



TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor's Thesis

Investigation of VoIP and Implementation

EDE AGHEDO

Degree Program in Information Technology

2011



Turku University of Applied Sciences		Abstract of Bachelor's Thesis	
Degree Program: Information Technology			
Author: Ede Aghedo			
Topic: Investigation of VoIP and Implementation			
Specialization line: Voice Communication		Instructor: Väänänen Ossi	
		Language Revision: Poppy Skarli	
Date: January 2011		Number of Pages: 49	
<p>Voice over Internet Protocol (VoIP) is the technology used to transmit conversations digitally over the Internet. VoIP is being adopted globally and changing the landscape of telecommunications for businesses and consumers. This thesis describes the investigation of VoIP and how it compares to traditional phone systems, voice characteristics, implementation challenges, digital voice process, testing and result, the standards organizations promoting the technology, and what this means for us now and in the future.</p> <p>The evolution of VoIP interconnection is examined with a simplified strategic process throughout this thesis, where the current state of interconnection is first identified, followed by the definition of interconnection as a desired future state in the evolution of VoIP networks and different interconnection models are identified as routes to this future state. Different VoIP interconnection models are then analyzed with an intention to find out if some of the interconnection models suits better than the others for VoIP interconnection purposes in order to become a dominant design on this area.</p>			
Keywords: VoIP, PSTN, ADC, DAC, IP Telephony			
Deposit at: Library of Turku University of Applied Sciences.			

Foreword

This thesis is based on voice communication using VoIP technology and comparing with PSTN, having in mind the generation and/or evolution from the old telephony system. The good work presented in this thesis could not have been possible without the guidance of my instructor, company, friends and family.

First I would like to thank my thesis supervisor Ossi Väänänen for the opportunity he granted me to pursue my thesis work and leading my effort to accomplish it. My gratitude also goes to IF Insurance Company who granted me the opportunity of interview on VoIP and giving me encouragement on how to carry on my work to a successful end.

Finally, I would like to thank my family (Aghedo's Family) for their patience and support to see me accomplishing my academic goal. Same gratitude goes to Poppy Skarli, Head of Degree Program Patric Granholm, all the staff in Cisco Laboratory and generally to all students and other staff of Turku University of Applied Sciences.

Acronyms and Abbreviations

ACELP	Algebraic Code Excited Linear Prediction
ADC	Analog-to-Digital Conversion
ADPCM	Adaptive Differential Pulse Code Modulation
ANI	Automatic Number Identification
AM	Amplitude Modulation
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ASK	Amplitude Shift Keying
ATA	Advance Technology Attachment
CDMA	Code Division Multiple Access
CODEC	Coder-Decoder
CRM	Customer Relationship Management
CS-ACELP	Conjugate Structure Algebraic Code Excited Linear Prediction
DAC	Digital-to-Analog Converter
DNIS	Dialed Number Identification Service
DSL	Digital Subscriber Line
DSP	Digital Signal Processing
FDMA	Frequency Division Multiple Access
FSK	Frequency Shift Keying
IETF	Internet Engineering Task Force
IM	Instant Message
IN	Intellegent Networking
IP	Internet Protocol
ISP	Internet Service Provider
ITSP	Internet Telephony Service Provider
ITU	International Telecommunication Union
ISDN	Integrated Services Digital Network

LD-CELP	Low Delay-Code Excited Linear Prediction
MP-MLQ	Multi-Pulse - Maximum Likelihood Quantizer
NAT	Network Address Translator
PAM	Pulse Amplitude Modulation
PBX	Private Branch Exchange
PCM	Pulse Code Modulation
POTS	Plain Old Telephone Service
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAM	Random Access Memory
ROM	Read Only Memory
RTP	Research Triangle Park
SBC	Server-Based Computing
SLA	Site-Level Aggregation
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TLA	Top-Level Aggregation
TLV	Type-Length-Value
TTL	Time to Live
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
WiFi	Wireless Fidelity
XMPP	Extensible Messaging and Presence Protocol

Table of Content

Abstract	i
Forward.....	ii
Acronyms and Abbreviation	iii
Introduction	1
1.1 Making VoIP Call	2
1.2 Minimum Requirement	4
1.3 Implementation.....	5
1.4 Advantages of VoIP.....	5
1.5 Drawback of VoIP.....	6
1.6 Applications.....	7
2.0 Technology Supporting VoIP.....	8
2.1 Voice Signal Processing.....	8
2.2 Low Bit Rate Voice Signal Encoding.....	8
2.3 Voice Signal Framing and Packetization.....	9
2.4 Data Transmission.....	9
2.5 Quantization.....	10
2.6.0 Transmission.....	12
2.6.1 Encoding.....	12
2.6.2 Sampling (Pulse Amplitude Modulation).....	12
2.9 Analogue versus Digital Communication.....	14
2.9.1 Modulation.....	15
2.9.2 Amplitude Shift Keying.....	16
2.9.3 Frequency Shift Keying.....	16
2.9.4 Phase Shift Keying.....	17
2.9.5 Multiple Access.....	17
3.0 Empirical View.....	19
3.1 Reasons Why Networks Interconnect.....	19

3.2 Externalities and Effect of Network.....	20
3.3 Contact Centers and Web-Based Call.....	20
3.4 Feedback Loops.....	21
3.5 Scanning a VoIP Network.....	23
3.6 Supporting Infrastructure Attack.....	23
3.6.1 DNS Cache Poisoning.....	24
3.6.2 DNS Cache Poisoning Countermeasure.....	24
3.6.3 DNS Flood DoS.....	25
3.6.4 Vulnerability in Underlying OS or Firmware.....	25
3.7.0 VoIP Privacy.....	25
3.7.1 TFTP Configuration File Sniff.....	25
3.7.2 Number Harvesting.....	26
3.7.3 Call Pattern Tracking.....	26
3.7.4 Conversation Eavesdropping and Analysis.....	26
3.7.5 ARP Poisoning.....	26
3.7.6 Static OS Mapping.....	27
3.7.7 Switch Port Security.....	27
3.8.0 Management Structure.....	27
3.8.1 Centralized Management Structure.....	27
3.8.2 Distributed Management Structure.....	28
3.8.3 End-to-end Approach.....	29
3.8.4 Management Structure of PSTN and VoIP Networks.....	30
3.9.0 Alternative VoIP Interconnecting Models	31
3.9.1 End-to-end Model.....	31
3.9.2 Bilateral Model.....	32
3.9.3 Bilateral Ad Hoc Model.....	33
3.9.4 Multilateral.....	34

4.0 Data Compression (Coding).....	35
4.1 Lempel Ziv Algorithm.....	37
4.2 Huffman Code.....	37
4.3 Testing.....	39
5.0 Conclusion.....	40
5.1 References.....	41

INTRODUCTION

Voice over Internet Protocol (VoIP) is a technology that permits voice conversations to be conducted over the Internet instead of the Plain Old Telephony System (POTS). Nowadays, people are turning to VoIP technology instead of the local telephony due to its efficiencies and cost effectiveness.

Voice over IP is not a totally new technology. People have been using software like Microsoft, Netmeeting etc to communicate through the Internet for many years. Many Internet users are already familiar with VoIP technology like Skype. What makes VoIP an interesting technology is that it is an evolution to the ordinary telephony conversations and the hardware requirement are easily affordable as long as one could lay hand on a computer.

In VoIP the voice data flow over a packet switched network instead of the traditionally dedicated circuit switched voice transmission lines. This could be done by sending a voice signal to a remote destination through digital means as well as analog. To send this, the voice packet (data) should be digitized with an Analog-to-Digital Converter (ADC) transmitter and at the end, it is transformed back to the original analog format using Digital-to-Analog Converter (DAC). Voice information is sent in a discrete packet in form of digital signals.

Since the introduction of VoIP technology it is now possible to use IP networks for telephone calls and presently this convergence of voice and data traffic into the IP network is a fast growing trend. However, big enterprises, who are motivated by the promised cost saving/reduction in communication, are in love with VoIP experimentation which will in future push out the old telephone system.

By neglecting the old telephone infrastructure and using only IP networks and IP-based equipment for all communication purposes, enterprises are expecting huge gain from cost savings. Communication over IP, however, is not yet unproblematic.

Though this technology has its problems just as several IP based telephone networks (VoIP-networks like Free call or corporate networks) allow only calls within the same network. It is not always possible to call from user's own VoIP network or "VoIP island" to another VoIP network because there is no interconnection between VoIP networks, or the interconnection might be possible only through Public Switched Telephone

Network (PSTN) network, which is not a very desirable alternative as will be discuss later.

1.1 Making VoIP Call

There are three fundermental methods of making a call using VOIP:

Analogue Telephone Adapter (ATA)

IP Phones

Computer to Computer

Analogue Telephone Adapter (ATA) - With this, one could be able to use an existing telephone mobile/handsets, and additional hardware are not required. It is the most commonly used VoIP method which simply connects a regular telephone/handsets to the Internet connection. ATA is an analogue-to-digital converter (ADC) which takes the voice signal from the phone and converts it into digital data for transmtion over the Internet. ATA can either be provided free when one sign up with a VoIP Service Provider or simply by purchase. An ATA is basically simple to use by plugging the cable from your phone into the ATA instead of the wall socket.

The connection details are in Fig. 1

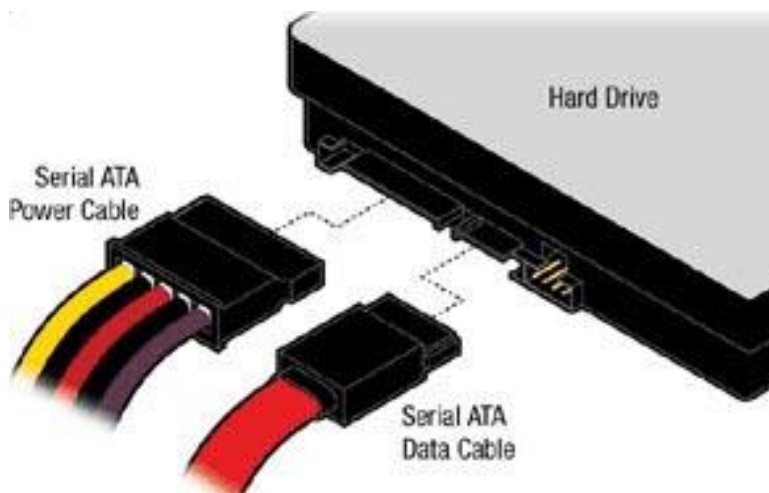


Fig. 1 Analogue Telephone Adapter (ATA) showing the hard drive and connecting cable (Power and Data cables.) [12]

IP Phones are seen as specialized/standard phones, with features having handset, buttons and a cradle. IP phones use an RJ-45 Ethernet connector. They contain the necessary circuitry to convert voice sound to digital information. An IP phone has the following advantages like- call display, call waiting, call forwarding, voicemail etc. Wi-Fi IP phones are also now available allowing you to make VoIP calls from any Wi-Fi point. Flexibility is another additional benefit that makes VoIP so attractive for homes and small businesses.



