St. Mary's University

Faculty of Informatics

Department of Computer Science

Improving the Quality of Service of Voice over Internet Protocol in Ethio Telecom Service Level Agreement Customers

By

Bisrat Saboka

Advisor

Dr. Asrat Mulatu

A Thesis Submitted to the Faculty of Informatics in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science

January 2021

Addis Ababa, Ethiopia

Improving the Quality of Service of Voice over Internet Protocol in Ethio Telecom Service Level Agreement Customers

By

Bisrat Saboka

Accepted by the Faculty of Informatics, St. Mary's University, in partial fulfillment of the requirements for the degree of Master of Science in Computer Science

Thesis Examination Committee:

Full Name Signature Date

Internal Examiner

Full Name Signature Date

External Examiner

Full Name Signature Date

Dean, Faculty of Informatics

Full Name Signature Date

January 2021

Addis Ababa, Ethiopia

Declaration of Originality

I, Bisrat Saboke, declare that this thesis entitled **“Improving the Quality of Service of Voice over Internet Protocol in Ethio Telecom Service Level Agreement Customers’’** is the outcome of my original work, except the guidance and suggestion of Dr. Asrat Mulatu. The work contained in this thesis has not been presented for a degree in this or any other university, and all sources of materials used for the thesis have been duly acknowledged and do not breach any law of copyright.

Bisrat Saboqa Dinagde

Full Name of Student

____

Signature

Addis Ababa, Ethiopia

This thesis has been submitted for examination with my approval as an advisor.

Dr. Asrat Mulatu

Full Name of Advisor

____

Signature

January 2021

Addis Ababa, Ethiopia

Dedication

From the rest of the others, my first interest in the dedication of this thesis is dedicated to my mother, Chaltu Tolosa. She gave me endless sacrifices and support me starting from when I start walking up to she pass away from this world and, I had never and ever completed my graduate studies without help. I love you mom and I appreciate everything that you have sacrificed for today's success.

I love you both and I appreciate everything that you have done for my success and me. This thesis is also dedicated to my sister, Mesert Seboka who was there for me throughout this process and gave me lots of support. I will miss you when I leave, but you know where to find me. Without their endless love and encouragement, I would never have been able to complete my graduate studies without the support of my wife Tsion Fentenaw

Acknowledgments

In the beginning, I would like to say thank you, my God, who blessed me in every step of my life and select me for this opportunity. Secondly, I would have respect and thanks for my lecturer, Dr. Asrat Mulatu, for supporting me during thesis title selection, facilitating thesis title approval. Thirdly and Again, I would like to thank Asrat Mulatu for his immense and constant guidance during the development of this MSc thesis proposal and MSc thesis report writing. When this journey started, I was so lost and unsure of where and how to start, the meetings and communication with my adviser guided me in the right direction. The opportunities and knowledge you have provided me within my academic career are also much appreciated. I would also be happy say to thanks to all my class meta of the Computer science student for their assistance and input starting from title selection up to the end of my thesis work. The fun conversations we had in the lab, class, and St. Mary's Restaurant and Library about things happening in our lives kept me smiling throughout. To the Computer science department, it has been many years since I started the MSC program in 2009. Thank you all for the solid foundation laid during my undergraduate years. I would also like to thank the Ethio Telecom IP Quality of Service Management Section staff for their provision of necessary data to prepare my graduation final thesis paper. Finally, I would be happy when to say great acknowledgments to my mother Chaltu Tolosa that was my wish if you could have been here to see the man I have become, this is all for you. Thanks, mom, for your greater and restless sacrifices you had given in my life...I miss you, mom, Rest in Peace in the holy place.

Table of Content

List of Figures

List of Tables

List of Abbreviations and Acronyms

ADSL	Asymmetric Digital Subscriber Line.
ATM	Asynchronous Transfer Mode.
BGP	Border Gateway Protocol.
CE	Customer Edge router (CPE).
CME	Call Manager Express.
DSL	Direct Subscriber Line.
ERP	Enterprise Resource Planning.
ETC	Ethiopian Telecommunications Corporation.
FCC	Federal Communications Commission
FEC	Forward Error Correction.
FIFO	Frist Input Frist Out.
GNS3	Graphical Network Simulator three.
GW	Gateway.
IETF	Internet Engineering Task Force.
IGP	Interior Gateway Protocol.
Intserv	Integrated Services.
IP	Internet protocol.
IPSec	IP Security
IS-IS	Intermediate System to Intermediate System Routing Protocol.
ISP	Internet service providers.
ICT	Information Communication Technology
IT	Information Technology
ITU	International Telecommunication Union.
LAN	Local Area Network.
LDP	Label Distribution Protocol.
MGCP	Media Gateway Control Point
MGCs	media gateway controllers
MCs	media gateways
MOS	Mean Opinion Score.
MP BGP MPL	Border Gateway Protocol Multi-Protocol Label Switching.
MPLS	Multi-Protocol Label Switching.

MPLS-DiffServ	Multiprotocol Label Switching-Differentiated Service.
MPLS VPN	Multi-Protocol Label Switching Virtual Private Network.
MSAG	Multiple Service Access Gateways.
MSAN	Multiple Service Access Nodes.
LSP	Label Switched Path.
OPNET	Optimized Network Engineering Tool.
OSPF	Open Shortest Path First.
P	Provider core router.
PC	personal computer.
PE	provider edge router.
PESQ	perceptual evaluation of speech quality.
PHB	Per Hop Behavior
POTS	Plain old telephone system.
PSTN	Public switched telephone network.
QoE	Quality of Experience
QoS	Quality of service.
RR	Route Reflector.
RSVP	Resource Reservation Protocol.
RTC	Real-Time Communications.
RTP	Real-Time Protocol.
SIP	Signaling Initiation Protocol.
SLA	Service Level Agreement.
SP	Service Provider.
SSL	Secure Sockets Layer
TTL	Time To Live
TE	Traffic Engineering.
ToS	Types of Service.
UDP	Unreliable datagram protocol.
VoIP	Voice over Internet Protocol.
VPN	Virtual Private Network.
VSAT	Very Small Aperture Terminal.
VRFs	VPN routing and forwarding instances.
WAN	Wide Area Network.

Wi-Fi	Wireless Fidelity.

Abstract

Voice over Internet Protocol is the recent communication channel and innovative service through the internet which has devoted to replacing IP network to incorporate additional value-added service like multimedia applications. VoIP permits substantial profits for both telecommunication service providers and end-users like cost savings, phone or product movability, flexibility, combined with other software or applications. However, the implementation of VoIP faces different problems like interoperability, security, and Quality of Service issues. This thesis focused on the improvement of VoIP Quality of Service problems, which are the most critical point because real-time traffic is highly sensitive to delay, packet loss, jitter, and bandwidth requirement. QoS is based on different service levels agreement in between customer and ISP network (backbone, the access, and the IP core network). Ethio Telecom signed an SLA agreement to verify guaranteed VoIP QoS with the customer but Ethio Telecom IP Network fails to fulfill the required traffic prioritization, classification, and VoIP QoS performance requirements like delay, packet loss, jitter, and bandwidth. As a result of this research gap, this thesis carried out a thorough analysis and improve VoIP QoS using BGP MPLS VPN TE and DiffServ model. Firstly, it presents a brief overview of VoIP technology. Then, it discusses the QoS issues related to real-time packet communication. Finally, develop an artifact that guarantees the real-time voice packet and QoS performance like voice packet delay, jitter, packet loss, and utilization of bandwidth. The designed artifact improves VoIP QoS performance parameters by applying BGP MPLS VPN TE and DiffServ model. DiffServ model implements a different class of service at the border of service provider Edge Router by setting traffic policing, shaping (class-based marking and policing), traffic prioritization (class-based weighted fair queue,) and congestion control technique (weighted random early discard) to improve VoIP QoS. The researcher had used a Design science Research methodology to identify data of VoIP Quality of service the problem. To Design the proposed prototype, simulation, and analysis of end-to-end VoIP QoS Architecture GNS3 and Wireshark are used, respectively. The simulation result and evaluation of the proposed end-to-end VoIP QoS Architecture show decreased packet loss, delay, jitter, and increased bandwidth utilization. which eventually boost the need of VoIP QoS Threshold parameters for SLA customer and the ITU requirement.

Keywords: *VoIP, QoS, bandwidth utilization, delay, jitter, packet loss, GNS3, and Wireshark, Analysis SLA, and ITU Threshold.*

