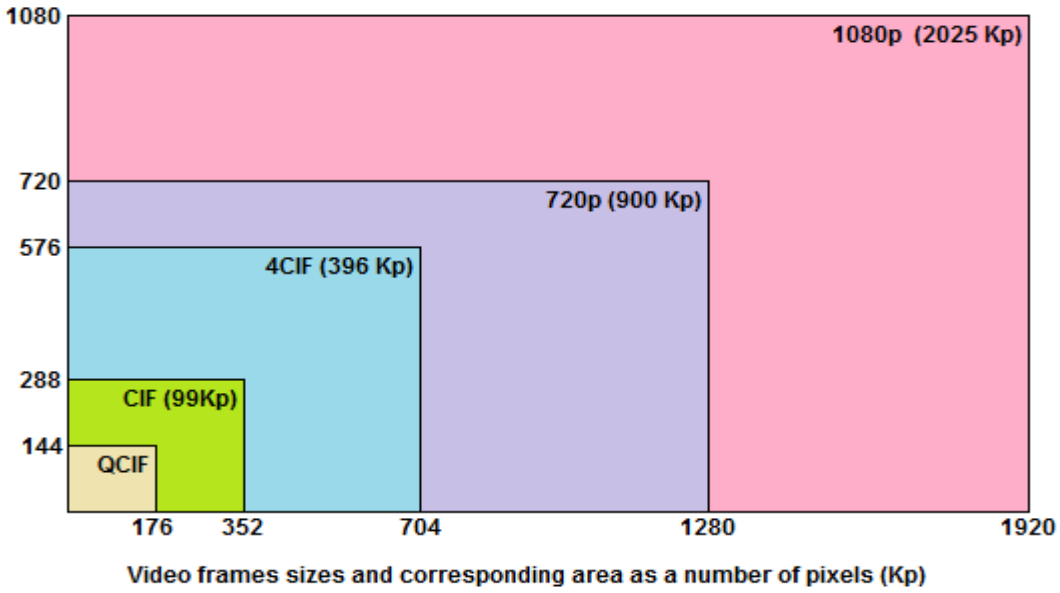

Figure 14: Video frame sizes

Bearing this figure in mind, it's easy to see how a raw (uncompressed) HD 720p60 video stream can be around 1.0 gigabits per second. It is clear from this example that video can place enormous demands on the network and hence why available bandwidth is a limiting factor with video conferencing systems.

There are essentially two ways of reducing the impact of this limitation. One is to use a faster method of communications that increases the available bandwidth to the conference (eg. Fast Fiber ADSL); the other is to utilize methods that reduce the amount of data required to be transmitted by using systems that support the latest video compression technologies.

By applying H.264 Baseline Profile compression to an HD 720p60 video stream, the 1.0 gigabits can now be reduced to about 1024 kbps. But by applying the very latest H.264 High Profile compression instead, the video stream can be reduced to an impressive 512 kbps - a 2000:1 reduction in the raw stream.

1.3.10) Video Conference Room Design

To sufficiently reproduce the experience of a live, in-person, face-to-face meeting, you must design the environment where you install the VC systems to produce near-perfect replication of lighting, sound and ambiance. Careful adherence to the design principles and specifications provided here can result in an experience that is so lifelike, realistic, and free

from technological distractions that participants can focus 100 percent of their attention on the people they meet with and the meeting content, and experience most of the same emotional and psychological interactions that occur when people meet face-to-face.

Proper design of a VC environment involves a number of different aspects, each of which by itself is critical to the experience, and some aspects are inter-related and can influence each other. Some of these aspects are:

3.10.1) Room Dimensions, Shape, and Orientation

This is about the physical size, shape, and orientation of the room and the location of doors, windows, columns, and furniture within the room.

3.10.2) Wall, Floor and Ceiling Surfaces

This talks of recommended colors, patterns, and materials of wall, floor, and ceiling surfaces within the room.

3.10.3) Lighting and Illumination

It is all about illumination considerations and specific lighting requirements and recommendations.

3.10.4) Acoustics

This treats the concepts of sound reproduction and the effects of ambient noise and reverberation within the environment and how they are measured.

3.10.5) HVAC

Heating, ventilation, and air conditioning (HVAC) is very important in VC.

For example, even if the network performs perfectly, an improperly lit room can lead to grainy and pixilated video quality. As another example, if the acoustical behavior of the room, such as the amount of ambient noise and reverberation within the environment, is not controlled, the quality of the audio might sound muffled, reverberant, and even choppy, the audio detection algorithms used to facilitate switching in multipoint meetings could fail, resulting in false switching to a participant who is not speaking, or a failure to switch to a participant who is speaking. Many of the audio and video issues that at first glance might seem to be attributed to system hardware and software quality or network performance can actually be the result of an improperly designed room environment.

CHAPTER 2:
METHODOLOGY

The methodology starts with a presentation on how SNH's standard video conference architecture will look like giving step-by-step run down of how to set up the system.

We will later on talk about video conference technologies, which is extremely important in our design of a high definition system permitting rapid decision making.

We shall be ending with security policies needed when running such a system as well as some constraints and hypothesis used during our work.

2.1) Diagnostic report of the present state of SNH regarding a video conference network.

2.1.1) Review of goals and objectives.

SNH over the years has been faced with the problem of:

- Rapid decision making especially when incident occur at various exploration sites
- Reaching local and international partners within short periods of time without necessarily passing through a third party
- Reducing the risk of accident employees face when they travel to the multiple sites severally
- Reduction of high expenditure on mission allowances

2.1.2) Present functioning

In order to meet these goals, SNH has done some things which presents limitations as can be seen on the table below:

Present state	Limitations
Acquisition of cars to ease displacements	Time consuming and cost ineffective
Employment of new staff	Increase in budget and slow decision making as personnel still have to travel to and from site to lay down complains,
Use of audio phones	Slow decision making because people still have to displace physically before decisions are taken

Table 2: Present state of functioning

2.1.3) Reasons for lower output

The prime reason for a lower output is the inexistence of a reliable and secure video conferencing network in the company which permanently interconnect the different branches to the headquarter in Yaoundé therefore causing a multiplication of employee displacements across the national territory and internationally.

2.2) Design of the video infrastructure for SNH

In what follows we shall give a step-by-step explanation of the network to be put in place since we are going from scratch. The infrastructure being a simple one, the difficulty here comes with setting up its components so as to meet the objective of the company but more importantly selecting the right standards and protocols to be used which we are going to see in section 2.3) of this work. The system we propose is simple but scalable when need be especially as the company grows and looks thus:

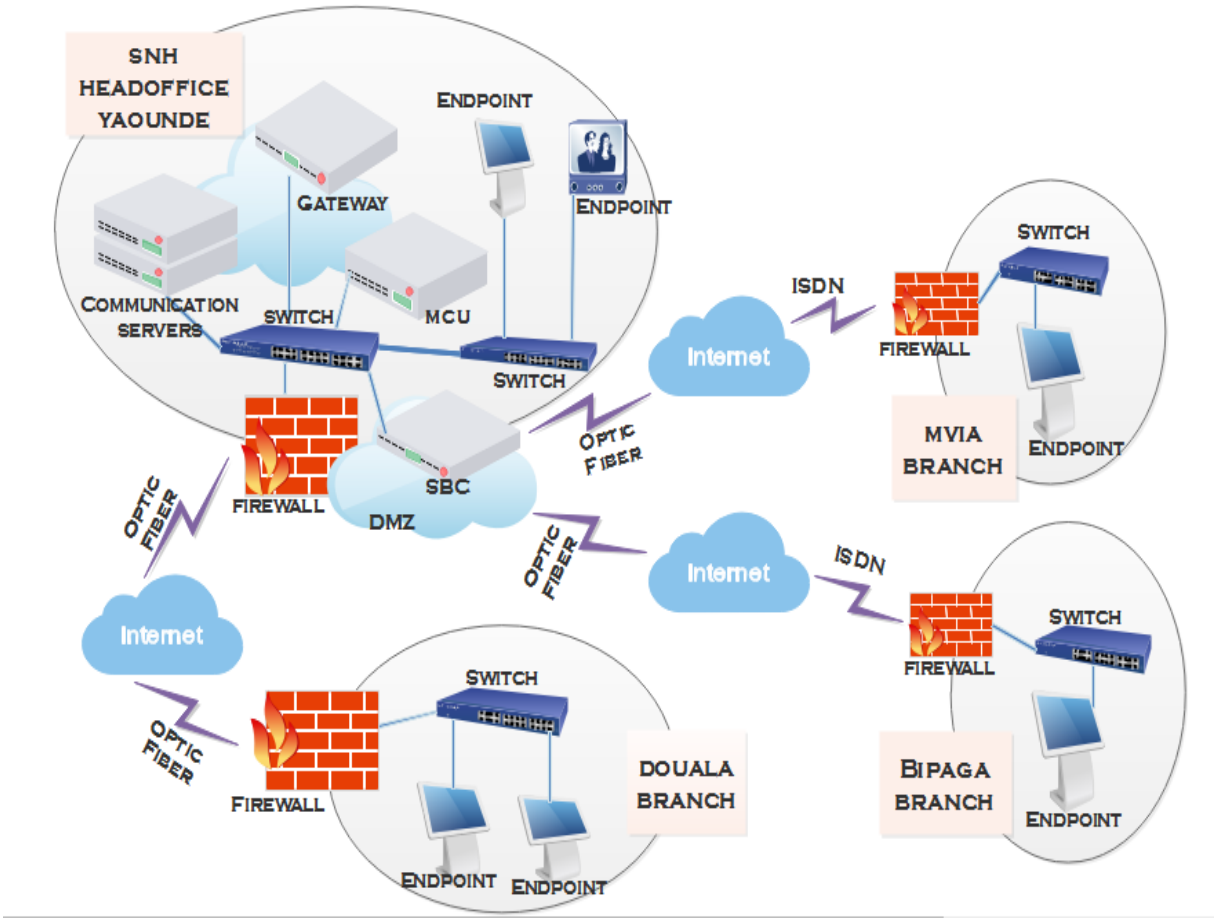

Figure 15: Proposed designed Video infrastructure

The core of the network includes the communication server, the conference server (MCU), the Session Border Controller (SBC) located in the De-Militarized Zone (DMZ) and the gateway to other networks and redundancy purposes too. This is a complete solution as it provides the ability to integrate third-party applications. It is important to note here that the company finding recording of its calls not relevant, a recording server wasn't added in the infrastructure. This made our infrastructure basically a standard one for providing high quality conference. To summarize it all we have:

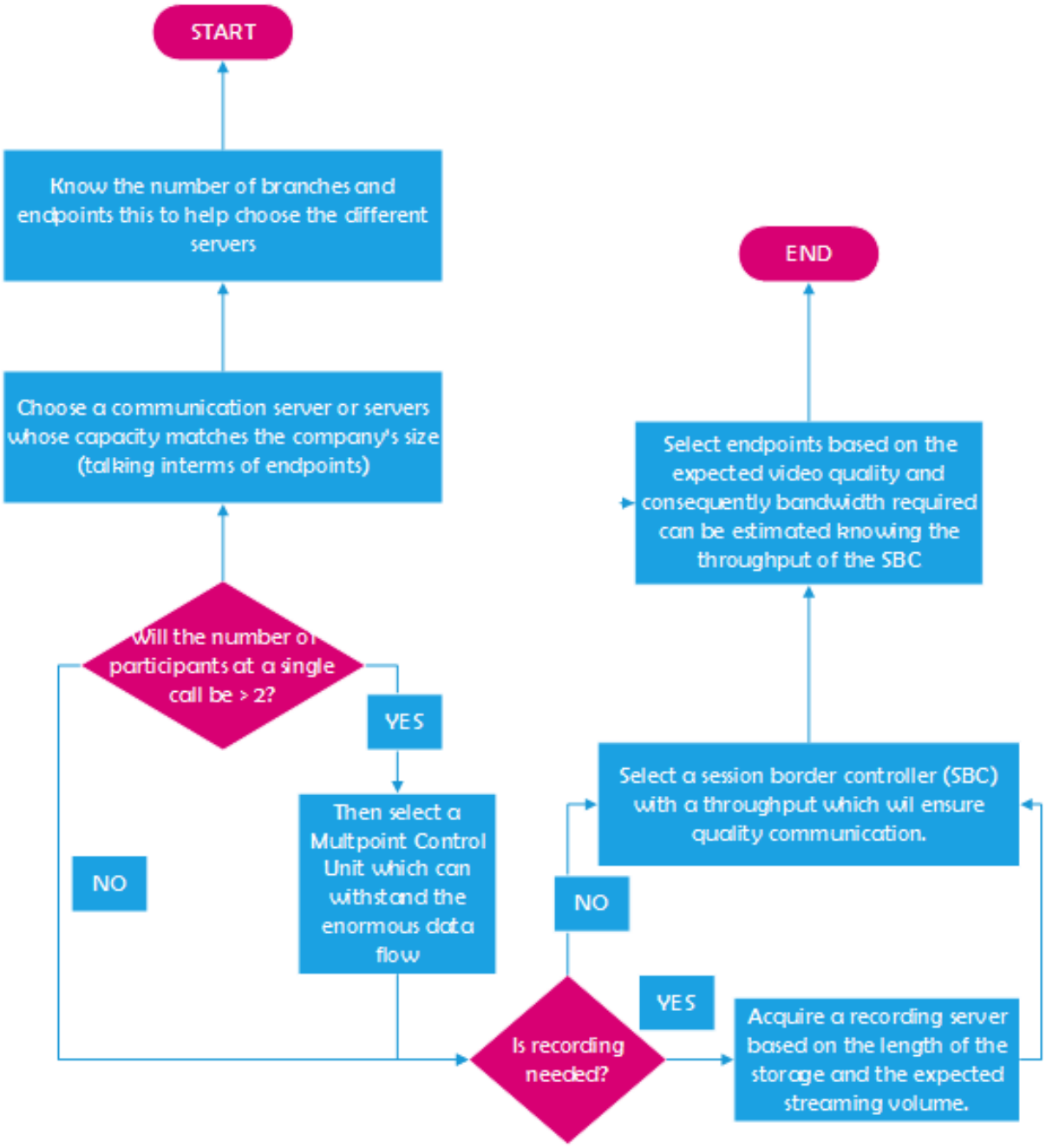

Figure 16: How to setup a simplified video infrastructure

SNH looking for immediate implementation, we equally looked at the endpoints too and as general configurations rule for both the server and endpoint (client side) we came out with the following:

- **Functions of the servers**

Server side applications will perform the following functions:

- ✓ **Registration of the users:** Each user must be registered at the server in order to take part in the conference. At the time of registration user will provide his information to the server along with his/her public key. User will get a unique user-id and server's public key. These public keys will be used at the time of authentication.
- ✓ **Authentication of users:** At the time of joining a conference by a user the server (particularly the communication server) and the user, both will authenticate each other using their private-public key pairs.
- ✓ **Distribution of the session key:** After authenticating a user, the server will send the session key to the client application running at the user side in a secure manner. This session key will be common for all users taking part in a particular conference.
- ✓ **Maintaining the state of the conference:** Whenever a user will join or leave a conference, the server (here we are talking about the communication and conference servers) will inform the other users of that conference and provide them necessary information in order to maintain the state of the conference.
- ✓ **Controlling QoS:** Server will also be responsible of controlling quality of service (QoS) of the audio/video data exchanged between the clients. In order to do that, the conference server (MCU) gets the feedbacks from the clients about every media stream they are receiving. For each client, the server maintains QoS statistics from the feedbacks of all receivers of that client and whenever required it sends the QoS control signals to the client to maintain the quality of media stream being sent by that client.

Functions of the clients

Following are the basic functions performed by the client side application:

- ✓ **Session setup**: The client application will interact with the server to get the session key and information of other users to setup a conferencing session.
- ✓ **Capturing the audio/video stream:** The client application will be responsible of capturing user's real time audio and video streams from the capturing devices.
- ✓ **Compression and Encryption of the audio/video streams**: The client will compress the audio and video streams to reduce the bandwidth requirements. It

will also encrypt each packet of the audio video stream before transmission using the session key gotten from the server.

- ✓ **Creation of RTP session:** The client application will create RTP sessions for transmitting real time audio/video streams of the users to other users taking part in the conference. Two separate sessions will be created for audio and video.
- ✓ **Opening RTP sessions:** The client application will open RTP sessions for each user whose audio/video streams the user wants to receive.
- ✓ **Decryption and Decompression:** Decryption and Decompression will be done both audio and video streams of each user to get the streams in their original form.
- ✓ **Rendering the audio/video stream**: Finally the incoming audio and video streams will be rendered and will be sent to the speakers and display unit respectively.
- ✓ **Maintaining QoS:** The client application will monitor the incoming audio/video streams and will send the feedbacks to the MCU. It will change the parameters of the media streams being transmitted accordingly whenever it will get the QoS controls from the server for example reducing the bit rate.

This haven been done, we will proceed with critical configurations parameters for each chosen server in the system we have designed which will help us achieve our goals. This will be done for the mandatory elements of our infrastructure. Before we do this, we will make two following hypothesis:

Bandwidth

Following talks with the Computer Science department and the Maintenance and Security service at the Department of General Affairs, it was brought to our understanding that as concerns bandwidth, SNH had no problems with that as they are supplied with a close to 1.5Gbs optic fiber connection link. Based on this, we use the hypothesis that bandwidth is not a hindrance to the implementation of this system.

Room Design

Knowing that VC is very demanding when we talk of the meeting room design, we decided to go in for endpoints which are adaptable to the existing meeting rooms found both at their headquarter and the extension buildings.

2.2.1) Scalable Communication Server Architecture

The heart of our communication system is the communication server. There are many names for it—call manager, communication manager, Gatekeeper, SIP server, IP-PBX and so on—but they all perform essentially the same core tasks. Traditional communication servers keep track of all communication endpoints (terminals) in the network and provide services according to a profile set up for a particular endpoint, for example, endpoints installed in corporate branch office may be restricted from making external calls. Modern communication servers recognize users (through a logon/authentication procedure) and can apply policies to the user instead of the endpoint. For example, a support technician might be authorized to place high definition video calls while an accountant might only be able to place standard definition video calls.

UC server process calls among endpoints, keep track of the call state, and interact with the endpoints in the network to provide logical prompts and options to users. So this communication server will keep records for each call (call detail records) which will be used for interdepartmental accounting and for billing.

- **CONFIGURATION**

Parameter	Explanation
Lightweight Directory Access Protocol (LDAP)	Used by endpoints and the communication servers to retrieve information from directories, see 2.2.1.1
Automated alternate routing (AAR)	Provides a mechanism to reroute calls through the PSTN or other network by using an alternate number when the Communications Manager blocks a call due to insufficient location bandwidth. With AAR, the caller does not need to hang up and redial the called party.
Credential Policy	Provides options to change the default credential policy assignment for a user and credential type (for example, end user PINs).
Annunciator	Play prerecorded announcements (.wav files) and other tones. The annunciator alert callers as to why a call fails. It can also play tones for some transferred calls and some conferences.

Gatekeeper	Supports the H.225 Registration, Admission, and Status Protocol (RAS) message set that is used for call admission control, bandwidth allocation, and dial pattern resolution (call routing). Address translation from one format to the other
Gateway	To permit communication with non IP networks
Enterprise parameters	Provides default settings that apply to all devices and services in the same cluster. (Cluster comprises a pair of communication servers that share the same data base)
SIP dial rules	The administrator uses SIP dial rules configuration to configure dial plans for phones that are running SIP and associate them with phones that are running SIP
Auto registration	Use if you want the Communications Manager to assign directory numbers automatically to new phones as they connect to the server
Service parameters	Allow you to configure different services on selected servers.

Table 3: Communication server configuration

In the lines that follow we have taken time to explain some concepts to help understand some functions of this server.

2.2.1.1) Endpoint Intelligence

Protocols between an endpoint and server can be stimulus or functional. For example, proprietary signaling protocols used in legacy PBXs are stimulus protocols and some standard protocols such as MGCP are stimulus, too. Stimulus protocols are used to keep endpoints simple and inexpensive. Information such as the endpoint's profile (number of keys, size of display, for example) and the call state information (whether the endpoint is on-hook or off-hook or whether there is an active call, for example) are kept in the server. If the user presses a key, the endpoint sends a code to the server. The server then interprets the user's action and sends instructions to the endpoint on how to respond, that is, what string of symbols to show

on the display. Therefore, the system fully controls the endpoint and can place calls, answer calls, and perform all call features on the endpoint's behalf. Since all information about the device is centrally stored in the communication server, scalability of such systems is limited.

Standard protocols such as H.323 and Session Initiation Protocol (SIP), on the other hand, are functional, that is, the endpoint itself is intelligent and can, for example, place calls and initiate transfers based on user input. The server only receives signaling messages, executes them, or passes them to other network elements that can execute them. Putting intelligence in the endpoints allows communication servers to be simplified and made more scalable.

For example, many recent systems support both SIP and H.323 simultaneously, and can dynamically switch between the two protocols. This allows endpoints to simultaneously register with SIP servers and H.323 Gatekeepers, which takes configuration flexibility to a new level.

2.2.1.2) Lightweight Protocols

Lightweight protocols, such as SIP, require fewer messages to setup and tear down a call. The server also has to store less call state information. This automatically increases the scalability of the communication server. The Lightweight Directory Access Protocol (LDAP) is another example for such a protocol and is used by endpoints and communication servers to retrieve information from directories. The directory is the list of all users with their contact information, access rights, etc. If the directory is embedded in the communication server, the complexity of the directory access protocol directly affects server performance, thus using LDAP is a requirement for a scalable communication system.

2.2.1.3) Separating Signaling and Media

Media includes the audio, video and content streams that flow between endpoints. Audio is typically compressed using one of the standard G.7xx codecs, while video is usually compressed by one of the standard H.26x codecs. Following the ITU-T H.239 standard, content is compressed similar to live video using H.264, H.263, etc. Processing media—and especially video media—is very resource-intensive; therefore, the best way to keep the communication server scalable is to process the media separately. This is possible with most modern protocols and both SIP and H.323 clearly separate signaling from the media. If the

communication server processes signaling messages, but no media, its scalability can be increased by several magnitudes. Figure 1 depicts an example of a point-to-point call between two endpoints.

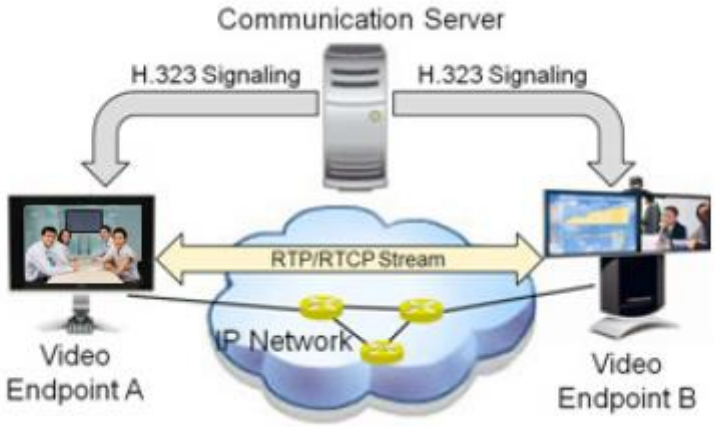

Figure 17: Scalability through signaling and media separation

2.2.1.4) Server Pool

A way of deploying multiple servers is as a redundant pool of resources that serve the same but larger group of users. This configuration has excellent redundancy with two servers and can have even higher redundancy with three or more servers. If one server fails or is taken down for maintenance (for example, a scheduled software upgrade), incoming calls are simply routed to another operational server. Figure 4 shows the configuration with two servers.

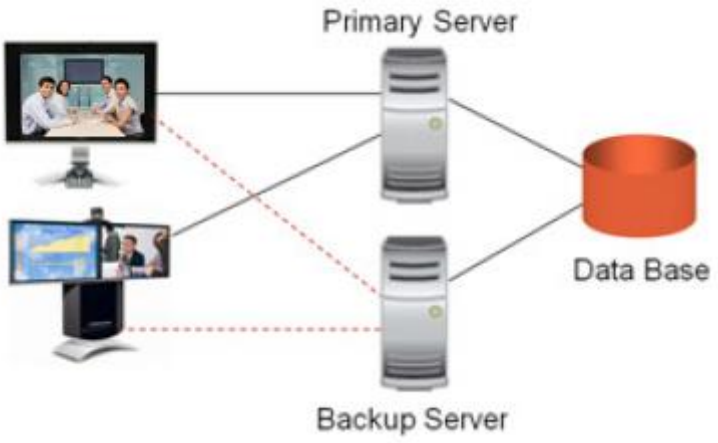

Figure 18: Server redundancy and load balancing

2.2.2) Scalable Conference Server

The conference server, also called Multipoint Conferencing Unit or MCU in a video conference architecture, is the main component for multipoint calls. It receives audio and video streams from each endpoint participating in the conference, combines multiple images into one (this technology is known as Continuous Presence) and sends the combined image to the participating endpoints.

- **CONFIGURATION**

Being a key element in this infrastructure, we will talk about 3 of its key features while that which has to do with Codecs is critically studied in section 2.3).

Parameter	Explanation
Transcoding	This being the core function of this server, it has to do with: • Audio algorithms • Video algorithms • Networks • Resolution • Frames rates • Bit rates • Content Transcode for H.263 and H.264 on the same conference, see section 2.3)
IP QoS	This goes with working on: • Lost Packet Recovery • DiffServ • Dynamic jitter buffer • Voice and video error concealment
Security	We want to make sure there is: • AES media encryption (IP and ISDN) • Transport layer security (SIP and management network) • Strong password policy

	• Tiered administrative access levels • Secure conference mode

Table 4: Conference server configuration

The conference server can translate the audio and video from one format to another, for example, it can receive video in H.264 and send video in H.263 format, receive audio in G.722.1 and send audio in G.711 format. This function is known as transcoding and requires significant computing resources (typically through Digital Signaling Processors, DSPs). This is especially true for video because it involves decoding the digital video stream from one format into uncompressed video and then encoding it in another format.

For example, a 1080p30 packet reaching the MCU in a H.264 compression form, is uncompressed as shown below:

(1080 x 1920) pixels x (3 x 8) colour x 30 (frames per second)

Giving 1,492,992,000 Gbits ≈ 1.5 Gbits

The MCU works on this raw information and recompresses it to 2Mbits or less for transmission.

Scalability can be increased by using conference servers in video-switched mode which circumvents transcoding (and therefore the server needs far less computing resources) but also limits the flexibility because all parties have to use the best common codec, resolution, and bit rate. The external interfaces of the conference server require very high input and output speeds for the multiple audio-video streams. For example, if a server supports 80 participants at 4 megabits per second each, the conference server must support 80x4 or 320 megabits per second input (from endpoints to server) and another 320 megabits per second output (from server to endpoints). Internally, the server works with uncompressed video which takes many gigabits per second on the internal interfaces, and requires fast internal communication links.