Fig. 2 An IP Phone [13]

Computer-to-Computer or SoftPhones as it is otherwise known, is possibly the easiest method to use VoIP. This method can be used to make free Internet phone calls over the globe. It is implemented by connecting a PC to a broadband internet connection, and a headset consisting of earphones and microphone connected to the soundcard of your computer. The VoIP software is usually installed first. Distance does not matter as far as there is an internet connection. Examples of Instant messenger programs based on VoIP are Skype, Yahoo Messenger, Gizmo Project all these have the ability to send messages and make calls over the internet.

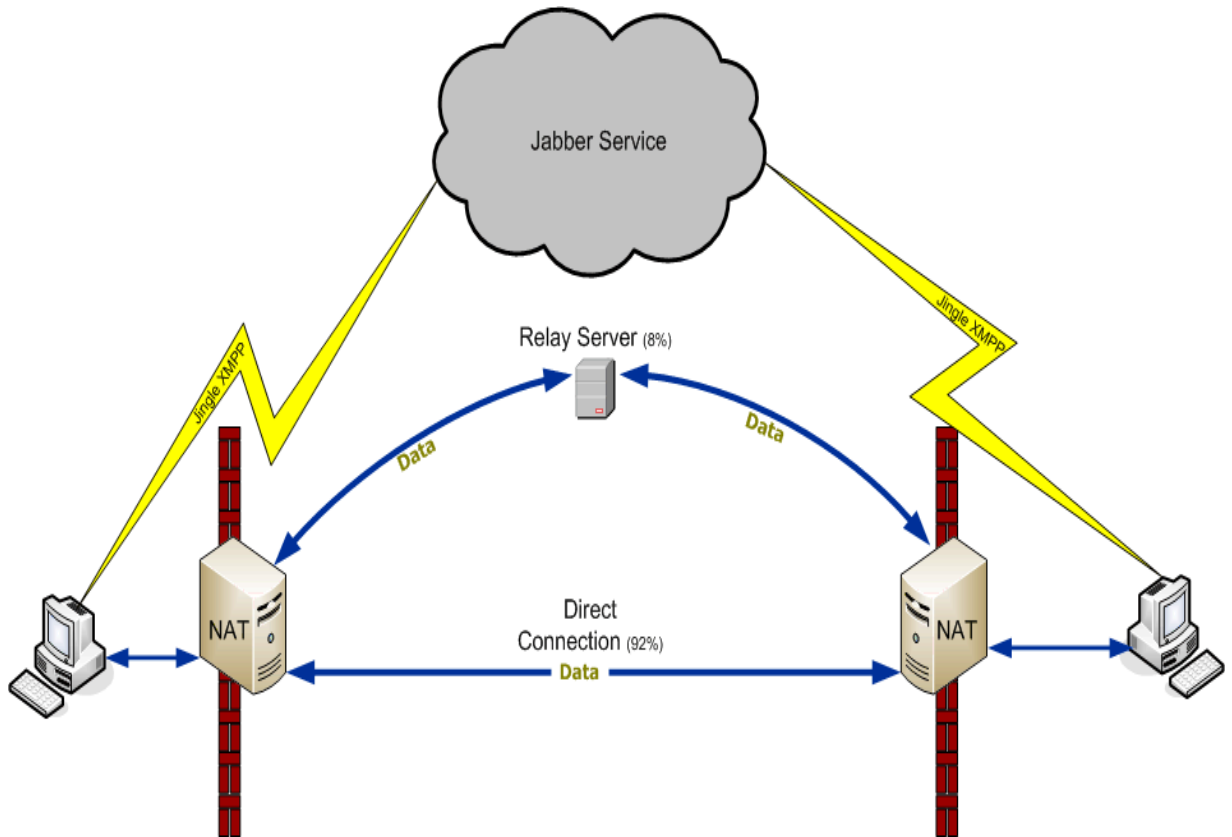


Fig 3: illustration of computer-to-computer voip call: picture from Wikipedia.

1.2 Minimum Requirement

VOIP is an easy way of communication. Due to its flexibility and scalable solutions it is a revolution of sorts in the present day world. VoIP users can use this technology service and select a distinctive different area from where they live, which goes with the advantages reaching unlimited long distance calls to friends and family members living in a different area.

VoIP implementation requires certain conditions to be met for the successful use of this innovative technology. This includes a computer with a high speed Internet access. This computer should be updated with sound card (audio and video codes). This helps VoIP users to produce a good quality of audio as well as graphics. Digital video compression format should also be present in the computer that is being used.

Furthermore, a telephone adapter, which is often delivered by the VoIP service providers, as an integral part of VoIP packages is required. A 386 processor can

support VoIP, full duplex capability, network card a broadband network which could be on a modern cable or high speed services from DSL or LAN can be used for VoIP implementation.

1.3 Implementation

VoIP Implementation varies depending on the size and type of the organization. In computer-to-computer within the same locality, the implementation is simple but complex when it involve larger/intercontinental connections.

However, whether close or far distance, the connective materials are usually the same which runs from layer 2 of the network to the ethernet layer.

Figure 4 below shows an implementation of VoIP.

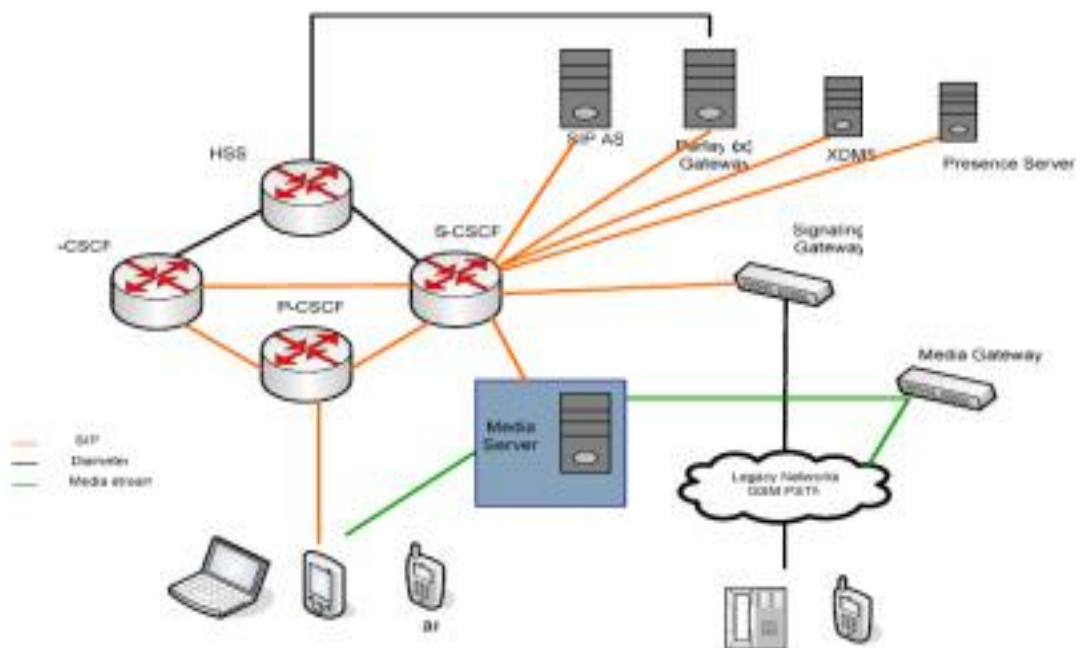


Fig 4: An overview of a VoIP Implementation with different cable colors to illustrate data transmission and connectivity. (Picture from Wikipedia).

1.4 Advantages of VoIP

VoIP is modifying the way that we use phone service. The advantages of VoIP are easily being recognized by the users and the relatively new technology is becoming the norm in many organizations and homes all over the world.

It gives room for a user to make long distance calls cheaply by combining this VoIP technology with a broadband, to provide the inexpensive way to make phone calls all over the world.

Understanding how the technology works, the advantages of VoIP become clearer when compared to traditional phone service. Traditional phone service make use of long distance phone calls which are routed from local provider's network to a chosen destination network and finally, to their home phone line.

This is done by using the internet as the routing method that transfers the call from a local phone provider to a receiver. When a call is initiated, the analog voice signal is translated into a digital signal. That signal is then sent through the internet service, where it is routed to the receiver and then translated back to analog signal and sent to the receiver party's phone. This method is as fast as the traditional phone calls.

This is also an advantage for businesses since VoIP are growing all the time as many companies are beginning to offer high-quality, reliable VoIP service more than telephone calls. Many companies offer packages that include internet service and video conferencing via VoIP.

1.5 Drawback of VoIP

Voice over IP is the integration of VoIP architecture and internet technology. It has some drawback and one of the greatest disadvantages of VoIP lies on the quality (clarity or package drop) of voice delivered. There are other drawback such as a non reliable broadband connection or unsteady/slow internet connection; which could make VoIP probably not good enough for one to use.

Constant power/electricity supply is another imminent problem. Since VoIP depends on live Internet connection, losing electricity means losing VoIP service. In this case, one needs to install a UPS for the cable/DSL modem and the ATA. This UPS would keep those devices powered for several hours which mean that UPS is another assessorry necessary in case of power outage.

Emergency call for example 112 in Finland is another challenge for VoIP call, unlike traditional telephone it is difficult to locate exactly the IP address with geographic certainty. Without knowing the exact location, it is difficult to know which call center should receive a VoIP generating the emergency call.

The voice quality/clarity of VoIP call is also another consideration. Since information move through the Internet, there is the potential for attenuation or "bubbles" just as one would experience on a cell phone.

1.6 Applications

Due to fall in the price of bandwidth, internet call is becoming popular everywhere. Voice call is taking over the inconvenience text chat, with a widely distributed cost effective ways of communication. There are many VoIP applications which support this:

VoIP to VoIP calls: Here a remote user could log on through the internet to the main server where they can run their communication to the main office phone system. This is beneficial to both home workers and sub-offices. This is otherwise called point-to-point connection.

VoIP to PSTN: This is usually found in commercial enterprise where internet usage could not be done without. It is most efficient at schools, cyber café and other offices where internet usage is the order of the day. Here long distance calls can be ascertained.

In – House PBX System: Using VoIP directly will be cheaper and cost effective compared to call transfer, hold and dedicated wiring through the office in PBX system. However, VoIP could use a Program that can easily handle these transfer and data queue.

2.0 TECHNOLOGY SUPPORTING VoIP

There are many technologies supporting VoIP. But this thesis will be concentrating on the basic and familiar ones which can be found in telecommunication. Since VoIP technology could be incorporated into telecommunication devices like mobile phones, some software features are also required to carry out VoIP implementation successfully and these processes involved are explained below.

2.1 Voice Signal Processing

The base-band signal for traditional telephony/voice communications is usually between 0.3 to 3.4kHz. This is considered as speech signal or telephone-band voice.

However, this exhibits a wide dynamic amplitude with a minimum range of 40dB. For a perfect reproduction to be achieved after switching and transmission, the voice-band signal needs to be sampled at more than or equal to twice the maximum frequency of the signal.