CHAPTER ONE

1.INTRODUCTION

1.1 Background of the study

Nowadays technological advancement creates opportunities for Ethiopian peoples of nation's nationalities to communicate using recently emerging Voice over Internet protocol (VoIP) service provided by Internet Service Provider (ISP) [1]. Despite recent large-scale deployments, enterprise multimedia applications on Internet Service Provider like Voice and online video meeting still face the significant intermittent voice and blurred presentation of video problems. They reported that measurements collected from a commercial enterprise of the VoIP system had shown about 26 percent of VoIP sessions experienced poor quality of service [2]. Managing and improving Voice over Internet Protocol Quality of Service in wire networks is challenging. Delivering attractive Voice over Internet Protocol Quality of Service to the customers may broaden the density or complexity to distributing the existing capacity of the resource to achieve the expected quality of service. At the same time, The potential capacity of access and technical usage of Voice over Internet Protocol downgrade the expectations of a good quality experience [3]. The volume of voice traffic on Internet Protocol (IP) networks continues to increase at speedy strides, with substantial growth in the use of voice applications [4]. Voice over Internet Protocol new real-time application service through the internet that allows users to make online telephone calls send faxes with the best quality and superior cost or profit [5]. The Ethio Telecom has been merely ISP in Ethiopia and it provides one of the recent value-added services known as VoIP with limited QoS and VOIP allow the user to make call voice through the internet. VoIP allows us to propagate Voice packets across the data network instead of a dedicated fixed line or phone network. VOIP provides additional services which the old system cannot provide. The current generation internet user has gain greater benefit from Voice over Internet Protocol service mainly it minimizes the phone cost if they paid for an international and local call, it also provides additional features, simple to access and adaptability by the customers [6]. The technology progressively advanced the demand of customers will also increase with the demand for the quality of service. VoIP provider or ISP was forced to work hard to satisfy their customer need and QoS. As a result, Ethio Telecom is now working for a world-class telecom services provider, Connect Ethiopia through advanced telecom services, delivered expected excellence, smart and cheap Telecom goods and services which accelerate the growth of our people and guarantee Ethio Telecom customer satisfaction. Ethio Telecom also works for high-level quality, client provision excellence, company-level excellence, and ceaseless development of Quality of Service [6]. In the future VoIP fully dominate and control standard public switched telephone network telephony services, as a result, the EthioTelecom network should have worked hard to improve VoIP QoS and achieve customer satisfaction feedback on high-quality voice transmissions over the internet. Voice over Internet Protocol application service is the most tremendously affected by limited or low bandwidth and high delay. The successful transmissions VoIP needs a clear voice to the listener, speech packages must not be lost, too many delayed and jitter [7]. To fulfill these VoIP requirements, EthioTelecom struggles to provide sufficient network coverage and quality of service to manage a continuously increasing number of both residential and enterprise customers. As a result, EthioTelecom had made continuous expansion projects starting from NGNs, which Intention to boost the Excellence of Service in the real-time streaming system. mainly on VoIP on the network. In addition to that recently reported by Mihratu Daka in 2017, EthioTelecom has made TEP network expansion on the existing IP backhaul for mobile customers, Multiple Service Access Gateway (MSAG), and Multiple Service Access Node plantation projects for PSTN and broadband internet users [8]. EthioTelecom Provide voice plus internet service to its residential and enterprise customers. Ethio Telecom is connected to the internet (WAN) through two options. The first option is through Space Satellite communication from the Djibouti satellite station and the second option is fiber optic from our neighboring countries like Kenya, Sudan, and Djibouti [9]. Still, Now Ethio Telecom network performance is limited due to different factors like power fluctuation, low equipment quality, lacks of continuous follow-up. As a result, there are intermittent internet connections that affect service provision of affordable quality of service and real-time application. VoIP QoS Models are provided for user services to ensure QoS according to the user's requirements and the quality of the network. The common service models are as follows: Best Effort service model, Integrated service model, and Differentiated service model. The best Effort service model is also known as the Best Quality Model. Mostly it is the default model in the network. It provides equal service like priority and bandwidth for all types of traffics. It is simple to implement, all packets are given the same treatment at the same level and there is no separate treatment of different types of sensitive real-time Multimedia traffics in terms of end-to-end packet delay and packet loss. [1] [10]. IntServ is a guaranteed service model for some specific level of traffic in a specific period. The IntServ limitations are Each router needs to contain a lot of state information that is why it runs on a small-scale network. If the network increases, then it can be challenging to store all traces of all the reservations [1][10]. It was designed by the working group of the IETF (Internet Engineering Task Force, 1998) for specific standards and definitions of services that fall under Differentiated QoS [11]. MPLS is a Mature Technology for providing Reliable services through speeding up network traffic and quality of service by using BGP MPLS VPN TE and DiffServ that enable us to provide VoIP over reliable transmission [1], [12]. Generally, the main goal of this thesis is to improving Voice over Internet protocol Quality of Service (VoIP QoS), which will help to guarantee end-to-end delivery of VoIP QoS. VoIP QoS includes end-user or service provider perception and network performance issues. Optimization of the VoIP QoS network by using different algorithms is the best to suit and increase the network performance or VoIP QoS. In the end, increasing network performance also increases end-user and service provider perception.

1.2. Statement of The Problem

There is a growing need for VoIP QoS and these services provided by Ethio Telecom for its Service Level Agreement (SLA) customers. VoIP is widely used in IP MPLS networks for connecting customers in different locations. But according to the literature review done on the different countries Telecommunication QoS level, faced different challenges such as low bandwidth, high jitter, high packet loss, and high packet delay which highly degrade the quality of service and overall network performance parameters. In addition to this, as shown in the questionnaires conducted from the company's VoIP SLA customers 45 percent of their connection has QoS problems [7],[13]. FCC predicts that 44 percent of corporate organizations were transforming their service into VoIP lines [18] improving the QoS of VoIP, Demand for the integration of Voice and Data integration helps to Cost Reduction of long-distance telephone calls [18] [19]. To provide excepted QoS for its customers, Ethio Telecom has done continuous Telecom Expansion Projects and detailed analysis done by Mehretu Daka in 2017 on the VoIP SLA customer's network [14]. The analysis result shows that there are some disparities between the company's SLA targets and analysis results. Again, Ethio Telecom announces on its portal the three years Strategic plan to perform network expansion and is committed to being a world-class telecom competitor operator with those newly joined in the Ethiopia Telecom industries in the coming 2021. The researcher was also Done a preliminary investigation of what the current Ethio Telecom network looks like by pinpointing the degree of its failure to fulfill QoS requirements set by ITU and the SLA it gives for its customers. Since, Ethio Telecom uses the Best Effort QoS model, which is used for the data or Internet service which cannot guarantee packet loss rate, delay, bandwidth, and jitter. and this model has also a gap of prioritization of sensitive traffic. As a result, the researcher is motivated to address the above problems by Design science research method and optimizing the network logically using BGP MPLS VPN TE -Diffserv, traffic prioritization of multimedia applications or sensitive service like VoIP [10] [15] [16].

1.3 Research Questions

Most of the time all research focuses on answering the research questions to achieve the main goal of the research. accordingly, the researcher focuses to answer the following research questions:

1.What approaches are used to improve Voice over Internet protocol Quality of Service in the Ethio Telecom network environment?

2.What are the network parameters that influences the quality of Voice over Internet protocol traffic.

3.How BGP MPLS VPN TE and DiffServ work together to improve Voice over Internet protocol Quality of Service in the Ethio Telecom network.

4.What improvements shown in QoS of VoIP within the Ethio Telecom network after the deploying of BGP MPLS VPN TE and DiffServ QoS?

1.4 Objective

1.4.1 General Objective

The main objective of this thesis is to design, demonstrate, and evaluate possible solutions to improve the Voice over Internet Protocol Quality of Service.

1.4.2 Specific Objectives

To meet the general objective of the study, the following specific objectives are identified:

- Compare and contrast the status of the Ethio Telecom VoIP QoS and International Telecommunication Union (ITU) threshold.
- Identify, QoS gap, and improve Voice over Internet Protocol Quality of Service is provided by Ethio Telecom to its customer.
- Analyzed VoIP Quality of Service with ITU standard threshold metrics like packet loss, delay, and jitter and bandwidth link.
- Design, develop the Artifact, Demonstrate, Evaluate, and Communicate the solutions to improve the VoIP Quality of Service provided by Ethio Telecom to its SLA customers.
- Recommend Ethio Telecom approaches or ways to improve Voice over Internet Protocol Quality of Service.

1.5 Significance of the study

Quality of Service provides the capability to control network traffic successfully by identifying variations in the network, by restricting or preferential network traffic treatment, and controlling bandwidth usage. DiffServ and MPLS are two different technologies that allow you to manage network traffic with QoS. This is known that voice traffic is higher significant than data traffic. When the network depends on Voice over Internet Protocol by integrating QoS, then VOIP cloud is unquestionable to offer a sustained stage of Service expected by Ethio Telecom. The BGP MPLS VPN TE and DiffServ combined to transport Real-time passage through Internet Service Providers network. MPLS used edge routers to tag packets without searching the routing information at every hop and MPLS labeled packets were directly sent from source to its destination. since MPLS cannot distinguish types of packets whether it is voice or data in any network. To improve the inability of MPLS to distinguishing service of type DiffServ is used. DiffServ allows MPLS traffic to be classified and prioritized based on the network queuing service. e.g., Voice traffic is assigned priority over the data packet. This research identified that the numerical analysis of Quality of Service of Voice over Internet Protocol (VoIP QoS) of Ethio Telecom SLA customer's status. Then this numerical output was compared to SLA targets and ITU threshold standards. By using the numerical output as input and proposed a technique of enhancing Voice over Internet protocol Quality of Service for Ethio Telecom customers. For the final proposed solution, practical demonstration, and modeling to operate high speed and optimized network usage have been conducted. Then the study has designed, developed, demonstrated, and evaluated the possible solution to improve VoIP QoS of Ethio Telecom SLA customer satisfaction has increased.

1.6 Contributions

Internet service providers use QoS parameters to control and advance how they propose their services, to their customers or other partner providers for cross-checking whether gain the level of quality that they are buying for. Ethio Telecom joins commercial contracts or Service Level Agreement with its customer for invention and confirmation [20]. The integration of Voice over Internet Protocol with MPLS VPN TE allows using profits of addition ability of network proficiencies in the network. These network proficiencies upgraded the QoS of Voice over Internet Protocol by integrating LSPs as a transporter for Voice over Internet Protocol packets: allow the most well-organized transportation method, layer two neutrality, permit the combination of access technologies of networking protocols or addressing, and finally assured Quality of Service through Internet Service Provider MPLS core network. From the above input and results entities, the researcher combines diverse knowledge and investigating the dissimilar situations of Voice over Internet Protocol connecting with BGP MPLS VPN

TE for a well Quality of Service, profitable, and consistent communication [21]. The role of thesis research was improving the Quality-of-Service Voice over Internet protocol (QoS VoIP). It is most areas of the study that need very strict follow-up in telecommunication industries. Meanwhile, Ethio Telecom provides VoIP service to its Enterprise customer based on SLA. This is because every SLA customer needs uninterrupted services to support their day-to-day activities. This, in turn, demands network traffic optimization end-to-end. Hence, attention must be given to improving the QoS of VoIP. To utilize the maximum possible capacity of the network and know its usage after deploying the network, there should be continuous and organized traffic optimization on end-to-end networks. This research work contributed, to improving the QoS of VoIP of Ethio Telecom SLA customer's connection. This is done by traffic classification, marking, shaping, and policing using different KPIs by the Diffserv QoS model. The proposed solution has been designed, developed, simulated, analyzed, and evaluated using computer-aided tools.

1.7 Scope and limitations.

1.7.1 The Scope of the Study

This thesis research has evaluated the current quality of services of VoIP of two Ethio Telecom core site edge routers to SLA customer's connection throughout put. After the evaluation has been done, the researchers compare the level of existing VoIP quality of services of Ethio Telecom to the company's SLA targets and ITU Voice over Internet Protocol QoS parameters (standard threshold values). Based on variation found from the SLA targets and ITU Voice over Internet Protocol QoS parameters, the researcher identifies VoIP Quality of Service Difficulties as input and designs the test-based porotype to solve the problem of VoIP quality of services. The final proposed solution has been designed, demonstrated, and evaluated using computer-aided tools (GNS3, Wireshark, and CME) in a well-organized manner. Meanwhile, the existing infrastructure of VoIP Quality of Service implementation and improvement can be done by using BGP MPLS, VPN TE, and Diffserv, traffic management, and queueing algorithms. The researcher simulated the proposed porotype using GNS3 with Cisco ISO image of a switch, and Routers to show how BGP MPLS, VPN, TE, and Diffserv work together to improve VoIP Quality of Service. Traffic was generated using Wireshark and measured by how designed the network and the packet loss, delay, jitter, and bandwidth utilization.