2.2.3) Scalable Gateways

Gateways are the gates to other networks. Going in for a SIP deployment, gateways will be necessary to connect to the H.323 or ISDN systems. For connectivity to mobile video

deployments, a gateway to H.324M will be required. A gateway in our case is especially important since the technology is new, e.g., SIP system being installed, because most of the users we want to talk to will likely still be using legacy systems. Most of the calls in these early stages will therefore be gateway calls. The principal configuration here will be that of translation from the SIP protocol to the H.320 and H.324M terminals, since our MCU has been designed to support H.323.

- **CONFIGURATION**

Parameter	Explanation
Translation	Permits signals from SIP to be converted to H.323 signals for fluid communication between the two systems.

Table 5: Gateway configuration

In what follows, we decided to separate this translation function into two and have a detailed study of each.

2.2.3.1) Signaling Gateway

A gateway being required, the scalability of the gateway is critical in this early day of deployment. As with the communication server, the best way to achieve scalability here is through separating signaling from media and limiting the gateway function to signaling only. In this case the gateway is no different from a multiprotocol communication server. It receives messages in one format (SIP, for example) and translates them into another (for instance, H.323) and vice versa. This architecture does not allow the gateway to scale to the levels of a single-protocol communication server but it can handle much higher load than if media is involved

A signaling gateway is only a feasible solution if the media (audio and video) is in the same format. For example, both H.323 and SIP use the Real Time Protocol (RTP) for media and therefore are candidates for signaling-only gateway interoperation. Figure 7 depicts the configuration. There are several issues with the signaling gateway approach. Probably the most important one is that media encryption is broken if the server follows the respective standards. SIP, for example, refers to the Secure Real Time Protocol (SRTP) for media encryption. This mechanism is completely different from the Advanced Encryption System

(AES) specified by H.323. Therefore, if you follow the standards on both sides and use a signaling gateway, you have to disable encryption, and send audio and video in the clear.

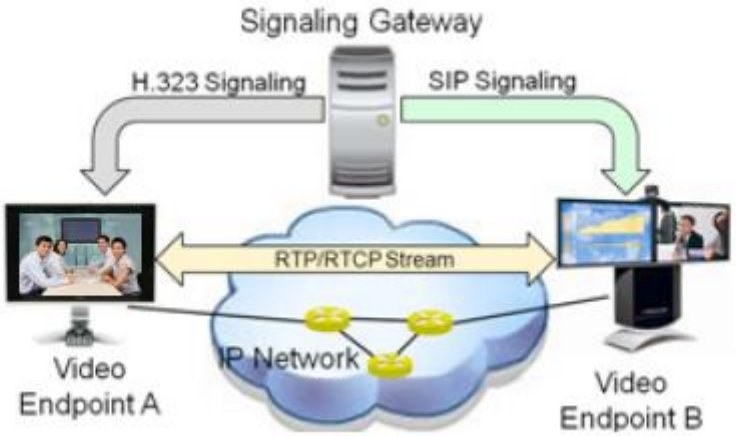

Figure 19: Signaling gateway between SIP and H.323

2.2.3.2) Media Gateway

Using a media gateway helps overcome the security problem and gives network administrators more flexibility during the transition from one protocol to another. It does limit the scalability since the media gateway often needs to transcode video, that is, it requires DSPs and fast external and internal interfaces. Similar to conference servers, media gateways can scale by avoiding transcoding. The media gateway controls the communication with the endpoints, and transcoding is only necessary if the endpoints negotiate different audio/video algorithms, resolutions, and bit rates.

If the gateway enforces the same audio/video algorithm, resolution, and bit rate between the endpoints, then no transcoding is necessary. Therefore, the media gateway is very similar to a conference server, and if a call goes through a conference server and through a gateway (see Figure 8) it may be transcoded twice which typically results in decreased picture quality. Why is this? Let's remember the analogy with language translation. If you translate from English to German, you lose some information but the quality is still acceptable. If you then give the German version to someone else to translate it into Russian, the final version will be farther from the original, and probably not acceptable. Moreover, gateways inject additional delay in the communication path and therefore decrease the interactivity.

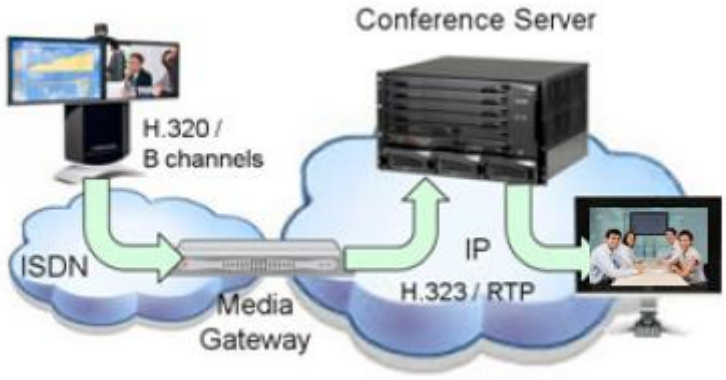

Figure 20: Media gateway configuration

Therefore, the logical question is, why not avoid standalone gateways and use the conference server as a gateway instead? The conference server is already in the network, and it does have the required functionality to support multiple protocols.

2.2.4) Scalable Firewall Traversal

Firewalls constitute a major problem for IP communications, both with VoIP and visual communications. Application-aware firewalls have been discussed for long time, but in reality, most firewalls require a traversal mechanism such as H.460.17/18/19 for the H.323 family of protocols and ICE for SIP. Both architectures require a Session Border Controller (SBC) that is usually deployed in the so called de-militarized zone (DMZ) of the organization's headquarters or the service provider data centre. There are two connectivity requirements for an SBC. It must have a public IP address to connect to endpoints over the Internet. It also must connect to the internal servers which can be—H.323 gatekeepers, SIP servers, MCUs, recording, and streaming servers. Figure 18 depicts the configuration.

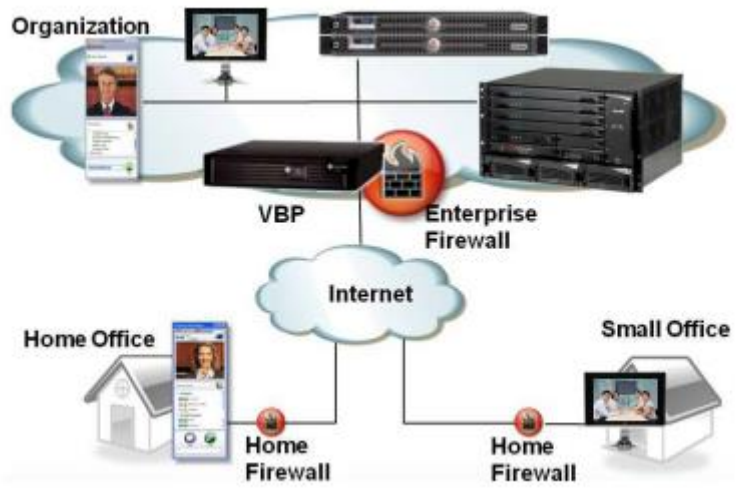

Figure 21: Scalable Firewall Traversal

- **CONFIGURATION**

Parameter	Explanation
Registration	Permit end points to register with the SBC making it easier for them to communicate across company firewall.
Prioritization	Enables better fluidity and shaping of traffic

Table 6: SBC configuration

In selecting this server the number of endpoints the system is expected to have has to be taken into account so as have an estimate of the desired average number of participant we expect for a conference. From that value we can now determine the server's throughput from where an estimate of the bandwidth will be made.

2.2.5) Scalable Firewall

Firewalls control the traffic between the internal and external networks and are the core of a strong network security policy. One of the primary goals of a firewall is to control access and traffic to and from the internal and external networks. The Firewall lets us securely control

access to computers, clients, servers and applications. For our network, we require the following firewall features:

- Identity and computer awareness
- Internet access and filtering
- Application control
- Intrusion and threat prevention
- Data Loss Prevention

Configuration:

Configuration of the firewall is of two types based on our use of it:

- **Front-end firewall:** Configuration intended to handle traffic for 'De Militarized Zone' alone.
- **Back-end firewall:** Configuration between DMZ and internal network. Traffic management handled for DMZ and internal network.

2.2.6) Conferencing Architectures

The implementation of a physical and or virtual Network at SNH is based on the following comparative advantage offered by each. This section presents the advantages and disadvantages of each design option.

Design Option 1—Physical Network

Advantages of using physical network include:

Security: Because each network segment is separated from another network segment with no physical connectivity between them, the devices that provide connectivity for hosts on physical network segments are not susceptible to a hacker breaching one device and gaining access to any logical network managed by the device.

Less firmware updates required: Because the firmware of the physical devices is so much simpler, they are less likely to require firmware updates.

Disadvantages of using physical network include:

More physical devices to manage: With more physical devices to keep track of, the ongoing management costs are higher. This is especially true when a highly available solution is required.

Expense: Purchasing multiple physical devices is generally more expensive than buying a single device that permits simpler network configuration.

Difficult to reconfigure: If the network topology changes, the process of "re-plugging" the physical devices is slower due to the requirement for physical cabling changes.

- Design Option 2—Virtual Network

Advantages of using a virtual network include:

Flexible configuration: Configuration is manageable, although this requires people in

SNH with the requisite skills to do this.

Fewer physical devices to manage: With fewer devices to track and manage, the ongoing management is likely to be simpler.

Expense: Purchasing a single physical devices is generally less expensive than buying multiple devices that permits physical network configuration.

Disadvantages of using a virtual network include:

Security: Because all the logical network segments are on the same physical device, all segments are at risk if the device is breached by an intruder.

Higher skill set requirements: Virtual devices require specialized skills to administer; for an organization to configure and support this device in house, time and money will have to be invested in training the support staff.

2.3) Video conference technologies

In this section, the focus is on the most important standards and protocols related to the video conferencing field. This technical part will help us not only to understand the choice of the technology to be use but it's equally going to help us understand the demands required in the configuration of the core network servers we just saw earlier in this dissertation. In the

following subsections, all G.xxx and H.yyy standards refer to the corresponding specifications of the International Telecommunications Union (ITU). Each section also contains an example of a proprietary codec popularly used in the area in question.

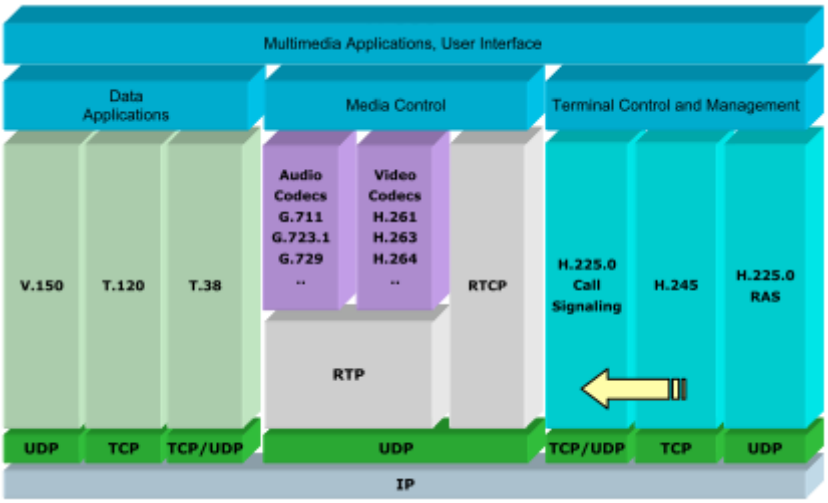

Figure 22: Standard stack

2.3.1) Signalling

Signalling means the different kinds of standards used in video conferencing systems to control communications between systems. As a rule of the thumb it can be said, that basically video conferencing is possible only between systems using the same standard. However, there are specific gateways which can be used to interconnect endpoints using different standards, which will be discussed separately. In this subsection, the most common video conferencing signalling standards are introduced.

2.3.1.1) H.320

The ITU H.320 standard describes a video conference connection over ISDN networks. The method gained momentum after the introduction of ISDN telephone lines and thus brought standardised video conferencing to a larger audience. On the upside, it was possible to use a basically universal digital phone network for calling sites around the world (although differences in the national ISDN implementations caused some problems). Although this was much cheaper than leasing a special fiber optic or satellite connection, the expenses could still be noticeable: holding a one hour international video conference at 384kbps speed would have six times the cost the caller would incur through international dialing multiplied by 60 minutes call duration. So, while cheaper than travelling, the

H.320 standard video conferencing was not a cheap option; the equipment was expensive to acquire, and the operating cost including the telephone line fees did cost another overhead as well. Also, the interoperability between systems from different vendors is often considered problematic.

Despite the problems stated above, H.320 video conferencing is still being utilized around the globe and it is especially important in areas where broadband internet connections are not yet available or where they fail to provide a reasonably reliable bandwidth. Lately the quality of H.320 conferencing has gone up thanks to the new, more efficient audio and video compression techniques. H.320 is an overall standard and requires, as a minimum for Video Conferencing intercommunication, that the following standards are used:

1. G.711 Audio 3KHz bandwidth.
2. H.261 Video Quarter Common Intermediate Format.
3. H.221 Packaging.
4. H.242 Handshaking.
5. H.230 Frame-synchronous Control

2.3.1.2) H.323

The ITU H.323 standard from 1996 mapped out the way for video conferencing systems to connect over the Internet. Compared to the older H.320 standard, the telecommunications fee was now considerably lower – no billing per minute depending on the destination; instead, the VC system used the normal internet connection of the facility.