Usually, an 8kHz sampling rate is used and each of this sample is can now be quantized uniformly or non-uniformly using a predetermined number of quantization levels. Example is – to support 256 quantization levels, an 8 bits is needed, that is 2^8 . A bit stream of (8000×8) or 64,000 bps (64Kbps) is generated.

This mechanism is known as the *pulse code modulation* (PCM) encoding of voice signal as defined in ITU-T's G.711 standard and it is widely used in traditional PSTN networks.[1]

2.2 Low-Bit-Rate Voice Signal Encoding

Due to technological advancement in the production/building of processor, memory and DSP, researchers have developed a large number of low-bit-rate voice signal encoding algorithms. Most of these coding techniques have been standardized by the ITU-T. The most popular frame-based vocoders that utilize linear prediction with analysis-by-synthesis are the G.723 standard, generating a bit stream of 5.3 to 6.4kbps and the G.729 standard, producing a bit stream of 8kbps and many more. These standards (G.723 and G.729) have few variants that support lower bit rate and/or robust coding of the voice signal.

Also, we have the G.729A coder-decoder (CODEC) it is simpler to implement than many others. This design utilizes approximately 2k and 10k words of RAM and ROM storage respectively. The voice quality delivered by these CODECs is considered acceptable in a variety of network impairment designs. Therefore, most VoIP product manufacturers support G.723, G.729 and G.711 voice coding options in their products.[1]

2.3 Voice Signal Framing and Packetization

PSTN uses the traditional circuit switching method to transmit the voice encoder's output from the caller's phone to the destination phone. The circuit switching method is very reliable, but neither flexible nor efficient for voice signal transmission, where about 60% of the time, the channel/ circuit remains idle.

In the voice signal method, the information to be transmitted is first divided into small fixed or variable sized piece called pay loads, and then one or more of the piece could be packed together for transmission. These packs are then encapsulated using one or more appropriate sets of headers to generate packets for transmission. They are called IP packets in the Internet, frames in frame relay networks, ATM cells in ATM networks.

In real-time telephone conversation, loss of larger number of contiguous speech frames may give the impression of connection dropout to communicating parties. The designers and network operators must therefore be very cautious, in designing the acceptable ranges of these parameters.

ITU-T recommends the specifications in G.764 and G.765 standards for carrying packetized voice over ISDN-compatible networks. For voice transmission over the internet, the IETF recommends encapsulation of voice frames using the RTP for UDP-based transfer of information over an IP network.[1]

2.4 Data Transmission

VoIP is built on digital data transmission. This is done by first converting VoIP calls from analog signals or human voice into digital data. With the help of Analog-to-Digital Converter (ADC) data are divided in analog signals into discrete steps which are represented by numbers. The next stage is to compress the audio data using a codec (enCOder/DECOder) which significantly reduces the amount of digital data while maintaining audio quality.

The compressed digital data are now ready to be sent over the Internet. The data stream must be divided into packets which, besides containing the audio data, also have information concerning their destination and their place in the data stream. All data that is sent over the Internet is encapsulated in 'layers' which aid in its proper delivery.

Most VoIP uses a transport layer called User Datagram Protocol (UDP) which is faster than TCP. A commonly used application layer is Real-time Transmission Protocol (RTP) — originally developed for delivering audio and video over the Internet. RTP provides information about the sequence of the data packets so they can be reconstructed in the correct order at their destination.

RTP also has the ability to drop packets if they do not arrive within a certain amount of time. This is necessary for telephone conversations because if the telephone software waited for every packet of information to arrive before reassembling it there would be unacceptable delays in the audio stream.

Even though some of the packets are dropped, there is usually still enough information to make the conversation legible. The number of packets that will be dropped depends on the speed of your Internet connection in the distance between the two parties.

Once the voice data has arrived at its destination, it is reassembled in the correct order and converted back from digital to analog.

2.5 Quantization

To transmit signals in digital forms, the sample amplitude needs to be converted to binary bits of 1s and 0s. This is done by changing the number values to the power of 2, this value depends on the degree of precision required. Examples of such are the cases of $2^5 = 32$, $2^8 = 256$. In this case, the values at the left show analogue signal being quantized and test shows that this provides adequate fidelity for the average telephone listener.

Basically, the inputs to the quantizer are sequences of sample amplitude where there are infinite number of values. The result or output of quantizer is restricted to a finite number of values. The degree of inaccuracy depends on the number of output levels and the amplitude needed for assigning those levels. This placement is turn depending on the nature of the waveform being quantized. Generally, an optimal quantizer places

more levels in amplitude where the signal is more likely to occur and fewer levels where this is less likely. This technique is known as Non-Linear Quantization. This can also be demonstrated by passing the signals through a compressor circuit where weak signal components is amplified and attenuates its strong components.

The compressor signals now occupy a narrower dynamic range and can be quantized with a uniform or linear spacing of the thresholds and output level. In the case of the telephone signal, the compressed signal is uniformly quantized at 256 levels. At the receiving end, the reconstituted signal is expanded to its original range of amplitudes. This sequence of compression and expansion also known as commanding can yield an effective dynamic range equivalent to 13 bits.

Table 2

Quantized Level	Binary Codes
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

2.6.0 Transmission

For data to be transmitted, it has to pass through some phases or processes. In this thesis, the processes are treated and some other algorithm which explain VoIP transmission process are also treated.

2.6.1 Encoding

The transmission of telecommunication data in a given media is restricted to the quantity of signal it can transmit. This parameter is measured by bandwidth. Also bandwidth of signal expands with the number of bits to be transmitted in every second; an important function of a digital communication system is to represent the digitized signal by as few bits as possible, which is to reduce the redundancy. Redundancy reduction is done by a source encoder, which often operates in conjunction with the analogue-to-digital converter.

2.6.2 Sampling (Pulse Amplitude Modulation)

For the intelligence of the signal to be present in the pulsed wave, some characteristic of the sampling pulses must be varied by the modulating signal. Illustration below shows three example waveforms in which the pulse amplitude is varied by the amplitude of the modulating signal.

(A) illustrates a sinusoidal wave of intelligence to be modulated on a transmitted carrier wave,

(B) demonstrates the timing pulses which determine the sampling interval/range, while

(C) shows Pulse-Amplitude Modulation (PAM) where the amplitude of each pulse is monitored by the instantaneous amplitude of the modulating signal at the time of each pulse.

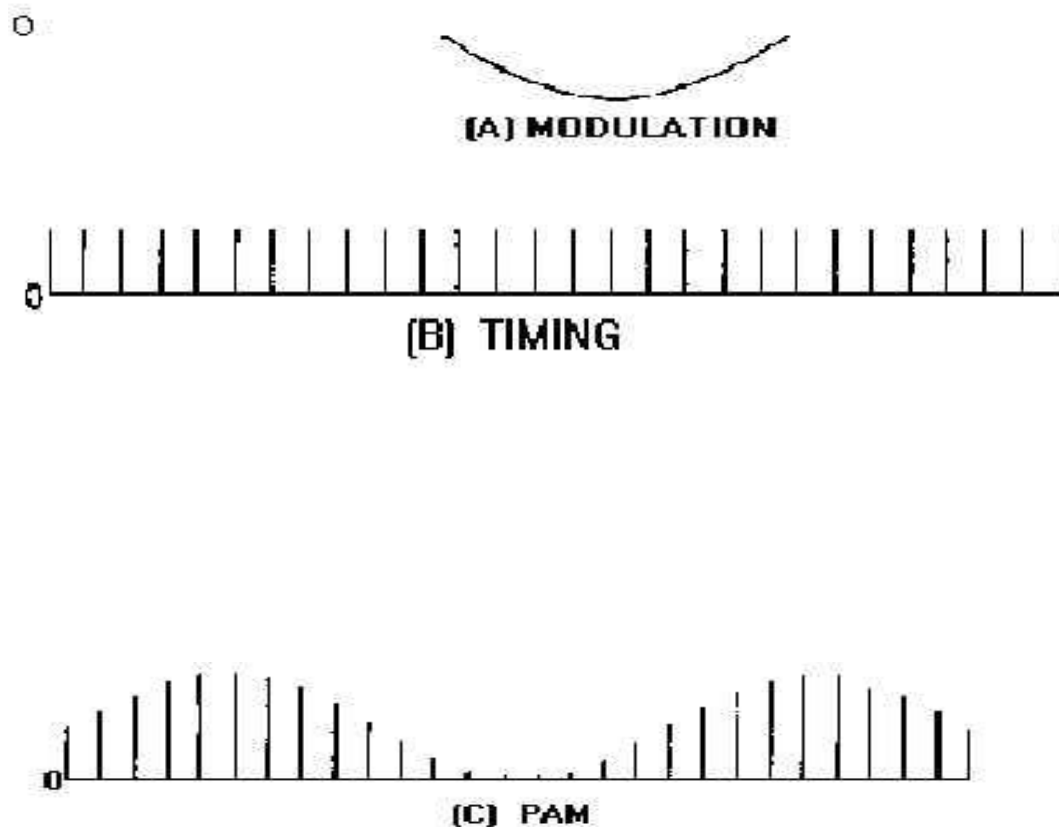


Fig 6: sampling – generation of PAM signals

PAM- Pulse-amplitude modulation is the simplest form of pulse modulation. It is generated just as analog-amplitude modulation. The timing pulses are applied to a pulse amplifier where the gain is controlled by the modulating waveform. Since these variations in amplitude actually represent the signal, this type of modulation is basically a form of AM. The only difference is that the signal is now in the form of pulses. This means that PAM has the same in-built weaknesses just like any other AM signal, which is highly susceptibility to noise and interference. This susceptibility to noise is because any interference in the transmission path will either add or subtract from any of the voltage signal. Hence, the amplitude of the signal will be transformed. Since the amplitude of the voltage represents the signal, any unwanted or irregular change to the signal is considered as a SIGNAL DISTORTION. Due to this reason, PAM is limited and not often used. When PAM is used, the pulse train is used to frequency modulate a carrier for transmission. Techniques of pulse modulation other than PAM have been developed to overcome this shortcoming of noise interference.

2.7.0 Analog Versus Digital Communication

The sound generated by human voice bound air waves together over a relatively short period. This result to a sinusoidal wave which is then converted to electrical pulse. The range of sound generated by human voice is between 300 to 3000Hz of electric cycles. As with communication channel capacity, the telephone company does not need to give users more than they need to carry voice conversation.

When analog signals are transmitting through a wire, the resistance in the wire reduces its amplitude, this makes it becomes weaker and weaker as the distance travelled in wire increases. This term is refered to as attenuation of electrical signals. This signal can travel so far before it run out of strength and finally disappears.

In order to keep the signal moving along wires, amplifiers are used to boost the signal strength, however, noise is usually introduced by line loss, lightning, frayed wires, electrical induction, resistance, heat etc and these also reduces the signal strength. Amplifiers cannot discern the noise from the actual conversation. Thus the amplifier only boosts the signal, it also boosts the noise. This creates a stronger but noisier signals. The result of amplification are cummulative over distance, the more amplifiers that must be used, the worse the overall signals become.