1.7.2 The Limitations of the Study

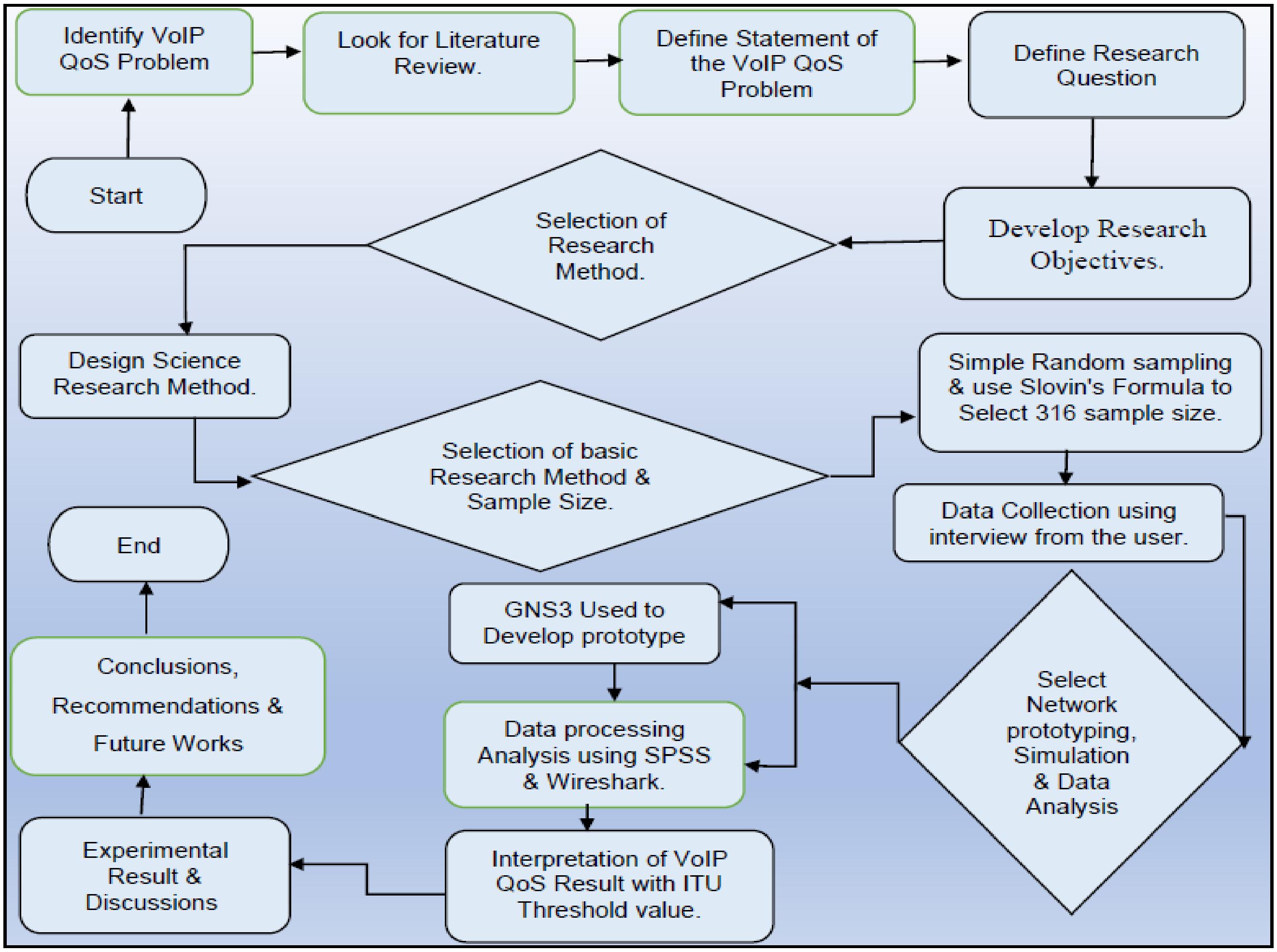
This research is only limited to improve VoIP Quality of Service of Ethio Telecom SLA customers by combining routing technologies like Border Gateway Protocol, multiprotocol label switching, Virtual Private Network, with traffic engineering and differentiated services (DiffServ). The best practice of implementing end-to-end quality of services of VoIP is done by optimizing by physical and logical architectures of the current network. But the researchers have not to focus on the design of the physical architecture to improve the existing quality services of VoIP of Ethio Telecom SLA customers [22]. In designing a VoIP network different influences interrupt the VoIP quality of service. The major influences listed below: packet-loss, Jitter, delay, Delay-budget, Frame-Loss, CODEC, synchronized time, echo control, choice of voice code, design of IP Network, improper Network device configuration, poor internet connection [13], [22]. Additionally, due to limited laptop capacity, the researcher is limited to show simulation only at the network level and not at the application stage. During simulation and implementation of VoIP qualities of service by using GNS3 it assumed that: it emulated packet related to an actual network packet, GNS3-replaced real devices or hardware which functions as an equal or same performance of Cisco IOSs, the Bandwidth limitations are known that, and the pathway of the packets does not alter in the network link. From all these factors or parameters, the researcher's study is only limited to delay, Delay Variation (Jitter), packet loss, and bandwidth utilization. Additionally, simulation use sample-developed models and randomly selected variables for the packet arrival rate. The variables are generated offline after close inspection of the real network scenario. The researcher used Wireshark to capture the traffic of packets in real-time, but analysis can be made offline.

1.8 Organization of the Rest of the Thesis

This thesis paper encompasses Five chapters. Chapter One deals with the introduction of the whole thesis. It covers the background of the study, the statement of the problem, objectives, Research Methodology (Overall Approach and detailed method, Data Type and Source Data, Sampling Procedures and Sample dimension or size, Data gathering Instruments, Process, procedures) and specifies software tools used for implementation for improving VoIP QoS in ISP network, thesis contribution, scopes, and limitations. Chapter two presents the literature Review and Related work on the area of VoIP BGP MPLS VPN, TE, and the QoS model used. It also showed some light on what other authors and researchers have forward their ideas on the area of improving VoIP and Network QoS by using technologies like BGP MPLS VPNs TE and the DiffServ model were presented. Chapter Three focuses on Research Methodology and specifies software tools used for implementation for improving VoIP QoS in ISP network. Chapter four: Explains Proposed VoIP QoS Network Architectures, provides the detailed experimental work, how VoIP Prototyped, or designed, implemented in VoIP network using the GNS3 simulator, at the end analysis and evaluation of simulation results. The experimental results and discussions were also presented. Finally, chapter five concluded the paper by presenting the conclusions, Recommendations, future work, references, and appendices.

1.9 Research Methodology

To achieve the main and explicit goal of the study, the researcher has made a Literature Review that was related to my topic from different sources. This Literature is reviewed to understand what factors affecting VoIP QoS and selecting proper VoIP protocol, routing, and switching techniques to Improve VoIP Quality of Service. Secondly, the researcher had used design science research methods to identify data regarding the problem of VoIP Quality of Service from both Ethio Telecom staff and SLA customers. Thirdly the researcher analyzes the data result on the VoIP quality of service measurement with reverence to ITU threshold values. Fourthly to enhance the VoIP QoS provided by Ethio Telecom to its SLA customers. Fig.1.1: shows the proposed flow chart of the VoIP QoS Research Method.


Identify VoIP QoS Problem
Look for Literature Review.
Define Statement of the VoIP QoS Problem
Define Research Question
Start
Selection of Research Method.
Develop Research Objectives.
Design Science Research Method.
Simple Random sampling & use Slovin's Formula to Select 316 sample size.
Selection of basic Research Method & Sample Size.
Data Collection using interview from the user.
End
GNS3 Used to Develop prototype
Conclusions, Recommendations & Future Works
Data processing Analysis using SPSS & Wireshark.
Select Network prototyping, Simulation & Data Analysis
Experimental Result & Discussions
Interpretation of VoIP QoS Result with ITU Threshold value.

In the end, the researcher focuses on the following attributes to achieve the overall mentioned goal: the general approach and specific method, Source of Data Type and Study population, Sampling Techniques, and Sample size, Data collection Instruments and methods, Data Process and Analysis, and Designing Tools and Network simulators. evaluation all stated the approaches explained below in a well-organized manner.

1.9.1 General Approach and specific method

For the success of research goal, the researcher decides on Qualitative research approaches and design science research methods because most of the time it identifies the problem and provides a possible recommendation, it creates new methods or innovations that explain the ideas, practices, technical capabilities, and products through which the analysis, design, implementation, and use of it can be effectively and efficiently accomplished. First, the researcher designed the questionnaire, which helps to assess and improve the VoIP Quality of Service on the current status of an organization.

In this study, Questionnaires help to collect information on VoIP Quality of Service from the organization, customers and show the relation sheep between VoIP Quality of Service and bandwidth, delay, jitter, and packet loss ratio. Then select the design tool to develop an artifact that creates an optional way to improve VoIP Quality of Service provided by Ethio Telecom to its customers, demonstration, and evaluation of improved VoIP QoS for Ethio Telecom SLA customers was done. Finally, to identify and analyze the present status of VoIP Quality of Service, compare it is the existing condition with Ethio Telecom SLA target, and ITU threshold values had reviewed research findings then, draw a general conclusion of the study.

1.9.2 Source of Data Type and Study population

The researcher had search sources of data for improving VoIP Quality of Service provided by the organization from both primary and secondary sources. The first primary source, data were collected from Ethio Telecom network sites dimension and secondly perform survey using designed the questionnaire, then intervening both Ethio Teleco network technician and different VoIP customers in Addis Abebe. Finally, collect the secondary data from Ethio Telecom relevant documents such as SLA charter, Quality of Service guide, network element configuration guide, achieved configuration, published and unpublished theoretical works of literature, and empirical studies.

1.9.3 Sampling Techniques and Sample size

The researcher has collected data from two dimensions. The first dimension of data collection was done by performing preliminary Investigation on Ethio Telecom network sites. The second dimension of data collection was done to check the expectation or satisfaction of Ethio Telecom VoIP SLA customers. The preliminary investigation was done on two Ethio Telecom network sites to measure the existing performance of bandwidth utilization, packet loss, delay, and jitter. On the other side, the researcher uses a simple random sampling technique to select a sample size of 316 peoples from the total population of 1500 VoIP SLA, ADSL broadband customers, and Ethio Telecom backbone network quality technicians. Here is how sample size is taken using Slovin's Formula which is relative to the objectives of the study and design. Slovin's formula is written as: $n = \frac{N}{1 + Ne^2}$

where n = number of samples, N = Total population and e = Error tolerance.

$$n = \frac{1500}{1+1500*0.05*0.05}=316$$

Table 1.1: Total VoIP QoS Ethio Telecom SLA customers and Sample size.

Type Customer	**Sample Size Selected**	**Total Customers**
ADSL broadband	82	742
Voice over Internet Protocol	179	554
EthioTelecom Network Technicians	55	204
Total	**316**	**1500**

Based on the sampling standards, all qualified Respondents those who selected to answer a questionnaire. Respondents were communicated continually up to the expected sample size of 316 is gotten from both customer and Ethio Telecom network quality technicians.

