PERFORMANCE ANALYSIS OF VOIP NETWORK USING QOS PARAMETERS.

BY

MD.NAZMUL HUSSAIN
ID: 071-19-661
MD.LIAKAT ALI
ID: 071-19-667
BELAYET HOSSIAN
ID: 071-19-670

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

Supervised By

MOHAMMAD MIRZA GOLAM RASHED
Assistant Professor
Department of Electronics and Telecommunication Engineering (ETE)
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITYDHAKA,

BANGLADESH

FEBRUARY 2011

APPROVAL

This Project titled **"**Performance Analysis of VoIP Network Using QoS Parameters"submitted by Md.Nazmul Hussain, Md.Liakat Ali and Belayet Hossain to the Department of Electronics and Telecommunication Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Electronics and Telecommunication Engineering and approved as to its style and contents. The presentation has been held on *date*.[**Font-12**]

BOARD OF EXAMINERS

Mr.Golam Mowla Choudhury
Professor and Head
Department of ETE
Faculty of Science & Information Technology ----------
Daffodil International University Chairman

A K M Fazlul Haque
Assistant Professor
Department of ETE
Faculty of Science & Information Technology ----------
Daffodil International University (Internal Examiner)

Mohammad Mirza Golam Rashed
Assistant Professor
Department of ETE
Faculty of Science & Information Technology ----------
Daffodil International University (Internal Examiner)

Dr. Subrata Kumar Aditya
Professor
Department of Applied Physics,
Electronics and Communication Engineering ----------
University of Dhaka (External Examiner)

ABSTRACT

This report “Performance Analysis of VoIP Network Using QoS Parameters” presents the results of experiments and the analysis by which we found the characteristics in different sets of VoIP QoS, with software.

There are about 1 billion fixed telephone lines and 2.5 billion cell phones in the world that use the traditional public switched telephone network (PSTN) systems. Soon, they will move to networks based on open protocols- known as Voice over Internet Protocols (VoIP). This migration is fueled by many factors, like the tremendous growth of the Internet and the World Wide Web, the rapid and low cost coverage capability through wired and wireless networks, the availability of a variety of fixed and mobile Internet accessing tools (e.g., desktop, laptop, pocket pc, dual-band cellular, etc), and the feasibility of integrating voice and data into a single infrastructure.
There are three major areas of our VoIP study. First, VoIP protocols; second, VoIP Basic Network Architecture; and the third is, Performance measurement of VoIP Quality of service. from which more useful predictive models can be generated. This study falls into the combination of these three areas. Since more and more VoIP systems are appearing, characterizing the traffic of a VoIP system and studying the protocols to increase the quality of service can help to better understand and improve these systems.

We have estimated the QoS obtained by the end user and analyzed performance metrics, i.e. average packet loss rate and average jitter, maintained stable values and acceptable QoS levels. In VoIP there are also unique sources of degradation including codec compression, packet loss, discarded packets, bit errors, frame erasures and various compression schemes. Voice quality measurement considers the extent of all of these factors, whether they occur in the network or outside it, and determines the overall impact of quality in the opinion of the customer, a measurement known as a Mean Opinion Score (MOS). As a result, the paper presents VoIP software and VoIP hardware phones only for the G.711 codec.

APPROVAL [capital letter, Bold, Font-14, Alignment-middle]

This Project titled **"Title**", submitted by *Name1* and *Name2* to the Department of Electronics and Telecommunication Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Electronics and Telecommunication Engineering and approved as to its style and contents. The presentation has been held on *date*. [**Font-12**]

BOARD OF EXAMINERS

_____

(Name) [**Font-12, Bold**] **Chairman**
Designation
Department of ETE[**Font-12**]
Faculty of Science & Information Technology
Daffodil International University

_____

(Name) **Internal Examiner**
Designation
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

_____

(Name) **Internal Examiner**
Designation
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

_____

(Name) **External Examiner**
Designation
Department of -------
University of Dhaka

DECLARATION

We hereby declare that, the work presented in this project report titled “Performance Analysis of VoIP Network Using QoS Parameters” has been done by us under the supervision of Mohammad Mirza Golam Rashed, Assistant Professor, Department of ETE, Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Mohammad Mirza Golam Rashed
Assistant Professor
Department of Electronics and Telecommunication Engineering
Daffodil International University ……...
(Signature)

Submitted by:

Md.Nazmul Hussain
ID: 071-19-661
Department of Electronics and Telecommunication Engineering
Daffodil International University ……...
(Signature)

Md.Liakat Ali
ID: 071-19-667
Department of Electronics and Telecommunication Engineering
Daffodil International University ……...
(Signature)

Belayet Hossain
ID: 071-19-670
Department of Electronics and Telecommunication Engineering
Daffodil International University ……...
(Signature)

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty Allah for His divine blessing which made it possible to complete this project successfully.

We feel grateful and indebted to Mohammad Mirza Golam Rashed, Assistant Professor, Department of ETE, Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in Voice over Internet Protocols influenced us to carry out this project. His endless patience, scholarly guidance, continuous encouragement, constant and energetic supervision, constructive criticism, valuable advice ,reading many drafts and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to Mr.Golam Mowla Choudhury, Professor, and Head**,** Department of ETE, for his kind help to finish our project and also to other faculty member and the staff of ETE department of Daffodil International University.

We would like to thank our all the course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT[capital letter, Bold, Font-14, Alignment-middle]

This project is on "**Configuration of a Wireless Router with Password Authentication**". This is a kind of network using wireless router, which help a Network Administrator build up a control over the total network using a security key.

The aim of the Wireless Network is build up a WLAN using broad band router by assign a real IP address .After assigning IP address we configure the router in DHCP mode and create a secrete key for the network. When router will configure in DHCP mode every computer will get a IP address automatically but when a user new user try to acess the network it will must essential the desire secret key that are provide by network administrator.

To develop this project the most essential device is broad band router and wireless NIC card. The brands of router that are use in the project is Netgear WGR614 v6 router. The configure of the router are described in the project.

With network security function using this project network administrator can also get other facility such as printer & scanner sharing, use more then one IP series in a LAN card, sub netting process are also describe in the project

After implementation of all functions, the system is tested in different stages and it works successfully as a prototype. [**Font-12**]

TABLE OF CONTENTS[capital letter, Bold, Font-14, Alignment-middle]

CONTENS[Font-12, bold] **PAGE**

LIST OF FIGURES[Font-14,Bold]

FIGURES[Font-12,Bold] **PAGE NO**

Some Other Instruction

Thesis/Project Size: 50-60 page limit

Page Setup: Left- 1.25"

Right-1.25"

Top: 1.0-1.25"

Bottom-1.0-1.25"

Orientation- Portrait

Paragraph Line Spacing: 1.5

Font: Time New Roman

Header: Bold, Capital letter, Alignment-Center, Font-14

Inner Text: Font-12, Plain text

TABLE OF CONTENTS

CONTENTS **PAGE**

LIST OF TABLES

CHAPTER 4: PERFORMANCE MEASUREMENT OF VOIP USING QOS PARAMETERS

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

CHAPTER 2: VOIP PRINCIPLE AND PROTOCOLS

CHAPTER 4: PERFORMANCE MEASUREMENT OF VOIP USING QOS PARAMETERS

CHAPTER 01: INTRODUCTION

Voice over Internet Protocol is a rapidly growing Internet service. It gained popularity as a way to cut costs of international telephone connections by transporting voice over public IP network. Today it is being implemented in many IP applications, where it enables direct, often free communication over the Internet to people from all over the world. As a consequence, VoIP technology slowly replaces traditional telephony.

The current IP networks are designed based on an open architecture to mainly support best effort applications, like file transfer, web browsing, and email, which are not delay or delay-jitter sensitive. Due to the current very low voice traffic volume, the available IP networks are still able to report an acceptable quality of service (QoS) for the VoIP applications.

1.1 What Is VoIP?

Voice over Internet Protocol (Voice over IP, VoIP) is a general term for a family of methodologies, communication protocols, and transmission technologies for delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms frequently encountered and often used synonymously with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, and broadband phone. (Voice over IP) A digital telephone service that uses the public Internet and private backbones for call transport. Support for the public switched telephone network (PSTN) is also provided so that VoIP calls can originate and terminate from regular telephones [2].

Internet telephony refers to communications services — voice, fax, SMS, and/or voice-messaging applications — that are transported via the Internet, rather than the public switched telephone network (PSTN). The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, optionally compression, packetization, and transmission as Internet Protocol

(IP) packets over a packet-switched network. On the receiving side similar steps reproduce the original voice stream.[2]

VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs which encode speech allowing transmission over an IP network as digital audio via an audio stream. Codec use is varied between different implementations of VoIP (and often a range of codecs are used); some implementations rely on narrowband and compressed speech, while others support high fidelity stereo codecs.

VoIP converts the voice signal from your telephone into a digital signal that can travel over the Internet. If you are calling a regular telephone number, the signal is then converted back at the other end. Depending on the type of VoIP service, you can make a VoIP call from a computer, a special VoIP phone, or a traditional phone with or without an adapter. In addition, new wireless "hot spots" in public locations such as airports, parks, and cafes allow you to connect to the Internet, and may enable you to use VoIP service wirelessly. If your VoIP service provider assigns you a regular telephone number, then you can receive calls from regular telephones that don't need special equipment, and most likely you'll be able to dial just as you always have[11].

Figure 1.1: How VoIP service works

1.2 Reasons for VoIP Deployment

There are three major reasons to use VoIP: lower cost than traditional landline telephone, increased functionality and Flexibility. Each of these will be described in the remainder of this section.

1.2.1 Lower Cost to Consumers

VoIP becoming popular can be mainly attributing to the cost advantages to consumers over traditional telephone networks. The traditional business model for telephone services has been that most people pay a flat monthly fee for local telephone call service and a per-minute charge for long-distance calls. The deployment of VoIP has led to the possibility of change in this because the companies and organizations have offered different business models. Though the cost for an organization to convert to VoIP is not trivial, the monthly operational costs could be lower, so the overall long-term cost of VOIP is expected to decrease.

VoIP calls can be deployed using just Internet resources from computers equipped with microphones and speakers. Additional VoIP handsets can be directly connected to the Internet or to an Intranet. Most Internet connections are charged using a flat monthly fee structure. For International calling, the savings can be significant to the consumer by switching to VoIP technology. Using the Internet connection for both data traffic and voice calls can allow consumers to eliminate one monthly payment for telephone. In addition, VoIP plans do not charge a per-minute fee for long distance [15].

1.2.2 Increased Functionality

VoIP makes various tasks, which are difficult or impossible with traditional phone networks, easy.

- Incoming phone calls can be automatically routed to the VoIP phone wherever the phone is plugged into the network. So incoming calls can be received anywhere in the network.
- Call center agents using VoIP phones can easily work from anywhere with a good Internet connection.
- Multi-party conferencing is also much easier and cheaper because no bridge is required for small conferences.

1.2.3 Flexibility

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

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

Another advantage of VoIP is that a stand-alone telephone or videophone can be integrated with the personal computer. One can use a computer entirely for voice and video communications (soft phones), use a telephone for voice and the computer for video, or can simply use the computer in conjunction with a separate voice/video phone to provide data conferencing functions, like application sharing, electronic white boarding, and text chat.

VoIP technology provides more abundant and flexible foundations for establishing communication services [12]. IP networks support independent connections for signaling and media traffic. Interference between the information flows has been avoided by the decoupling of signal and bearer traffic. Signaling and media traffic don't need to be in the same band and on the same channel, and in-band signaling is not required. Thus, communication with application servers is simplified.

Though VoIP is becoming more and more popular, there are still some challenging problems such as how to improve quality and robustness of VoIP service. VoIP quality still remains sensitive to performance degradation in the network [3].

CHAPTER 02: VOIP PRINCIPLE AND PROTOCOLS

2.1 VoIP Architecture

VoIP is the routing of voice traffic over the Internet or any other IP-based network. Using the Internet's packet-switching capabilities, VoIP technology has been implemented to provide telephone services [10]. Figure 2.1: illustrates a typical VoIP architecture though many "possible" modifications of this architecture are implemented in existing systems.

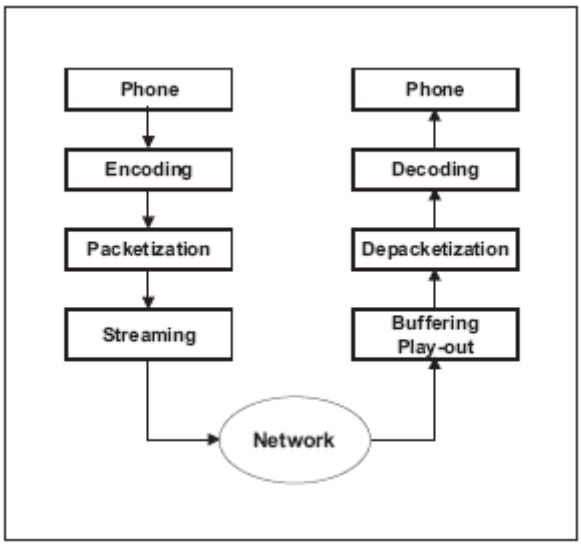


Figure 2.1: VoIP architecture

At the sending end, the original voice signal is sampled and encoded to a constant bit rate digital stream. The digital stream can then be easily compressed. This digitized and compressed data is then encapsulated into packets of equal sizes for easy transmission over the Internet. Along with the compressed voice data, these packets contain information about the packet's origin, the intended destination, and a timestamp that allows the packet stream to be reconstructed in the correct order. These packets flow over a general-purpose packet-switched network, instead of traditional dedicated, circuit-switched voice transmission lines. At the receiving end, the continuous stream of packets are depacketized and converted back into the analog signal so that it can be detected by the human ear. In general, this means voice information is sent in digital form in discrete packets rather than using the traditional

circuit-committed protocols of the Public Switched Telephone Network (PSTN). In addition to IP, VoIP uses the Real-Time Transport Protocol (RTP) to help ensure that packets get delivered in a timely way. Over the last few years, VoIP has become increasingly popular and is already starting to replace existing telephone networks. It has the potential to completely substitute for the world's current phone systems.