Since analog signals have many shortcomings, digital transmission solution is a better substitute for communication. Though both are sometimes, interdependent, but digital transmission has better advantages.

In order to convert analog to digital signals, ADC converters were used. This converter employs sampling techniques. Sampling refers to the process of measuring representative portions of a signal over a given time. If the sampling are taken frequently enough and playedback correctly at the other end, the ear will not be able to differentiate the playback from the original.

At the end of the conversion, a digital signal equivalent approximately to the analog signal is obtained. Bits of 0 and 1 are used to represent digital signals, in representing these signals, two different voltage levels are used. A +3V is used to represent the state of 1 and a no voltage is used to represent a 0 state. The measurement is taken in the middle of a bit time when the likelihood of getting a precise level is maximized. Because voice is inherently analog, an analog-to-digital conversion must be performed if voice has to be transmitted digitally.

Digital signals provide a better voice quality than analog signals. They also have a better signal to noise ratio than analog signals. The digital equivalent of an amplifier is a repeater. It must be placed at 3000-5000ft intervals.

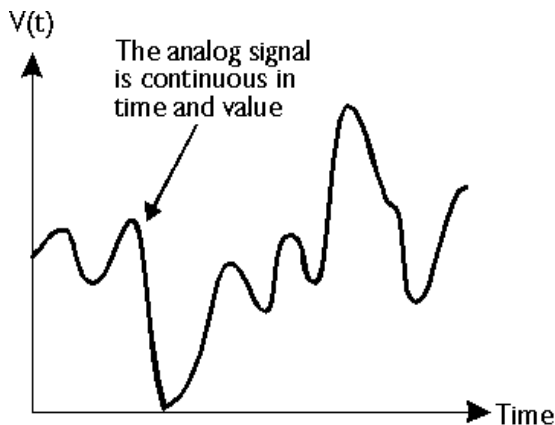


Fig 7a continuous analog signal

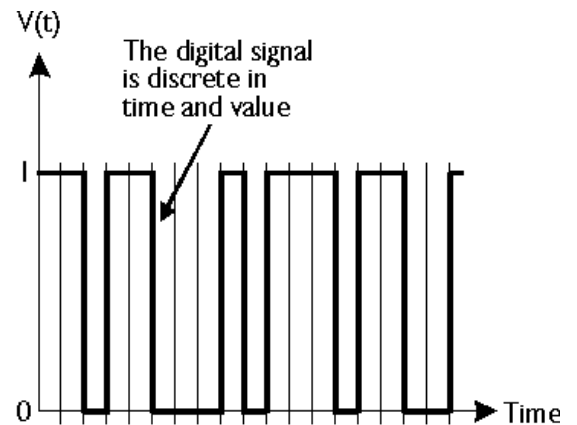


Fig 7b discrete digital signal.

Just as analog signals experience attenuation, so do digital signals experience attenuation. As the pulse is placed on a media, it travels down the wire, this wire is acted upon by the pulse and results to diminishing strength. This can be avoided by using a repeater in every 3000ft interval, as the amplifier boosts the input signals, the repeater detects the 0s and 1s of the original signals and retransmit them. In general, any noise introduced into the signals between the source and repeater is completely ignored as long as it stays below a certain tolerance level. Though decrease in amplitude still occur between repeaters which allow noise to be introduced, but as far as the repeater could identify the pulse (1's) which are the only parts of the received signals that will be used to build the output signals, noise will be minimized.

Since pulse is short in duration and a discrete value of energy rather than a constantly varying voltage level, more repeaters are required in the link.

2.7.1 Modulation

Modem is used to modulate digital encoded signals. The word modem comes from modulator and demodulator. A modulator is the device that allows systems to communicate over a single pair of dedicated wire or the switched telephone network. It is capable of communicating digital information over a long distance in order to transmit sound data and other digitized information over a communication channel. An analog

carrier wave can be modulated to reflect the binary nature of the digital baseband signal. The parameters of the carrier that can be modified are the amplitude, frequency and phase.

2.7.2 Amplitude Shift Keying

Amplitude Shift Keying (ASK) is a digital version of analog amplitude modulation. The amplitude of the carrier wave is highest when a 1 is transmitted and lowest when it is a 0. Note that the modulation method is called ASK when amplitude is the only parameter of the carrier wave to be altered by the information signal.

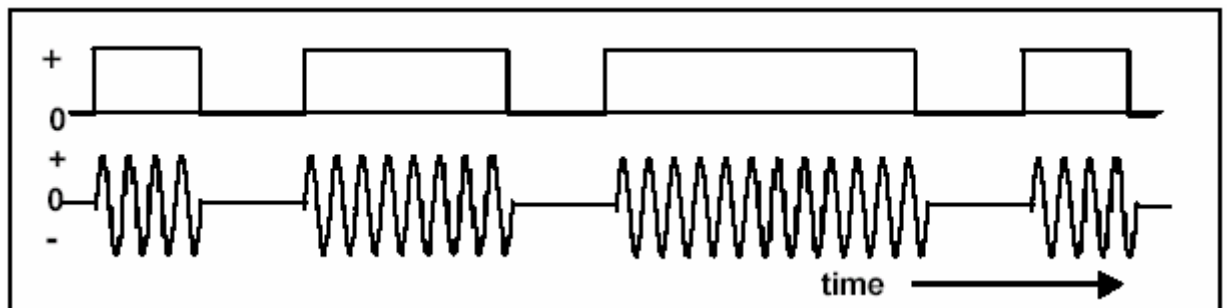


Fig 8: an ASK signal (below) and the message (above)

2.7.3 Frequency Shift Keying

In this case, frequency is the only parameter of the carrier wave to be altered. It is the simplest form of digital data transmission, by using one or two frequencies, where one frequency transmit a 1 and the other transmits a 0.

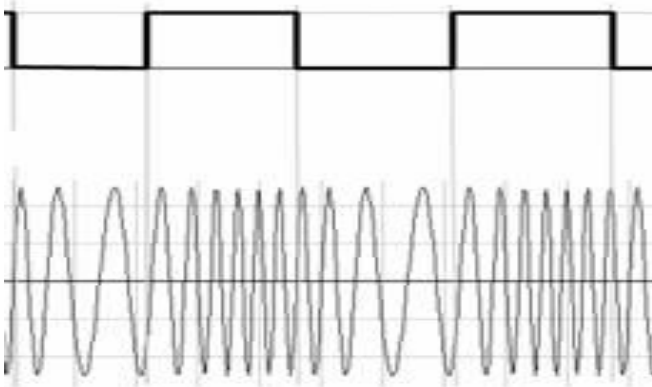


Fig 9: illustrating an FSK signal

2.7.4 Phase Shift Keying

This method is called Phase Shift Keying (PSK) when the phase is the only parameter of the carrier wave to be altered by the information signal. Here a single radio frequency is sent with a fixed phase to represent a 0 and a 180° phase shift to represent a 1. This 180° phase shift represents an opposite polarity to the first signal. This scheme is employed by modems using the Bell 212 standard. This has one of the highest data rates up to 1,200bps.

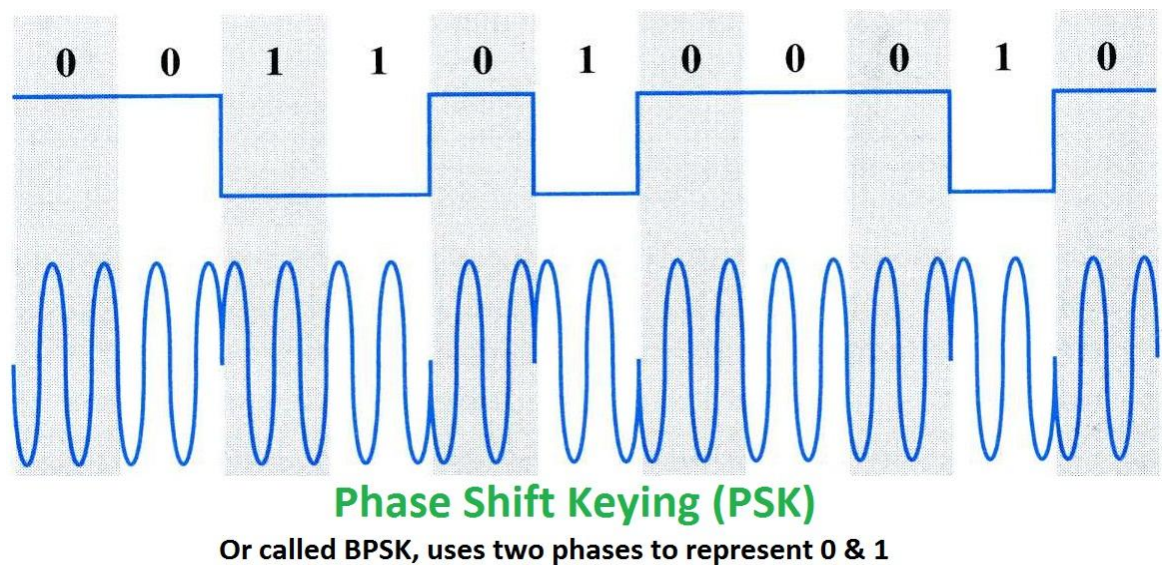


Fig 10 illustration of PSK signal

2.7.5 Multiple Access

When communication channels are limited, then multi access is necessary for efficient sharing of the channel amongs the users in different geographic location trying to communicate at random point in time. There are three scheme for multiplexing the communication channel:

i **FDMA (Frequency Division Multiple Access)**

Due to division in frequency spectrum into slots, the signals of different users are separated and placed in separate frequency slots. Here frequency slots are reused to overcome the problem of queing as a result of many potential communicators.

ii TDMA (Code Division Multiple Access)

Here the signals of different users are separated and placed into their individual time slot. So a given time frame is divided into slots. There is also a problem here since request to use a single communication channels occur randomly, thus the number of request for time slots is more than the numbers of available slots.

iii CDMA (Code Division Multiple Access)

Using the same frequency band, all signals are sent at the same time. At the receiver, signals are selected or rejected by the recognition of a user specific signature wave form which is constructed from an assigned spreading code.

3.0 EMPIRICAL VIEW

So far, this thesis work has been concentrated on the basic requirement on VoIP implementation, data transfer, quantization, signal processing, application and the challenges faced in the process of implementation. In this chapter, the theoretical perspective will be looked at, which starts by adopting a more precise definition of interconnection from European Commission Directive on access and interconnection (CEC 2000), referenced also by Intven (2007): "Interconnection is the physical and logical linkage of public Telecommunications networks used by the same or a different organization which allows the users of one organization to communicate with the users of the same or another organization, or to access services provided by another organization." This chapter will be treating: The context of VoIP interconnection by discussing about theories that encourage networks to communicate with one another and also about the technology trend that might explain the present state of VoIP communication and security issues. On the other part of this chapter, peculiar characteristics that are linked to interconnection, and also characters of the exact interconnection agreements, will be considered.