1.9.4 Data collection Instruments and Method

In this thesis research the researcher first made a comprehensive study of international kinds of literature and local archived data of the Ethio Telecom Service Level Agreement (SLA) charter, Quality of Service guide, CPE configuration guide, and network element configuration guide. Research cannot reach its goal without literature review and selection of papers. To fulfill the research gap, he develops questioners to collect primary data from Ethio Telecom VoIP SLA customers. The researcher had taken his measures to keep the quality and trustworthiness of the questionnaire with his Advisor and few respondents before distributing the Questionnaire. These measures are helping to check whether the questionnaire improves VoIP Quality of Service provide in Ethio Telecom service and to identify if there is any ambiguous idea or statement. The questionnaires are a close-ended type. The researcher continues to search data by performing preliminary investigation on two Ethio Telecom network sites to measure the existing performance of bandwidth utilization, packet loss, delay, and jitter. The questionnaire is designed in a well-organized manner with consistent, acceptable standards and that measures the network performance parameters or VoIP QoS variables. As obviously known primary sources of data are collected by questionnaires. For this work, the deductive approach has used as explained by Saunders et.al. [94].

1.9.5 Data Process and Analysis

The data collected through questioner was analyzed using the statistical package for social scientists (SPSS) version 20.0. Tables and graphs are used to show both questioners analyzed by SPSS results and preliminary investigation on existing VoIP QoS parameters like bandwidth utilization, packet loss, delay, and jitter. Finally, evaluate VoIP QoS of Enterprise SLA customers satisfaction stage. By using SPSS analysis and preliminary investigation of Ethio Telecom network to measure the existing performance of bandwidth utilization, packet loss, delay, and jitter result as an input for proposed VoIP QoS artifact. In the proposed architecture GNS3 is used to design and Wireshark is used as a data analyzer.

1.9.6 Designing Tools and Network simulators

Due to financial constraints, equipment limitations, and unavailability of a real VoIP DiffServ aware MPLS and VPN network in academic research and it is very important to chosen simulation as an alternative in the fields of computer networking and Telecommunication [94]. To design and simulate real QoS for real VoIP DiffServ aware MPLS VPN and TE network, a Network simulation tool is an important issue. Network simulation is a technique for modeling the behavior of a network, either by computing the interaction between different network entities (end devices, intermediate devices, links, packets, etc.) by using laborious mathematical methods, or by observing the behavior of a functional network [94].OPNET Modeler, NS2, NS3, GNS3, Packet Tracer, OMNeT++ are some of the dedicated software solutions, being known as network simulators. They implement network simulation techniques, enabling the development of simulation models within this field [95]. To design and simulate, the implementation of VoIP QoS the researcher selects the following tools:

- Choosing an appropriate model to run the real-time application or VoIP service.
- Manipulate a model for the simulation using the simulation tool known as GNS3.
- Perform simulation to find out the parameter's value for VoIP QoS in BGP MPLS VPN TE and Diffserv.
- Wireshark is used for analyzing network traffic, protocols, and fixing network problems.
- Cisco call manager expresses IOS Router and switch.
- Justify the research using the simulated data as a measure for analysis.
- Study of the documents for understanding and determining the constraints and parameters that need to be taken under consideration for the analysis.

To use this Network designer and simulator software, the PC must accomplish several minimum performance conditions: Processor: Intel Core i7, Memory: 2 GB RAM, Space on Hard Disk: 50 MB, operating system: Microsoft Windows (64bits), Connection: Connection to a network (broadband, LAN, wireless), permanent connection to the Internet, and Sound adaptor: Full-duplex, 16 bit or using a USB Headset.GNS3 (Graphical Network System 3) is a graphical network simulator that allows the simulation of complex networks. To function, it is dependent on three other programs that must run simultaneously:

Dynamips (the core for GNS3 that emulates IOS CISCO images), Dynagen (text-based software that is necessary to Dynamips), and Qemu (open-source emulator and virtualization tool). Wireshark is the most common tool for analyzing the network protocols (protocol analyzer or “packet sniffer”), fixing the network problems (troubleshooting), developing software products, and communication protocols. Wireshark captures the traffic of packets in real-time but analyzes offline [27].

This software can monitor the real network traffic and do protocol analysis that can capture and log data traffic passing over a data network. For example, packet source IP, destination IP, packet size, protocol, each protocol data unit (PDU). It can decrypt and analyze its content according to the appropriate specifications available in the market. It may be used with network lab, ISP, and network solution industry for data analysis and troubleshooting [97].

CHAPTER TWO

2 LITERATURE REVIEW AND RELATED WORKS

2.1 Introduction

Chapter two presents theoretical literature and Related Works that have been conducted to understand the problem related to the objectives of this thesis and identify the applicable direction to improve VoIP of quality of service. An extensive review is made by several authors and researchers focus on the area of enhancing VoIP of quality of service. Some of them have tried to describe the state-of-the-art in VoIP, VoIP quality of services from having affordable and well-optimized IP Network Design, increasing bandwidth, reducing delay, data packet loss, and jitter. In this section, notable Literature reviews and related works are explained to lay the foundation for this study.

2.2 Literature Review

This section presents theoretical works of literature conducted to understand the problem related to the objectives, of VoIP, the working principle of VoIP, and enhancing VoIP of quality of service. To fulfill the gap of VoIP the quality-of-service problem and achieve the objectives of the thesis, the researcher made a review of earlier contributions on improving VoIP QoS using different approaches and different model such as best effort, integrated service, differential service models, and combine DiffServ with Network optimization and routing technologies like BGP MPLS VPN TE and DiffServ, to enhance VoIP Quality of Service. The main goal of the study is to understand the problem and emphasize the research gap with the study. An extensive review has been made on Network optimization technologies like BGP MPLS and VPN, MPLS TE, and DiffServ model for expected VoIP quality of service, using the appropriate QoS tools for the functioning of real-time Voice traffic over IP MPLS Network, VoIP modeling architecture approaches, Configuring Network rather than the device running on the VoIP [22]. The other supportive review and ideas for VoIP of QoS are included like Securing IP networks, Network availability. VoIP QoS threshold, QoS model, traffic shaping, congestion management can provide ensured service quality that meets different expected standard VoIP quality network [23]. There are known that are parameters like bandwidth, delay, jitter, and packet loss rate that influences VoIP QoS. QoS measurement based on these influences provides quality assurance for key factors of services [13] [22], [24]. Based on network quality and user requirements, QoS provides end-to-end services for users through different service models. These service models are listed below: The Best-effort (internet default), integrated and differentiated. These models are integrating with routing technologies like BGP MPLS VPN TE and DiffServ [24] [25]. Different service models are provided for user services to ensure

QoS according to users' requirements and the quality of the network. There are different ways used to guarantee the QoS in VoIP networks. e.g traffic classification, traffic policing, traffic shaping, congestion management, congestion avoidance, resource reservation protocol, and link efficiency [1], [11], [25] [26].

2.2.1 Basics of VoIP Technologies

VoIP creates a way for computer networks and other devices to replace traditional phones and phone lines. PBX systems have already transformed into VoIP systems. In the future, legacy phone lines (PSTN or POTS) would not be available, and VoIP is the only the best choice for all customers throughout the world. VoIP can be given by an ISP and an end-user who subscribed for this service should have used or experienced on IP phone, or free IP phone software working with a Personal Computer [27].

VoIP allows users to make or receive a call from or to its telephone to telephone or personal computer (PC) to the personal computer (PC) or telephone to personal computer (PC) and vice versa communication by using IP network or internet [28]. During VoIP user call to another end user by using the ISP network there is a process that should be followed to improve the QoS and the success of clear or visible communication among end-users. The communication of process VoIP call session started by the converting of the guest's analog speech signal into a digital setup (zero's or ones), next Compression, and converting of zero's or ones into discrete Internet Protocol packets, then propagate the packets through the Internet and finally Reverse conversion of packets into an analog speech signal for the call receiver [5] [29]. VoIP comes up with allows different benefits for internet service providers and customers. Some VoIP applications or benefits are Phone portability Integration and collaboration with other applications, Provision of new communication services, Cost savings, Service mobility. Even though VoIP service has more applications and Benefits, it indirectly impacts and Quality of service (QoS) issues [30].

2.2.2 VoIP Protocols

The utilization of VoIP service needs a signaling protocol to create sessions from source to destination, and it needs a unique protocol that transports continuous data or packets. The usual protocol is used to transport continuous data or packets between two terminals of a recognized session. Globally VoIP has used two well-known protocols, these are signaling and media transfer protocols. These protocols simply enable two or more devices to send and accept real-time audio traffic which allows their callers and receiver to communicate [30]. When an IP network is combined with the following protocols and quality of service model it can support real-time services. These protocols can be Resource Reservation Protocol (RSVP)**,** Real-time Transport Protocol (RTP), and Real-time Control Protocol (RTCP), Differentiated

Services. It is known that the normal Internet uses TCP or IP whereas VoIP uses RTP, UDP, and IP [31]. Transmission Control Protocol or Internet Protocol (TCP or IP) is Non-Real-Time Transport Protocols. IP is a connectionless best-effort network communications protocol; TCP is a reliable transport protocol that uses acknowledgments and retransmission to guarantee packet delivery. TCP IP Offers a consistent connection-oriented network communications protocol suite. Generally, TCP or IP is not appropriate for real-time communications, such as speech transmission since the acknowledgment can lead to being extreme delays [31]. UDP: Universal Datagram Protocols. It is a Non-Real-Time Transport Protocol that delivers an unreliable connectionless service to transport messages from source to destination. UDP is suitable for VoIP or real-time speech transmission but or communications, but if combined with RTP it ensures end-to-end network packet transporting functions for VoIP applications packet transmitting services like audio and video, over unicast versus multicast network services [30] [31]. RTP Protocol: Most VoIP systems depend on the use of the Real-Time Transport Protocol for packet propagation at a time VoIP conference. Even if a Real-Time Protocol cannot reserve resources and not ensure the quality of service in VoIP communication. RTP Well-defined in RFC 3550, is a consistent packet format for transporting audio and video over IP networks with the help of UDP.RTP protocols are used for Audio and Video transmission in multicast and unicast atmosphere [32]. There are two types of real-time protocols used for VoIP communication are RTCP and SRTP Protocols. RTCP works with RTP protocol and the combination of both multimedia data is transported between the parties are a sender and the receiver. VoIP offers RTP or UDP or IP packets regardless of packet loss or delay until the arrives receiver device. It uses to provide feedback on services, like QoS provided by RTP. Packet differentiation being transmitted is done through ports. RTP is comely used in IP telephony and contains information like Contents of the message, Sequence number, Jitter, and Monitoring Timely Delivery [32]. Security Real-Time Protocol (SRTP) defines a security profile of RTP, proposed to deliver authentication, confidentiality, and integrity of RTP messages. Since RTP is used to connect with RTCP and SRTP used for the session. [31] [32]. IP RTP header compression reduces the 40-byte IP, UDP, and RTP header to 2 to 4 bytes, thereby degrading the bandwidth obligatory per voice call on point-to-point links. These techniques used to compress the header at the source of the link and decompressed at the destination point are known as compressed RTP (cRTP). Since cRTP are dependent on CPU-intensive, then you must bound the number of compressed flows to increase the router performance or reduced the degradation capacity of the router. Compressed RTP is suggested on low-speed links in which the amount bandwidth is limited and there is only a few VoIP calls. VoIP Signaling Protocols cover both abstract notions, quality, and network equipment configuration or administration seen as the signaling protocol. The signaling protocols used in the designing of client-server VoIP systems: SCCP, H.323, MGCP, or SIP and IAX [30] [33]. H323: it is the first signaling protocol officially used to be designed for VoIP systems combined with RTP protocol.it is invented by the International Telecommunication Union, which has different versions of protocols like H225, H245, and H235. H.225 describes call setup messages and procedures, used for user's registration, or to establish a call [33]. Session Initiation Protocol: it is the most well-known and current VoIP signaling protocol. It works on the application layer combined with Session Description Protocol which recognizes and transports the voice, the video then finally forwarded to SRTP [33]. Inter-Asterisk Exchange (*IAX*): Currently the most implemented methods for the integrating of a VoIP application system. When compare with H323 and SIP protocols it is only restricted to signaling activity, It guarantees signaling and media transmission in an IAX-based VoIP application system. IAX has a suite of security services and allows message authentication, confidentiality, supports NAT traversal [33].