2.2 Overall Architecture Public Network

Public network is a complex organism consisting of many entities and elements. However, its primary sense of being is a platform providing some sort of services. Because of that, almost every subject that is a part of public network may be classified either as a client or provider. Client uses the services, while provider delivers them. Of course both entities have to be connected together through some kind of network. As a result one could say that public network is a set of interconnected clients and providers. The example of such architecture is shown in Figure 2.2:

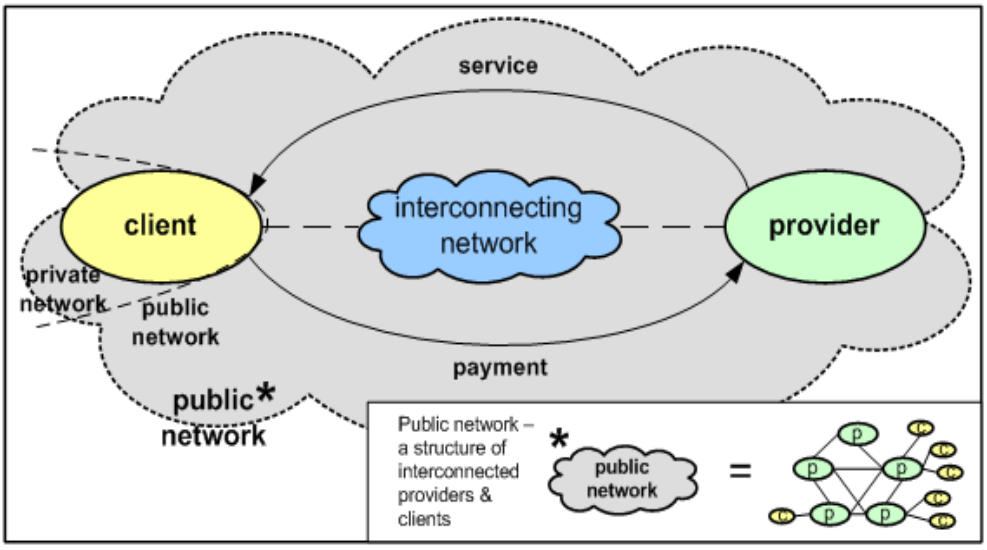


Figure 2.2: Public network abstract architecture

There is also some specification of what is a private network in the figure. It is a part of the client's (but can also be a part of provider's) network that is managed by the client and is not freely available from the public network. Most of the time it is not even fully visible from the outside. As in case of an abstract example from Figure 2.3:

public network consists of Internet Service Providers (ISPs) that offer services to users, users and some interconnecting network. Many different services may be offered in public IP network – WWW, Instant Messaging, email, VoIP, etc.

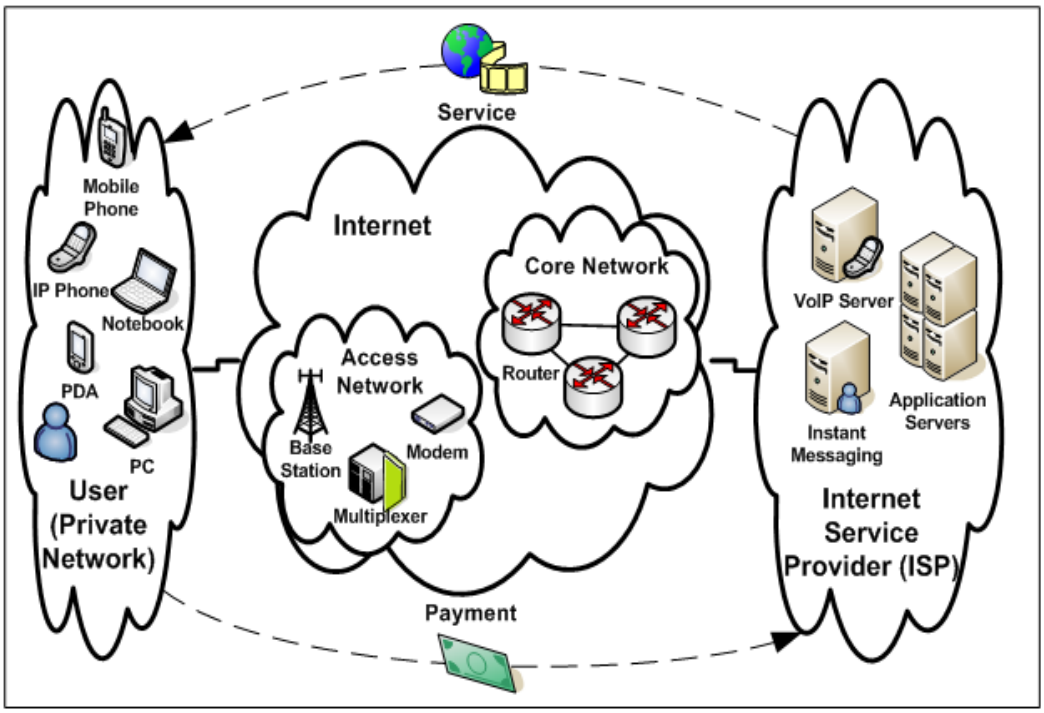


Figure 2.3: Public IP network general architecture

In this case an interconnecting network is the Internet. Actually the Internet is very often identified with a public IP network itself. We say that services are offered in the Internet, not through it. It is true from the client's perspective. Additionally, the Internet is often described as a network of networks, what in practice means that each ISP's network or client, when connected to the Internet is also a part of it [9].

2.3 VoIP Next-Generation Network Architecture

VoIP can be deployed in many different network segments. To date, it has been mostly deployed in the backbone and enterprise networks.

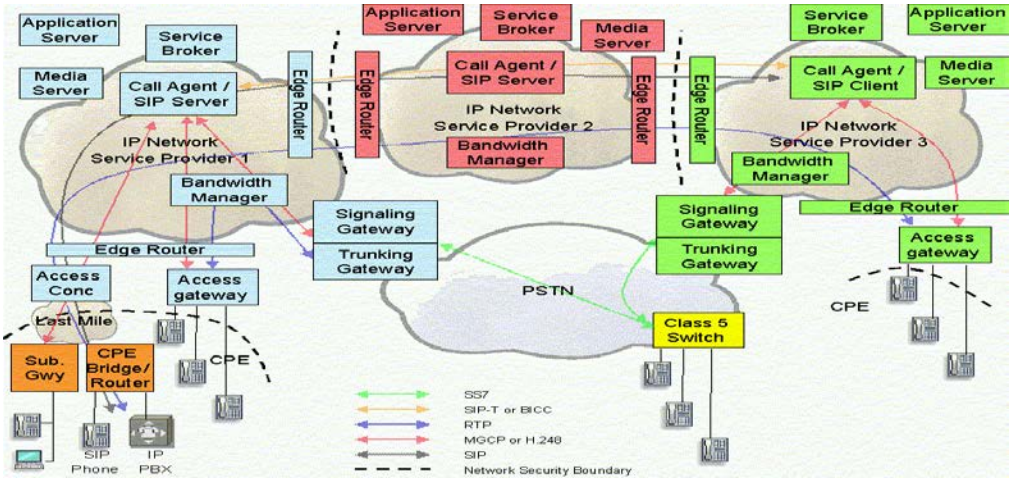


Figure 2.4: Next Generation VoIP Network

Figure 2.4 shows an example VoIP Next Generation network with 3 service provider networks.

- Service Provider 1 is offering local access acting as a LEC (local exchange carrier). This Service Provider supports IP phones and IP PBX systems using SIP and POTS phones via either an Access Gateway (Next-Gen DLC) or a Subscriber Gateway (using either H.248 or MGCP).
- Service Provider 2 is acting as an inter-exchange carrier (IXC) and supports SIP and SIP-T or BICC signaling through its network.
- Service Provider 3 is offering local access acting as a LEC, but only supports POTS phones(Plain old telephone service) using an Access Gateway. SIP signaling is supported but is terminated by the SIP Server rather than using a SIP Phone or other CPE device.

2.4 Network Components

This section describes the function of the network components listed in Figure 4. Depending upon the particular network architecture some of these network components may be combined into a single solution, for example a combined signaling and trunking gateway.

2.4.1 Call Agent/SIP Server/SIP Client

The Call Agent/SIP Server/SIP Client is located in the service provider's network and provides call logic and call control functions, typically maintaining call state for every call in the network. Many call agents include service logic for supplementary services, e.g. Caller ID, Call Waiting, and also interact with application servers to supply services that are not directly hosted on call agent. The Call Agent will participate in signaling and device control flows originating, terminating or forwarding messages. There are numerous relevant protocols depending upon the network architecture including SIP, SIP-T, H.323, BICC, H.248, MGCP/NCS, SS7, AIN, ISDN, etc. Call Agents also produce details of each call to support billing and reconciliation [9].

2.4.2 Service Broker

The service broker is located on the edge of the service provider's service network and provides the service distribution, coordination, and control between application servers, media servers, call agents, and services that may exist on alternate technologies (i.e. Parlay Gateways and SCP s). The service broker allows a consistent repeatable approach for controlling applications in conjunction with their service data and media resources to enable services to allow services to be reused with other services to create new value added services.

2.4.3 Application Server

The Application Server is located in the service provider's network and provides the service logic and execution for one or more applications or services that are not directly hosted on the Call Agent. For example, it may provide voice mail or conference calling facilities.

2.4.4 Media Server

This Media Server is located in the service provider's network. It is also referred to as an announcement server. For voice services, it uses a control protocol, such as H.248 (Megaco) or MGCP, under the control of the call agent or application server.

2.4.5 Signaling Gateway

The Signaling Gateway is located in the service provider's network and acts as a gateway between the call agent signaling and the SS7-based PSTN. It can also be used as a signaling gateway between different packets based carrier domains. It may provide signaling translation, for example between SIP and SS7 or simply signaling transport conversion e.g. SS7 over IP to SS7 over TDM.

2.4.6 Trunking Gateway

The Trunking Gateway is located in the service provider's network and as a gateway between the carrier IP network and the TDM (Time Division Multiplexing)-based PSTN. It provides transcoding from the packet based voice, VoIP onto a TDM network. Typically, it is under the control of the Call Agent / Media Gateway Controller through a device control protocol such as H.248 (Megaco) or MGCP.

2.4.7 Access Gateway

The Access Gateway is located in the service provider's network. It provides support for POTS phones and typically, it is under the control of the Call Agent / Media Gateway Controller through a device control protocol such as H.248 (Megaco) or MGCP.

2.4.8 Access Concentrator

The Access Concentrator is located in the service provider's network and terminates the service provider end of the WAN links used over the "last mile". For example, in a DSL network, this is a DSLAM; in a cable network, a CMTS.The Access Concentrator may also include the Access Gateway function, for example a Next-Generation DLC that combines DSLAM capability with direct POTS termination.

2.4.9 Bandwidth Manager

The Bandwidth Manager is located in the service provider's network and is responsible for providing the required QoS from the network. It is responsible for the setting up and tearing down of bandwidth within the network and for controlling the access of individual calls to this bandwidth. It is responsible for installing the appropriate policy in edge routers to police the media flows on a per call basis.

2.4.10 Edge Router

The Edge Router is located in the service provider's network and routes IP traffic onto the carrier backbone network. Typically the edge router will provide many other functions and can be combined with the Access Concentrator.

2.4.11 Subscriber Gateway

The Subscriber Gateway is located at the customer premises and terminates the WAN (Wide Area Network) link (DSL, T1, fixed wireless, cable etc) at the customer premises and typically provides both voice ports and data connectivity. Usually, it uses a device control protocol, such as H.248 (Megaco) or MGCP/NCS, under the control of the Call Agent. It provides similar function to the Access Gateway but typically supports many fewer voice ports.

2.4.12 Bridge/Router

The Bridge/Router is located at the customer premises and terminates the WAN (Wide Area Network) link (DSL, T1, fixed wireless, cable etc) at the customer premises. The difference between this and the Subscriber Gateway is a bridge/router does not provide any native voice support, although voice services for example SIP phones, can be bridged/routed via this device.

2.4.13 IP Phone/PBX

IP Phones and PBX systems are located at customer premises and provide voice services. They interact with the Call Agent/SIP Server using a signaling protocol such as SIP, H.323 or a device control protocol such as H.248 (Megaco) or MGCP.

2.5 Protocols

In the Internet and computer worlds, there are many different protocols which have been established. The Internet has protocols for various purposes depending on the type of data that is being transmitted and its relative importance. Protocols can be layered -- used with each other to form a set of protocols which must be recognized at every point along the Internet pathways.

The basic protocol for the Internet is the Internet Protocol (IP). This allows computers to send data back and forth, but offers very little guarantee that the data will arrive intact. Other layers are used on top of IP in order to guarantee data integrity or speed of delivery. VOIP depends on rapid delivery of data packets, but is not overly concerned if a few of the packets are dropped en route.

When data integrity is important (for example when transmitting program files) a protocol like TCP (Transmission Control Protocol) is used on top of IP. However, it is too slow for VOIP.

2.5.1 H.323

H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any network. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences.[20]

It is widely implemented by voice and videoconferencing equipment manufacturers, is used within various Internet real-time applications such as GnuGK and NetMeeting and is widely deployed worldwide by service providers and enterprises for both voice and video services over IP networks. It is a part of the ITU-T H.32x series of protocols, which also address multimedia communications over ISDN, the PSTN or SS7, and 3G mobile networks.