3.1 Reasons Why Networks Interconnect

This question is one of the fundamental works behind this thesis. It means in a different way as the reason networks interconnect/communicate with others instead of just driving their own network alone? As introduced earlier in the previous chapter, interconnection is a wide spectrum with linkages to many organizations from technological, social areas, political, business/economical and so on.

For instance, social area of interconnection deals with things like the communication demands between individuals. These needs are not subject to any limitation set up by network operators and further create the end-user demand for interconnected networks.

Regulation answers the political reasons for networks to interconnect. When a rival gains remarkable market power by limiting competitors' access to its facilities, it is possible that this method reduces competition on the market and on the other hand rises end users cost. Mandatory rules are set by regulators to enhance the inefficient market, boosting the competition and reducing market monotony. [9]

3.2 Externalities and Effect of Network

Externalities are side-effects that arise from economic activity but do not affect the price. They can be either negative or positive, like the smoke polluting coming out of factory chimney, or they can be like the spillover effect of technology development or employing effect of a new factory respectively. Network effect otherwise known as demand-side economies of scale is a term used to describe situations where each new user adopting a network, increases the overall attractiveness (value) of the network. For example users of a sophisticated programming language benefit directly when others adopt that language as it boosts the number of people who one can work with. This same phenomenon is one of the characteristics of telecommunication networks where each new user adapting to a telephone network increases the value of the network as the number of users who one can communicate with also increases. However in telecommunication networks as the value generated increases as a result of users joining the network will not affect the adaptation price for new users or the usage free for existing users although the value of the network increases. Therefore the network effect causes economic externalities that are in this case called network externalities. [9][11].

Similarly, negative externalities can result from negative network effect. When there is growth in network spontaneously, it comes to a point where new users tends to decrease the value of network rather than increase, this could be due to congestion in network as a result of more users coming into the network and causing traffic. When such occurs, each new user reduces the overall value of the network which causes a negative network effect. [9][11].

3.3.0 Contact Centers and Web-Based Call

Apart from the support to all the economic and operational advantages of VoIP by web-based call and contact centers, flexibility and other benefits of IP telephony are equally offered. Traditional circuit-switched and automatic call distribution based call and contact centers can be upgraded to support VoIP and web-based management and control by incorporating a VoIP GW and an IP interface along with the required software.

The support of VoIP in the call center makes adding/changing of stations and invoking of remote call agent to be simple and affordable. In addition by using ANI/DNIS and

instant retrieval of up-to-date customer information, the call agent interaction can be made as personalized and current as possible at the lowest possible cost. In the case of multisite call centers operating in multiple time zones, the internetworking of the VoIP GWs in different call centers using intersite IP links makes centralized messaging and management of services inexpensive and efficient. In addition, since IP telephony supports open telephony and intelligent networking (IN) application programming interfaces (API) like Java API for intelligent networking (JAIN), Paraly, and TAPI/JTAPI, many of the required sales automation and inventory management (for e-commerce applications), trouble ticketing and accounting software packages and servers can be developed and integrated easily and cost-effectively with the main customer care and customer resource management (CRM) system. To guarantee the privacy and security of electronic transactions (for e-commerce applications), the encryption authentication, and firewall mechanisms can be utilized.[1].

3.4 Feedback loops

The result loop is a source of a self-reinforcing cycle usually referred to as the network effect.

These loops could be noticed in different aspects of life for instance the phenomenon in which there is an irregular sound as a result of microphone and speaker setup. When the sound coming from the speaker reverberates to the microphone, it amplifies, here the sound becomes progressively loud.

For systems that have feedback loop, the result from the system is recycled back as an input, here the microphone and speaker generate the sound which come from the result/output of the speaker that was reused by the microphone as the input. Generally, systems with a progressive feedback, have their feedback amplifies the system, which makes strong loop to grow stronger and the weak becomes weaker. Contrarily, in the negative feedback systems, the feedback reduces/diminishes the current trend in the system. [7].

Negative feedback loops can be found in old industrial economies. A good example is the continuous use of coal to generate power, leading to the increase in price for coal which on the other hand will limit the usefulness of a coal based power production and creates room for alternative power sources to become more attractive. The competitive nature of the positive feedback loop could be described as “winner-takes-all” where an

organisatin takes a dominant position on the market. This envigorates the current trend, making information about the economy of the markets to have virtuous cycles or loop that either drives the system into high success or complete failure.

Figure 11 below is an illustration of a positive feedback in a system leading to vicious and virtuous cycles or loops. The system (network) value is proportional to the number of compatible users. This means that as the network gains more users or customers, the value of the network proportionately increases. When there are new customers in a virtuous cycle, the network becomes more valuable which attracts more and more customers growing the attractiveness of the system. Users have strong incentive in adopting a well known network which can exchange information/resources with existing customers or users. On the other hand, when the number users are reducing, then every customer leaving the network system reduces the output of the network, thus encourages more users to leave the network causing a “death spiral” known as the “vicious cycle” which will totally lead to failure of the entire system. [9][11].

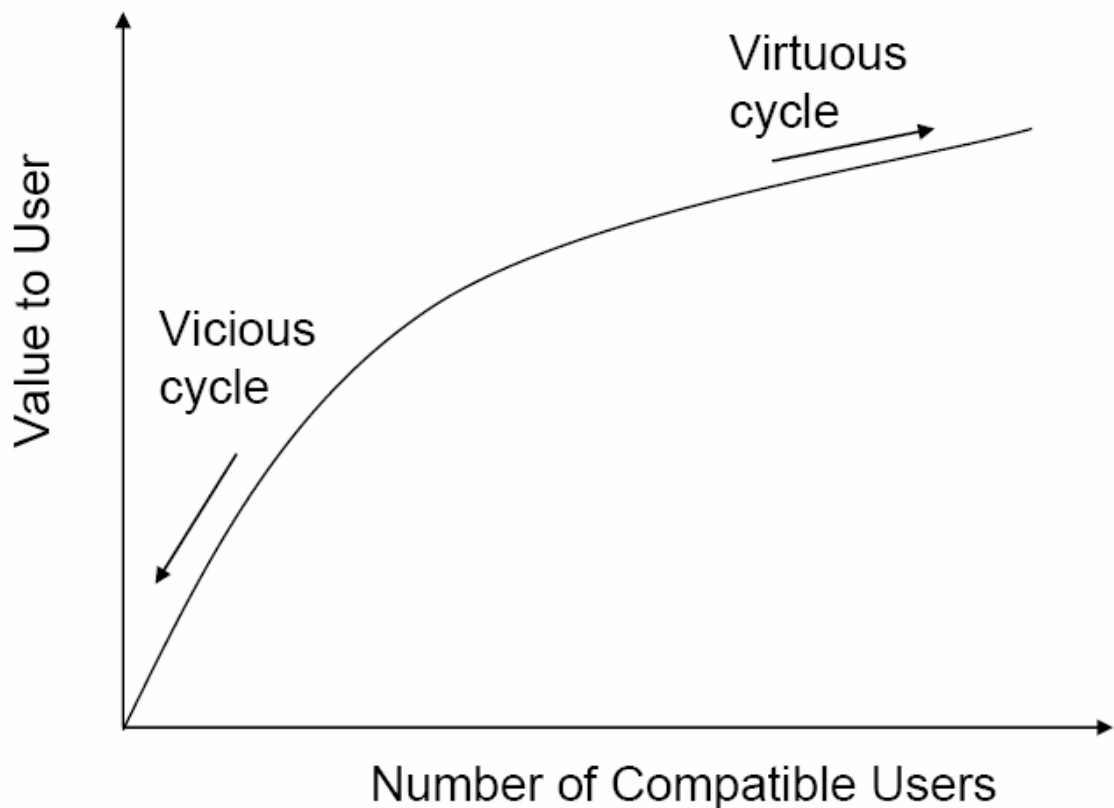


Fig 11: positive feedback describing vicious and virtuous cycles.

Basically, at the foundation of the network cycle, it will be important to attain the critical mass, which means that the number of users before the popularity of the network starts to work against the vicious cycle when the system cannot reach the critical mass then, it means it will be highly liable to failure. For the system to attain the critical mass, the companies should try to get early adopters interested in the system which in some situation, companies could give free samples to boost the numbers of compatible users. A good example is the new “web 2.0” services which became well known in offering basic services as a free trial for all users and this act as a means of gaining customer base. Additional charges comes after this.

3.5 Scanning a VoIP Network

A VoIP environment is so much more than just phone and services. Since the availability of VoIP networks relies so heavily on supporting infrastructure, an attacker will not confine his scope on just devices running VoIP services. An attacker identifies and maps out other core network devices, including routers, and VPN gateways, web servers, TFTP servers, DNS and DHCP servers, firewalls etc. If the TFTP server is located or knocked down, several models of phones trying to download configuration files on bootup might crash or stall. If an attacker can use one core routing and switching gear to reboot at will by breaking into administrative port, your VoIP traffic will obviously also be adversely affected. If the DHCP server is overwhelmed or maliciously crashed, phones trying to request an IP address on bootup will not be usable either.

3.6 Supporting Infrastructure Attacks

Basic VoIP architecture elements such as phones, servers and PBXs rely highly on one’s supporting network infrastructure. If one of those supporting elements is attacked or taken offline, a side effect maybe that your VoIP applications are crippled or severely limited in usability. The following are just a few examples of attacks on dependent data infrastructure elements.

Many VoIP phones are configured, by default, to request an IP address dynamically every time they turned on or rebooted. If the DHCP server is unavailable at the time they bootup, or the maximum number of IP addresses have already been allocated by that DHCP server, then the phone might not be usable on that network A tool for exhausting DHCP addresses, called dhcpx, is included with the latest version of the

Internetworking Routing Protocol Attack Suite (IRPAS). DHCP is a broadcast protocol which means that REQUEST messages from DHCP clients such as IP phones are seen by all devices at the local network, but are not forwarded to the additional subnetworks. If the DHCP server is present on a different network, DHCP forwarding must be enabled on the router. DHCP forwarding converts the broadcast message into a unicast message and then forwards the message to the configured DHCP server. DHCP forwarding is offered on most routers and layer 3 switches. DHCP messages are bootp (bootstrap protocol) messages. UDP port 67 is the bootstrap server port and 68 is the bootstrap client port. Bootp messages payloads maybe carried over UDP and TCP, however one can only witness UDP/IP messages being exchanged during experinments.

3.6.1 DNS Cache Poisoning

DNS cache poisoning attacks involve an attacker tricking a DNS server into believing the veracity of a fake DNS response. The purpose of this type of attack is to redirect the victims dependent on that DNS server to other addresses. This type of attack has traditionally be used in phising schemes to redirect a user trying to surf to their banking site owned by the hacker.

A DNS SRV record assists SIP phone dialing in much the same way that MX records help map email addresses to the appropriate mail servers. Some sites are beginning to use DNS SRV records to forward certain SIP requests to particular proxy addresses, potentially outside of the organization. This has particular dangerous implications if an attacker can poison these resource listings to redirect all calls going to your domain to her external proxy.