2.2.3. VoIP Architecture

Nowadays VoIP technology comes up with different features and architecture .it can be designed and deployed based on management. These are the most well-known architectures, which can be centralized or distributed [33]. Selection of Architecture for deployed Voice over Internet Protocol service into Enterprise or ISP network is based on the selection of signaling protocols. Generally, there are two types of VoIP Architecture are   Peer-to-peer and a client-server model [34].

The most popular Voice over Internet Protocol is connected by a client-server centralized architecture. A client-server VoIP system like that used in traditional telephony and depends on the set of interconnected central servers like proxy servers, or soft switches and gatekeepers. The central servers are accountable for centralized call processing components, call control, users' registration; establish VoIP sessions between registered users. The client-server model has the following benefits. It allows unified administration and service, call management; It simplifies call flows for emulating legacy voice structures; It minimizes the total of memory and CPU usage on the phone, and It is simple and understood by legacy voice engineers [33], [34]. Each central server handles registers, which establishes a session with local or distance customers. All customers should be recorded on the main servers or registrar server to communicate with other registered customers. A customer gets privilege only by the main server. Here some examples of client-server: protocols MGCP and SCCP [35].

Media Gateway Control Point **(**MGCP) is the updated protocol when compared to H.323, SIP, and not widely implemented. It includes media gateway controllers (MGCs).it is known as call agents, which perform the entire call connection and control within an MGCP network. These MGCs signal and control media gateways (MCs) to link and regulate VoIP communication. MeGaCo needs different improvements and features that MGCP cannot have, such as interoperability with IVR applications as well as the capability to cooperate with non-VoIP networks [35]. Peer-to-peer model This model allows network intelligence like call state, calling features, call routing, provisioning, billing, to be distributed between the endpoints and call-control components. The endpoints can be VoIP gateways, IP phones, media servers, or any device that can initiate and terminate a VoIP call. The peer-to-peer model has advantages of flexibility, scalability, and easily understood by engineers who are accustomed to running IP data networks. SIP and H.323 are examples of peer-to-peer protocols [4] [21] [36].

Session Initiation Protocol (SIP) was invented by IETF for VoIP connections and implemented by many Internet service providers for call session management and provides functions like a fixed telephone with all value-added service. SIP is work on application-layer control protocol to initiate, modify, and terminate sessions between endpoints for internet calls. The SIP architecture is the same as web and Mail Protocol, a client sends its needs to the server, and then the server internalized the client's need and forwards the response back to the client. SIP allows multicast conferences by inviting and inviting members to the meetings [4] [6] [36]. SIP allows users mobility, name mapping, redirection services and works with both versions of IP which give different security services, like integrity prevention, authentication, encryption, and privacy services. In Addition to security services SIP provides the following Functionalities: r a session User location, User capabilities, User availability, the session setup establishes the session parameters for both parties involved in the session, Session management, SIP Network Elements, and SIP servers [4] [6] [21] [36]. SIP Operations: during user communication, both agents are identified by SIP addresses. For the call arrangement, the caller locates a server and directs an application to the server. An invitation is the most common SIP operation. Instead of a direct connection to the end-user, SIP requests may be triggered by proxies. Customers register their locations with SIP servers [6],[36]. SIP Interworking: The gateway router allows communication with the SIP network of PSTN using signaling system seven (SS7) protocol. SIP devices allow to make and receive calls from the PSTN or POTS network, whether wired or cellular. In this case, both the SIP channel and the RTP sessions are made to a server at the ISP, and the provider acts as a gateway for the voice call to the “legacy network” [26],[36]. Generally, Session Initiation Protocol has the following most essential Benefits: Extensibility, Modularity, Simplicity, Scalability Integration, and Interoperability [35],[36].

2.2.4. VoIP Audio Codecs

VoIP Audio codecs play a very important role in VoIP performance and QoS. There are three types of audio codecs: Waveform codecs, parametric codecs, and hybrid codecs. Waveform codecs shape the original message by digital values, resulting in a high-quality performance for high bit-rate coding. One example of this is Pulse Code Modulation (PCM) [3] [37]. Audio codecs are allowed to encode and reduce analog flows (voice or video) into digital signals transmitted across an IP network. As a general is good, if bandwidth allows, it is best to use a single codec throughout the network to minimize the necessity for transcoding streaming signal, [18] [38]. The audio codec has the following characteristics: it can be narrowband or wideband. Narrowband refers to the fact that the audio signals are passed in the range of 300-3500 Hz. In the case of a wideband, the audio signals are transmitted with the range of 50 to 7000 Hz. Therefore, a wideband codec is good for audio with richer tones and better quality [26] [38]. The sampling rate or frequency is the number of samples taken per second, defined in Hz or kHz.the sampling rates of digital audio can be narrowband, wideband and ultra-wideband it ranges from 8, 16, and 32 kHz respectively. For digital video, typical sampling rates are 50Hz, which is Phase-Alternating Line, PAL, used largely in Western Europe, and 59.94 Hz (for National Television System Committee, NTSC, used largely in North America) [26] [38]. The compression ratio shows the comparative variation between the initial size and the condensed size of the audio or video flow. Lower compression ratios give up improved quality but need bigger bandwidth. In general, lower-condensed codecs are suitable for voice-over LANs and qualified and helpful for DTMF and fax. High-compression codecs are better suited for voice-over WANs. The complications refer to the amount of processing required to perform the compression [26] [38]. Codec complexity reduced the number of calls reconciled on the DSPs. With higher Codec complications, fewer calls can be managed. The general order of the fixed-rate codecs listed in the table, from best to worst performance in tandem, is G.711, G.726, G.729e, G.728, G.729, and G.723.1 [31] [38]. Since Ethio Telecom uses an SS7 signaling protocol. ITU Recommended G.722 for VoIP Speech CODEC and Compression.G.722 is the well-known encoder for calls that are categorized as “HD Voice” in the VoIP world. All Comrex codecs and VoIP devices support G.722 [18] [38]. The researcher uses VoIP networking technology (BGP MPLS VPN and DiffServ because they avoid excessive network congestion.) instead of G.722 which is similar services. Table3: Correlation between R factor and MOS R-Factor Quality of voice rating MOS [8] [38].

Table 2.1 ITU’s G.114 Recommendation for VoIP Delay evaluation using MOS versus R-Factor [39].

R-Factor	**Quality of voice rating**	**MOS scale**	**MOS Values**
90 < R < 100	Best	5	4.34 - 4.5
80 < R < 90	High	4	4.03 - 4.34
70 < R < 80	Medium	3	3.60 - 4.03
60 < R < 70	Low	2	3.10 - 3.60
50 < R < 60	Poor	1	2.58 - 3.10

2.2.5. Mechanisms to Improve VoIP QoS

Different multimedia applications such as video streaming, VoIP, and video conference have got higher demand and create enormous congestion on the IP networks. In the IP networks, With the advent of multimedia applications create higher bandwidth consumption has become a serious issue between the Internet Society and Internet providers. The current multimedia applications and services have problems of bandwidth requirements QoS assurances, like end-to-end delay, jitter, and packet loss likelihood. These QoS requirements problems create new challenges in the Telecommunication industry [27][39]. The Internet Engineering Task Force (IETF) has proposed various standards to attain the quality of service in the IP networks. These include the MPLS Network and Differentiated Services where several Requests for Comments (RFCs) for these services and interoperability [6] [39]. In the following sections, the MPLS VPN Network, and Differentiated Services architectures, with operational behavior, interoperability is explained, to improve the quality of service (QoS) of VoIP service requirements [32] [39]. Quality of service (QoS) is the skill of delivering enhanced services to voice traffic using dissimilar technologies like BGP MPLS VPN etc. The main purpose of QoS is to give the first rank for voice traffic over data (email, FTP, HTTP) i.e., to take into consideration Jitter, Latency, data Packet Loss, and Burst of Jitter and minimize all factors for that flow. The QoS is considered to prioritize one traffic flow, but not to make another traffic to be failed. QoS of all service is tolerable when it satisfies SLA and leads to proper customer satisfaction [1], [32] [39]. Since VoIP is operational on Layer two and three protocols. As a consequence, the investigator used BGP MPLS VPN and Differentiated Services (Multiprotocol Label Switching & Differentiated Service) technology to maximize VoIP QoS for proper network traffic administration, diminish cost and install an efficient, consistent, and scalable private network. many ISP Connecting enterprises to remote locations, customers, and vendors via the MPLS

[40] The differentiated services have the problem of poor end-to-end QoS guarantees. In general, differentiated services treated traffic based on the class of service not on a per-flow. The differentiated services field replaces the TOS field in the header [32] [40]. According to network quality and user requirements, QoS provides end-to-end services for customers via diverse QoS service models. These models are the Best-effort, integrated service, and differentiated service model. In addition to QoS service models, there is another technique to guarantee the QoS for VoIP service such as traffic classification, traffic policing, traffic shaping, congestion management, congestion avoidance, resource reservation protocol, and the link efficiency mechanism. Although QoS service models are combined with networking technologies like BGP MPLS VPN, and DiffServ-for further guarantee the QoS of VoIP [1], [11], [25] [32], [24], [41]. Explained theory of a service architecture model where part of the underlying technology used for IP transport is MPLS -Diffserv, traffic engineering .generally they conclude that MPLS -DiffServ is simpler and more scalable than IntServ with Standard RSVP [42].