Video conferencing over the internet also brought many new problems. One was the bandwidth; to have a reliable 384kbps VC connection, it is generally suggested that one should have double of the bandwidth in their disposal to compensate for possible network congestion (in this case 768kbps upstream and 768kbps downstream would be recommended although 512kbps for both directions might be sufficient). One thing to notice here is, that the aforementioned internet speeds are needed for the video conference connection alone – and as the units often share the internet connection with all other traffic from the organization, this other traffic can easily make momentary bottlenecks for the VC connection unless special techniques such as bandwidth throttling or QoS (quality of service) settings are used on the network layer.

Nowadays broadband internet connections are generally fast enough for video conferencing, but still especially in rural areas the access to fast broadband can be problematic

and thus limit the call speed and the quality of the conference. International video conferencing calls also seem to present a problem in some countries and sometimes a guaranteed bandwidth from a network operator might be needed.

Another problem related especially to H.323 video conferencing standard is in the definition of the protocol. Besides using readily agreed ports, such as port 1720 for connection signalling, the ports for audio and video are dynamically selected for each session in the range of 1024 to 65535. This causes understandable problems with many firewalls or NAT (Network Address Translation) implementations. There are some workarounds and a new tunneling standard H.460, but these solutions usually include setting up special software and/or hardware to handle the connection between the local endpoint and the public internet.

2.3.1.3) H.324 and H.324m

The ITU H.324 is a standard for video conferencing over 'normal' PSTN. In a way, it's the modern standard for picture phones, but the technology is not widely adopted. A newer technology based on the H.324 specification is the ITU H.324m, which is probably more familiar to people as the video call capability on the new 3rd generation (3G or UMTS) mobile phones. Usually, a dedicated gateway is needed for interoperability between H.324m and H.320/H.323, but some newer H.323-endpoints are capable of handling H.324m calls independently.

2.3.1.4) SIP

SIP is a signaling protocol for establishing, maintaining, modifying, managing, closing interactive sessions for Internet conferencing, telephony, presence, events notification and instant messaging. SIP was developed by the IETF. The IETF standard SIP differs in many ways from the H.323 video conference standard. Modelled after the ideas in HTML and SMTP, SIP uses simple text-based signalling and allows much freedom to the implementation used in the actual session. Because of the differences in implementation and functionality SIP and H.323 are not directly interconnect able.

In the recent years, SIP has become quite popular in VoIP products and video call implementations. SIP forms the basis for signalling in many familiar applications such as iChat and Live Messenger (formerly MSN Messenger), etc. SIP is generally seen as a lightweight protocol with more flexibility and extensibility than H.323 and thus it is considered as a strong advocate for the future implementations in the field.

SIP call control uses Session Description Protocol (SDP) to describe the details of the call (i.e., audio, video, a shared application, codec type, size of packets, etc.). SIP uses a Universal Resource Identifier (URI) to identify a logical destination, not an IP address. The address could

be a nickname, an e-mail address (e.g., sip:chintanv@mit.edu), or a telephone number. In addition to setting up a phone call, SIP can notify users of events, such as "I am online," "a person entered the room," or "e-mail has arrived."

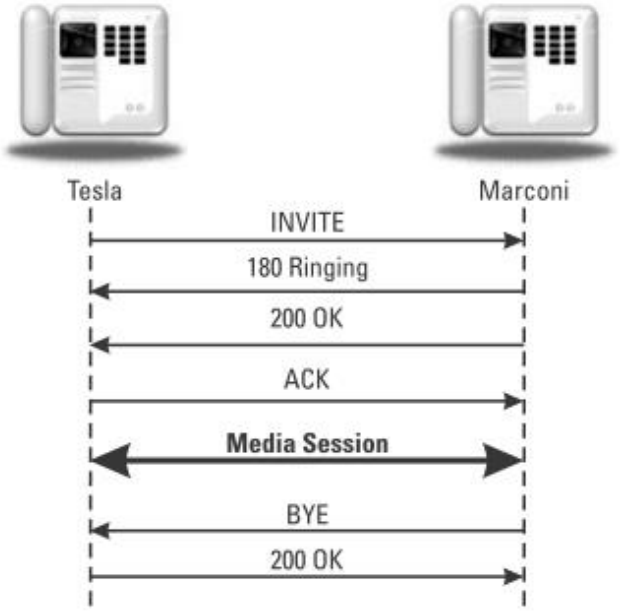

Figure 23: A simple SIP session establishment example

Last years have seen SIP becoming a more common feature even in standalone video conference units and MCUs (usually accompanying the H.323 as an alternative connection standard), but so far the SIP implementation in the video conferencing endpoints has usually been on a basic level, not yet utilizing many of the possibilities in the standard. Still, this direction of integrating multiple connection technologies into single endpoints is an encouraging sign suggesting increase in the interoperability between different systems.

2.3.2) Video codecs

Video codecs are essential for video conferencing as they are the technology used to compress the video signal into a series of data packets relayed over the network, to be decompressed at the receiving site to reform the video image. In this subsection the most

popular video compression codecs related to the video conferencing field and implications of the quality they provide are described [3].

2.3.2.1) H.261

ITU H.261 is an older video coded, implemented in almost all video conferencing systems. It was originally introduced in 1988 and later revised in 1990 and 1993. Because of its long history it is still an important codec for interoperability as nearly all video conferencing solutions support it. The picture quality of H.261 is not very good and the colour information is reduced, but the video stream still requires a relatively large amount of bandwidth (compared to the newer video codecs). Thus, with the limited bandwidth of 1990-s, the experienced image quality of older video conference systems was often relatively degraded.

2.3.2.2) H.263

The ITU H.263 is a more developed video codec. Compared to earlier H.261, this newer codec improved compression efficiency and offered a better colour dynamic. The codec also got multiple extensions, e.g. the so called H.263+ (a.k.a. H.263v2) and H.263++ (a.k.a. H.263v3) which introduced for example customised image sizes and improved decoder memory management. Old Flash players utilised a proprietary Sorenson Spark codec which was based on H.263.

2.3.2.3) H.264

ITU H.264 (also ratified as the ISO's MPEG4 AVC) is a standard for efficient picture compression. Relatively new and complex, it requires much more processing power than its predecessors and thus cannot often be implemented on old hardware. Besides better compression, H.264 also includes advanced functionalities such as an in-loop de-blocking filter which effectively eliminates possible packing artefacts from the image, which were often considered as a noticeable picture quality problem when using older video codecs.

The efficient compression of H.264 resulting in a reduced need for bandwidth enabled the possibility to use bigger video resolutions at reasonable connection speeds, which in turn has largely contributed to the growing use of HD resolutions in video conferencing. H.264 is also an integral part of many other high definition video implementations such as Blu-Ray, HD-DVD and DVB-T2 (Digital TV Broadcasting). It is also emerging as a new de-facto standard of streaming internet video (supported by many

popular media players such as QuickTime, VLC and even by the newest Adobe Flash Player 9).

2.3.3) Audio codecs

Audio codecs are protocols used to compress audio signals for network transport. In this subsection, the most common audio codecs utilised in video conferencing are described with some technical detail [2].

2.3.3.1) G.711

The old G.711 sound codec (ratified in 1988) is widely used around the world. This codec is probably familiar to the reader as the 'telephone quality' as it is the codec actually used to encode voice in landlines and mobile phones.

The efficiency of G.711's Pulse Code Modulation (PCM) encoding is left far behind in comparison to the newer codecs as it uses either 48kbps, 56kbps or 64kbps bandwidth but is still only able to provide 3.1 KHz audio band (300 Hz – 3400Hz) which cuts out both low and high sounds. Still, as a de-facto standard it's very important especially regarding backwards compatibility between different video conferencing solutions.

The G.711 can be used for basic speech, but loses a lot of the dynamic and clarity of the voice, and the narrow frequency bandwidth does not function very well with other sound types such as music. However, it is still used in everyday telephone discussions all the time, and this will probably also be the case for many years to come.

2.3.3.2) G.722

The G.722 sound codec, also ratified in 1988, uses the same bandwidths than G.711 (48, 56 or 64kbps), but is more advanced by offering a wider sound spectrum (7kHz, 50Hz-7000Hz) and thus making the sound clearer and more understandable. As G.711, the G.722 is a widely implemented protocol and forms a good basis for interconnectivity, but provides clearly better quality.

2.3.3.3) Other widely used audio codecs

The G.722.1 offers the same 7KHz audio band as G.722, but thanks to better compression it uses less bandwidth, namely 24 or 32kbps. This makes G.722.1 a better

option when bandwidth is an issue, although there are also codecs, such as G.723.1, which function with even less bandwidth. The G.722.1 annex C, Standardised from the originally proprietary Polycom Siren 14 codec, offers a more advanced 14 kHz (50Hz – 14400Hz) audio band allowing more high frequencies and thus enhancing the clarity of sound. The difference is very clear for example when using music or other sound sources than speech.

The G.723.1, ratified in 1996, is a very low bitrate audio codec, which offers an 8 kHz audio band and uses only 5.3 or 6.3 kbps of network bandwidth, thus making it ideal for conferencing when bandwidth is an issue.

The G.728 audio coded from 1992 uses a 16 kbps bitrate to produce 3.3 KHz audio band (50Hz – 3400Hz). This codec is also quite widely implemented and thus offers good interconnectivity. However the quality is poor compared to some of the newer codecs.

2.3.4) Proprietary methods

There exist a number of systems that utilise other than standardised methods either for call signalling or audio or video encoding, or both. The reasons for this can be versatile – to avoid licensing costs, or to overcome limitations ingrained in existing standardised solutions.

Systems using proprietary signalling are usually not interoperable with others, but can only connect to other similar systems – however it is possible to construct special gateways to provide interconnectivity. One example of a system, utilising speciality signalling, is Skype, which even uses encryption to cipher the messaging on the network.

The VP6 video codec from On2 Technologies is probably one of the most utilised proprietary video codecs in the video conferencing field – especially when it comes to desktop video conferencing. The VP6 codec is widely used in applications such as Skype, AOL AIM, etc. The codec is also built in to Adobe Flash Player 8 and 9 and is usable on almost any computer with a modern web browser – thus the success of the codec in web based video conferencing solutions.

The proprietary codecs iLBR (internet Low Bit Rate codec) and iSAC from Global IP Systems are widely used in everyday internet applications such as Skype, Yahoo Messenger and AOL AIM as well as in net2phone, Marratech, WebEx, Gizmo, Google Talk, etc. The iLBR offers 4 kHz audio band at 15.2 or 13.3kbps while iSAC offers better 8 kHz audio band with adjustable network bandwidth between 10-32 kbps [3]. As technologies specially

developed for internet use, they have a standard response to delay and jitter thus smoothing out the occasional problems with the network connection.

2.3.5) Other related standards

Other standards related to video conferencing include H.239 for additional media – usually utilised for sharing computer screen – as well as other internet and H.xxx family related standards. In the following these are briefly introduced.

2.3.5.1) H.239

The ITU H.239 is not a VC standard in a sense of H.320 or H.323, but it's a way of including a second video stream within a H.323 (or H.320) VC connection. Basically, this means that, it is possible for example to send images of both the speaker and his slides in a single video conference connection so that the receiving end sees both streams simultaneously (for example on two different screens).

Previously, most of the manufacturers had their own proprietary 'dual stream' implementations, such as Tandberg's DuoVideo and Polycom's People+Content, but as a standard, H.239 has levelled the field and now the interoperability between different manufacturers is much easier. Many new MCUs are also capable of handling H.239 in a multipoint session, which greatly expands the usability of the standard.

2.3.5.2) Internet standards

On the quite standardised field of video conferencing, there are a huge number of other protocols and standards. They work mostly in the background though important but they will not be described in as much details as the ones above.

Standard	Use
IP	the layer transporting traffic on the internet
TCP (Transmission Control protocol)	used for example for transport layer protocol
IP Multicast	used to efficiently transport audio & video in multicast enabled networks
UDP (User Datagram protocol)	used often for audio and video feeds

RTP	used for audio & video data transport over UDP
RTCP	Real-time Transport Control protocol – used to control RTP traffic

Table 7: Internet standards related to video conferencing

Standard	Use
H.233, H.234, H.235	security and encryption in H.323, H.320
H.245	multimedia control in H.323
H.450	generic added functionality for H.323, like call transfer (H.450.2) and call diversion (H.450.3)
H.460	firewall traversal for H.323 signalling/media

Table 8: ITU standards related to H.320 and H.323 video conferencing

The IP-video conferencing field (that is video conferencing over internet) builds on a number of Internet related protocols and standards, which are not evaluated within a scope of this thesis. The most important internet standards are briefly introduced in Table 4. There exist also a number of ITU ratified standards that function within the H.320 and H.323 video conferencing. A selection of the most important standards is introduced in Table 5.

2.3.5.3) Video resolutions

Besides video codecs, there is another variable having a strong impact on the video quality – video resolution. The resolution can be understood as the actual size of the video image (while even a small video image can be zoomed in to fill the whole screen, it would appear to be pixelated and thus of low quality).

Name	Resolution (pixels)	As a digital image
SQCIF	128 x 96	0.012 mpix
QCIF	176 x 144	0.025 mpix
QVGA	320 x 240	0.076 mpix
CIF	352 x 288	0.1 mpix
VGA	640 x 480	0.3 mpix
4CIF ("Television")	704 x 576	0.4 mpix
720p ("HD ready")	1280 x 720	1 mpix
1080p ("Full HD")	1920 x 1080	2 mpix

Table 9: Popular video resolutions

The most popular video resolutions are listed in Table 6. The formats QCIF and CIF are defined in the specifications of H.261, while SQCIF and 4CIF are specified in H.263. VGA and QVGA resolutions are commonly utilised in computer-based communications solutions alongside varying codecs. High definition is normally used with H.264 encoding.