H.323 call signaling is based on the ITU-T Recommendation Q.931 protocol and is suited for transmitting calls across networks using a mixture of IP, PSTN, ISDN, and QSIG over ISDN. A call model, similar to the ISDN call model, eases the introduction of IP telephony into existing networks of ISDN-based PBX systems, including transitions to IP-based PBXs.

2.5.2 IP Multimedia Subsystem (IMS)

The IP Multimedia Subsystem (IMS) is an architectural framework for delivering Internet Protocol (IP) multimedia services. It was originally designed by the wireless standards body 3rd Generation Partnership Project (3GPP), as a part of the vision for evolving mobile networks beyond GSM. Its original formulation (3GPP R5) represented an approach to delivering "Internet services" over GPRS. This vision was later updated by 3GPP, 3GPP2 and TISPAN by requiring support of networks other than GPRS, such as Wireless LAN, CDMA2000 and fixed line.

To ease the integration with the Internet, IMS uses IETF protocols wherever possible, e.g. Session Initiation Protocol (SIP). According to the 3GPP[1], IMS is not intended to standardize applications but rather to aid the access of multimedia and voice applications from wireless and wire line terminals, i.e. create a form of fixed-mobile convergence (FMC). This is done by having a horizontal control layer that isolates the access network from the service layer. From a logical architecture perspective, services need not have their own control functions, as the control layer is a common horizontal layer. However in implementation this does not necessarily map into greater reduced cost and complexity.

2.5.3 Media Gateway Control Protocol (MGCP)

MGCP is an implementation of the Media Gateway Control Protocol architecture[1] for controlling media gateways on Internet Protocol (IP) networks and the public switched telephone network (PSTN). The general base architecture and programming interface is described in RFC 2805 and the current specific MGCP definition is RFC 3435 (obsolete RFC 2705). It is a successor to the Simple Gateway Control Protocol (SGCP).

MGCP is a signaling and call control protocol used within Voice over IP (VoIP) systems that typically interoperate with the public switched telephone network (PSTN). As such it implements a PSTN-over-IP model with the power of the network residing in a call control center (soft switch, similar to the central office of the PSTN) and the endpoints being "low-intelligence" devices, mostly simply executing control commands. The protocol represents a decomposition of other VoIP models, such as H.323, in which the media gateways (e.g., H.323's gatekeeper) have higher levels of signaling intelligence. MGCP uses the Session Description Protocol (SDP) for specifying and negotiating the media streams to be transmitted in a call session and the Real-time Transport Protocol (RTP) for framing of the media streams.

2.5.4 Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP) is an IETF-defined signaling protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. The modification can involve changing addresses or ports, inviting more participants, and adding or deleting media streams. Other feasible application examples include video conferencing, streaming multimedia distribution, instant messaging, presence information, file transfer and online games.

The SIP protocol is an Application Layer protocol designed to be independent of the underlying transport layer; it can run on Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or Stream Control Transmission Protocol (SCTP).[21] It is

a text-based protocol, incorporating many elements of the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP).[22]

2.5.5 Real-time Transport Protocol (RTP)

The Real-time Transport Protocol (RTP) defines a standardized packet format for delivering audio and video over IP networks. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications and web-based push to talk features. For these it carries media streams controlled by H.323, MGCP, Megaco, SCCP, or Session Initiation Protocol (SIP) signaling protocols, making it one of the technical foundations of Voice over IP.

RTP is usually used in conjunction with the RTP Control Protocol (RTCP). While RTP carries the media streams (e.g., audio and video), RTCP is used to monitor transmission statistics and quality of service (QoS) and aids synchronization of multiple streams. When protocols are used in conjunction, RTP is originated and received on even port numbers and the associated RTCP communication uses the next higher odd port number.

2.5.6 Session Description Protocol (SDP)

The Session Description Protocol (SDP) is a format for describing streaming media initialization parameters. The IETF published the original specification as an IETF Proposed Standard in April 1998,[24] and subsequently published a revised specification as an IETF Proposed Standard as RFC 4566 in July 2006.[23]

SDP is intended for describing multimedia communication sessions for the purposes of session announcement, session invitation, and parameter negotiation. SDP does not deliver media itself but is used for negotiation between end points of media type, format, and all associated properties. The set of properties and parameters are often called a session profile. SDP is designed to be extensible to support new media types and formats.

SDP started off as a component of the Session Announcement Protocol (SAP), but found other uses in conjunction with Real-time Transport Protocol (RTP), Real-time Streaming Protocol (RTSP), Session Initiation Protocol (SIP) and even as a standalone format for describing multicast sessions.

2.5.7 Skinny protocol

Skinny Client Control Protocol (SCCP). Telephony systems are moving to a common wiring plant. The end station of a LAN or IP- based PBX must be simple to use, familiar and relatively cheap. The H.323 recommendations are quite an expensive system. An H.323 proxy can be used to communicate with the Skinny Client using the SCCP. In such a case the telephone is a skinny client over IP, in the context of H.323. A proxy is used for the H.225 and H.245 signaling [1].

The skinny client (i.e. an Ethernet Phone) uses TCP/IP to transmit and receive calls and RTP/UDP/IP to/from a Skinny Client or H.323 terminal for audio. Skinny messages are carried above TCP and use port 2000.

2.5.8 Skype protocol

Skype uses a proprietary Internet telephony (VoIP) network based on peer-to-peer architecture. The protocol has not been made publicly available by Skype and official applications using the protocol are closed-source.

The Skype network is not interoperable with most other VoIP networks without proper licensing from Skype. Digium, the main sponsor of Asterisk PBX released a driver licensed by Skype dubbed 'Skype for Asterisk' to interface as a client to the Skype network, however this still remains closed source.[25] Numerous attempts to study and/or reverse engineer the protocol have been undertaken to reveal the protocol, investigate security or to allow unofficial clients.

CHAPTER 03: ISSUES IN A VOIP NETWORK

There are several issues that need to be addressed in order to provide a toll-quality, PSTN equivalent end-to end VoIP network [7]. These include:

- Service set to be offered, and the types of end user terminal supported.
- Choice of signaling protocol(s).
- Security.
- Quality of Service (QoS).
- Reliability / availability.
- Regulatory Issues
- Lawful Interception
- Emergency and Operator Services
- Call routing and Number Plans.
- DTMF and Other Tones and Telephony Events
- Firewall and NAT traversal.
- Billing and Reconciliation.
- Network Interconnection.
- Migration Path.
- OSS support.
- Bandwidth Utilization.
- Fax, Modem, and TTY support.
- Auto-configuration.

3.1 Service set

A crucial decision facing an operator looking to deploy a VoIP network is the service set that needs to be supported. This could range from a minimal set of services for a “cheap teen line” offering possibly alongside broadband data services, through to full PSTN equivalence and advanced services for carriers wishing to replace their current infrastructure with a new converged network for all subscribers.

Another important part of the service design is the choice of end user terminals that are to be supported by the service offering, possible choices include:

- POTS "black phones"
- IP phones.
- PBXs and key systems
- PC soft clients (including web-based applications)

3.2 Choice of Signaling Protocol

Numerous different signaling protocols have been developed that are applicable to a VoIP solution. They include

- Device control protocols such as H.248 (Megaco), MGCP, NCS, etc
- Access services signaling protocols such as SIP, H.323, etc
- Network service signaling protocols such as SIP, SIP-T, BICC, CMSS, etc

The choice of which protocol to use in a service provider network is dependent upon both the service set being offered and the equipment available to provide these services. For example a network must support SIP in order to provide access to SIP phones.

3.3 Security

The PSTN has been very resistant to security attacks and has not suffered from significant problems since the introduction of SS7 out-of-band signaling. A VoIP Next-Generation network is much more susceptible to security attacks and must address three key security issues [5].

· Denial of service

· Theft of service

· Invasion of privacy

3.4 Denial of Service

A denial of service attack prevents legitimate users of a network from accessing the features and services offered by that network. Denial of service attacks is extremely difficult in the PSTN but all too common in IP networks. There have been several successful attacks on web servers on the Internet, even including the high security government sites.

In a complex network, there are many possible denials of service attacks. Some examples include sending false signaling messages so that a call agent is fooled into believing that a party has gone on-hook, bombarding a device with pings or other packets so frequently that it has no spare processing power to process legitimate requests and hacking a Subscriber Gateway to send ftp or other data traffic as high priority voice traffic [14].

3.5 Theft of Service

Theft of service attacks are aimed at the service provider, where the attacker simply wants to use a service without paying for it. The most common form in the current PSTN is called subscriber fraud, where a subscriber sets up an account with a service provider using false billing information, for example a stolen credit card. Other forms of theft are more technical, often utilizing black boxes or similar to fool the network into providing free service. It is interesting to note that fraudulent long-distance calls were more common when the network used in-band DTMF signaling which could be mimicked using a blue box.

Even in a VoIP access network using for example DSL, bandwidth is still a limited resource – especially the low packet loss and jitter required for good voice quality. Therefore, the network needs to be protected from subscribers misusing this high-priority bandwidth, one example would be if two SIP User Agents could set up a direct call between them, accessing the high priority bandwidth but bypassing the SIP Server(s) and hence not get billed.

3.6 Invasion of Privacy

Subscribers to the PSTN expect that their calls are private, and that no third party can eavesdrop (with the exception of lawful interception). The PSTN achieves this privacy mainly by physical security mechanisms i.e. the wire from a subscriber's home is only connected to the local exchange or digital loop carrier and cannot easily be accessed [5].

This is not necessarily the case with VoIP networks; in particular cable and wireless networks use a shared media which allow eavesdropping unless encryption is used. However it is important to note that there is no "one size fits all" approach to security for VoIP.

3.7 Quality of Service

One of the key requirements for the widespread deployment of VoIP is the ability to offer a toll quality service equivalent to the existing PSTN. Indeed some carriers are even looking for Next-Generation Networks as a means for delivering much higher voice quality as a service [8].

Perceived Voice quality is very sensitive to three key performance criteria in a packet network, in particular:

- Delay
- Jitter
- Packet loss

IP, by its nature, provides a best-effort service and does not provide guarantees about the key criteria. Therefore it is necessary to implement a suitable QoS solution in the majority of cases where simple over provisioning cannot guarantee success. There are a large number of technologies that can be chosen to provide QoS support such as Diffserv, RSVP, MPLS and even ATM. However the objective of such a solution is always to guarantee prioritization of voice media streams over best-effort data, and to ensure that the voice service is not compromised by unforeseen traffic patterns.

3.8 Reliability / Availability

The PSTN achieves five-nine reliability, equivalent to fewer than five minutes per year downtime, and it handles millions of simultaneous calls. A VoIP network needs to achieve similar levels of reliability and scalability.

The required reliability and scalability can be achieved in a VoIP network by using redundant and load sharing equipment and networks. The call agent, access gateway, trunk gateway, signaling gateway and media server need to be fault tolerant. The types of functionality often used to achieve fault tolerance include:

· Redundant hardware
· Redundant network connections
· Hot-swap capability
· No single point of failure
· Software and firmware that can be upgraded without loss of service.

3.9 Lawful Interception

Historically, lawful interception (wiretapping) of telephone conversations has been a relatively well-defined and straightforward process. Typically, a law enforcement agency applied to a court for an order to tap a particular phone number. Once the agency had the order, it served that order on the provider of the telephone service for the number to be tapped. The service provider then put a tap on the circuit, extracted all the necessary information and passed it to the law enforcement agency. The introduction of VoIP complicates this process considerably [8].

The law varies according to location (in the United States, the relevant legislation is the Communications Assistance for Law Enforcement Act - CALEA). The following requirements are typical for any network including VoIP networks and the PSTN.

- No wiretap is permitted without a court order.
- Wiretaps apply to phone numbers, not particular suspects.
- Wiretaps fall into two categories.

- Call detail – a tap in which the details of the calls made and received by a subscriber are passed to the law enforcement agency. (Referred to as pen register and trap and trace in the U.S.).

- Call content – a tap in which the actual contents of a call are passed to the law enforcement agency.

- The suspect must not detect the tap, so the tap must occur within the network and not at the subscriber gateway. Also, the tap may not be detectable by any change in timing, feature availability or operation.
- A suspect may be tapped by more than one agency. The taps are separate, and the various agencies are not aware of each other's taps. The taps do not have to be of the same category.
- It is the responsibility of the telecommunications carrier that originates or terminates calls to provide lawful interception.

3.10 Emergency and Operator Services

The PSTN supports extensive Emergency and Operator Services. Subscribers can dial 911 or the local equivalent and reach Emergency Services under almost any conditions. A Next-Generation VoIP Network needs to provide similar support leading to the following requirements:

- Support for legacy Emergency and Operator Services Interfaces, for example MF and SS7.
- Support for lifeline support where this is a regulatory requirement.
- Provision of location information so that a caller's physical location can be determined.

3.11 Call Routing and Number Plans

The PSTN is able to route calls between telephones anywhere in the world, for example a user can call Australia from Canada. This is achieved by having a well-defined number plan both nationally and internationally. Routing tables can be built using this numbering plan to provide end-to-end connectivity.

A Next-Generation VoIP Network must provide the same capability, which requires the following:

- International and National numbering /addressing plans, for example ENUM implementations
- Interconnection to the PSTN and E.164 numbers
- SIP endpoint addressing schemes
- Allocation of numbers/addresses and number portability issues
- Call routing between numbers/addresses

3.12 Firewall and NAT traversal

For equipment that is resident at customer premises, such as IP phones and Subscriber Gateways it is likely that there will be a firewall at the edge of the customer premises. In addition, Network Address Translation (NAT) may be used to convert internal IP addresses to external IP addresses.
Therefore it is important that both the RTP media traffic and the signaling flows (SIP, H.248, MGCP) can negotiate both NAT and the firewall. For the firewall to be effective it needs to ensure that only authorized flows enter or leave the networks.