2.2.6. Border Gateway Protocol (BGP)

BGP is the recent Internet direction-finding protocol that is used to exchange network layer reachability information (NLRI) among routing domains or autonomous systems. BGP version 4 (BGP4) is the de facto direction-finding protocol. BGP is today's Internet routing protocol, because of its capability and nature of Reliability, Stability, Scalability, and Flexibility [43].

BGP work with three well-known protocols (Internal Routing Protocols (IGPs), internal iBGP, and External eBGP) to carry or Exchange prefixes. iBGP is used to carry: Some or all Internet prefixes through backbone and Customer prefixes. eBGP is used to Exchange prefixes with other AS Implement routing policies. Internal Routing Protocols: IGPs uses other link-state protocols like ISIS OSPF) Used for carrying infrastructure addresses. IGP is not used for carrying Internet prefixes or customer prefixes. IGP is to minimize the number of prefixes that support scalability and rapid convergence [44].

BGP works as an inner AS protocol that operates on TCP for connection-oriented transmission and higher reliability. It works through TCP port 179, which delivers support in route aggregation and classless inter-domain routing. TCP can create a connection among diverse two routers with internal and external AS to deliver a reliable conversation of routing tables and their updates stored in the routing information base (RIB). BGP has a constant 152-bit message header, which encompasses four message types i.e., Update, open, keep-alive, and notification messages: only keep-alive message provides automatic message requests [43],[44]. Tag Switching was explored in 1996, which was starting to evolve when Cisco Calls a BOF at IETF to Standardize Tag Switching and finally MPLS Group Formally Chartered by IETF Proposed MPLS in 1997.MPLS was proposed by IETF in 1997 to improve the scalability of network-layer routing, provide routing flexibility, increase network performance, and simplify the integration of equipment using non-IP forwarding paradigms [39], [45]. MPLS can create mechanism of high-performance carrier networks that transport traffic from one network end to the next end based on labels rather than long network addresses and avoiding complex lookup in the routing table.

MPLS can compress packets of diverse network protocols, and support dissimilar access technologies like STM- 64,10GE, T1/E1, ATM, Frame Relay, and DSL [39], [45]. Previously frame relay uses frames while ATM uses cells to map labels, to label switching techniques, frames cannot be of fixed length while the cells consist of fixed length with 5 bytes of header and 48 bytes of payload. ATM and frame relay are identical in a way when label traversing each hop in the network causes the label to change the header value [45]. MPLS is a developed technology for delivering reliable services through fastmoving network traffic and quality of service by using DiffServ-MPLS that enables us to deliver voice over IP (VoIP) over reliable transmission [32] [45]. know days there are Four major technologies that allows as to make possible to build MPLS-based VPNs:

- Multiprotocol Border Gateway Protocol (MP-BGP) carries routing information from PEs to CE.
- Route filtering based on the VPN route target extended MP-BGP community attribute.
- MPLS forwarding carries packets between PEs (across the service provider backbone).
- Each PE has multiple VPN routing and forwarding instances (VRFs).

MPLS routing process performed by using two routers. These are edge routers, which is the border of the MPLS domain and core routers. The routing decisions are made only at the edge routers and the core routers forward packets based on the labels. These two functions provide a fast-forwarding method of packets. The core router then swaps the label with a new label and sends the packet to the edge router. The edge router performs routing lookups and removes the label and sends it to the destination as a simple IP packet. The packet goes through the path called the Label Switched Path (LSP) [16], [21] [32], [45]. MPLS “Shim Header” is located and works in between layers L2 and L3 OSI model protocols. It is integrated into four parts has an overall length of 32 bits; 20 bits for Label, 3 bits for Experimental (EXP), 1 bit for Bottom of Stack, and 8 bits for Time to Live (TTL). Data packets when arrives at the LER. MPLS Shim Header is integrated into four parts has an overall length of 32 bits: 20 bits for Label, 3 bits for Experimental (EXP), 1 bit for Bottom of Stack, and 8 bits for TTL [46].

MPLS-enabled routers might need to insert multiple labels to send packets through the MPLS network. To determine which label is the last in the packet, a bottom of the stack (BoS) bit is used, if the bit is 1 it means that it is the last label. The last 8 bits are used to time to live (TTL) they have the same function as the usual IP header [32], [47]. Generally, in an MPLS network, incoming packets are assigned a "label" by an “LER or label edge router”. Packets are forwarded along a "label switch path (LSP)" where each "LSR (label switch router) or core routers” makes forwarding decisions [32] [47].

A shim header is located between the link header and the network header to transport the labels [58]. The MPLS architecture is split into two separate components: the forwarding component (data plane) and the control component (control plane) [12], [16], [21], [32], [48]. The control plane is accountable for creating, maintaining, routing, and labeling information exchanges with the connected or adjacent routers. The signaling plane allocates the transfer information. It uses Link state or Unicast routing protocols (OSPF, IS-IS, and BGP) to advertise routing information among the routers which are not necessarily adjacent, whereas label binding information distribution is limited to adjacent routers. It maintains the content of a label switching table is LFIB [12],[21],[49].

MPLS architecture consists of MPLS routers connected through mesh topology. MPLS infrastructure network consists of Ingress or Egress and Intermediate Label routers [39]. Ingress/Egress LSRs deployed at the border of the MPLS network which provides an interface to inside the MPLS domain and to outside the IP network [43] [49]. The role of ingress/egress LSR is to insert and remove labels when deployed as ingress and egress. An ingress LER inserts label on the data packet called imposing LSR and forward it towards egress LSR after passing through several hops where egress LSR removes the label called disposing of LSR and forwards it towards the data link. These two routers (Provider and Edge Routers) [32] [43] [49]. Intermediate LSR is devices present in the MPLS domain to perform swapping, push, and pop operations of incoming and outgoing packets towards ingress/egress LSRs. They receive incoming label packets swap, push and pop labels perform packet switching, and forward it towards the correct data link. The packet forwarding mechanism is based on information present at each label [32]. MPLS is completely dependent on Cisco Express Forwarding (CEF) to determine the next hop. Previously Cisco used Multilayer switches which contain both a switching and routing engine. Multilayer switches can route once; switch many is called NetFlow switching or route-cache switching [32] [49]. Finally, cisco replaced NetFlow multilayer switching with a more advanced method called Cisco Express Forwarding. CEF contains two basic components: Layer 3 Engine: Builds the routing table and then “routes” data Layer 3 Forwarding Engine: “Switches” data based on the FIB [21] [32] [49]. The Layer 3 Engine builds its routing table using either static or dynamic routes learned through a routing protocol (such as RIP or OSPF). The routing table is then reorganized into a more efficient table called the Forward Information Base (FIB). FIB contains the information of Destination networks, Destination masks, Next-hop addresses, and The MAC addresses of each next-hop or Adjacency Table [21] [49].

MPLS Control plane generally exchanges Layer 3 routing information and labels, and also uses a different routing protocol to exchanges information such as Open Shortest Path First (OSPF), IS-IS, Border Gateway Protocol (BGP) and also defined a new set of signaling and routing protocols such as Label Distribution Protocol or Tag Distribution Protocol (LDP/TDP), Multiprotocol Border Gateway Protocol (MP-BGP), Resource Reservation Protocol(RSVP), RSVP-TE, Constrained Routed- Label Distribution Protocol (CR-LDP), etc. [21] [49]. To fully extend the capability of MPLS, engineers are developing new standards such as Virtual Private LAN Services (VPLS), Hierarchical Virtual Private LAN Services (HVPLS), and Generalized Multiprotocol Label Switching (GMPLS). MPLS has traffic management and QoS mechanisms (such as traffic policing, congestion management, traffic shaping, and priority queuing) to manage traffic flows. MPLS increases network speed, supports scalability, QoS management, and traffic engineering. MPLS provides data, voice, and video over the same network [21] [49]. Data Plane: Forwards packets based on labels, it contains the information required to transfer a packet, the plane has a simple forwarding mechanism, it is independent of the control plane and Use LFIB to forward packets based on labels [12] [21],[47], [50].MPLS uses labels to transfer the packets to improve packets forwarding speed, and it supports the ability to control traffics and to override several boundaries such as high packet loss and extreme delay in the network [51].

2.2.7. MPLS Network Applications

The number of services and applications which deploy in the MPLS network can support virtual private networks, Quality of service, Traffic engineering, MP-BGP, protocol-independent and allows for creating end-to-end circuits across any type of transport medium using any protocol. MPLS Traffic Engineering (MPLS-TE): customized link-state routing protocols (IS-IS or OSPF) are used to discover resources and distribute attributes in the network. Control processes the FEC binding through RSVP, and FIB is modified based on MPLS labels [51]. MPLS-TE provides control of traffic routing and optimized network utilization. MPLS VPNs: FIBs are created for one or more VPN clients. The customer routing information and MPLS labels are distributed by Multiprotocol BGP (MBGP) across the network [21] [51]. Layer 2 VPN: It can be created via a Layer 2 circuit over MPLS, known as Any Transport over MPLS (AToM). It provides auto-configuration, management and QoS are the Layer-2 VPN services. Layer 3 VPN: BGP is used for Layer-3 VPN in the service provider’s (SP) network, and IP routing or static routing protocols are used between SPs and clients. MPLS QoS: provides a mechanism for differentiated service that enables the creation of LSPs with guaranteed bandwidth [21] [51]. In ATM networks, four labels are assigned to each IP prefix by customized LDP that enables different QoS classes for each label. There are different technologies for a base of MPLS applications and services, such as Layer 3 VPNs, traffic engineering, differentiated services, and Layer 2 VPNs. Multicast, IPv6, and GMPLS. There are different MPLS applications incorporated into the common structure and they might have their own set of characteristics. The LSRs can integrate with new MPLS applications without affecting the existing services by sharing common LFIB [21] [51].

2.2.8. Virtual private network (VPN)

Most of the traditional private network requirements are the following requirements: Security, Availability, QoS, Reliability, Compatibility, and Manageability [21] [52]. The main VPN objective is to address three basic requirements that are as follows: Anytime access to the network resources for remote and mobile users, interconnectivity between remote offices, and Controlled policy to access necessary network resources [21],[32] [52]. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. VPN technology was developed to allow remote users and branch offices to securely access corporate applications and other resources. To ensure safety, data travels through secure tunnels and VPN users must use authentication methods- including passwords, tokens, and other unique identification methods to gain access to the VPN [21] [52]. VPN creates a private network over an infrastructure. Essentially, VPNs provide a transparent network infrastructure that allows multiple customer sites to communicate over a shared backbone network, as though they are using their private network, regardless of geographical location. Most probably each small company has one VPN network and if there is a large company then there may be more than one VPN network and these VPNs are mostly connected in the ISPs [32] [52].