2.4) Network Security

Having a solid security policy for our infrastructure is not only to prevent but equally mitigate human or natural attacks on the network. The objective of a security policy is to protect the computer systems from unauthorized persons and at the same time allow access to the authorized users. We will begin by studying the fundamentals of security then examining possible threats to our system.

2.4.1) Security Fundamentals [6]

When the term security comes up, we think of encryption. However, security encompasses several important areas of protection. These areas of protection roughly comprise six groups:

- ✓ Confidentiality
- ✓ Availability
- ✓ Authentication
- ✓ Identity
- ✓ Authorization
- ✓ Integrity

Confidentiality between a sender and a receiver means that only the sender and receiver can interpret the data. Two endpoints achieve confidentiality using encryption. To establish an encrypted link, the sender and receiver exchange a cryptographic key in a secure manner, and then each side uses the key to encrypt or decrypt the data stream.

Availability ensures that infrastructure resources are protected from resource depletion from an attacker.

Availability requires protection against denial-of-service (DoS) attacks.

Authentication and identity often describe the same concept and may mean two things: An endpoint can authenticate data to prove that the data is valid. An endpoint can authenticate data without authenticating identity. A section later in this chapter reveals how cryptographic hashes can authenticate data. An endpoint can authenticate its identity by presenting

cryptographic credentials that proved its identity. As explained later in this chapter, the participants in the connection use either pre-shared secrets or cryptographic certificates to establish identity.

Authorization is not to be confused with authentication. Authorization maps the authenticated identity (an endpoint or user) to a set of permissions or capabilities allowed for that user. Secure video conferencing systems often implement authentication and authorization with an AAA (authentication, authorization, and accounting) server.

Integrity allows a receiver to detect whether an attacker has tampered with data while in transit on the network. One of the ways for an endpoint to provide integrity for a data packet is to authenticate the contents of the entire data packet.

2.4.1) Security threats and proposed solutions

Without measures to ensure the six fundamental security protections, the network infrastructure and endpoints are open to threats from attackers. This section describes several types of threats and actions we are taking into consideration to mitigate these threats.

- Confidentiality Attacks

Without confidentiality, an attacker can listen to the audio and video streams between two endpoints. Hacker tools are available on the Internet for eavesdropping on voice packet data. One of these tools is called VOMIT (Voice Over Misconfigured IP Telephony). VOMIT processes a stream of captured voice packets and plays the audio.

Solution: We will apply encryption to the media packets. Vendors of conferencing products are universally adopting the Advanced Encryption Standard (AES) to encrypt media streams. In IP networks, Voice over IP (VoIP) gear typically uses the Real-time Transport Protocol (RTP) to transmit media streams. Secure Real-time Transport Protocol (SRTP) is an extension of RTP that encrypts media streams, defined in IETF standard RFC 3711. See the "Media Encryption" section later in this chapter for details.

- Denial-of-Service Attacks

Attacks on availability are called denial-of-service (DoS) attacks. A DoS attack is any attack that disrupts the availability of service to legitimate users and can take several forms:

- Depletion of network bandwidth

- Replay attacks
- Malware
- Connection hijacking
- RTP hijacking

The following sections describe each of these DoS attacks in more detail.

Depletion of Network Bandwidth

Depletion of network bandwidth attacks involve flooding the host network with enough data to clog the ingress/egress points in the enterprise network. These attacks appear primarily as a flood of UDP packets. Often, these attacks are launched from a large number of external endpoints on the public Internet, in which case they are referred to as distributed denial-of-service (DDoS) attacks.

Solution 1: When a flood attack overwhelms the bandwidth of the connection that links a service provider to an enterprise, the only way to stop the attack is to discard attack packets in the service provider. Service providers typically perform this type of packet shunning with an anomaly detector device and a guard device. The anomaly detector identifies potential attack traffic and instructs the guard to scrub the traffic. The guard pinpoints and discards attack packets before they reach the enterprise network.

Solution 2: Routers and switches can implement bandwidth rate limiting. Cisco routers and switches offer a feature called microflow policing to limit the bandwidth of data from an attacker. Enterprises use microflow policing to protect server infrastructure, such as a scheduling server, H.323 gatekeeper, Session Initiation Protocol (SIP) proxy, or CallManager. However, this bandwidth-limiting protection is most effective if it is deployed with two strategies:

Replay Attacks

Another attack that can cause disruption is the replay attack. The attacker begins by sniffing and recording the packets flowing on the network between two entities during a legitimate connection. The attacker then replays these packets to one of the endpoints. The target endpoint may consider this replayed stream to be legitimate and attempt to process the data, resulting in excessive resource consumption.

Solution: Endpoints thwart a replay attack by using cryptographic authentication, along with a time stamp or sequence number. The receiver verifies the authentication and then verifies that the time stamp or sequence number is valid.

Malware

Malware is any type of data that can compromise an endpoint or server. A worm is a type of malware that consists of network packets that cause a server to execute a program. When the worm is running on the machine, the worm can take over the server and cause it to fail.

Solution: Endpoints or servers can use an intrusion prevention system (IPS), which is a standalone network device that identifies malware located in packets and then discards the packets before they reach a host. A host-based IPS (HIPS) is a software-based IPS that resides on the server itself, usually at the kernel level. The HIPS identities malware packets and discards them before a running process receives them.

Connection Hijacking

After two video conferencing endpoints establish a legitimate connection, an attacker might attempt to hijack the connection by impersonating one of the participants by issuing signaling commands to take over the conversation. The attacker might also use this type of spoofing to cause the connection to fail, in which case the attack is also considered a DoS attack.

Solution: Endpoints can thwart connection hijacking by authenticating the signaling messages.

RTP Hijacking

Whereas connection hijacking is a method that attempts to take over the signaling layer of a conversation, RTP hijacking operates at the media layer and is an attempt by an intruder to inject RTP media packets into a conversation. The intruder essentially becomes an additional, unwanted participant.

Solution: Endpoints can thwart RTP hijacking by authenticating the media packets.

- Authentication and Identity Attacks

Attackers may compromise authentication or identity to exploit theft of service or man-in-the-middle (MitM) attacks.

Theft of Service

By compromising identity, attackers can perpetrate theft of service or toll fraud. As you learned in the "Connection Hijacking" section, an attacker can impersonate another user and then take over an existing connection. An attacker may also steal services by spoofing another endpoint directly and then attempting a direct connection.

Solution: Authenticate signaling packets and use cryptographic identity.

Man-in-the-Middle Attacks

A MitM attack occurs when an attacker inserts a rogue device between two connected endpoints. The MitM can then listen to packets that flow between the endpoints and can modify packets in transit. The MitM is invisible to the two endpoints, which are unaware of the attack. One way for an attacker to become a MitM is to spoof the identity of each endpoint to the other. Figure 8-3 shows this scenario.

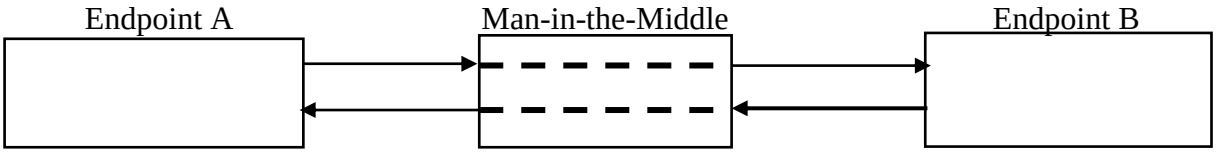

Figure 24: A Man-in-the-Middle Attack between Two Endpoints

The attacker connects to endpoint A and pretends to be endpoint B, and then connects to endpoint B and pretends to be endpoint A. The MitM acts as a router and can observe packets flowing between endpoints A and B, without either endpoint knowing about the attack. This attack can also work if both endpoints use encryption, without authentication; in this case, the MitM sets up an encrypted link with each endpoint. The MitM can decrypt and then re-encrypt each packet that passes through it. The MitM can also inject data into the media stream or change the media stream.

Solution: We will use authentication and integrity for each signaling message and media packet.

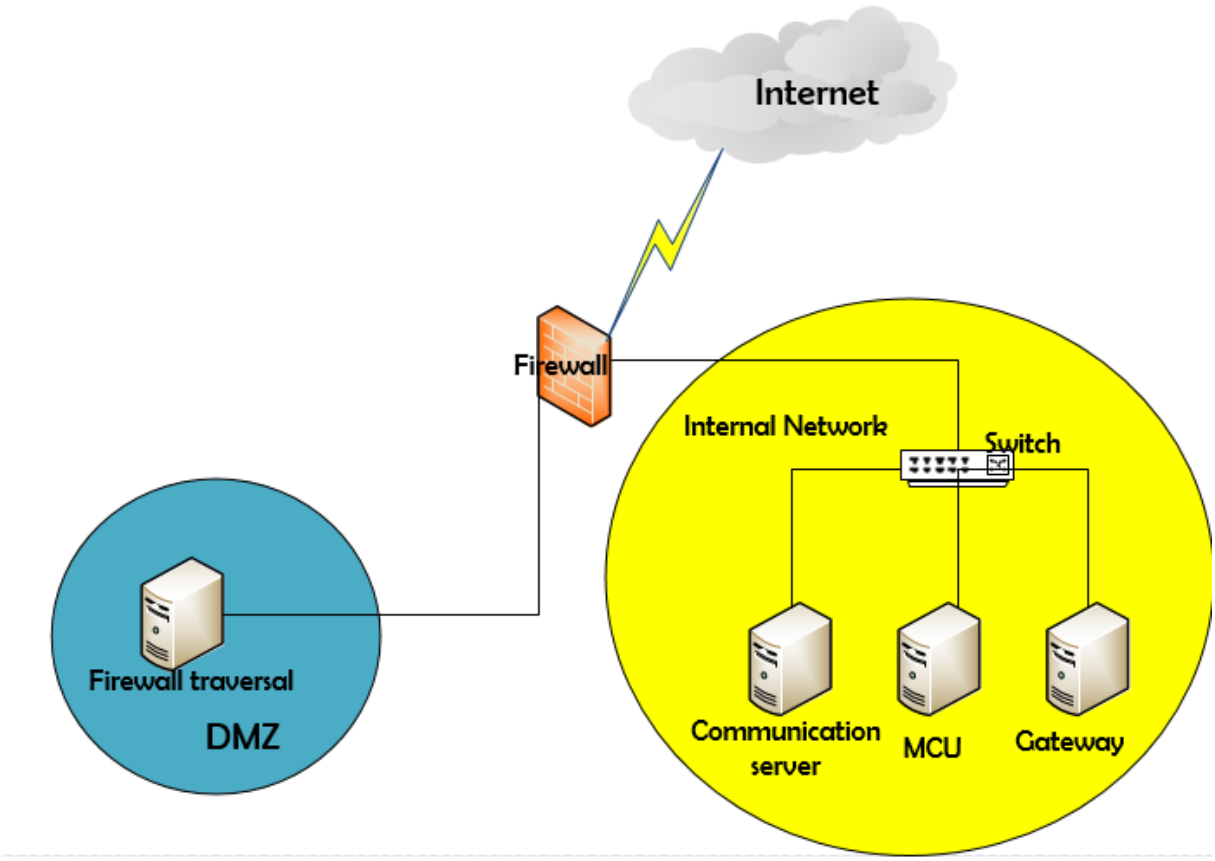

Figure 25: Basic security configuration

The internal configuration of individual servers is what solidifies the security of the infrastructure we are putting in place.

CHAPTER 3: RESULTS AND COMMENTS

Here we begin with presenting the 2 design options we were asked by SNH to propose then we proceed with the choice of technology for acquisition of equipment in view of immediate implementation. We continue with attributing the most suitable video conferencing system mentioned in chapter 2 above to the different meeting rooms found both at the SNH headquarter and its extension buildings (in Yaoundé like the various branches).

We shall be ending with handling security both of facility and data of the system as well as the CAPITAL EXPENDITURE (CAPEX) estimate.

3.1) State of the art or the cutting edge technology

SNH needing an infrastructure to permit them carry out video call, we propose a solution meets 4 principal requirements for effective communication when dealing with IP networks. From the work carried out in chapter 2, we realize it is of great importance to have these parameters taken seriously into account especially in the choice of vendors with cutting edge technology talking about video conference. These are:

- Jitter with acceptable limits
- Latency which does not exceed **150ms**
- Packet loss with limits of less than 5%
- Bandwidth

These parameters all work towards increasing tremendously the QoS of the network.

- A virtual deployment made of Cisco Systems, Inc.,
- A centralized UC network infrastructure made of both Polycom and CISCO

Our choices of Polycom and Cisco fall in line with the fact that these vendors have not only succeed in taking into account the points we just listed above but are equally the worldwide leaders in Video conferencing solutions providing networks that can securely and reliably handle all types of traffic, throughout an entire network, over virtually any media, while also providing consistent service delivery to all users.

Before we move with our proposals aimed at meeting SNH's goals, we will look at the expected data flow for a secure video conference system.

Data Flow Diagrams

Figure 26 below shows the base level data flow diagram for the client side application. It has one data store which maintains static data like user's settings for audio/video streams, user information (user_id, private_key used for encrption etc), server information. Data store is also used to store runtime information like information of remote participants. The Secure Video Conferencing Client (SVCClient) interface helps the user configure parameters like joining a conference, creating new conference etc. It interacts to the server and other clients through the session border controller.