3.6.2 DNS Cache Poisoning Countermeasures

Dns cache poisoning is almost entirely avoidable if you configure your DNS server properly. This include forcing it to scrutinize any forwarded DNS response information passed by other non authoritative servers and dropping any DNS response records passed back that do not relate to the original query. Most recent DNS server are immune to this attack in their default configurations.[10].

3.6.3 DNS Flood DoS

DNS can be critical in relaying SIP calls through an organization. It is possible to perform any of the aforementioned flooding attacks on DNS server in order to consume all available network traffic or available connections. UDP floods are particularly effective at crippling exposed DNS servers simply because most firewalls differentiate between bogus DoS traffic and a legitimate DNS request/response travelling to/from the sever.

3.6.4 Vulnerabilities in Underlying OS or Firmware

Like many VoIP applications, most supporting infrastructure services run on top of popular operating systems (Windows and Linux for example) or firmware (IOS, VxWorks) that are also widely known to be vulnerable to a plethora or newly discovered vulnerabilities each day. It goes without saying that if the underlying operating system can be compromised, then any of these components are typically the TFTP, DHCP, DNS and authentication servers.

3.7.0 VoIP Privacy

VoIP privacy as treated here, will be concern with four major eavesdropping attacks. These include:

TFTP configuration file sniffing, number harvesting, call pattern tracking and conversation eavesdropping. Each of these attack requires that an attacker gain access to some part of your network where active VoIP traffic is flowing. This access can be obtained anywhere from VoIP endpoints to switch access to VoIP proxy/gateways to the Session Border Controller. To gain this type of access, there are a varieties of tools and techniques that attackers can leverage.

3.7.1 TFTP Configuration File Sniffing

Most IP phones rely on a TFTP server to download their configuration file after powering on. The configuration file often contain passwords that can be used to connect back directly to the phone and administer it. An attacker who is sniffing the wire when the phone downloads these files, can learn these passwords and potentially reconfigure and control the IP phone.

3.7.2 Number Harvesting

Number harvesting describes an attacker passively monitoring all incoming and outgoing calls in order to build a database of legitimate phone numbers or extension within an organization. This type of database can be used in more advanced VoIP attack such as signaling manipulation or SPIT attacks.

3.7.3 Call Pattern Tracking

Call pattern tracking goes one step further than number harvesting to determine who someone is talking to, even when their actual conversation is encrypted. This has obvious benefits to law enforcement if they can determine any potential accomplices or fellow criminal conspirators. There are also corporate espionage implications as well as evil corporation is able to see which customers their competitors are calling. Basically, this attack is akin to stealing someone monthly cell phone bill in order to see all incoming and outgoing phone numbers.

3.7.4 Conversation Eavesdropping and Analysis

This most hyped and the threat of most concern to many VoIP users is conversation eavesdropping. Quite simply, this attack describes an attacker recording one or both sides of a phone conversation. Beyond learning the actual content of the conversation, an attacker can also use tools to translate any touch tones pressed during the call. Touch tones also known as dual-tone-multifrequency (DTMF) tones are often used when callers enter pin numbers or other authoritative information when on the phone with their bank or credit card company. Being able to capture this information could result in an attacker being able to replay these numbers to gain access to the same account over the phone.

3.7.5 ARP Poisoning

ARP poisoning is one of the ways to perform an eavesdropping attack. It is the most popular technique to perform an MITM attack in which eavesdropping is simply one of the potential impact possible. ARP poisoning is possible because some operating systems will replace or accept an entry in their ARP cache regardless of whether or not they have sent an ARP request before. This means that an attacker may be able to trick one or both hosts into thinking that the attacker's MAC address is the address of the other computer or of a critical server (SIP proxy, DNS server etc). This then means

that the attacker can act as a gateway”Man-in-the-middle”, silently sniffing all the traffic while forwarding it onto the intended host. [10].

3.7.6 Static OS Mapping

This is an ARP poisoning countermeasure, here you can manually enter the valid MAC address to IP mappings into a static ARP table for each host on the network. Typically, it is easier to apply port security settings on your switch that do this for every possible host on your network; however, for critical workstations and servers, this may not be a bad investment of time.

3.7.7 Switch Port Security

ARP poisoning can also be mitigated by applying strict port security settings on your switches. By manually entering the lists of source MAC addresses allowed to access each port on a switch, rouge or foreign network nodes will be unable to gain access to the network.

3.8.0 Management Structure

This aspect will be explaining different managerial approach on VoIP network, the benefits and shortcomings and the processes involved in carrying out these connectivity.

3.8.1 Centralized Management Structure

Intelligence exists at the network and dumb endpoints in a centrally managed network that connect the network to access the network services. This structure creates opportunity for the total control of end users by the central hub. The management at the central hub can easily be aware of all the end users who are logged on to the hub and also know what they are doing. In PSTN for example, each node that is connected knows about the connection and keeps state information on each connection it has. This provides protection for users and allows easy collection of charging records from each other.

However, it is difficult for users to be anonymous in the network even if they would like to be. Centralized management structure allows more efficient use of resources as economies of scale can be applied.

The inflexibility of central management structure only allows very little possibilities for experimentation since it provides a wide range for users. Central hub has a drawback as it is a single point of failure for the network and provides a single point of attack for crackers to gain access on the central hub. [8][9].

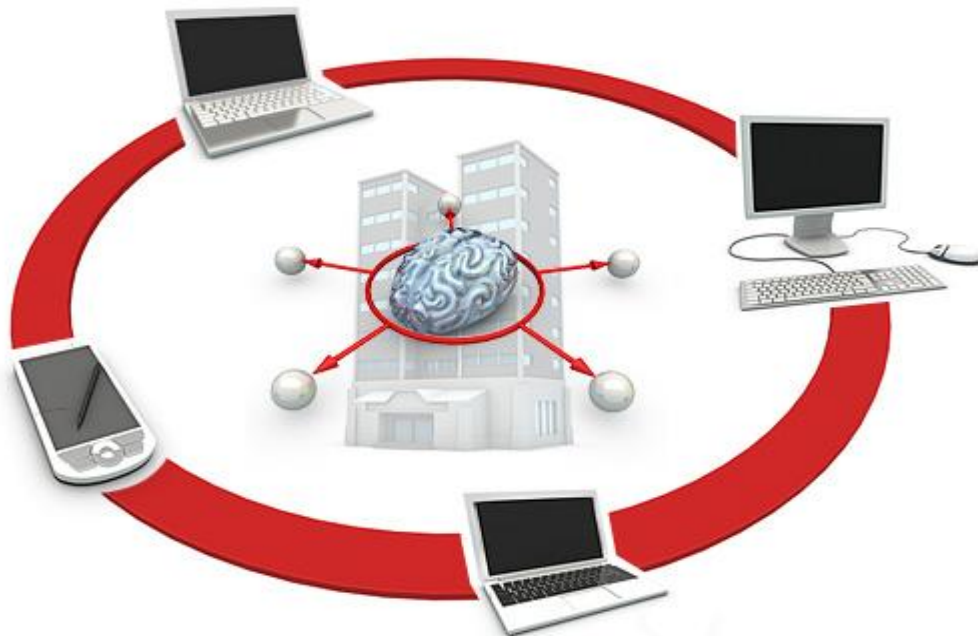


Fig 12 Centrally managed network from NCP Network Communications Products Engineering, Inc.[18].

3.8.2 Distributed Management Structure

The intelligence in a distributed network exists at network's edge, (at the endpoints of the network). The actual network which is the transport medium is not aware of the data transferred or applications and services used by any end user at that point in time. From this properties of a distributed network management structure, end users have control over upgrades and maintenance schedules which allows anyone to easily experiment with their own systems.

Furthermore, if users desire to have enough technical skills, they can remain anonymous. The drawback of distributed management is that it cannot use limited resources effectively and it is hard to impose charge users since the operator might not know what services they are using. Maintenance at network's edges at distributed management is highly needed, this means that end users or their organization should

have skills and resources to maintain their systems. In distributed systems users privacy is difficult to protect as one user can try to gain advantage in harming other users. This could be a company network with servers at different geographical locations serving local end-users. [8][9]

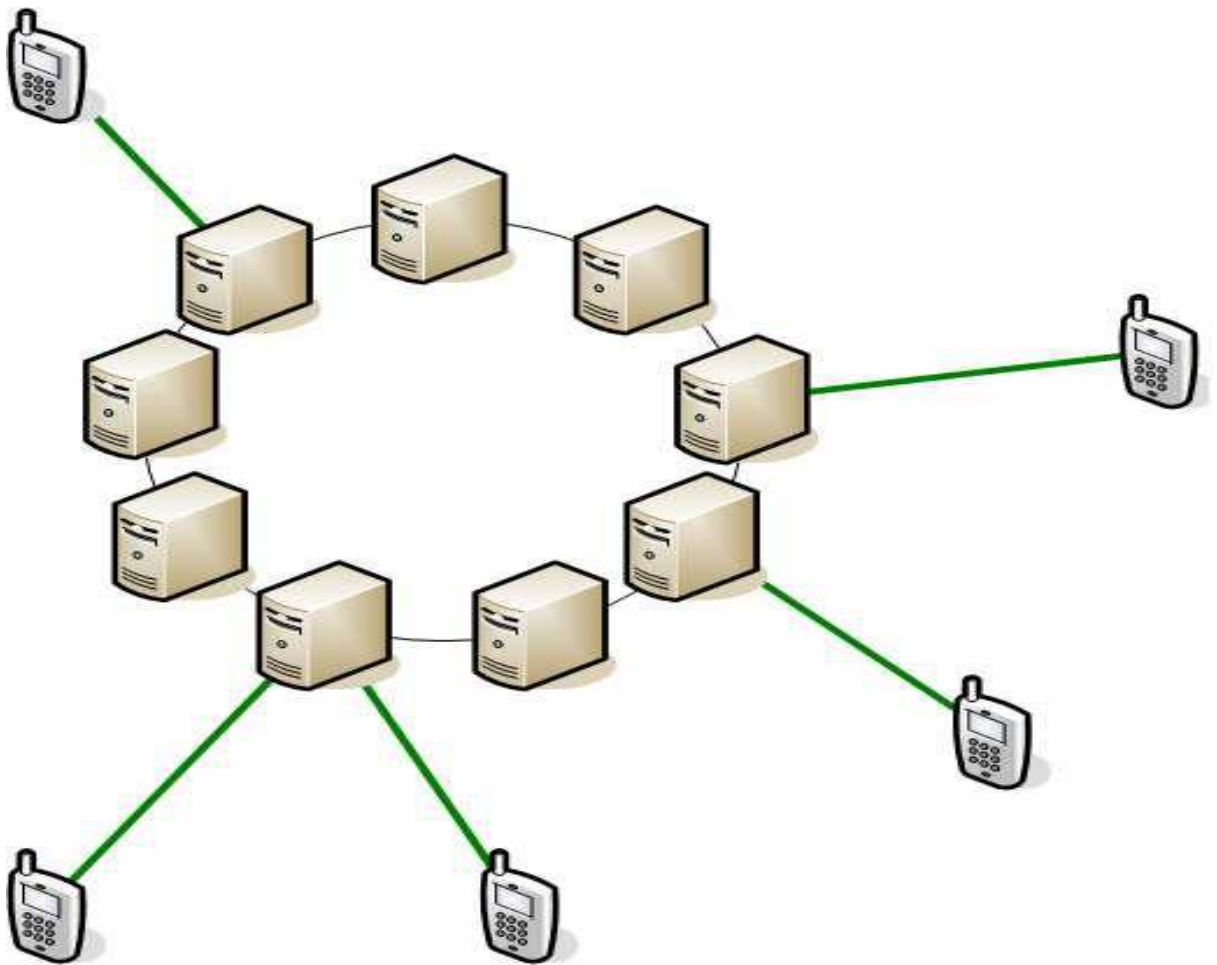


Fig 13 Network with a distributed management structure [9]