VPN requires Internet connectivity and if it is connected to MPLS VPN it provides internet by default. ISP has gained the most benefit from VPN service and application service given to its enterprise customer. Typical applications that run across organizations' VPN include corporate Intranet, mail services, and VoIP telephony. VPNs can be classified into two which are IP-based VPN and MPLS-based VPN [32], [34], [21] [52]. VPNs can be classified in a variety of ways. The more detailed VPN classification focuses on the underlying technology that is used to transport Layer 3 packets over the VPN [52]. There are also three different situations of ISP provide can be secure VPN communication solution among its central and branch office of the different organization [32] [52].

Intranet-Based VPN service: Intranet VPNs are used to provide interconnectivity between remote offices of an organization. Extranet-Based VPN service: This type of VPN allows controlled access to necessary network resources to external suppliers. Remote-Access VPN service: It can provide anytime access to the network resources for remote and mobile users. Components of RA-VPNs: Remote Access Servers (RAS), Dial-up connection, Support person, responsible for configuration, maintaining, and managing

RAS [21] [32], [52]. There are Three major VPN tunneling protocols and models or are prominently used to enable site-to-site and remote access VPNs to ensure the safety aspects of VPN-based transactions. These protocols are Protocols for Site-to-Site and Remote Access VPNs [21] [52]. In site-to-site VPNs, data traffic is tunneled between CE or PE devices**.** Protocols used to enable site-to-site VPNs to include IP Security (IPsec), Point-to-Point Tunneling Protocol (PPTP), Generic Routing Encapsulation (GRE), Layer 2 Tunneling Protocol (L2TP), Layer 2 Tunneling Protocol version 3 (L2TPv3), and IEEE 802.1Q tunneling (Q-in-Q) and MPLS Label Switched Paths (LSP) [21] [52]. Protocols used to enable remote access VPNs to include Layer Two Forwarding (L2F), Point-to-Point Tunneling Protocol (PPTP), IP Security (IPSec), Layer 2 Tunneling Protocol versions 2 (L2TPv2) and Layer 2 Tunneling Protocol versions 3 (L2TPv3) and Secure Sockets Layer (SSL)[21] [52] [53]. The other point is about VPN Blocks' based solution has a framework of six fundamental elements. These elements are listed below VPN hardware: VPN servers, VPN clients, VPN routers and VPN Gateways, VPN software: Server and client software and VPN management tool, Security infrastructure: RADIUS, TACACS, NAT, and AAA-based solutions, ISP supporting infrastructure: Service provider's network access switching backbone and ISP network Internet backbone, Public networks: Internet, PSTNs, and POTS and Tunnels: PPTP and L2TP and L2F [21] [52] [53]. VPN Architectures can be divided into four main categories according to the security requirements of the setup, and into two groups depending on the layer of the OSI model, and into five classes depending on the scale and the complexity of the VPN setup. Generally Based on VPN requirements by the service provider or subscriber, VPN architecture can be classified as follows Implementer-base VPN Architecture, Security-base VPN Architecture, Layer-based VPN Architecture, and Class-based VPN Architecture [21] [52] [53].

2.2.9. Multiple Protocol Label Switching - Virtual Private Network (MPLS VPN)

Nowadays, MPLS VPN is becoming a popular technology that replaces Layer 2 technology like ATM or frame relay, IPV4, IPV6, PPP, and Ethernet networks for WAN system [48], [51] [53]. MPLS is a non-destination-based forwarding strategy used to forward IP packets. Forwarding is done by a Label Switching Router that performs a match on a label associated with a packet in an MPLS domain [53].

Despite ATM services, frame relay, Ethernet is old protocols, which are very reliable technology at a time before the invention of MPLS Virtual Private Network [32] [53]. MPLS Virtual Private Network is known popular and most widespread implementation in WAN technology. MPLS VPN is the best network solution for the WAN connection among the different ISP Brach and remote. MPLS VPN provides simplicity, network scalability by dividing the networks into subparts and provides security in the way of VPN technology [32], [53]. There are different MPLS VPN models used to interconnects customer sites through the common ISP network infrastructure. ISPs can deploy either overly VPN models or peer-to-peer VPN models. Generally, there are three MPLS VPN models are below: Peer-to-Peer VPN Model: ISP provides point-to-point virtual circuits' links between customer routers at the desired location. ISP is unaware of customer routes due to direct peering routing between customer routers. ISP routers participate in customer routing at layer 3. Overlay VPN Model: can be implemented through the IP network or frame relay switches at either location implementing the tunneling mechanism. Optimal Traffic Flow Model. Nowadays three major classes of MPLS-based VPN networks are Layer 3 VPNs, Layer 2 VPNs, and Virtual Private LAN Services [32], [53].

2.2.10 Blocks of ISP MPLS VPN Architecture

MPLS VPN Building blocks at Provider edge routers are Virtual Routing Forwarding (VRF) Route Distinguisher (RD).and Route Targets (RT) [32], [47], and [50] Virtual Routing Forwarding (VRF): Virtualization is a technique for hiding the physical characteristics of computing resources from how other systems, applications, or end-users interact with those resources. A virtual network is a generic term that uses many different technologies to provide virtualization [54]. There are different types of virtualization occurs in different network layer this includes [54]:

- ❖ Physical (Layer 1): A Time Division Multiplexer (TDM) allows making a single physical connection look like many physical connections and maintaining separation.
- ❖ Datalink (Layer 2): Frame Relay, Asynchronous Transfer Mode, and Ethernet switch all show how a single physical link may provide multiple logical or virtual connections per physical connection.
- ❖ Network (Layer 3): Routers show how multiple sessions can be carried over a single connection using IP addresses as the identifier.

Virtual Route Forward (VRF) is a technique that creates multiple virtual networks within a single network entity. Virtual Route forward is Layer 3 virtualization and implemented on the PE router. In a single network component, multiple VRF resources create isolation between virtual networks [54]. A Virtual Routing Forwarding is the instance of the VPN forwarding table. It is the combination of three routing table, which are given below [32], [54]:

- ❖ VPN Routing table.
- ❖ VRF Cisco Express Forwarding table.
- ❖ PE router has an IP routing table.

Route Distinguisher (RD): A route distinguisher is an address qualifier used only within a single internet service provider's Multiprotocol Label Switching (MPLS) network. It is used to distinguish the distinct VPN routes of separate customers who connect to the provider [32]. When VPN prefixes passing through the MPLS VPN network through the multiprotocol BGP then in case of ISP is concerned it should be unique in case of IPV4 IP addressing if there is an overlapping IP is used at the customer side then the problem comes so, to solve the problem by using RD [54]. The main task of the RD is that it generates a unique IPV4 IP in the ISPs and there will be no overlapping IP problems come [32], [54]. Route Targets: In the case of RT mechanism, there is some restriction among the different MPLS VPN network that one VPN communication with the other or which one is not to solve this kind of problematic scenarios RT came in into being to solve the issue regarding process among the VPNs network [32].

2.2.11 MPLS and VPN network

MPLS VPN has four Classes of Service (CoS) to support QoS: Gold, Silver+, Silver, and Bronze: Gold: it supports Real-time packet forwarding designed to meet delay-sensitive application requirements – e.g. VoIP and videoconferencing, Bronze support The standard level of performance for normal applications – e.g. email, file transfer, and intranet, Silver support Assured Level of performance with packet-loss commitments for business-critical applications – e.g. SAP, SNA, Oracle and Telnet. , Silver+ supports an Assured Level of performance with packet-loss commitments for mission-critical applications – e.g. streaming video and signaling [55].

2.2.12. MPLS VPN Security Concern

Security Association states “MPLS VPN Security is establishment secured connection between the two networks by using security attributes like cryptographic keys, digital certificates so that secure communication achieved”. To manage all security attributes, security information is grouped logically. This logical group itself is a Security Association. Security Association is identified with three parameters which are given below [32] [55]. Security Parameter Index (SPI), IP destination address, and Security Protocol Identifier. The internal structure of the MPLS core network (PE and Provider router devices) should not be visible to outside networks (either the Internet or any connected VPN). While a breach of this requirement does not lead to a security problem itself; it is generally advantageous when the internal addressing and network structure remains hidden from the outside world [32] [50]. In a VPN-only MPLS network (no shared Internet access), this is equal to existing Layer 2 models, where the customer must trust the service provider to some degree [32]. MPLS VPN network has a higher Advantage over the other technologies [50].

2.2.13. MP-BGP MPLS VPN

Multiprotocol BGP (MP-BGP) is used to distribute VPN routes to other PE devices across the SP network. Since VPNs can use Overlapping address spaces, BGP may determine routes to destinations with the same address prefix [35] [56]. BGP MPLS VPN stands for Border Getaway Protocols Multi-Protocol Label Switching Virtual Private Network. BGP MPLS VPN layer 3 virtual private networks (L3VPN). It uses the BGP to advertise VPN routes and uses MPLS to forward VPN packets on backbone networks [57]. The BGP MPLS VPN model consists of the following routers: Provider (P), Provider Edge (PE), and Customer Edge (CE) routers. Between two internal border gateway protocols (iBGP), a route reflector (RR) is used to offer an alternative logical full mesh instead of physical full-mesh connectivity to optimize the routes as shown below in Fig. 2.1 [57].