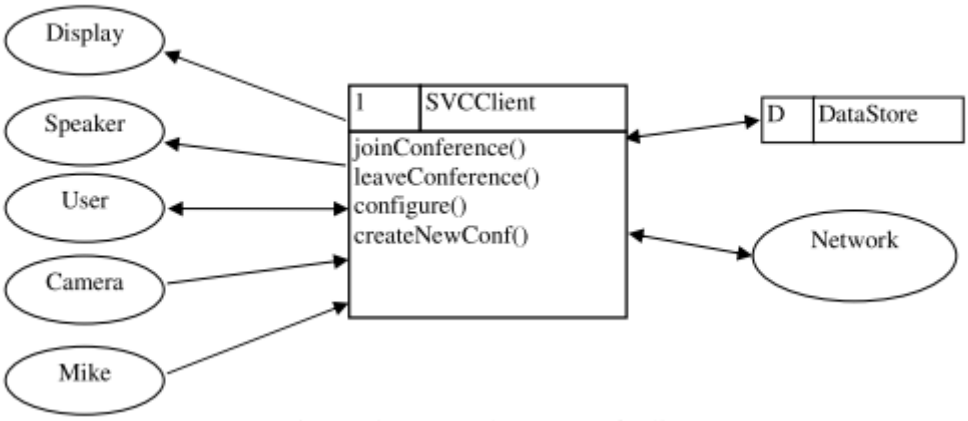

Figure 26: Client level data flow diagram

Figure 26 shows the general client data flow when scheduling and running a video conference. It is divided into five processes. UserInterface provides GUI (Graphical User Interface) to the user. DataHandler maintains the information stored in DataStore and provides the stored information to the different processes as needed. SessionManager process interact with the servers to maintain the state of the conference and to send the feedbacks of the client to the servers and finally to get the QoS signals from the servers. Whenever it gets the new participant information from a server, it starts a new receiver for that participant and also adds the participant in the target list of transmitters. After every fix interval of time it collects the feedbacks of all receivers and sends to the different server.

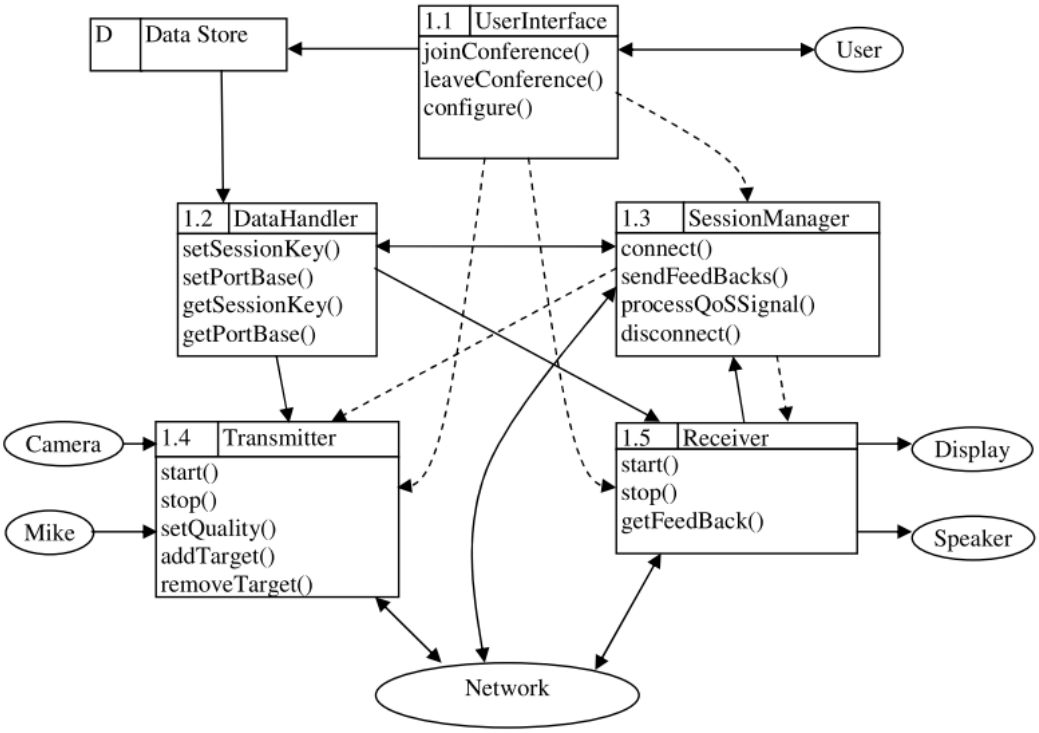

Figure 27: General client data flow diagram

3.1.1) Virtual Network Architecture.

One of our proposals for SNH is option 1 which is that of a virtual network to have:

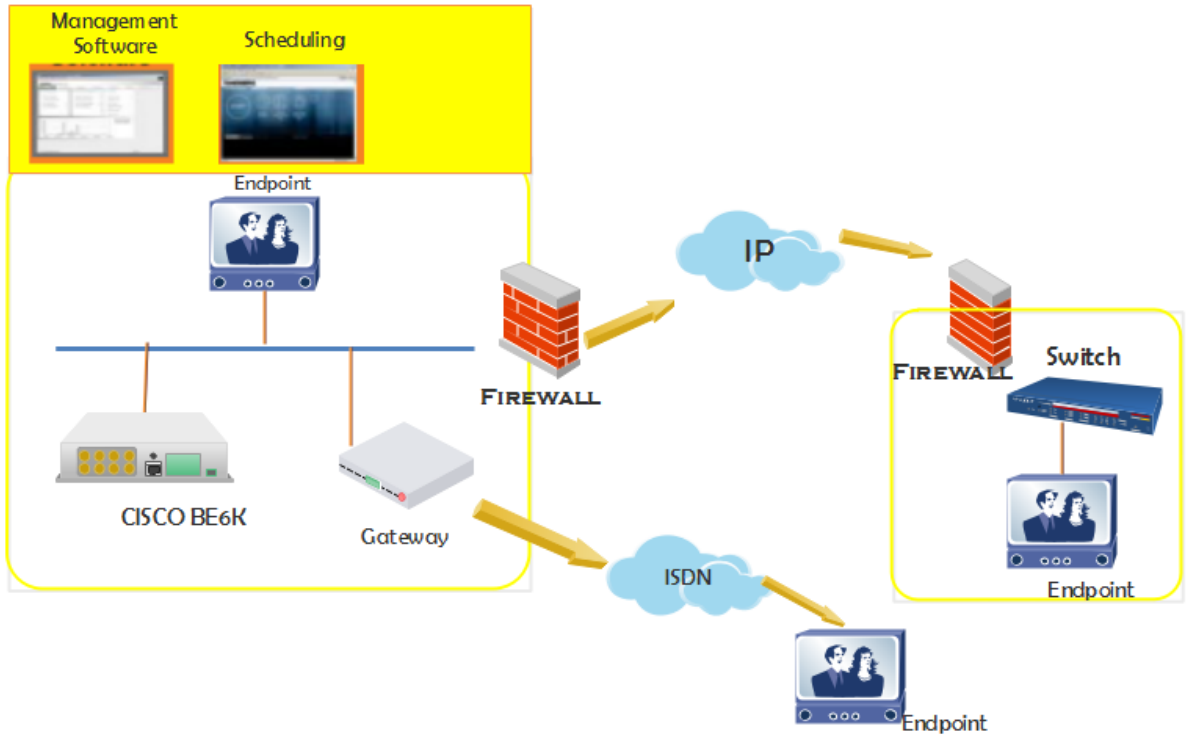

Figure 28: Proposed virtual Video core Network Architecture

To provide video calls, SNH will acquire principally:

- CISCO BE6K [10]

This the main server with different virtual servers in it notably the communication server, management server and the firewall traversal. It is going to be configured as earlier described in chapter 2.

- Checkpoint NG640 Appliance (Firewall)

This one device offers integrated, multi-layered security; Firewall, VPN, IPS, Antivirus, Application Visibility & Control, URL Filtering and Email Security—all in a quiet, compact desktop form-factor. The NG640 Appliance runs the same industry-leading security that is used to secure ENGIE CAMEROON. It's going permit SNH meet most of its security preoccupations.

- H.320 and H.324M Gateways

SNH will use this to reach even its partners using old age video technology

- Endpoints

Through the endpoints principally the SX 20 [10] and a Samsung display to be described below, SNH by acquiring them will attain the goal of making video calls around and out of Cameroon given that they contain MCU to connect to up to 4 participants at a time.

This is a real simplified infrastructure especially for a company the size of SNH.

3.1.2) Centralized Polycom UC network Infrastructure

Our second proposal is that of physical centralized network.

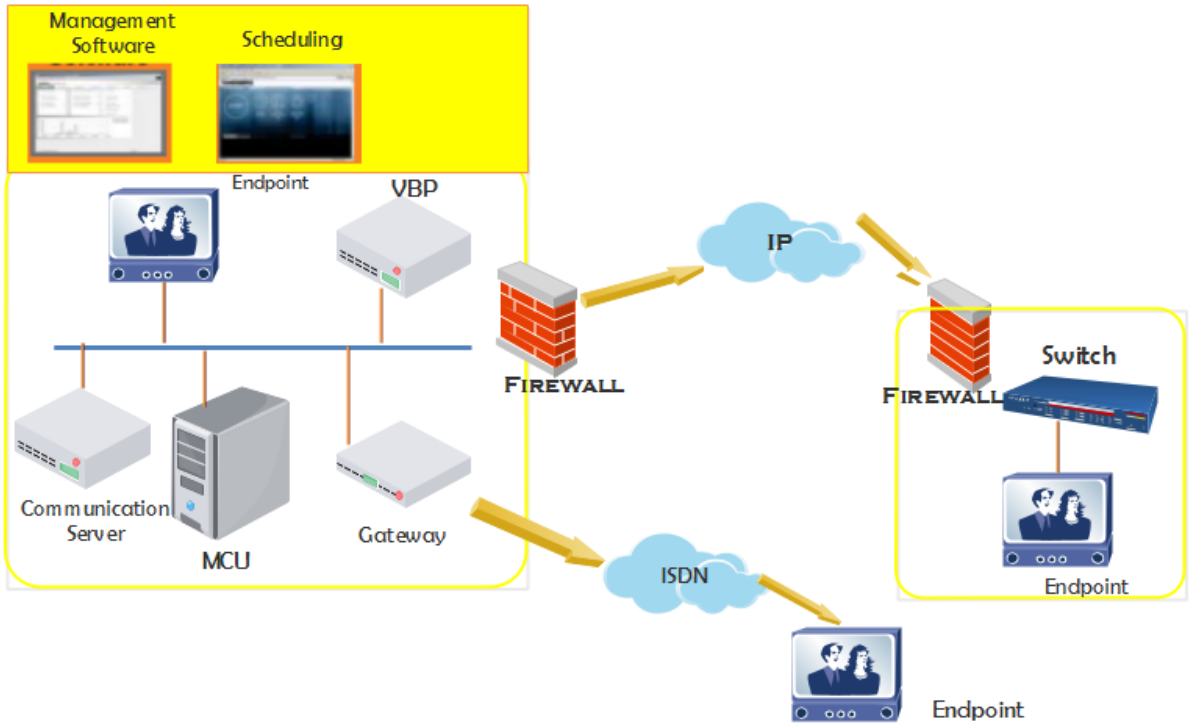

Figure 29: Proposed Physically located Video Core Network Architecture

The mandatory elements include:

- **Clustered Polycom CMA4000 and DMA7000 (Communications servers)**

The powerful Polycom RealPresence DMA and Polycom RealPresence CMA solutions will allow users to connect regardless of protocol standard, device, network, or location making communication between employees, partners and customers simple, yet effective. Administrators can expand and offer new services by leveraging existing communication network investments through the clustered Polycom RealPresence DMA and Polycom RealPresence CMA system. Database engine and storage are deployed on both servers and are kept in sync in real time using a data replication mechanism. This approach provides a simple deployment scenario and removes the single point of failure.

- Polycom RMX 4000 (Conference Server)

The conference server being one of the most important when we talk of video conferencing, the Polycom RMX 4000, it has ability to serve up to 1440 conference participants, of which up to 360 can be video. Its backplane (fabric switch) supports 4 times higher bandwidth (4 x 2 x 10Gbps = 80Gbps) that allows free flow of video across blades. This and the fact that it meets most of the requirements mentioned in chapter 3.1, we were pushed to go for it.

- Polycom Video Border Proxy (VBP) 6400

Because conferences would be held with partners around and out of Cameroon, there was a need to securely leave the company network in order to communicate with these partners as explained in chapter 3 above, thus Polycom VBP 5300-E25 being the largest Proxy (VBP) 5300 model and currently with a throughput of 25Mbps, was for us a good option.

- Checkpoint NG640 Appliance (Firewall)

This one device offers integrated, multi-layered security; Firewall, VPN, IPS, Antivirus, Application Visibility & Control, URL Filtering and Email Security—all in a quiet, compact desktop form-factor. The NG640 Appliance runs the same industry-leading security that is used to secure ENGIE CAMEROON. It's going permit SNH meet most of its security preoccupations.

- H.320 and H.324M Gateways

SNH will use this to reach even its partners using old age video technology

- Endpoints

Through the endpoints principally the SX 20 [10] and a Samsung display to be described below, SNH by acquiring them will attain the goal of making video calls around and out of Cameroon given that they contain MCU to connect to up to 4 participants at a time.

This infrastructure presents the advantages we sure in section 2.2.6) and will go a long way to boost the performances of SNH.

3.1.3) Endpoints

We shall talk of the endpoints we are proposing both of CISCO and POLYCOM. Before we shall look at how the SNH meeting rooms will look like in the figure below.