3.13 Billing and Reconciliation

The PSTN has extensive and accurate mechanisms for billing both subscribers and reconciliation between service providers. Currently most billing mechanisms are based on usage, e.g. per minute billing, although some services are charged on a flat-rate basis, e.g. local calls in the US [14].

Service Providers generate Call Detail Records (CDRs) for traffic entering or leaving their networks and generate bills based on these.

3.14 Network Interconnection

The PSTN is not a single network but a collection of networks operated by thousands of service providers. At each network boundary a network interconnection is required.

Network interconnection agreements are put in place to cover items such as interconnection points, signaling, timing, billing and tariffs, bearer transport, regulatory requirements, etc. In addition these normally require approval from the relevant regulator.

3.15 Migration Path

While the eventual goal is an end-to-end Next-Generation Network, it will be decades before legacy networks disappear. On the access side, this means that ongoing support for POTS telephone lines and DLCs may be a requirement; in the backbone network, interconnection with SS7 signaling and TDM trunks, 911 and operator services, databases for 1-800 and local number portability and CALEA, are all essential. In addition migration will happen piecemeal in different carrier networks and individual service providers may support both next-generation and legacy networks in parallel.

3.16 OSS Support

The existing PSTN has very extensive Operations Support Systems providing such functions as

- Flow-through provisioning
- Fault isolation
- Loop testing
- Performance monitoring
- Policy definition and enforcement

A Next-Generation VoIP network will need to offer similar levels of OSS support. In addition given the huge investment in existing OSS systems any new equipment will need to be integrated with these which may require support for protocols such as CORBA, SNMP, TL1, etc. VoIP networks also introduce new requirements such as the ability to dynamically measure end-to-end voice quality.

3.17 Bandwidth Utilization

In a VoIP network digitized voice is transported using real-time protocol (RTP). A typical voice sample is less than 100 bytes, but the combined headers are at least 40 bytes. For lower-bandwidth WAN links such as DSL or Cable, the header overhead is significant and reduces the number of voice channels or data bandwidth available. Given that one of the advantages of using VoIP is that it should be possible to use lower bit codecs to save bandwidth, a mechanism for reducing the overhead is required [32].

The main approach to reducing the overhead is to implement compression for RTP, UDP and IP headers. However this requires a point-to-point link and the endpoints to maintain state for each compressed RTP flow.

3.18 Fax, Modem and TTY support

The PSTN reliably supports fax, modem and TTY calls. Calls connect on almost every attempt and rarely fail. A VoIP network must provide a similarly reliable service. However, fax, modem and TTY traffic imposes some additional constraints beyond voice traffic.

Compared to voice traffic, fax, modem and TTY traffic is much more sensitive to packet loss but less sensitive to overall delay. In addition, lower-bit-rate codecs are optimized for voice traffic and cannot transport non-voice traffic [30].

3.19 Auto-configuration

One significant difference between a POTS (plain old telephone service) network and a Next-Generation VoIP network is that for some architectures intelligent subscriber gateways or IP phones now reside on the customer premises. These complex devices need more configuration than a POTS phone, so auto-configuration of subscriber gateways becomes important as the network scales up.

Some of these requirements can be addressed using DHCP, but others require some form of management interface using UPnP, SNMP or LDAP.

Considerable work has been done in the DSL Forum to address auto-configuration of DSL equipment, but to date the issue of auto-configuration in VoIP networks has not been addressed.

CHAPTER 04: PERFORMANCE MEASUREMENT OF VOIP USING QOS PARAMETERS

4.1 Quality of service

Communication on the IP network is inherently less reliable in contrast to the circuit-switched public telephone network, as it does not provide a network-based mechanism to ensure that data packets are not lost, or delivered in sequential order. It is a best-effort network without fundamental Quality of Service (QoS) guarantees. Therefore, VoIP implementations may face problems mitigating latency and jitter.

By default, IP routers handle traffic on a first-come, first-served basis. Routers on high volume traffic links may introduce latency that exceeds permissible thresholds for VoIP. Fixed delays cannot be controlled, as they are caused by the physical distance the packets travel; however, latency can be minimized by marking voice packets as being delay-sensitive with methods such as DiffServ[14].

A VoIP packet usually has to wait for the current packet to finish transmission, although it is possible to preempt (abort) a less important packet in mid-transmission, although this is not commonly done, especially on high-speed links where transmission times are short even for maximum-sized packets. An alternative to preemption on slower links, such as dialup and DSL, is to reduce the maximum transmission time by reducing the maximum transmission unit. But every packet must contain protocol headers, so this increases relative header overhead on every link along the user's Internet paths, not just the bottleneck (usually Internet access) link.

Voice, and all other data, travels in packets over IP networks with fixed maximum capacity. This system is more prone to congestion and DoS attacks than traditional circuit switched systems; a circuit switched system of insufficient capacity will refuse new connections while carrying the remainder without impairment, while the quality of real-time data such as telephone conversations on packet-switched networks degrades dramatically.

Fixed delays cannot be controlled as they are caused by the physical distance the packets travel. They are especially problematic when satellite circuits are involved because of the long distance to a geostationary satellite and back; delays of 400-600 ms are typical.

When the load on a link grows so quickly that its queue overflows, congestion results and data packets are lost. This signals a transport protocol like TCP to reduce its transmission rate to alleviate the congestion. But VoIP usually does not use TCP because recovering from congestion through retransmission usually entails too much latency. So QoS mechanisms can avoid the undesirable loss of VoIP packets by immediately transmitting them ahead of any queued bulk traffic on the same link, even when that bulk traffic queue is overflowing.

The receiver must resequence IP packets that arrive out of order and recover gracefully when packets arrive too late or not at all. Jitter results from the rapid and random (i.e., unpredictable) changes in queue lengths along a given Internet path due to competition from other users for the same transmission links. VoIP receivers counter jitter by storing incoming packets briefly in a "de-jitter" or "playout" buffer, deliberately increasing latency to increase the chance that each packet will be on hand when it's time for the voice engine to play it. The added delay is thus a compromise between excessive latency and excessive dropout, i.e., momentary audio interruptions. This suggests continually estimating the mean delay and its standard deviation and setting the playout delay so that only packets delayed more than several standard deviations above the mean will arrive too late to be useful. In practice, however, the variance in latency of many Internet paths is dominated by a small number (often one) of relatively slow and congested "bottleneck" links. Most Internet backbone links are now so fast (e.g. 10 Gb/s) that their delays are dominated by the transmission medium (e.g. optical fiber) and the routers driving them do not have enough buffering for queuing delays to be significant.

It has been suggested to rely on the packetized nature of media in VoIP communications and transmit the stream of packets from the source phone to the destination phone simultaneously across different routes (multi-path routing).[14] In

such a way, temporary failures have less impact on the communication quality. In capillary routing it has been suggested to use at the packet level Fountain codes or particularly raptor codes for transmitting extra redundant packets making the communication more reliable.

A number of protocols have been defined to support the reporting of QoS/QoE for VoIP calls. These include RTCP Extended Report (RFC 3611), SIP RTCP Summary Reports, H.460.9 Annex B (for H.323), H.248.30 and MGCP extensions. The RFC 3611 VoIP Metrics block is generated by an IP phone or gateway during a live call and contains information on packet loss rate, packet discard rate (because of jitter), packet loss/discard burst metrics (burst length/density, gap length/density), network delay, end system delay, signal / noise / echo level, Mean Opinion Scores (MOS) and R factors and configuration information related to the jitter buffer[2].

4.2 QoS Parameters

In ensuring the QoS for VoIP, researchers have come out with some QoS parameters as to be observed. In general, the focus of this paper is directed to the Network QoS, based on the QoS Framework as suggested by [8]. This simply means that the analysis that has been taken out is to evaluate the network environment in which VoIP communication is being conducted. There are several QoS parameters that have been identified to be implemented in this study. Table 1 provides a list of Network QoS parameters available as derived from [27].

Table 4.1: Network QoS Parameters

Category	*Parameters*
Timeliness	Delay Response time Jitter
Bandwidth	Systems-level data rate Application-level data rate Transaction time
Reliability	Mean time to failure (MTTF) Mean time to repair (MTTR) Mean time between failures (MTBF) Percentage of time available Packet loss rate Bit error rate

In our analysis, three QoS parameters have been selected, namely delay, jitter, and packet loss rate. The main justification for this selection is such that the study focuses on the performance of VoIP communication over different networking conditions and environment, and hence the time and reliability would be the major concerns for evaluation. The results of studies conducted by also shown that high delay and high delay variability (jitter) has been experienced by a large number of Internet paths that resulting in poor VoIP performance. It should be noted that these QoS parameters have also been adopted in a number of previous studies [8], [14], and [27].

4.3 VoIP Quality Metrics

In a well planned network, the Quality of Service (QoS) features in the network equipment intelli-gently distinguish and route traffic based on its priority. By helping to guarantee that voice traffic gets the bandwidth it needs, the network controls the factors that compromise voice quality. These factors are:

4.3.1 Latency

As a delay-sensitive application, voice cannot tolerate too much delay. Latency is the average time it takes for a packet to travel from its source to its destination. The maximum amount of latency that a voice call can tolerate one way is 150 milliseconds (100 milliseconds is preferred) 1. If there is too much traffic on the line, or if a voice packet gets stuck behind a bunch of data packets (such as an email attachment), the voice packet will be delayed to the point that the quality of the call is compromised [27].

4.3.2 Jitter

In order for voice to be intelligible, consecutive voice packets must arrive at regular intervals. Jitter describes the degree of variability in packet arrivals, which can be caused by bursts of data traffic or just too much traffic on the line. Jitter is the delay variance from point-to-point. Voice packets can tolerate only about 75 milliseconds (40 milliseconds is preferred) of jitter delay [14].

4.3.3 Packet loss

Packet loss due to congestion is the losing of packets along the data path, which severely degrades the voice quality. Packet loss occurs frequently in data networks, but many applications are designed to provide reliable delivery using network protocols that request a retransmission of lost packets (e.g. TCP [7]). Dropped voice packets, on the other hand, are discarded, not retransmitted. Voice traffic can tolerate less than a 3 percent loss of packets before callers feel perceivable gaps in conversation. When these factors are properly controlled by QoS mechanisms, VoIP delivers better quality voice than they are accustomed to from dedicated voice networks, even over the lower speed connections. At the same time, data applications are also prioritized and assured of their share of network resources.

4.4 Monitoring VoIP Vital Parameters

VoIP technology uses shared Internet bandwidth unlike other traditional communication technologies. Also, being a real-time application using the same bandwidth, VoIP quality is drastically affected by network parameters such as packet loss, delay and jitter as compared to other applications such as e-mail and Instant Messaging. This makes it important to have a monitoring system in place so as to keep one aware of the health of all vital VoIP quality parameters on a 24/7 basis[28].
For monitoring or analyzing VoIP QoS parameters and the sequenced schemes of a VoIP network here we use software called VQManager 6.3.To generate Bulk calls or virtual calls for the monitoring Test Call Generator System (TCS) is established. This is a demo version of the software, the snapshots are given below are captured from live machine.Here we use the machine as a Local host. The reason we use the machine as a local host is the bandwidth we get for simulation and observation are not acceptable for the software to use as a server. Now first of all the installation processes of the software is given below:

When cmd initialize the software installation the software opens as console mode and it also opens its login section in an internet Explorer.

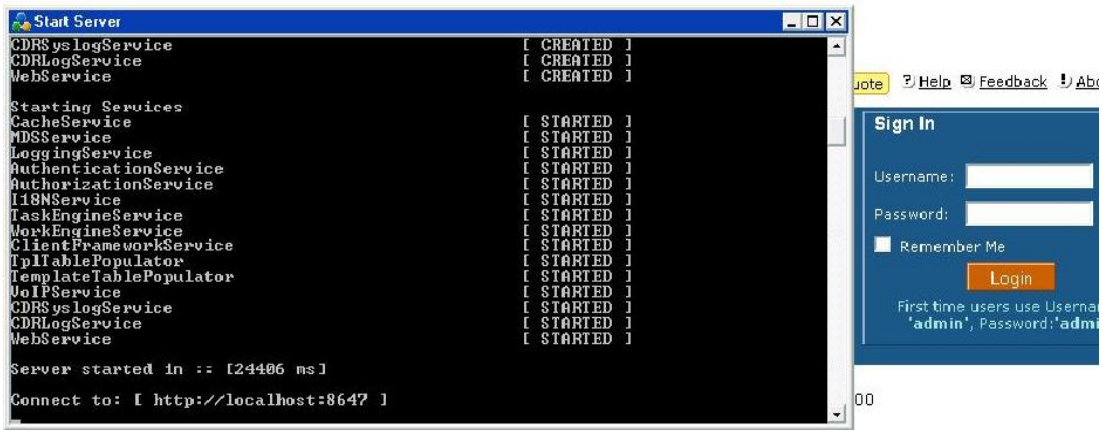


Figure 4.1: VQManager in a Console Mode and Login Screen

Login screens appear and we have to give the user name and Password for your VoIP account. For the first time user we have to give User Name and Password as Admin. Now we can log into our VoIP account and established its settings.