3.8.3 End-to-End Approach

For to the end-to-end principle, networks provide only the simple information transmission services, at the end points of the network, all the intelligence needed for services are provided. This principle, also found behind the Internet, provides room for

a very easy experimentation and will not restrict any future applications that might result later. “End-to-end idea argues that large centralized service providers, such as traditional telephone companies, cannot meet uncertain markets with services they think up themselves [8][9]

Network intelligence is distributed to endpoints in the end-to-end approach, which means that end points can communicate directly with each other without any knowledge of other network element of the communication taking part between those endpoints. In distributed management it means that experimenting by adding new end-to-end services to the network does not require any permission since the network knows nothing about a new service. It was also argued in 1984 that it is impossible to anticipate the services which new applications will need in the future, so by providing just basic services by the network like end-to-end networks will be appropriate. It was also pointed out that trying to meet the demands of unknown applications will only restrict these applications services later.

Isenberg (1998) in his article pointed out the advantages of simple network like the internet which is an additional benefit related to cost structure of this network. He also noted that due to the simplicity, network infrastructure is inexpensive to maintain and build. Therefore, entire networks are also inexpensive and easy to install, which is different from the case in PSTN due to complexity of that network.

3.8.4 Management Structures of PSTN and VoIP Networks

Since there are different developmental objectives at the foundation of the network development phase, management structures of PSTN and IP based network are very different. The PSTN has been centrally managed traditionally; the early development of IP-based networks for the purpose of academic and researches has laid the foundation for distributed and open management structure which is still valid in Internet and other IP-based networks. According to Shapiro and Varian 1999, Gaynor 2003, traditional telephone companies believe in the centralized model of the PSTN and they are keen to establish that structure also into VoIP networks. It also describes in more detail, that difference in routing and protocol structures of those two networks makes PSTN centrally managed and on the other hand, IP-based networks are managed in a more distributed approach. Different protocols for end user access and core network in PSTN allow operators to be in full control of end users while in IP networks the same IP

protocol is used in end-to-end and this gives more control for end user. These structural differences have great effects for example to charging principles.

3.9.0 Alternative VoIP Interconnection Models

Here, different types of VoIP interconnection models are treated. Different interconnection models are brought to play in relation to their appearance on a management structure from distributed management structure to centralized management structure.

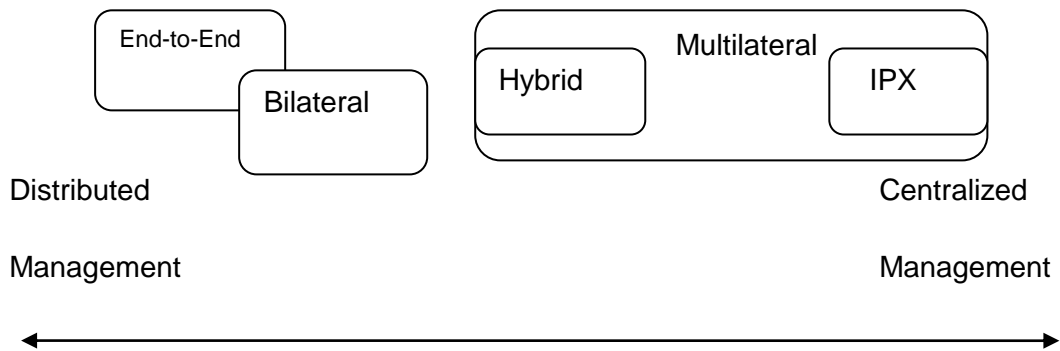


Fig 14 Continuum of management structures.

3.9.1 End-to-End Model

By using a common protocol, end users can interconnect and make VoIP calls directly to each other irrespective of their distance, location or region and community. In this completely distributed and usually open model, standard protocol enables the interconnection and uses the internet as the underlying transport layer for packets/data. Session Initiation Protocol (SIP) or Extensible Messaging and Presence Protocol (XMPP) allows this kind of interconnection though they are not yet fully complete for end-to-end VoIP purposes as working groups are still defining those services.

Products users of based on open communication protocols are able to connect with each other and communicate peer-to-peer using VoIP calls. Usually providers of those services based on open protocols have no intention to limiting the interconnection, which is not frequently in services that are based on proprietary protocols as free call

for instance is preventing interconnection. Using open protocols, they promote users' "flexibility to choose which clients, service providers, and platforms they use for their communication needs". In practice this means that users can use whatever standard instant messaging (IM) client, whatever IM service provider and any operating system to interact with others who are using some client that follows the same XMPP standard. Usually communication products, such as Instant Messaging clients which are based on standard protocols, can be downloaded freely. As there is no charging system in place for calls on this interconnection alternative, revenue can be generated from other sources. Most IM providers try to gain revenue from commercial advertising that is given to end users in IM clients. Other sources of revenue are in/out call services where the provider sets up local PSTN gateways in different regions/countries and then offers charged international inbound (PSTN to VoIP) or outbound (VoIP to PSTN) calls with a price that is remarkably lower than the price offered by traditional telephone companies on long distance calls.

This interconnection model is simple and has no central components and thus it permits totally distributed management structure. On the other hand, security components like Network Address Translation techniques and firewalls in some cases resist direct connections. Those situations require additional server in the network to allow those nodes that are behind NAT to connect with others. In some cases so called supernodes are used in the network to provide the necessary central connectivity which enables the connection for those who are behind NAT.

Harju 2006 define supernodes thus: "Supernodes are network nodes that are able to support other nodes on the network. They are for example users with powerful computers that are connected to network without NAT or firewall via a fast network connection".

3.9.2 Bilateral Model

Service providers and companies can agree to interconnect directly without any intermediate parties in bilateral terms that best suit for the purposes of those interconnecting parties. This model is most likely suitable in situations where the amount of traffic between interconnecting parties is evenly distributed/balanced, but depending on organization needs it can also be used in cases where the traffic between interconnecting parties is unevenly balanced. These parties may have bilateral interconnection agreements with more than one service providers.

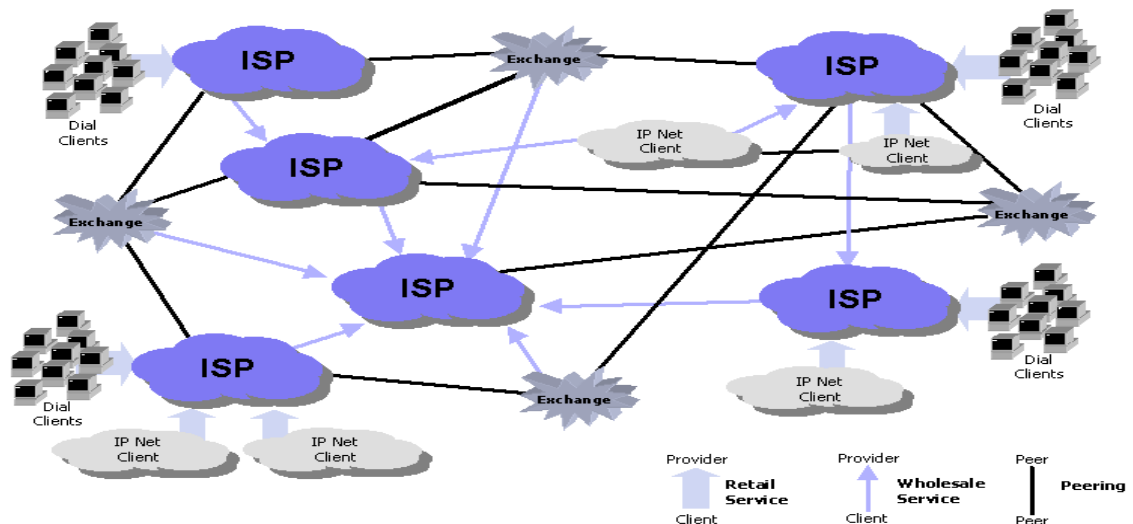


Fig 15 Illustration of Bilateral Interconnection (Picture from Wikipedia)

The important aspects of bilateral interconnection agreements are the Quality of Service (QoS) needed for the interconnection and charges applied for the exchange of traffic. Bilateral model, will probably be the most common charging model in interconnections where the traffic and advantages are evenly balanced. This is because of its simplicity, and on the other hand, in cases where benefits of interconnection are not evenly distributed between interconnecting parties, any agreement that follows the distribution of benefits will also be applicable. This uneven distribution of benefits can occur for instance in situations where smaller network gains access to a larger network. Bilateral interconnection is managed in a distributed manner by both interconnecting parties who define the rules of interconnection and acquire and maintain the resources that are required to fulfill this agreement. Session Border Controller (SBC) is an example of equipment that enables bilateral interconnection. Hardwick 2005, defines SBC: "An SBC is a VoIP session-aware device that controls call admission to a network at the border of that network." This means that SBC is like a firewall security for VoIP traffic. In addition to this basic performance/functionality, it might also contain other functionalities which are not so clear on the market of SBC's functions. [9]

3.9.3 Bilateral Ad Hoc Model

In a normal bilateral interconnection, the terms and conditions of interconnection are usually discussed and agreements are made before setting up the actual interconnection. But in some other bilateral interconnection solution, interconnection

agreements are negotiated only when they are needed. In Bilateral ad hoc interconnection (peering) model, the initiating network first sends query to the network peers to discover the called party. Once the terminating network is discovered, the terminating party then responds back (Acknowledge) that it is able to terminate the call to its network. Here the initiating network can make a direct call to the terminating network. The end users pay for their respective ITSPs for the connection and there are no monetary transactions between ITSPs.[9].

3.9.4 Multilateral

In multilateral interconnection a central interconnection point is used to handle and facilitate interconnection between several networks. Each network needed to interconnect with some other network sets up a single uniform agreement with a central interconnection provider and at the same time gains interconnection access to all the networks that complies to the interconnection through the same multilateral interconnection point

Central control by provider enables security control functionalities and collection of charging data/information records. This allows interconnection parties to decide the charging model from settlement-free (BAK) to any settlement-based model (IPNP, RPNP or other) according to what model suits best for their interconnection reasons.