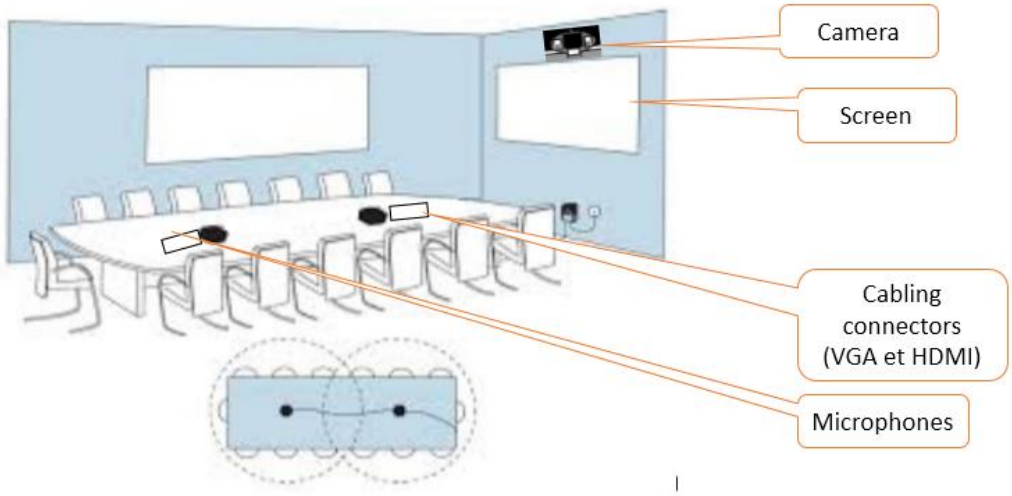

Figure 30: VC meeting room

From the figure above and what we covered chapter 2, there are mandatory elements that come into play. During our choice, we considered them while making our choices and it is reflected from the different datasheets that would be made available at the annex. These are:

- Camera
- Display (screen)
- Microphones
- Speakers
- CoDecs

It should be noted that these endpoints are flagship state of the art in ensuring high definition video communication much needed by SNH.

3.1.3.1) Cisco TelePresence SX20 Precision HD 12x Camera

Cisco through the telepresence offer have a number of offers when it comes to VC from which we have selected the following which suit our needs and the realisation of this project.

Given that the extension building of SNH has a 3D video room, we choose this system because it is a screen adaptable camera with characteristics that meet SNH's goals, this because the 3D video room already has a high resolution display.

Figure 31: Cisco TelePresence SX20 Quick Set with Precision HD 4x Camera, Table Microphone, and Remote Control

3.1.3.2) Polycom HDX 9000 Series

Just like the Cisco Telepresence SX20, the Polycom HDX 9000 Series is a package which has a codec, camera, microphones and a remote control. This will go a long way to enhance decision making at SNH.

Figure 32: Polycom HDX 9000 Series

3.1.3.3) Polycom HDX 4500 Executive Desktop

Polycom HDX 4500 is a proven solution for effective video collaboration. The system includes a built-in 24-inch HD display, camera, microphones and two speakers. The codec

supports high-definition video and audio standards, content sharing, and multipoint for four via licensing. Set up this all-in-one video conferencing system at your desktop, huddle space or small meeting room.

Figure 33: Polycom HDX 4500

3.2) SYSTEM FINANCIAL PROPOSALS

3.2.1) Quantitative and Estimated Budget for Integrating a Video Conferencing System into the existing SNH Network Architecture

Hall	Equipment placement	Quantity	Unit price (In Dollar)	Total price (In Dollar)
ADG	➢ CISCO MX300 G2 ✓ Display ✓ Camera ✓ Speakers ✓ Microphones ✓ Codec ➢ Touch control	1 1	23,900.00 1,500.00	23,900.00 1,500.00
All other meeting halls with Douala, Mvia and	➢ CISCO SX20 + MCU ✓ Camera ✓ Speakers ✓ Microphones ➢ Samsung 55” Display	23 46	11,095.00 2,500.00	255,185.00 115,000.00

Bipaga.	➢ Touch control	23	1,500.00	34,500.00
Server Room	➢ Cisco Telepresence Video Communication Server license	24	650.00	15,600.00
	➢ Cisco Expressway Series license	24	714.00	17,136.00
	➢ CISCO UCM licenses	24	750.00	18,000.00
	➢ CISCO BE 6000	2	7,000.00	14,000.00
	➢ Checkpoint NG640	4	1,500.00	6,000.00

Total: $500,821.00

NB: the prices of other peripherals aren't added here

NB: this amounts to close 40% mission order reduction

ANNEX

	Cisco TelePresence Precision Camera (option of 2.5x, 4x and 12x cameras).
	Touch Control graphical interface solution is a highly-intuitive touch screen device that enables users to quickly initiate video conferences, free from complicated interfaces or technical support.
	SX20 Codec

	55-inch. (1.4m) LED monitor, edge LED backlight ● Resolution: 1920 x 1080 (16:9) ● Contrast ratio: Typical 4000:1 ● Viewing angle: +/-178 deg ● Response time: Typical 8 ms ● Brightness: Typical 450 cd/m2
	Cisco TelePresence Table Microphone
	Cables • DVI-I • HDMI • VGA Power Supplies

3.2.2) Quantitative and Estimated Budget for Centralized Polycom UC network Infrastructure

Hall	Equipment placement	Quantity	Unit price (In Dollar)	Total price (In Dollar)
ADG	➢ Polycom HDX 4500 ✓ Display ✓ Camera ✓ Speakers ✓ Microphones ➢ Touch control	1 1	11,999.00 1,500.00	11,999.00 1,500.00
19 halls in	➢ Polycom HDX 9000 + HDX	19	24,748.00	470,212.00

Yaoundé, Douala, Mvia, Bipaga.	MPPlus 4-way Multipoint Software ✓ Codec ✓ Speakers			
	➢ Eagle Eye 1080p Camera	19	3,500.00	66,500.00
	➢ HDX microphones	19	1,500.00	28,500.00
	➢ Samsung 55" Display	19	2,500.00	47,500.00
	➢ Touch control	19	1,500.00	28,500.00
4 meeting halls in the Yaoundé Headquarter	➢ CISCO SX20 + MCU ✓ Camera ✓ Speakers ✓ Microphones ✓ Codec	4	11,095.00	44,380.00
	➢ Samsung 55" Display	8	2,500.00	20,000.00
	➢ Touch control	4	1,500.00	6,000.00
Server Room	➢ Cisco Telepresence Video Communication Server license	4	650.00	2,600.00
	➢ Cisco Expressway Series license	4	714.00	2,856.00
	➢ Checkpoint NG640	5	1,500.00	7,500.00
	➢ Polycom CMA 4000	1	12,500.00	12,500.00
	➢ Polycom DMA 7000 Redundant solution	1	30,000.00	30,000.00
	➢ Polycom RMX 1500 (10HD720p)	1	60,000.00	60,000.00
	➢ Polycom Video Border Proxy 5300-E25	1	10,100.00	10,100.00

Total: $850,647.00

NB: the prices of other peripherals aren't added here

NB: this amounts to close 25% mission order reduction

ANNEX

	The Polycom EagleEye 1080 III Camera offers full high definition capture with 1080p30 Resolution.
	Touch Control graphical interface solution is a highly-intuitive touch screen device that enables users to quickly initiate video conferences, free from complicated interfaces or technical support.
	HDX 9000 High Definition Codec
	The Polycom HDX 4500 is an all-in-one personal telepresence system that brings the UltimateHD experience to the desktop or small work group. With a 24 inch 1 080p display, powerful stereo speakers and a sleek design, the HDX 4500 offers up to 720p60 or 1080p30 video standard.
	HDX Microphone Array. Compatible with HDX 9000 Series. 360 Degree coverage with 22 kHz of high fidelity audio using Polycom Microphone Array. Includes 7meter cable.

	Cables • DVI-I • HDMI • VGA Power Supplies

3.2.3) Comparism with a software video conferencing system and reasons for the choice of our proposed solutions.

The prices of both software and web based video conferencing systems varying but amongst the cheapest in this domain, we decided to take the case of a popular software known as "Skype" for our analysis knowing it is amongst the lowest cost systems with an appreciable quality. An estimate is as follows:

Hall	Equipment placement	Quantity	Unit price (In Dollar)	Total price (In Dollar)
All other meeting halls with Douala, Mvia and Bipaga.	➢ Computer set with recommended characteristics as follows: 2 CPU cores (2GHz or higher) and 4GB RAM and 200 GB of disk space.	24	1,000.00	24,000.00
	➢ Webcams	24	300.00	7,200.00
	➢ Microphones	24	200.00	4,800.00
	➢ Speakers	24	300.00	7,200.00
Server Room	➢ Acquiring of a yearly premium license.	24	25.00	7,200.00

Total: 50,400.00

From this value it is clear we are at least 1/10 of our first option but we couldn't clearly estimate it impact because of the following reasons which equally pushed us to support any of the above two options:

- Software (like skype) and web based video conferencing solutions (also known as off-premises solutions) have their servers managed by the providers which possess a lot of security risk. SNH dealing with sensitive information, are very stringent when it comes to the protection of their information and thus prefer to manage their own thus increasing the security of their communications and network.
- Skype like many web based video conferencing solutions are best used for one-to-one meeting due to the size of the display (in this case the computer monitor) whereas an on-the-premises system like the ones proposed are best soot for one-to-one, one-to-many and even many-to-many meeting with sometimes 16 persons in a single meeting room making the participants feel they are besides each order therefore enhancing decision making.
- Due to its small size, it is difficult to do a whiteboard presentation with skype but easy with the systems we propose because endpoints have been chosen to permit this essential part of meetings.
- The quality is not the best coupled with lags that we frequently notice with skype, out proposed solution comes to lower this constraints.

3.3) Redundancy

To meet up the requirements of SNH concerning redundancy, it is primordial to know it comes in two forms with the way to go about it described below:

- Safeguarding of company data which we have taken into considerations by clustering the communication server to make sure data is replicated. This will increase the protection of company given that a server will be in Yaoundé and the other in Douala.
- Not being able to predict various incidences that could occur on IP networks especially the Optic fibre which is presently in use in SNH, we designed a fall back or redundant video network to tackle unforeseen incidences on the presently used optic fibre. As a support we decided to design a system that support the ISDN network for

rapid swap of systems in case incidences occur while a video call is on. Thus the need and introduction of a gateway to this network.

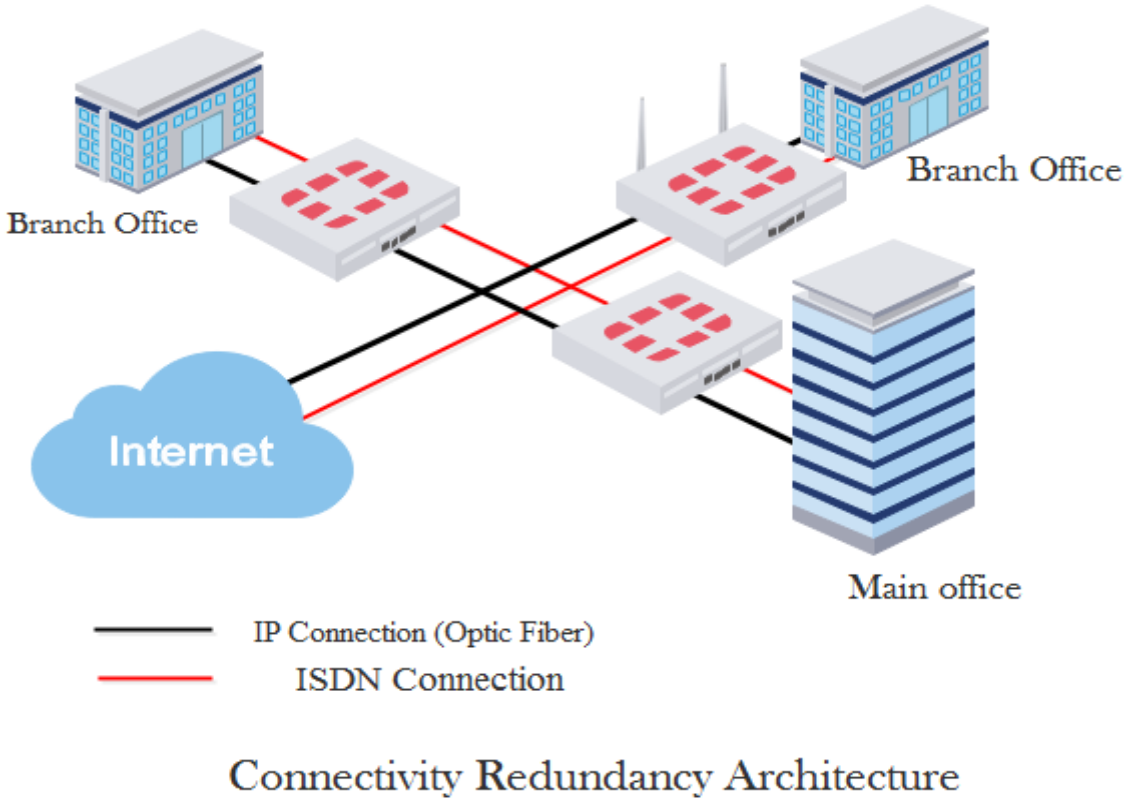

Figure 34: Connectivity redundancy architecture

3.4) Security policies

3.4.1) Physical Security Policy

A balanced security program must include a solid physical security foundation. A solid physical security foundation protects and preserves physical assets, and human assets by reducing the exposure to various physical threats that can produce a disruption or denial of computer service.