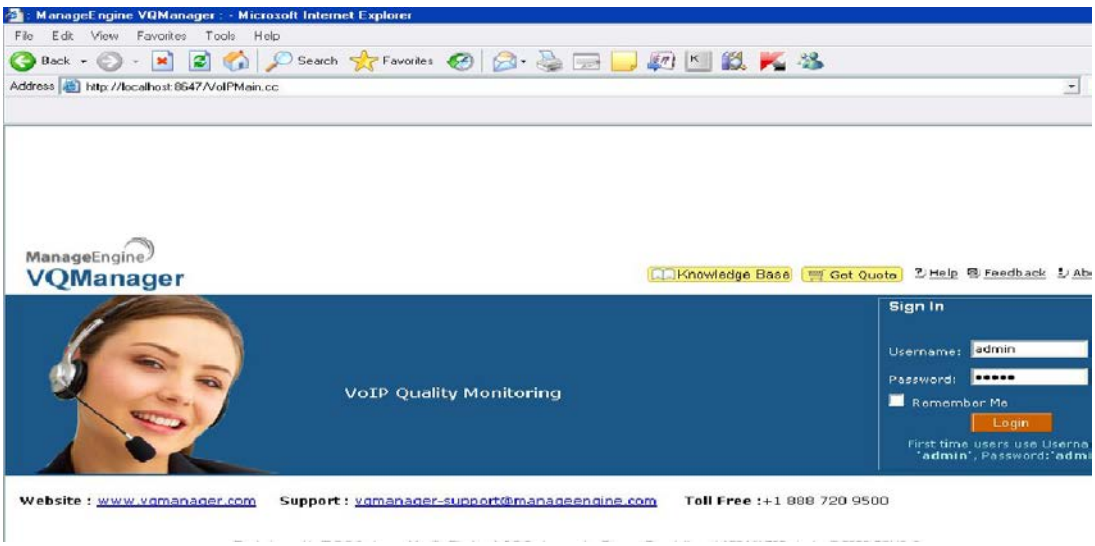


Figure 4.2: VQManager Login Screen.

Now the sniffer or packet analyzer Configuration Wizard is opened. Here we configure the protocol information for this Local host machine. The software supports the SIP (The Session Initiation Protocol), SCCP (The Skinny Call Control Protocol) and The H.323 Protocols for VoIP Transmission. All the ports are by default settings.

Figure 4.3: Settings for Sniffer configuration wizard.

After the sniffer configuration process is completed the protocols detection process is in progress. Here we select Interface Name and IP Address of the local host machine. In this case we use three IP address. They are:

192.168.14.103

192.168.16.157

And 172.16.3.20

The two interfaces we used are:

Device_1(C5C6C252-1C06-41D4-ACF9-952FC12847D4) for this IP:192.168.16.157

Device_2(56BBAF1B-9650-49D0-B968-AF7D942109F6) for this IP: 192.168.14.103

And 172.16.3.20

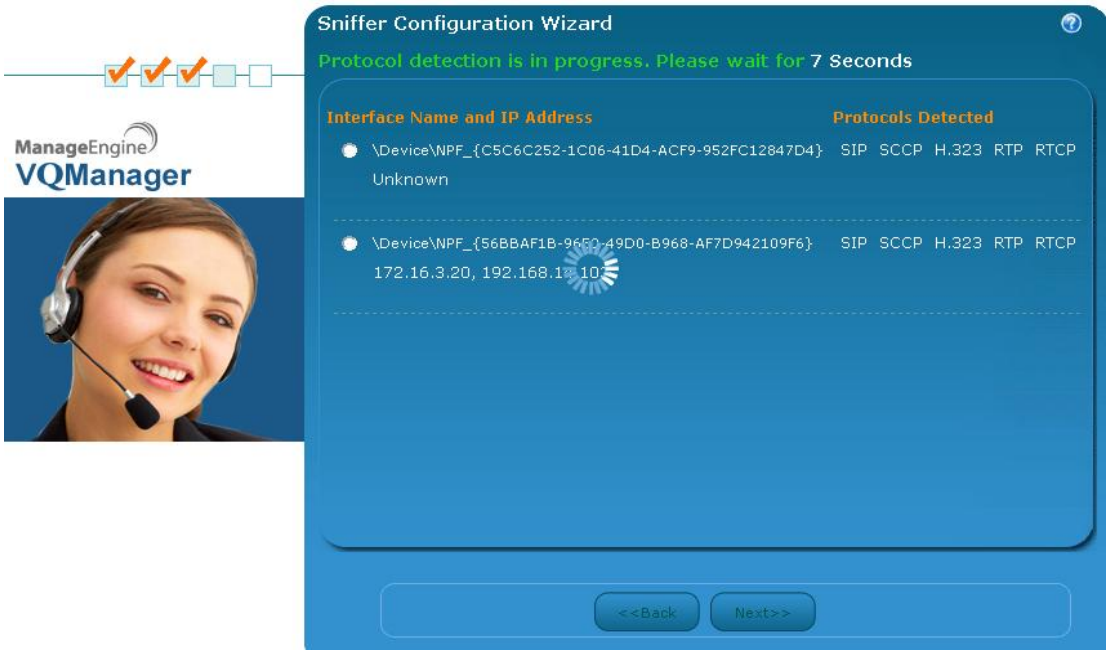


Figure 4.4: Sniffer Configuration section for Interface and IP address selection.

Now the Sniffer Summary unit appears and shows the selected Interface and IP Address.

Advanced Monitoring Options are also displayed in this portion of the settings. Here we can see that the selected ports of the protocols and the options supported by the software.

Figure 4.5: Sniffer settings advanced monitoring Options.

Now the software settings are completed it opens a monitoring page which deliver us the every portion of a VoIP systems and its information. Monitoring page is given below:

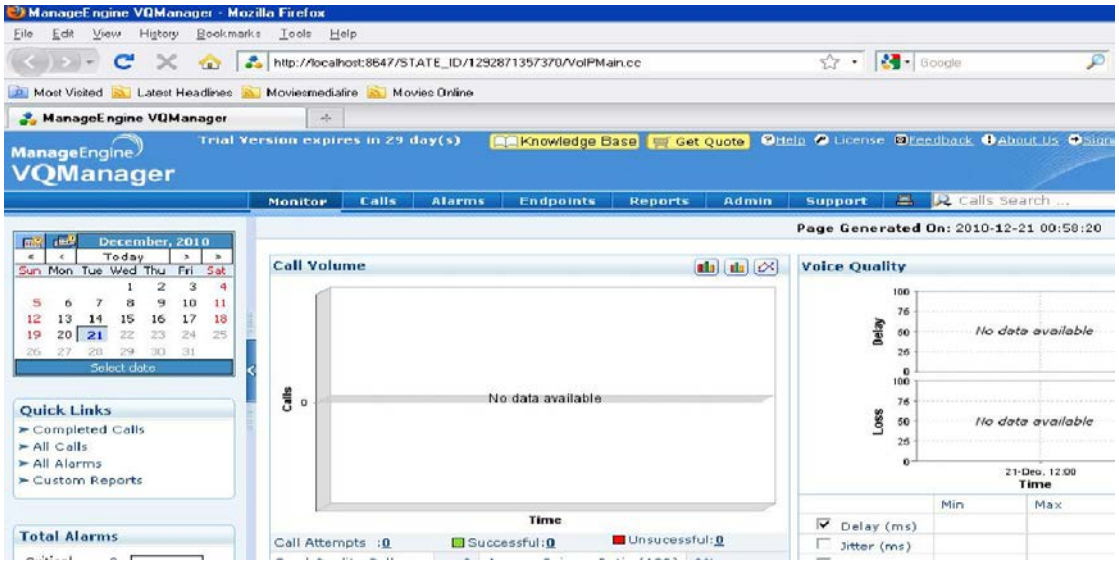


Figure 4.6: Basic Look of the VoIP monitoring cell which contains Call Volume Graph and Voice Quality Graph.

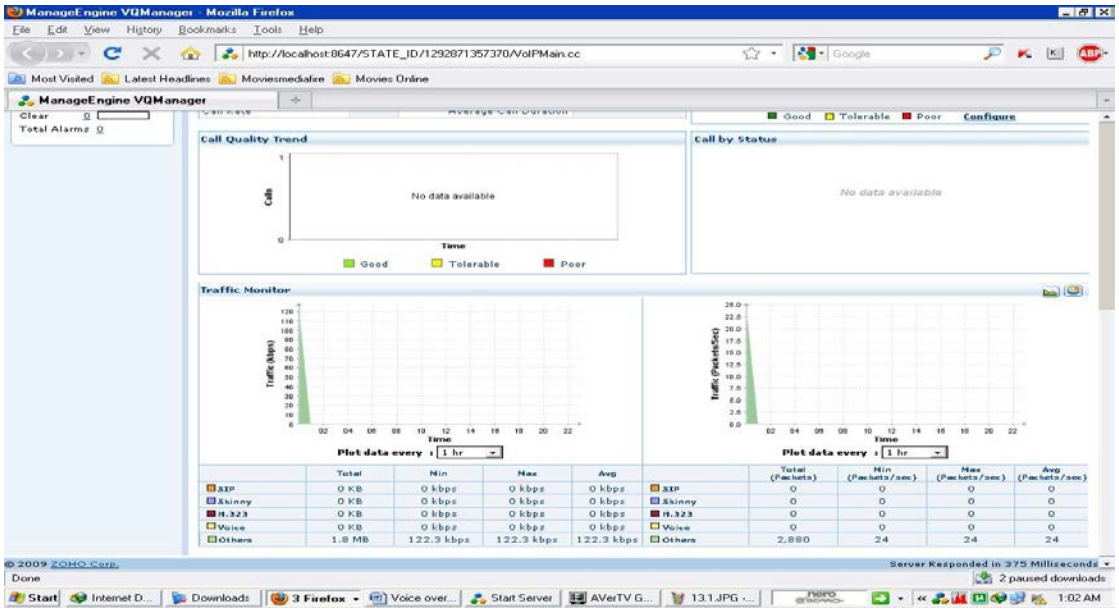


Figure 4.7: Basic Look of the VoIP monitoring cell which contains Call Quality Trend, Call by status and Traffic monitor Graph.

The "Monitoring" has the following:

- The Call Volume graph showing the volume of calls that were successful or unsuccessful, of good, tolerable or poor quality, the peak and low usage periods, the Average Call duration and overall ASR(Answer Seizure Ratio) etc..
- The Voice Quality graph that shows snapshot of the QoS metrics with their Min, Max and Avg values and whether good, tolerable or poor as defined by the user.
- The Call Quality Trend graph shows the quality parameter - Good, Tolerable and Poor quality calls on an hourly basis
- The Call by Status is a pie chart showing the percentage and number of Successful, Unanswered, Error and Un-monitored calls.
- The Traffic Monitor graph showing a split-up of bandwidth for each VoIP traffic component. Available only for Sniffer configuration.

4.4.1 Call Volume Graph

- Displays the statistics of all the calls that were initiated in the chosen time frame as set in the calendar.
- The bar graph has the green areas representing the successful calls while the red areas denote unsuccessful calls.
- Provides the number of call attempts, successful and unsuccessful as a linked number. When these linked numbers are clicked you can view the information of the respective calls.
- The successful calls are divided into calls based on quality - Good, Tolerable and Poor quality calls. Calls with MOS (Mean Opinion Score) greater than 3.6 are classified as Good Quality Calls. Calls with MOS less than 3.1 are marked as Poor Quality Calls. Calls with MOS between 3.1 and 3.6 are marked as Tolerable Quality calls.
- Answer Seizure Ratio(ASR) - ratio of successfully connected calls to attempted calls is displayed

- Lists the time period at which there were a maximum number of calls - its peak usage ; Similarly, time period at which the call volume was minimum - low usage
- Provides the average call duration time across all the calls during the selected time period

The Call Volume graph represents a summary of the calls that have happened over the time period as chosen in the calendar. You can split this time-period into intervals according to your requirement.

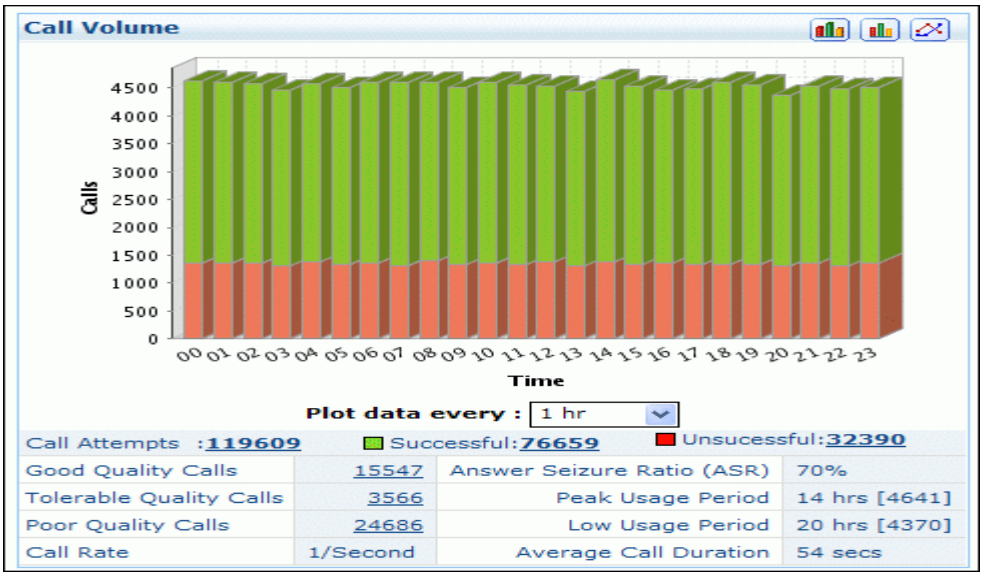


Figure 4.8: Call Volume Graph demo version of a system.

4.4.2 Voice Quality Graph

- Provides trends of vital quality parameters Delay, Jitter, Packet Loss, MOS and R- Factor over the defined time period as set in the calendar.
- A table of information shows the "Min", "Max" and "Avg" values for each quality parameter and also which of these values were "Good", "Tolerable" or "Poor" as defined by the user.
- Trend graphs are displayed for each parameter. Up to three graphs can be displayed at the same time by selecting the respective check-box next to each parameter. On reaching the maximum of three graphs displayed, you need to

de-select parameters to have the required additional parameters trend graph displayed.

- Each individual QoS value plot on the graph can be clicked to provide details of the calls that have contributed to the respective QoS value.

.