One good option of multilateral interconnection is to set up only a centralized telephone number mapping (ENUM) server that will permit ad hoc interconnection between networks. In that case ENUM is first used for finding the network that is able to terminate the call and then the actual calling is done directly with initiating and terminating network. "Multilateral operator provides any or all of the following services; Physical connectivity, ENUM directory management, signaling interoperability, security and identity services, media management and commercial management."

(XConnect (2007). Other multilateral interconnection models are centralized model which provides all of those services listed by XConnect, and another, with a kind of a hybrid structure between centralized and distributed models, since only some of those functions are provided centrally. [7][9].

4.0 Data Compression (Coding)

Codes are mappings of source data/messages (alphabet "alpha") into *codewords* (alphabet "beta"). Messages from the source are the basic units which the string to be represented are partitioned. These basic units may be single symbols alphabet, or strings of symbols. For string example alpha = { a, b, c, d, e, f, g, *space*}. Beta will be taken to be { 0, 1 }. Codes can be grouped as block-block, block-variable, variable-block or variable-variable, where block-block represent the source messages and codewords are of fixed length and variable-variable codes map variable-length source messages into variable-length codewords. A block-block code is shown in Figure 16a and a variable-variable code is given in Figure 16b. If the strings were coded using the Figure 16a code, the length of the coded message would be 120; using Figure 16b the length would be 30. [16]

source message	codeword	source message	codeword
a	000	aa	0
b	001	bbb	1
c	010	cccc	10
d	011	dddd	11
e	100	eeeeee	100
f	101	ffffff	101
g	110	gggggggg	110
space	111	space	111

Figure 16a: A block-block code Figure 16b: A variable-variable code.

The oldest and most widely used codes are ASCII and EBCDIC. When source messages of variable length are allowed, the question of how a message ensemble (sequence of messages) is parsed into individual messages arises. Many of the algorithms described here are "defined-word schemes". That is, the set of source messages is determined before the invocation of the coding scheme. For instance, in text file processing, each character may constitute a message, or messages may be defined to consist of alphanumeric and non-alphanumeric strings. In Pascal source code, each token may represent a message. All codes involving fixed-length source messages are, by default, defined-word codes. In "free-parse" methods, the coding algorithm itself parses the ensemble into variable-length sequences of symbols. Most of the known data compression methods are defined-word schemes; the free-parse model differs in a fundamental way from the classical coding paradigm. [16].

"A code is *distinct* if each codeword is distinguishable from every other (i.e., the mapping from source messages to codewords is one-to-one). A distinct code is *uniquely decodable* if every codeword is identifiable when immersed in a sequence of codewords. Clearly, each of these features is desirable. The codes of Figure 16a and Figure 16b are both distinct, but the code of Figure 16b is not uniquely decodable. For example, the coded message 11 could be decoded as either ddddd or bbbbbb. A uniquely decodable code is a *prefix code* (or *prefix-free code*) if it has the prefix property, which requires that no codeword is a proper prefix of any other codeword. All uniquely decodable block-block and variable-block codes are prefix codes. The code with codewords { 1, 100000, 00 } is an example of a code which is uniquely decodable but which does not have the prefix property. Prefix codes are *instantaneously decodable*; that is, they have the desirable property that the coded message can be parsed into codewords without the need for lookahead. In order to decode a message encoded using the codeword set { 1, 100000, 00 }, lookahead is required. For example, the first codeword of the message 1000000001 is 1, but this cannot be determined until the last (tenth) symbol of the message is read (if the string of zeros had been of odd length, then the first codeword would have been 100000)". [16].

A *minimal* prefix code is a prefix code such that if x is a proper prefix of some codeword, then $x\sigma$ is either a codeword or a proper prefix of a codeword, for each letter σ in β . The set of codewords { 00, 01, 10 } is an example of a prefix code which is not minimal. The fact that 1 is a proper prefix of the codeword 10 requires that 11 be either a codeword or a proper prefix of a codeword, and it is neither. Intuitively, the minimality constraint prevents the use of codewords which are longer than necessary. In the above example the codeword 10 could be replaced by the codeword 1, yielding a minimal prefix code with shorter codewords. The codes discussed in this paper are all minimal prefix codes.

In this section, a *code* has been defined to be a mapping from a source alphabet to a code alphabet; we now define related terms. The process of transforming a source ensemble into a coded message is *coding* or *encoding*. The encoded message may be referred to as an *encoding* of the source ensemble. The algorithm which constructs the mapping and uses it to transform the source ensemble is called the *encoder*. The *decoder* performs the inverse operation, restoring the coded message to its original form. [16]

4.1 Lempel Ziv Algorithm

The Lempel Ziv Algorithm is used for lossless data compression. It is an algorithm of a whole family, which was derived from the two algorithms proposed by Jacob Ziv and Abraham Lempel in their landmark papers in 1977 and 1978. Lempel Ziv algorithms are typically used in compression utilities such as gzip, GIF image compression and the V.42 modem standard.

Data compression algorithms exploit such technique to make the compressed data smaller than the original data. Lossless compression ensures that the original information/data can be reproduced exactly from the compressed data. Examples of lossless compression data are run-length coding, statistical techniques etc. In practice, standard algorithms for compressing binary files use code words of 12 bits and transmit 1 extra bit to indicate a new sequence. In using such code, Lempel-Ziv Algorithm can compress transmissions of English text by 55%. [14]

4.2 Huffman Code

Here an illustrating example in which the binary tree structure is of value. Consider the problem of coding (in binary) a message consisting of a string of characters. This is usually done in a computer system, using the code ASCII to allocate 8 bits to store each character. Hence A is represented using decimal 65, or 01000001 in binary and so on. Unicode uses a more modern representation with a much wider range of languages, which allocates 16 bits to each character. Java is an example of such language. ASCII character can be converted to Unicode by prefixing it with the zero byte. The problem of Unicode is that it wastes about half of the available space when storing plain ASCII. Also inefficiency may occur when using the same number of bits to represent a common letter, such as "e" as to represent "q" which occurs much less frequently.

The table below is an example of a prefix code for a small alphabet, and contrasts it with a simple fixed length code. Here, it is clear that there are savings in this case making it worthy to go further. However, we can check that the string "0000100111" in Code 2 decodes clearly as "acbd". [15].

message to locate the frequency of each symbol which occurs in it. Here the basic strategy will be to allocate short codes to symbols that occur regularly/frequently, while still insisting that the code has the prefix character.[15]

4.3 Testing of VoIP

VoIP systems that make use IP Phones or an Analog Phone coupled to an Analog Telephone Adaptor (ATA) need a very good internet connection for optimal performance. Cable companies usually provide adequate connectivity. For office use it is recommended the cable required should be of a high capacity business plan which is different from the cable internet at homes.

The network capacity and performance is dependent on the number of concurrent calls that one system support (usually, 15 concurrent calls require about 1Mbps), which is about the same for internet home service cable. A VoIP Phone Service Test, which will perform measurements of the network performance, can allow one to determine the capacity and expected QoS (Quality of service) of your internet connection. The combination of voice, data and video in some cases on the same corporate network is risky and requires a propal careful planning. One must ensure that the network can support all these services running concurrently, and that they will each deliver acceptable quality while providing non-stop availability even if new applications are added or the network itself changes. [17].

5.0 CONCLUSION

Though many network calls from VoIP networks still end up to PSTN numbers, due to interconnection from VoIP based company systems to customers PSTN numbers, VoIP to VoIP interconnection is gaining ground as many users are starting to use VoIP networks. Interconnection of VoIP is becoming the new era of high market uncertainty where a dominant design to meet the interconnection requirement has not yet emerged.

Presently, alternatives that allow users to test or experiment are considered to be valuable. Hence, a VoIP interconnection alternative with open and distributed management structures that allows experimentation are considered to be more valuable than those that are closed and restricts experimentation.

Furthermore, this Thesis work investigated how VoIP works, the cost and other clear benefits when compared to PSTN. Usually, Voice routed through the internet costs nearly nothing except the cost of initial subscription paid to the ISP. This is also made possible when the basic requirement are met.

VoIP goes with more feature when the software is installed, these features include chatting, video conferencing and sharing of files and applications. Some interconnection solutions allow experimentation, a hybrid model for example exploit the benefits of both centralized and decentralized structures and offers services centrally based on the need of interconnecting networks which seems to be viable solution for various purposes.

On the other hand end-to-end and bilateral models, seem viable in more narrow areas: End-to-end model is good for users who value the low costs of communication and where low costs subsidize the flaws of the system. Bilateral model is best used for purposes where large amount of traffic is exchanged between few partner networks.

VoIP advantages are limitless and many organizations such as school, business firms and home user are turning to the numerous advantages of VoIP which seems dominating and will be the future demand. This has also been seen from the implementation in IF insurance company (Interview session) which is my case study and their management methods comprise of different model depending on the company's location.

REFERENCES

- [1] Bhumip Khasnabish, 2003, Implementation of Voice Over IP
- [2] William Stallings, 2009, Business Data Communications, Sixth Edition
- [3] William Stallings, Data and Computer Communications, 2007, Ninth Edition
- [4] William A. Flanagan, 1997, Voice Over Frame Relay
- [5] Raymond R. Panko, 2001, Business Data Communications and Networking, Third Edition
- [6] STUN, [www document], <http://www.ietf.org/rfc/rfc3489.txt> Accessed on the 21th of November, 2010
- [7] XConnect (2007), *Bridging the VoIP Islands: White Paper*, [www document], <http://www.tmcnet.com/channels/voip-peering/articles/8730-kayote-networks-founder-joins-xconnect.htm> Accessed on the 12th December, 2010.
- [8] ZDNET (2007), *VoIP cost savings main draw for UK business*, [www document], <http://www.zdnet.co.uk/news/networking/2007/03/09/voip-cost-savings-main-draw-for-uk-business-39286239/> , Accessed on the 23th of November, 2010

- [9] Wikipedia [www document], <http://www.tml.tkk.fi/~anttiyj/Lahti-VoIP.pdf>
Accessed on the 15th of September, 2010.
- [10] David Endler and Mark Coiler, 2007, Hacking Exposed VoIP
- [11] Externalities and Effect of Network, [www document] ,
<http://www.utdallas.edu/~liebowitz/palgrave/network.html>, Accessed on the
17th of December, 2010.
- [12] Wikipedia [www document] <http://www.google.fi/search?q=ATA+picture>,
Accessed on the 9th of December, 2010.
- [13] Wikipedia [www document]
<http://www.google.fi/search?q=ip+phone+pictures>, Accessed on the 9th of
November, 2010.
- [14] Wikipedia [www document]
https://dspace.ist.utl.pt/bitstream/2295/51292/1/LempelZiv_Zeeh.pdf
Accessed on the 9th of November, 2010.
- [15] Wikipedia [www document]
<http://www.cs.duke.edu/csed/poop/huff/info/>, Accessed on the 9th of
November, 2010.
- [16] Wikipedia [www document]
<http://www.ics.uci.edu/~dan/pubs/DC-Sec1.html> , Accessed on the 20th
of April, 2011.
- [17] Sunra Software, Application Performance Engineering.
- [18] Centrally Managed Network, NCP Network Communications
Products Engineering, Inc.

[1]