Policy

The managers at SNH are responsible for ensuring that enterprise information assets under their control are properly protected through the implementation of cost-effective physical security measures.

Responsibilities

The manager in charge of the computer facility (server room and endpoints is responsible for providing adequate physical protection of computer equipment. The manager will consider the following as a minimum:

- Ensure control access to the facilities and computers if required.
- Put computers behind doors that can be locked when unattended.
- Do not assume that physical access to the machine is enough security. Require locked cabinets.
- Place computer and associated I/O hardware in locked cabinets as possible.
- Make sure that the computer is not in a room where it will overheat. Make sure that there is sufficient airflow to all parts of the computer to allow circulation of air.
- Install heating and cooling systems with air filters to protect against dust.
- Make sure that there is an adequate automated fire suppression system.

There are other requirements which can be put in place too but these appeal much.

3.4.2) Data security policies (Access control, integrity controls and backup procedures)

Keeping data secure

Measures that can be taken to keep data safe include:

- ✓ Protecting yourself against viruses by running anti-virus software.
- ✓ Always logging off or turning terminals off.
- ✓ Using a system of passwords so that access to data is restricted.
- ✓ Making regular back-ups of files. (Back-up copies should be stored safely in fireproof safes or in another building.)
- ✓ Safe storage of important files stored on removable disks.

CONCLUSION AND PERSPECTIVES

SNH faced with the problem of connecting it's headquarter to the different branches, we had as major task the "**Design of a Video Conference Network at the National Hydrocarbons Corporation (SNH), Case Study: Headquarter Extension Building Project**" with principal objective to connect it's headquarter to all branches first then to local like international partners. With this main came some specific objectives which where those of:

- Reducing the risk of accident their staff face each time they travel for work,
- Reduce expenditure (car acquisitions, flight tickets, fuel, hotel bills etc.) incurred in the form of mission orders,
- Protection of the environment through the reduction of travel rate which consequently reduces the emission of pollutants from cars, planes, ships etc. which are often used for displacements.

At the end of our work we were able to effectively design a system whose implementation will go a long way not in assuring SNH's headquarter office is connected to both the branches and partners but equally enhance decision making as a result of the quality of the video calls which would be made possible. Added to this and more importantly, SNH would be saving not less anyway between half to a quarter in mission orders as revealed by its budgetary department while contribution in the fight against global warning and reducing the risk of accidents its employees are under each time they have to half. The step-by-step explanation of its configuration was explained and an estimated budget made available in view of an immediate implementation as requested by the company.

This work being a great step aimed at boosting the performance of SNH, there are other aspects that can be done to make it even better. Amongst them is the perspective of introducing mobile workers (workers who can't have access to the VC room but are able to connect themselves to the internet through their PCs, Tablets or even Phones) to take part in VC meetings as well.

BIBLIOGRAPHY AND WEBOGRAPHY

BIBLIOGRAPHY

[1] Sami Andberg, "Video Conferencing in Distance Education," UNIVERSITY OF HELSINKI, 2008

[2] Gurmeet Singh, "Secure Video Conferencing for Web Based Security Surveillance System," Indian Institute of Technology, Kanpur, July, 2006

[3] AHMET Uyar, "Scaleable Oriented Architecture for Audio/Video Conferencing," Syracuse University, 2005

[4] Henry Sinnreich and Alan B. Johnston, "Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol," *Wiley Publishing, Inc., Second Edition*, 2006

[5] Alan B. Johnston, "SIP: Understanding the Session Initiation Protocol," *ARTECH HOUSE, Third Edition*, 2009

[6] Scott Firestone, Thiya Ramalingam, and Steve Fry, "Voice and Video Conferencing Fundamentals, Published by: Cisco Press 2013

[7] National Hydrocarbons Corporation, Computer department Achieve.

WEBOGRAPHY

[8] Networking: Optimizing the WAN: http://www.expressbusinesspublications.com

[9] Computer networks and internets: www.netbook.cs.purdue.edu

[10] Cisco business challenges, network Foundation solution: www.cisco.com

[11] Polycom solutions: www.polycom.com

[12] Web search: go green with 21st century video

ANNEX

Cisco TelePresence SX20 Datasheet

Features and Benefits

Table 8 summarizes the primary features for the Cisco TelePresence SX20 Quick Set.

Feature Summary	
Design Features	● Transforms a flat panel display into a 1080p high-definition meeting space ● Intuitive connections make setup as easy as connecting a DVD player ● Provides up to 1080p60 resolution - compatible with standards-based video without loss of features ● Sleek, compact design
Application Features	● Multimedia and presentations can be shared at the touch of a button ● Supports Cisco Intelligent Proximity for content sharing to mobile devices and wireless sharing from Macs and PCs ● Supports Switched Conferencing (SVC) for enhanced layouts and enabling video on both screens of dual screen endpoints ● Basic API available over IP (Telnet or Secure Shell Protocol [SSH]) ● Dual-display ● High-definition content sharing up to 1080p15 resolution ● One button to push (OBTP) to start a meeting
Performance Features	● Premium resolution (1080p60) ● H.323/SIP calls up to 6 Mbps ● Built-in individually transcoded multipoint conferencing (optional) offers ability to add three additional participants ● Easy provisioning and self-configuration with Cisco Unified Communications Manager (CUCM), Cisco TelePresence Video Communications Server (VCS), or Cisco WebEx TelePresence ● Takes advantage of the Cisco TelePresence Total Solution approach, including Cisco TelePresence ad-hoc conferencing features, recording and streaming, and firewall traversal services ● Cisco Unified Communications Manager native support (requires Cisco Unified Communications Manager Version 8.6 or higher)

Table 10: Cisco TelePresence SX20 Quick Set Feature Summary

- Product Specifications

Table 9 lists the product capability specifications for the Cisco TelePresence SX20 Quick Set.

Specification	Description	
Software compatibility	Cisco TelePresence Software Version TC 7.1 or later Cisco Collaboration Endpoint Software Version 8.0 or later (requires Touch 10 or TRC5 remote control)	
Default components in SX20 Quickset	● SX20 Codec, Cisco TelePresence Precision Camera (option of 2.5x, 4x and 12x cameras), Cisco TelePresence Table Microphone 20, remote control, cables, and power supply	
Optional hardware components	● Cisco TelePresence Touch 10 ● Wall mount kit ● Additional microphone	
Bandwidth	● H.323 and SIP up to 6 Mbps	
Minimum bandwidth for resolution/frame rate	● 720p30 from 768 kbps ● 720p60 from 1152 kbps ● 1080p30 from 1472 kbps ● 1080p60 from 2560 kbps	
Firewall Traversal	● Cisco TelePresence Expressway Technology ● H.460.18, H.460.19 firewall traversal	
Video Standards	● H.263, H.263+, H.264	
Video Features	● Native 16:9 widescreen ● Advanced screen layouts ● Intelligent video management ● Local auto-layout	
Video Inputs **(Two Inputs)**	One HDMI and One DVI-I (Analog and Digital); supports formats up to maximum 1920x1080 @ 60 fps (HD1080p60), including: ● 640x480 ● 720x480 ● 720x576 ● 800x600 ● 848x480 ● 1024x768 ● 1152x864	● 1280x720 ● 1280x1024 ● 1280x768 ● 1280x800 ● 1280x960 ● 1360x768 ● 1366x768 ● 1400x1050 ● 1440x900 ● 1680x1050 ● 1920x1080 Extended Display Identification Data (EDID)

Video Outputs **(Two Outputs)**	Two HDMI Outputs Supported Formats: ● 1920 x 1080@60 fps (1080p60) ● 1920 x 1080@50 fps (1080p50) ● 1280 x 720@60 fps (720p60) ● 1280 x 720@50 fps (720p50) ● 1366 x 768@60 fps (WXGA) ● 1360 x 768@60 fps (WXGA) ● 1280 x 768@60 fps (WXGA) ● 1280 x 1024@60 fps ● 1024 x 768@60 fps VESA Monitor Power Management EDID Live Video Resolutions (Encode and Decode):	● 176 x 144@30, 60 fps (QCIF) (Decode only) ● 352 x 288@30, 60 fps (CIF) ● 512 x 288@30, 60 fps (w288p) ● 576 x 448@30, 60 fps (448p) ● 768 x 448@30, 60 fps (w448p) ● 704 x 576@30, 60 fps (4CIF) ● 1024 x 576@30, 60 fps (w576p) ● 640 x 480@30, 60 fps (VGA) ● 800 x 600@30, 60 fps (SVGA) ● 1024 x 768@30, 60 fps (XGA) ● 1280 x 768@30, 60 fps (WXGA) ● 1280 x 720@30, 60 fps (HD720p) ● 1920 x 1080@30, 60 fps (HD1080p)
Audio Standards	● G.711, G.722, G.722.1, G.728, G.729, AAC-LD and OPUS	
Audio Features	● High quality 20 KHz stereo ● Two acoustic echo cancellers ● Automatic Gain Control (AGC) ● Automatic noise reduction ● Active lip synchronization	
Audio Inputs **(Four Inputs)**	● Two microphones, 4-pin minijack ● One minijack for line-in (stereo) ● One audio in from camera (HDMI)	
Audio Outputs **(Two Outputs)**	● One minijack for line out (stereo) ● One HDMI, (digital main audio)	
Dual Stream	● H.239 (H.323) dual stream ● BFCP (SIP) dual stream ● Support resolutions up to 1080p (1920 x 1080)	
Multipoint Support	● Four-way embedded SIP/H.323 conferencing capability with MultiSite option ● Ad-hoc conferencing supported through: ◦ Unified Communications Manager Media Resource Group (requires a Cisco TelePresence MCU) ◦ Cisco TelePresence Multiway [requires Cisco TelePresence Video Communication Server (Cisco VCS) and a Cisco TelePresence MCU] ● Ability to natively join multipoint conferences hosted on Cisco	

	Telepresence Multipoint Switch (CTMS) ● Switched conferencing (SVC)
MultiSite Features (Embedded Multipoint) (Optional upgrade)	● Adaptive SIP/H.323 MultiSite; resolution up to 720p30 ◦ 3-way resolution up to 720p30 ◦ 4-way resolution up to 576p30 ● Full individual audio and video transcoding ● Individual layouts in MultiSite continuous presence ● H.323/SIP/VoIP in the same conference ● Support for Presentation (H.239/BFCP) from any participant at resolutions up to 1080p15 or 720p30 ● Best Impression (automatic continuous presence layouts) ● H.264, encryption and dual stream from any site ● IP downspeeding ● Participants can be added by dialing in or host can dial out ● Conference rates up to 6 Mbps
Protocols	● H.323 ● SIP ● ISDN (requires Cisco TelePresence ISDN Link)
Embedded Encryption	● H.323 and SIP point-to-point ● Standards-based: H.235 v3 and Advanced Encryption Standard (AES) ● Automatic key generation and exchange ● Supported in dual stream
IP Network Features	● DNS lookup for service configuration ● Differentiated services (quality of service [QoS]) ● IP-adaptive bandwidth management (including flow control) ● Automatic gatekeeper discovery ● Dynamic playout and lip-sync buffering ● H.245 Dual Tone Multi-frequency (DTMF) tones in H.323 ● Date and time support using Network Time Protocol (NTP) ● Packet loss-based down speeding ● Uniform resource identifier (URI) dialing ● TCP/IP ● DHCP ● 802.1x network authentication ● 802.1Q Virtual LAN ● 802.1p (QoS and class of service [QoS]) ● ClearPath

CUCM (Requires CUCM Version 8.6 or Later)	● Native registration with CUCM ● Basic CUCM provisioning ● Software upgrade from CUCM ● Cisco Discovery Protocol and DHCP option 150 support ● Basic telephony features such as hold/resume/transfer and Corporate Directory lookup
IPv6 Network Support	● Single call stack support for both H323 and SIP ● Dual-stack IPv4 and IPv6 for DHCP, SSH, HTTP, HTTPS, DNS, DiffServ ● Support for both Static and Automatic IP configuration (stateless address auto configuration)
Security Features	● Management using HTTPS and SSH ● IP administration password ● Menu administration password ● Disable IP services ● Network settings protection
Network Interfaces	● One LAN and Ethernet (RJ-45) 10/100/1000 Mbit Other Interfaces; Two USB ports can be used for serial control
System management	● Support for the Cisco TelePresence Management Suite ● Total management using embedded SNMP, Telnet, SSH, XML, SOAP ● Remote software upload: using web server, secure copy (SCP), HTTP, HTTPS ● Cisco TelePresence Touch 10 (optional) ● Remote control and on-screen menu system
Directory Services	● Support for local directories (My Contacts) ● Corporate directory ● Unlimited entries using server directory supporting LDAP and H.350 (requires Cisco TelePresence Management Suite) ● Unlimited number for corporate directory (through Cisco TelePresence Management Suite) ● Received calls with date and time ● Placed calls with date and time ● Missed calls with date and time
Power	● Auto-sensing power supply ● 100 - 240 VAC, 50/60 Hz ● Maximum 40 watts for codec and main camera
Operating Temperature and	● 0°C to 40°C (32°F to 104°F) ambient temperature ● 10% to 90% Relative Humidity (RH)

Humidity	
Storage and Transport Temperature	● -20°C to 60°C (-4°F to 140°F) at RH 10% - 90% (non -condensing)
SX20 Codec Dimensions	● Width: 11.8 inches (30.0 cm) ● Height: 1.4 inches (3.4 cm) ● Depth: 7.1 inches (18.0 cm) ● Weight: 3.1 pounds (1.4 kg)

Table 11: Product specifications