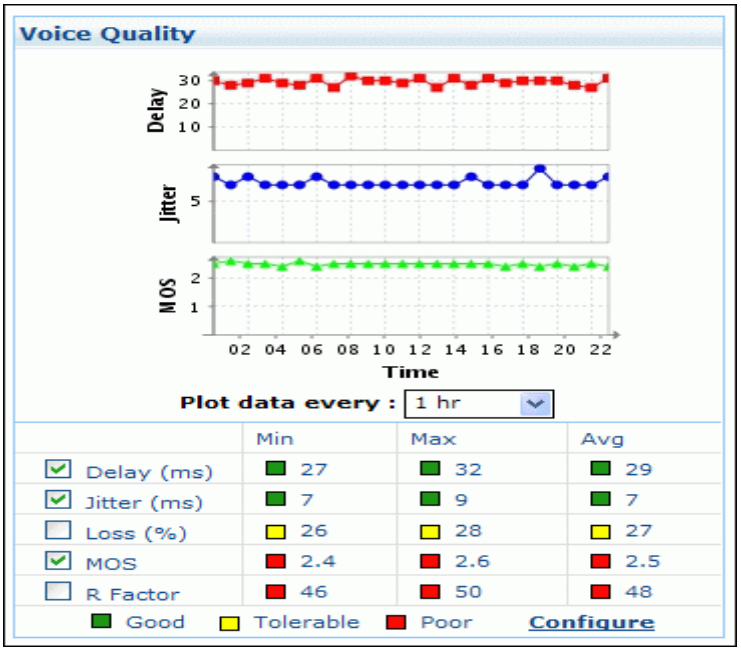


Figure 4.9: Voice Quality Graph

4.4.3 Configure QoS

The QoS metrics can be customized according to the VoIP quality requirements. The system administrators can define the threshold value for the Delay, Jitter, Packet Loss, MOS and R factor value. The minimum and maximum value of tolerable value helps in determining the good and poor quality score. QoS metrics below the minimum threshold level would be classified as "Good" while the metrics exceeding the maximum threshold value will be termed "Poor".

To configure QoS metrics tolerable range

- Go to "Monitor" Tab
- Click on the "Configure" link, below the "Voice Quality" graph
- A screen to "Configure QoS Min/Max thresholds" pops up

- Fill in the tolerable range of various metrics like Delay, Jitter, Packet Loss, MOS
- Click on "Update" button to confirm the values

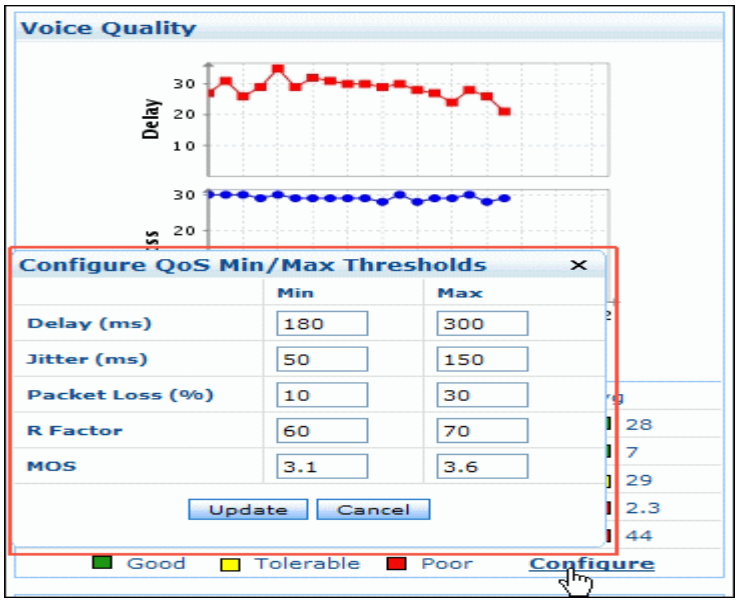


Figure 4.10: Voice Quality Graph and QoS configure

1. QoS metrics below the minimum threshold level would be classified as "Good" while the metrics exceeding the maximum threshold value will be termed "Poor". However for MOS metrics vice versa of this rule will apply.
2. After re-configuring the QoS thresholds in Configure link, the changes will take effect in the latest data to be collected. The history data will not get altered inline with new thresholds. This may lead to data mismatch on the day of re-configuring.

4.4.4 Call Quality Trend

- Call Quality Trend shows the quality parameter - Good, Tolerable and Poor quality calls on an hourly basis.
- Each individual Quality Trend plot on the graph can be clicked to provide details of the total number of calls for the selected time period.

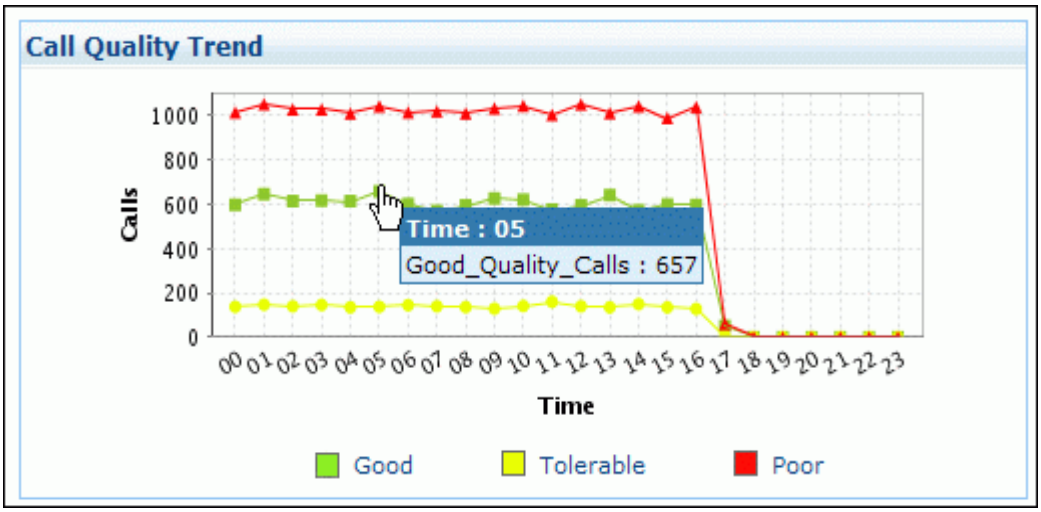


Figure 4.11: Call Quality Trend

4.4.5 Call By Status

- Helps to identify the percentage and number of Successful, Unanswered, Error and Unmonitored calls on a day to day basis as set in the calendar.
- These parameters are represented in a pie chart with respective color codes.
- The successful calls are shown in green and includes Good and Poor quality calls.
- The Unsuccessful calls are divided into unanswered calls and Error calls. Calls that were not answered by the user (user busy, user not available etc.,) fall into the Unanswered Call category. Other calls that failed due to errors in server or client are marked as Error Calls
- Unmonitored calls are those that VQManager has abruptly stopped monitoring - this could be due to an abrupt stop and restart of the VQManager server, or because there were no voice packets that were received for a continuous duration (30 seconds) of time.
- Hover over the pie chart to view the total number of successful, unanswered, error and unmonitored calls for a day.
- When the linked percentage for the parameter is clicked you can view the information summary of the respective calls.

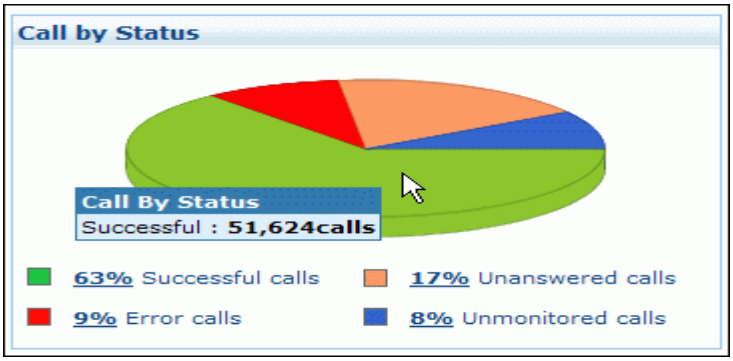
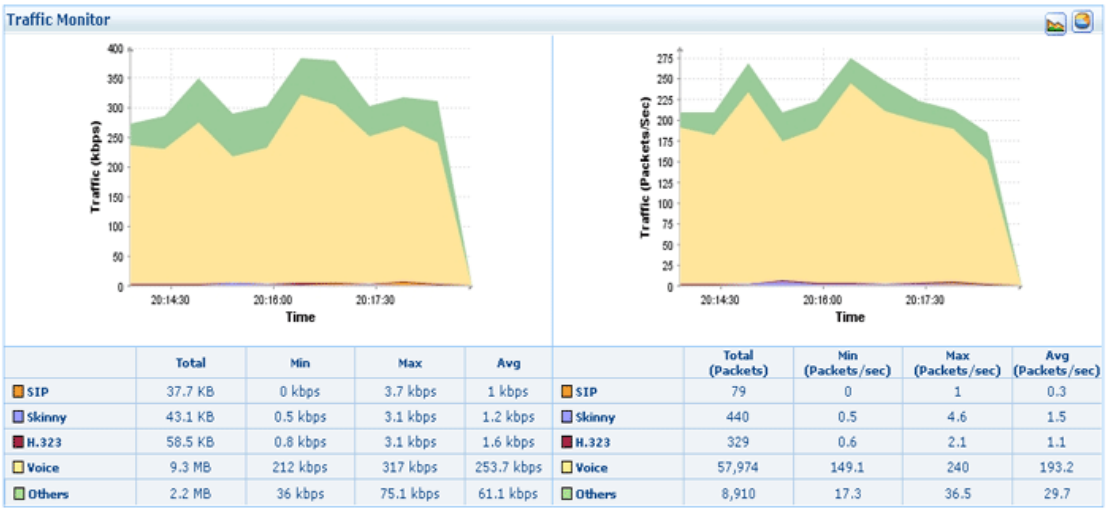


Figure 4.12: Call By Status

4.4.6 Traffic Monitor Graph

- Helps in finding out the traffic details (Bandwidth utilization) of the network managed by VQManager in a specific time interval as set in the calendar.
- The traffic information is plotted in two sets of graphs. One set depicts the total size (in kbps) of the packets transmitted and the other set provides the total number of packets transmitted per second (packets/sec).
- The bandwidth utilized by various components such as SIP, Skinny, H.323, Voice and others are depicted each by individual graphs.
- A table of information shows the “Min", "Max" and "Avg" values for each traffic component.



	Total	Min	Max	Avg
SIP	37.7 KB	0 kbps	3.7 kbps	1 kbps
Skinny	43.1 KB	0.5 kbps	3.1 kbps	1.2 kbps
H.323	58.5 KB	0.8 kbps	3.1 kbps	1.6 kbps
Voice	9.3 MB	212 kbps	317 kbps	253.7 kbps
Others	2.2 MB	36 kbps	75.1 kbps	61.1 kbps

	Total (Packets)	Min (Packets/sec)	Max (Packets/sec)	Avg (Packets/sec)
SIP	79	0	1	0.3
Skinny	440	0.5	4.6	1.5
H.323	329	0.6	2.1	1.1
Voice	57,974	149.1	240	193.2
Others	8,910	17.3	36.5	29.7

Figure 4.13: Traffic Monitor Graph

4.4.7 Active Calls Summary

- In Sniffer interface, this is the first UI that opens in the calls tab showing the details of the active calls happening in the network.
- The QoS of the active calls are depicted in the form of intuitive charts. The average values of all the QoS parameters such as Delay, Jitter and Packet Loss are plotted in the chart.
- A Bandwidth utilized graph is also provided that shows the most recent bandwidth utilization in the network. The bandwidth usage is split into SIP, Skinny, H.323, Voice and Others. On rolling the mouse pointer over the different areas in the pie chart, respective volume of packets for the bandwidth components is shown in kbps.
- By default, this page gets reloaded every 2 minutes to show the latest Active calls that are happening in the network. The user can configure this refresh rate. This option is found in the top left hand side of the UI just below the line of tabs. Next to the "Refresh every" field click on the edit icon next to the linked text entry. Select the required refreshing time interval (refresh rate) from the drop-down list that appears.
- Below the QoS charts is a list of all the current active calls in the network. Information such as the Initiator of the call, call initiation time, Duration, Status Code, and MOS of the call are displayed by default in the table.
- One can mark any stale/frozen calls in this list as unmonitored calls that wrongly appear as active in this list. This option is found above the list through the button "Mark as Unmonitored".
- You can view other details such as participant/initiator's ip, participant/initiator's url, call initialization time, duration, Call Status, Status Code, MOS. To view the additional columns, click the column chooser icon present at the top right of the 'Active Calls' table. Click "Save" after selecting the required columns.
- This list can be arranged by ascending or descending order of the Call Initialization Time and other column fields. Clicking on the column heading, that you want the list to be sorted according to, does this.

- The Active Calls list can be exported as a PDF or CSV file or emailed as a PDF attachment to a number of E-mail Ids. This can be done through the respective icons - CSV icon, PDF icon and mail icon, found on the right-hand side just above the Active Calls list.
- The list can be searched for a particular call by providing Initiator / Participant / Call Status / Status Code. Click on the lens icon found on the extreme right hand side of the lists header. Text-boxes will appear in which you can provide the Initiator / Participant / Call Status / Status Code to search for the endpoint. After providing the search criteria, click on the Go button found below the lens icon to search for the call according to the provided search term/terms.

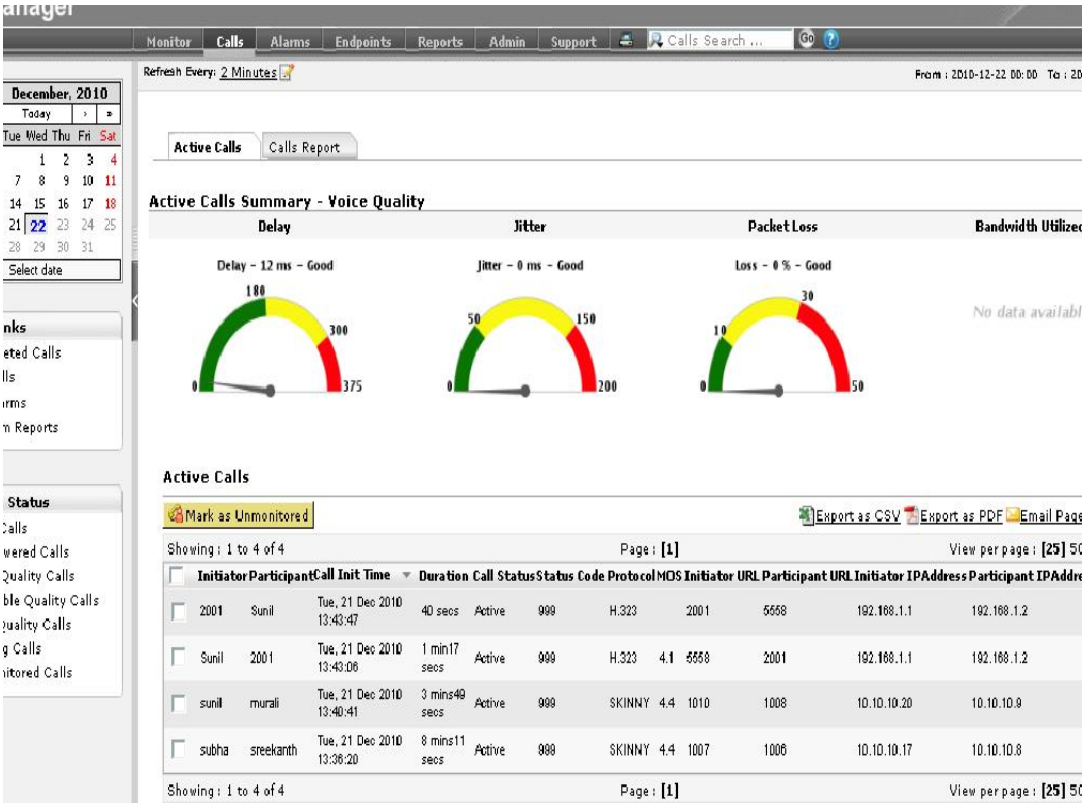


Figure 4.14: Active Calls Summary live simulated demo

4.4.8 Calls Report

- The Calls Reports tab opens to view Average Call Duration (ACD) graph and a pie chart on the quality split and Unsuccessful Calls Split.

- The Average Call Duration (ACD) Trend shows the duration of successful calls (in seconds) for every hour. Each individual plot on the graph can be clicked to provide details of the total number of calls for the selected time period.
- The Quality Split identifies the percentage and number of Good, Tolerable and Poor call quality. The min and max threshold MOS value configured under Voice Quality indicates the Good, Tolerable and Poor Quality calls.
- The Unsuccessful Call Split lists the top 10 classification for an unsuccessful call. The pie chart indicates the classification of all unsuccessful calls along with the reason for all failures and number of calls.
- All Calls displays the call summary of all the calls.

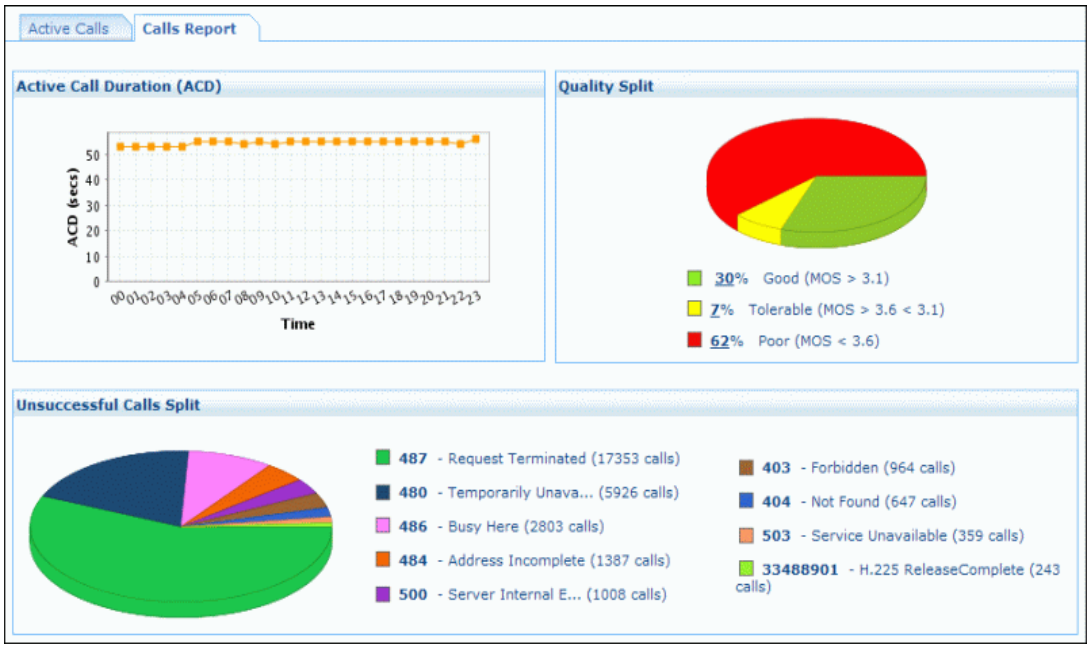


Figure 4.15: Calls Report

4.4.9 Call Details

- On clicking any Initiator of a call in any of the Call lists, you are brought to details of that particular call. This UI shows a graphical display of the call QoS trends, participating endpoint details, CODEC details and a pictorial representation of the packets exchanged during the call.

- The Call Trend graph is similar to the Voice Quality graph in the Monitor tabs Summary Report View. All the QoS parameters such as Delay, Jitter, Packet Loss, and MOS are plotted in the graph. This shows the trends for the various QoS parameters for the duration of the call.
- To the right of the Call Trend graph, the details of the call and the participants of the call are displayed. Call details such as Start Time, Duration, Call Identifier and Call Status are shown. The Call Identifier is provided for SIP-based and H.323-based calls and is a unique identifier for each call. The linked character set shown for the Call Identifier is displayed as a truncated item. To view the full Call Identifier, click on the displayed Call Identifier to open up a dialogue box having the Call Identifier in full. Endpoint details such as Phone ID, Name, Skinny/SIP/H.323 URL, IP Address, Media Port, Octets and Packets are shown.
- On clicking the linked item View Trend found below the Name of the participants, you can see the individual QoS trend graphs for each participant during the call.
- Codec Details give information about the Codec used in the call along with its characteristics such as Bits per sample, Frame Size, RTP Clock Rate, Payload Type, Sampling Rate, Packet Size and No. of Channels.
- The Call Flow ladder diagram provides a pictorial representation of the packets exchanged during the call initiation, progress and end. It plots all the SIP, Skinny and H.323 requests that took place from call start to call end. This is useful for debugging error calls that failed due to some unknown reasons
- Call Trace provides summarized information for each of the SIP/ Skinny/ H.323 and RTCP packets that were exchanged during the call process. Details of Capture Time, Protocol, Status, Code, Source Port, Destination and Destination Port are provided for each packet.
- You can see the raw SIP, Skinny and H.323 packet details along with their Call Trace information by clicking on each packet in the Call Flow diagram. This information is displayed below the Call Flow diagram. "Tunnelled" H.323 packets are represented in the call-flow diagram as a three-dimensional box.

Figure 4.16: Call Details

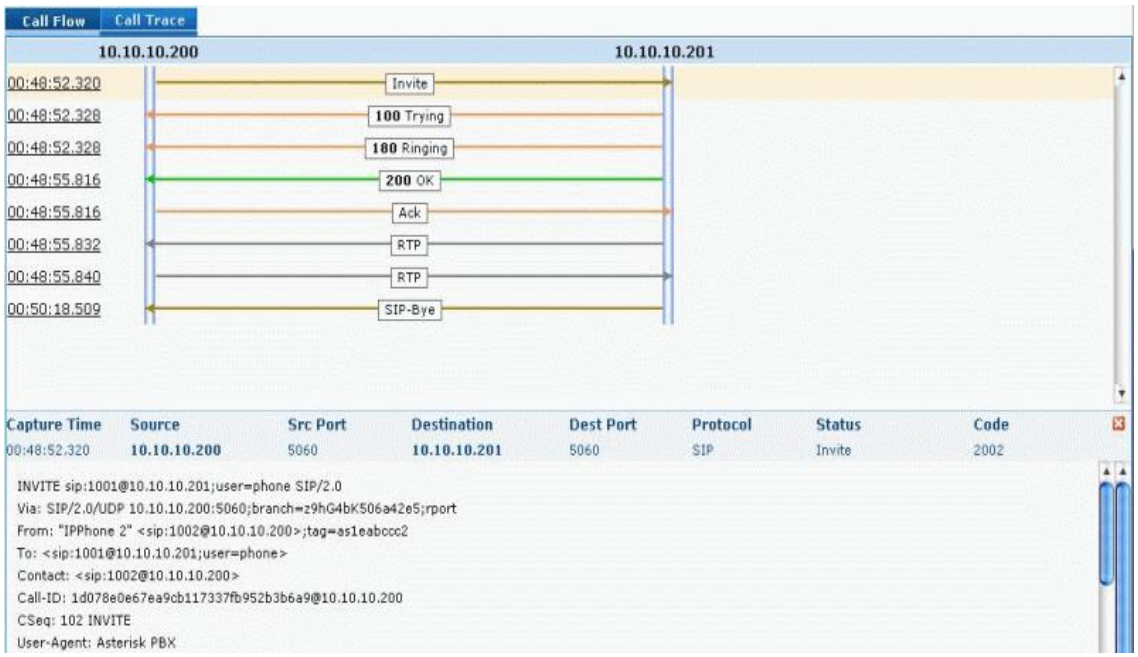


Figure 4.17: Call Trace

4.4.10 CDR Interface - Call Details

- The QoS of the active calls are depicted in the form of intuitive charts. The average values of all the QoS parameters such as Delay, Jitter, Packet Loss and MOS are plotted in the chart.

Figure 4.18: CDR Interface - Call Details

4.5 VoIP R-Factor and MOS

There are a variety of objective factors that contribute to call quality. Some of these factors, such as packet loss or packet delay variation (jitter), are reported in other VoIP graph summaries. However, these individual measurements do not tell a complete story and do not attempt to quantify user perceptions of voice quality. The R-factor metrics in VoIP, called R-factors, use a formula to take into account both user perceptions and the cumulative effect of equipment impairments to at a numeric expression of voice quality [36].

VoIP calculates two equipment impairment values to report as voice quality metrics: the Network R-factor and the User R-factor. The Network R-factor is generated based on the physical equipment impairments. The User R-factor adds perceptual effects to the equipment impairment, such as recency and delay. The user R-factor attempts to add the "perceived" annoyance that a user may experience during a call based on a

perceptual effect called recency. Recency is an auditory phenomenon where distracting events that have occurred more recently appear to have a greater impact on perceived quality. The User R-factor has been found to match well with users purely subjective ratings of voice quality [28].
Rating Factor (R-Factor) and Mean Opinion Score (MOS) are two commonly-used measurements of overall VoIP call quality.

- **R-Factor**: A value derived from metrics such as latency, jitter, and packet loss per ITU-T Recommendation G.107, the R-Factor value helps you quickly assess the quality-of-experience for VoIP calls on your network. Typical scores range from 50 (bad) to 90 (excellent)[36].

- **MOS**: A value is derived from the R-Factor per ITU-T Recommendation G.10 which measures VoIP call quality. Packeteer measures MOS using a scale of 10-50. To convert to a standard MOS score (which uses a scale of 1-5), divide the Packeteer MOS value by 10.

The VoIP software at the user-nodes is responsible for digitizing, encoding, streaming, decoding and playing out the voice signal [5]. First, the voice signal is sampled and digitized. Then it is encoded with one of many codecs available (G.711, G.723.1, G.729, etc.), packetized and transmitted using RTP/UDP/IP. At the receiver's side, data is depacketized and forwarded to a jitter buffer, which smoothes out the variation in network delay (jitter). The voice data is then reconstructed and delivered to the listener. Packet loss and delay affect the obtained quality of a VoIP stream in a complex manner. Packet loss and delay are caused by both the network and the VoIP application itself. Packets can be lost in the network or be dropped by the playout buffer due to large delay jitter. Delay is caused by the packetization process, in encoding and decoding data, and in the jitter buffer. The quality obtained is also affected by the nature of losses. Packet losses that are randomly distributed along the stream are considered to be less impairing than losses that are clustered together. Since the delays caused by encoding and packetization are fixed for a particular codec, the goal of routing the call is to minimize the negative impact caused by a network delay, a network loss, a jitter delay, a jitter loss and a clustering of errors[35].

The ITU-T E-Model [6] is an analytic model of voice quality that can be used for estimating the relative voice quality between two connections. The E-Model can be used to calculate the R-factor which is a simple measure of voice quality ranging from the best case of 100 to the worst case of 0. The R-factor uniquely determines the Mean Opinion Score which is the arithmetic average of opinions where 1 is .unacceptable and 5 is .excellent. The R-factor is related in a non-linear fashion to the MOS through the following equation [32]:

(1) MOS = 1 + 0:035 * R + 7 * 10-6 * R*(R - 60)*(100 - R)

The relationship of the R-factor values to the MOS and the typical categorization of the R-factor values are presented in Tab.1. It can be seen that connections with R factors of less than 60 are expected to provide poor quality, whereas R-factors of 80 and above provide high quality [7].

Table 4.2: Relationship of R-factor values to MOS and to the Quality of Voice Rating

R-factor	Quality of Voice Rating	MOS
0< R < 100	Best	4.34 – 4.50
80< R < 90	High	4.03 – 4.34
70< R < 80	Medium	3.60 – 4.03
60< R < 70	Low	3.10 – 3.60
50< R < 60	Poor	2.58 – 3.00

The main QoS parameters that quantify the quality degradation over a certain connection are the following: throughput, delay & jitter and packet loss [9]. Delay & jitter are probably the most important ones for VoIP as a real-time streaming application. Packets containing voice data must be delivered in a timely manner in order to ensure user satisfaction [34]. One-way delay influences interactivity: the larger the delay, the lower the perceived interactivity for the interlocutors. On the other hand, jitter (i.e. one-way delay variation) influences quality if it exceeds a maximum value. This maximum value is system dependent and is related to the size of the

dejittering buffer used. A large buffer means that jitter has a smaller effect on the quality obtained but it decreases interactivity through the effect of delay. If the induced jitter value exceeds the size of the dejittering buffer, the VoIP packets do not arrive in time for playback, and the playback signal quality decreases. Hence, this distortion is the main effect that jitters has on user satisfaction. Packets that do not arrive in time for playback can be considered lost; therefore this effect is sometimes termed jitter-loss. The jitter (delay variation) is an important factor that has a direct influence on the VoIP quality [8]. In order to counter the effects of the jitter, all VoIP applications use a jittering buffer to try to restore the initial distribution at the expense of adding a supplementary playback delay [30]. In the realization of VoIP applications, the availability of Quality of Services (QoS) is of great importance for the end users. The following parameter limits, the most significant ones for the IP telephony, can be found in the ITU-T recommendations:

One-way delay

up to 150 ms – acceptable;

from 150 ms to 400 ms – acceptable with a proviso

above 400 ms – unacceptable;

• Jitter - less than 50 ms.

4.6 The E-model, a computational model for use in transmission planning

The complexity of modern networks requires that for transmission planning the many transmission parameters are not only considered individually but also that their combination effects are taken into account. This can be done by "expert, informed guessing," but a more systematic approach is desirable, such as by using a computational model. The output from the model described here is a scalar quality rating value, R, which varies directly with the overall conversational quality. ITU-T Recommendation G.113 [32] gives guidance about specific impairments, including combinations effects based upon a simplification of the model. However, the output can also give nominal estimates of user reactions, for instance in the form of percentages finding the modeled connection "Good or Better" or "Poor or Worse", as

described in Annex B. Furthermore, detailed guidance on the proper application of the E-model – as described in this ITU-T Recommendation – is provided in ITU-T Recommendation G.108 [36]. In addition, the definition of categories of speech transmission quality can be found in ITU-T Recommendation G.109 [36].

The E-model is based on the equipment impairment factor method, following previous transmission rating models. It was developed by an ETSI ad hoc group called "Voice Transmission Quality from Mouth to Ear".

4.6.1 Calculation of the transmission rating factor, R

The result of any calculation with the E-model in a first step is a transmission rating factor *R*, which combines all transmission parameters relevant for the considered connection. This rating factor *R* is composed of:

$$R = Ro - Is - Id - Ie + A \qquad (1)$$

Ro represents in principle the basic signal-to-noise ratio, including noise sources such as circuit noise and room noise. The factor *Is* is a combination of all impairments which occur more or less simultaneously with the voice signal. Factor *Id* represents the impairments caused by delay and the equipment impairment factor *Ie* represents impairments caused by low bit rate codecs. The advantage factor *A* allows for compensation of impairment factors when there are other advantages of access to the user. The term *Ro* and the *Is* and *Id* values are subdivided into further specific impairment values. The following sub clauses give the formulae used in the E-model.

4.6.2 Quality measures derived from the transmission rating factor R

The transmission rating factor *R* can lie in the range from 0 to 100, where $R = 0$ represents an extremely bad quality and $R = 100$ represents a very high quality. The E-model provides a statistical estimation of quality measures. The percentages for a judgement Good or Better (GoB) or Poor or Worse (PoW) are obtained from the *R*-factor by means of the Gaussian Error function:

$$E(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \mathrm{e}^{-\frac{t^2}{2}} dt \tag{4-1}$$

The equations are:

$$GoB = 100E\left(\frac{R-60}{16}\right)\% \tag{4-2}$$

$$PoW = 100E\left(\frac{45-R}{16}\right)\% \tag{4-3}$$

The Mean Opinion Score (MOS) in the scale 1-5 can be obtained from the *R*-factor using the formulae:

For $R < 0$: $\mathrm{MOS} = 1$

For $0 < R < 100$: $\mathrm{MOS} = 1 + 0.035R + R(R-60)(100-R)7 \cdot 10^{-6}$ (4-4)

For $R > 100$: $\mathrm{MOS} = 4.5$

4.7 Defining Threshold Values

We have to define some threshold values to demonstrate the VoIP Quality of Service for a network. These values are for the some of the categories we have selected such as:

- For Incomplete Calls
- For ALOC(Average Length Of Call)
- For ASR(Automatic Speech Recognition)
- For Delay
- For Jitter
- For Packet Loss
- For Average Answer Delay
- For Concurrent Calls
- For Call Set-up Time
- For Voice Bandwidth Utilization
- For SIP Error Code

- For MOS (Mean Opinion Score)
- For R Factor
- For Call Volume
- For Disconnect Time
- For Talk Time

4.8 Summary Report for deployment of a VoIP Network

Summary reports include all the Factors of a VQManager. Such summary report is given below:

Figure 4.19: VQManager summary Report

The 'Reports' section provides you the information on 'what is going on' in your VoIP network and how your VoIP network is performing. The status and summaries of the different activities are provided in the form of tables and graphs, which assist the administrators in making well-informed decisions and taking precautionary measures to build a possible VoIP Network.

CHAPTER 05: CONCLUSION

This paper gives an overview of the approaches used for the assessment of the Quality of services in the realization of VoIP voice applications for deployment of a quality network.

In this report, at the earlier portion we have discussed about VoIP overview, its deployment reason, Network architecture of basic VoIP system, VoIP Protocols and Issues in a VoIP Network. We also learned theoretically the Basic mechanism of calculation of VoIP Quality of Service using ITU E model. Then we established a virtual machine using software like VQmanager 6.3 and Test call generator (TCS) (Bulk call generator). This virtual machine can generate bulk calls or virtual calls using different VoIP protocols and monitor the QoS parameters like delay, Jitter and packet loss which is using for calculate the Rating Factor (R-factor) and Mean Opinion score (MOS). R-Factor is recommended by ITU-T G.107 and it quickly assesses the quality-of-experience for VoIP calls on your network. MOS is recommended by ITU-T G.10 and measures VoIP call quality.

LIST OF ABBREVIATIONS

3GPP	: 3rd Generation Partnership Project
ALOC	: Average Length of Call
ASR	: Answer Seizure Ratio
BICC	: Bearer Independent Call Control
CDR	: Call Detail Record
CMTS	: Cable Modem Termination System
DHCP	: Dynamic Host Configuration Protocol
DSL	: Digital Subscriber Line
DSLAM	: Digital Subscriber Line Access Multiplexer
FMC	: Fixed-Mobile Convergence
HTTP	: Hypertext Transfer Protocol
IMS	: IP Multimedia Subsystem
IP	: Internet Protocol
ISP	: Internet Service Provider
ISDN	: Integrated Services Digital Network
ITU	
IXC	: Inter-Exchange Carrier
LEC	: Local Exchange Carrier
MGCP	: Media Gateway Control Protocol
MOS	: Mean Opinion Scores
NAT	: Network Address Translation

OSS : Operations Support System

PSTN : Public Switched Telephone Network
PBX : Private Branch Exchange
POTS : Plain Old Telephone Service

QoS : Quality of Service

RTP : Real-Time Transport Protocol
RTCP : RTP Control Protocol
RTSP : Real-time Streaming Protocol

SCCP : Skinny Call Control Protocol
SCTP : Stream Control Transmission Protocol
SDP : Session Description Protocol
SMTP : Simple Mail Transfer Protocol
SNMP : Simple Network Management Protocol
SRTP : Secure Real-time Transport Protocol
SIP : Session Initiation Protocol

TCS : Test call generator
TDM : Time Division Multiplexing
TCP : Transmission Control Protocol

UDP : User Datagram Protocol

VoBB : Voice over Broadband
VoIP : Voice over Internet Protocol

WAN : Wide Area Network

REFERRANCE

[1]“Voice over Internet Protocol. Definition and Overview". International Engineering Consortium. 2007

[2] http://en.wikipedia.org/wiki/Voice_over_IP

[3] Goode, B. “Voice over Internet Protocol (VoIP)”. Proceedings of The IEEE. Volume 90. No. 9. September 2002.

[4] Siemens; White paper providing Siemens IP-tech portfolio and technology description; The Big Communications Picture, February 2004

[5] Larkspur Group; A security analysis and comparison of the POTS and specific examples of VoIP systems (Skype and SIP); "A Comparison on the Security of VoIP and POTS", 2005 [6] Keith G. Knighston, Industry Canada; Presentation from the ITU NGN Technical Workshop in March 2005; Basic NGN Architecture & Principles, March 2005

[7] VOIP on the Verge". Telecommuncations Online. November 1, 2004. http://www.telecoms-mag.com/Americas/article.asp?HH_ID=AR_539

[8] Markopoulou A.P., Tobagi, F.A., and Karam, M.J., “Assessing the Quality of Voice communications over Internet Backbones”, IEEE/ACM Transactions on Networking, Vol.11, No. 5, October 2003.

[9] C. Long. IP network design. Osborne/McGraw-Hill, Berkeley, CA, 2001.

[10] AT&T; VoIP protocol architecture description by AT&T company; Common VoIP Architecture, December 2003

[11] http://www.basicprinciple.com/voip

[12] http://www.fcc.gov/voip

[13] http://communication.howstuffworks.com/ip-telephony.htm

[14]J. Mullin, L. Smallwood, A. Watson, and G. Wilson. New techniques for assessing audio and video quality in real-time interactive communications. IHM-HCI Tutorial, 2001.

[15] http://www.voip-info.org

[17]Paul E. Jones, Rapporteur, ITU-T; Presentation describing features and characteristics of H.323 by ITU; Overview of H.323, June 2004

[18] ITU-T Recommendation H.323. Infrastructure of audiovisual services- systems and terminal equipment for audiovisual services, series H: Audiovisual and multimedia systems, 1999.

[19] ITU-T Recommendation SIP. Infrastructure of audiovisual services- systems and terminal equipment for audiovisual services, series H: Audiovisual and multimedia systems, 2007

[20] Davidson, Jonathan; James Peters, Jim Peters, Brian Gracely. "H.323". Voice over IP fundamentals. Cisco Press. pp. 229–230. ISBN 9781578701681. http://books.google.com/books?id=S5P7-Xtq7W8C&pg=PA229.

[21] RFC 4168, The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP), IETF, The Internet Society (2005)

[22] Johnston, Alan B. (2004). SIP: Understanding the Session Initiation Protocol, Second Edition. Artech House. ISBN 1580531687.

[23] Handley, Mark; Van Jacobson, Colin Perkins (2006-07). "SDP: Session Description Protocol (RFC 4566)". IETF. http://tools.ietf.org/html/rfc4566. Retrieved 2008-04-19.

[24] Handley, Mark; Van Jacobson (1998-04). "SDP: Session Description Protocol (RFC 2327)". IETF. http://tools.ietf.org/html/rfc2327. Retrieved 2008-04-19.

[25] Skype for Asterisk – Production Released!, By pengler, August 31st, 2009, Digium - The Asterisk Company

[26] Han, J.S., Ahn, S.J., and Chung, J.W. “Study of Delay Patterns of Weighted Voice Traffic of End-to-End Users on the VoIP Network”, Int. J. Network Management 2002.

[27] Karam, M.J. and Tobagi, F.A. “Analysis of the Delay and Jitter of Voice Traffic over the Internet”. Proceedings of Infocom 2001.

[28]Miloucheva, I., Nassri, A., and Anzaloni, A., “Automated Analysis of Network QoS Parameters for Voice over IP Applications”, D41 – 2nd Inter-Domain Performance and Simulation Workshop (IPS 2004).

[29] O. Olorunda and A. Olorunda. Bridging the Digital Divide -c The Social and Cultural Impactof VoIP in Developing Countries: Nigeria as a Case Study. In Proc. of PTC’06, Honolulu,Hawaii, January 2006.

[30] Technical, Commercial and Regulatory Challenges of QoS: An Internet Service Model Perspective by Xipeng Xiao (Morgan Kaufmann, 2008, ISBN 0-12-373693-5)

[31] Markopoulou A.P., Tobagi, F.A., and Karam, M.J., “Assessing the Quality of Voice communications over Internet Backbones”, IEEE/ACM Transactions on Networking, Vol.11, No. 5, October 2003.

[32]A.E. Conway. A passive method for monitoring voice-over-ip call quality with itu-t objective speech quality measurement methods. In Proc. of IEEE International Conference on Communications, pages 2583–2586, New York, NY, April 2002

[33]Jha, S., and Hassan, M. “Engineering Internet QoS”. Artech House. ISBN: 1580533418.2002.

[34] C. Boutremans, G. Iannaccone, and C. Diot. Impact of link failures on VoIP performance.In Proc. of the 12th International Workshop on Network and Operating Systems Support for Digital Audio and Video. NOSSDAV 2002, pages 63–71, Miami, FL, May 2002

[35] S. Tao, K. Xu, A. Estepa, T. Fei, L. Gao, R. Guerin, J. Kurose, D. Towsley, and Z. Zhang.Improving VoIP Quality through Path Switching. In Proc. of IEEE Infocom 2005, pages 2268–2278, Miami, FL, March 2005.

[36] ITU-T Recommendation G.107. The e-model, a computational model for use in transmission planning, December 1998.