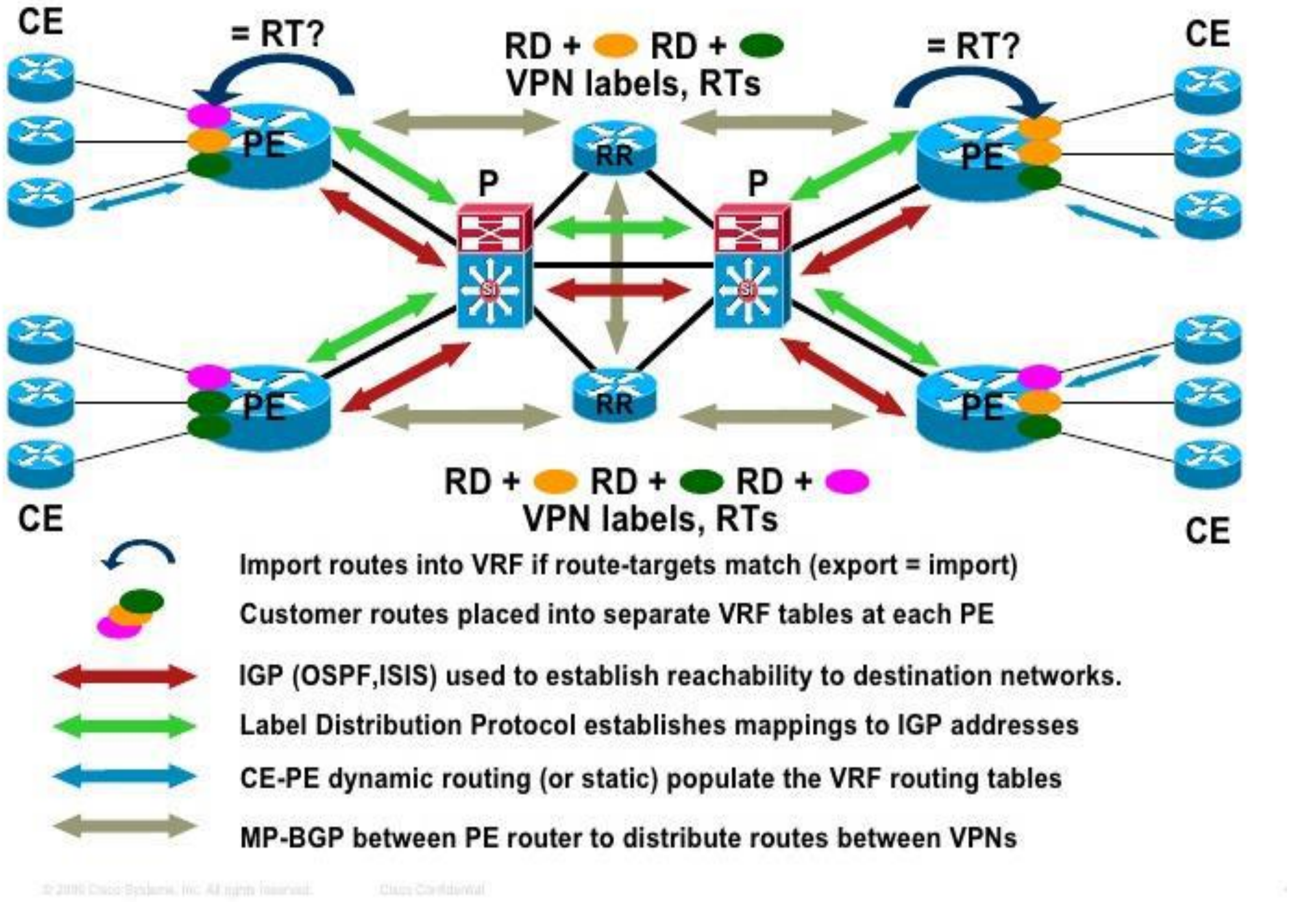

CE
= RT?
RD + ● RD + ●
VPN labels, RTs
= RT?
CE
PE
RR
P
P
PE
PE
RR
PE
RD + ● RD + ● RD + ●
VPN labels, RTs
CE
CE
Import routes into VRF if route-targets match (export = import)
Customer routes placed into separate VRF tables at each PE
IGP (OSPF,ISIS) used to establish reachability to destination networks.
Label Distribution Protocol establishes mappings to IGP addresses
CE-PE dynamic routing (or static) populate the VRF routing tables
MP-BGP between PE router to distribute routes between VPNs
© 2000 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Fig.2.1: BGP MPLS VPN components and working principles [15],[57].

2.2.14. Traffic Engineering (TE)

Know days there are two kinds of Engineering Network Engineering and Traffic Engineering. Network engineering is manipulating your network to suit your traffic. It allows you to make the best predictions you can about how traffic will flow across your network, and you then order the appropriate circuits and networking devices (routers, switches, and so on). Network engineering is typically done over a long scale. Traffic engineering is manipulating traffic to fit the required network [16] [58]. Network traffic will never match your predictions 100 percent. Sometimes, the traffic growth rate exceeds all predictions, and you cannot upgrade your network fast enough. For example, a flash event (a sporting event, a political scandal, an immensely popular website) pulls traffic in ways you could not have planned for. This causes an unusually painful outage of the network or congestion [58]. This is a definition of TE employed by the Traffic Engineering Working Group (TEWG) within the IETF [RFC2205]. “Internet traffic engineering is concerned with the performance optimization of operational networks. It encompasses the measurement, modeling, characterization, and control of Internet traffic and the application of techniques to achieve specific performance objectives, including the reliable and expeditious movement of traffic through the network, the efficient utilization of network resources, and the planning of network capacity”. By performing TE in their networks, ISPs can greatly optimize resource utilization and network performance. The common optimization objectives include [16] [58]:

- Minimizing congestion and packet losses in the network,
- Improving link utilization,
- Minimizing the total delay experienced by packets,
- Increasing the number of customers with current assets.

Congestion is one of the most difficult problems that service providers face in their networks. Two main factors have caused network congestion: Inadequate network resources and unbalanced traffic distribution. Although the problem of inadequate network resources must be solved with new capacity or by reducing and controlling the demands; unbalanced traffic distribution can be addressed through better management of the resources in the network. With carefully arranged traffic trunks, service providers can spread traffic across the network to avoid hot spots in parts of the network [57][58].

The main objective of TE is an efficient mapping of traffic demands onto the network topology to maximize resource utilization while meeting QoS constraints such as delay, jitter, packet loss, and throughput. To do TE effectively, the IETF introduces MPLS, Constraint-based Routing, and an enhanced link-state IGP [16] [57][58]. Generally, rapid traffic growth, application service or VoIP, flash events, and network outages can cause major demands for bandwidth in one place, at the same time you often have links in your network that are underutilized. Traffic engineering, at its core, is the art of moving traffic around so that traffic from a congested link is moved onto the unused capacity on another link.

2.2.15.BGP MPLS VPN, MPLS -DiffServ Aware (MPLS -DS-TE)

Most of the telecom industries have been built their networks based on BGP and MPLS technology as a converged network that able to carry and support different types of traffic such as VoIP, video, and Internet data, therefore it is essential to construct a reliable network that provides guaranteed bandwidth and which can support congestion management mechanism [12] [59]. A reliable network can be developed through the integration of MPLS and DiffServ technologies; the MPLS provides end-to-end connectivity with multiple paths, while DiffServ classifies traffic based on its type [12], [59].

2.3 Quality of Service Overview

Quality of Service (QoS) refers to the capability of a network and networking equipment to provide better service to selected network traffic over various technologies including Ethernet and 802.1 networks, IP-routed networks, Asynchronous Transfer Mode (ATM), and Frame Relay (FR) and IP MPLS that may use any or all these underlying technologies. It can also be interpreted as a method to provide preferential treatment to some sensitive traffic like VoIP (voice or video) [11], [60]. QoS is a generic term. It provides a different level of treatment to the different types of traffic or applications that flow over the network. QoS is required to provide the good management of network resources that makes the sophisticated usage of resources and gives comfort to the network user. Business networks are widely expended with different types of applications. These applications have different network requirements. It needs to lead to different administrative policies that control applications as per their requirements individually [47],[61]. QoS within a network is essential to guarantee the requirements of today’s converged (voice video and data) networks. QoS provides different levels of service for delay-sensitive applications. QoS is to manage the following network elements: bandwidth, buffering, priority, CPU usage, End-to-end delay, end-to-end jitter, and packet loss [47],[61]. End-to-end QoS is like a chain that is only as strong as the weakest link. Therefore, it is essential for enterprises (with converged networks) subscribing to VoIP services to choose service providers that can provide the required SLAs for their converged networks. SLA provides the entire information of all QoS parameters. It defines QoS and parameters. It provides the intelligence to network devices to treat different applications traffic as their defined service level called SLA [50],[61]. For example, these are the end-to-end SLA requirements of voice and interactive video. QoS provides different levels of service for business-critical and VoIP applications. QoS enables the network administrator to manage the following VoIP network elements or parameters [14],[47], [61]. Bandwidth, Delay Jitter, and Packet Loss. To guarantee, these networks must provide perfect service capabilities. QoS is designed to provide a different level of service quality based on different requirements to guarantee users’ requirements for different services.

2.3.1. Bandwidth

The bandwidth is data transmission capacity in bits/second or the amount of data that can be transmitted over the link is bandwidth. The bandwidth of a network path is composed of different LAN and WAN links concerning the bandwidth of the slowest link in the path. The network link with the lowest bandwidth on a network path is often referred to as a bottleneck. Bottlenecks in a network cause congestion which results in QoS problems for voice traffic. Figure 2 presents an example of a network path between two VoIP terminals over an IP network [33], [62]. On the network, IP Packets travel through the best route. The maximum bandwidth of the route is equal to the smallest value of bandwidth on the route. The available bandwidth is the path bandwidth divided by several traffic flows. As a result, Real-Time classes of traffic require special bandwidth provision and consideration. Due to the low bandwidth Real-Time application or VoIP users experience a delay, jitter, and packet loss in the communication [14] [47], [63]. This problem can be solved and improve VoIP QoS by following multiple Mechanisms: Increase link bandwidth or Link capacity increasing, which is effective but costly, Delay-sensitive traffic prioritization by Classify, mark traffic, apply to the queue, and Forward important packet first, finally Traffic compression or Use Compression technique by Layer 2 payload compression, TCP header compression, and compressed RTP (cRTP) are some examples. Usage of hardware compression is preferable over software-based compression because compressions are CPU intensive and create a latency [33], [63].

2.3.2 End-to-end delay

End-to-end delay is the total time that a packet takes from source to destination. There are different types of End-to-end delays in IP networks and those delays are listed below: Network delay, Algorithmic Delay, Serialization delay, Processing delay, Propagation delay, Queuing delay, and Budget delay. Today, many ISPs offer a VPN service with a Service Level Agreement (SLA). An SLA will typically guarantee a certain round-trip delay between sites. As a result, VPN decreases delay when compared to normal connection [14] [22],[33], [63].

2.3.3 Jitter (Delay Variation)

Jitter occurs when the variation in the inter-packet arrival time is introduced by the variable transmission delay over the network. Packets for the same destination may not arrive at the same rate. Jitter can occur due to different traffic loads at different timings. For converged or Real-Time applications like VoIP service, it is crucial to keep the order or sequence of the packets from source to destination to achieve a good quality of voice [11], [63].

2.3.4 Packet loss

IP networks do not guarantee delivery of packets, much less in order. Packets will be dropped under peak loads and during periods of congestion Packet loss occurs due to the low buffer space [51] [41]. When the buffers space of the interface full then packets are dropped. In queue scheduling, packet loss will occur if the queue is exceeded [11][47] [64]. Data Packet loss creates extended delay and jitter.

Packet loss can be controlled by applying some techniques such as tail drop, random early detection, weighted random early detection, and traffic shaping and policing [47] [64].

2.4. Quality of Service and Quality of Experience from the ITU perspective

QoS is not dependent only on the four-pillar bandwidth, delay, packet loss, and jitter. QoS also depends on the end-user perception of Telecommunication services such as trends, advertising, tariffs, and costs which are interrelated to the customer expectation of the QoS. In general, this framework shows how end-user perception reaches the QoS satisfaction level [64].

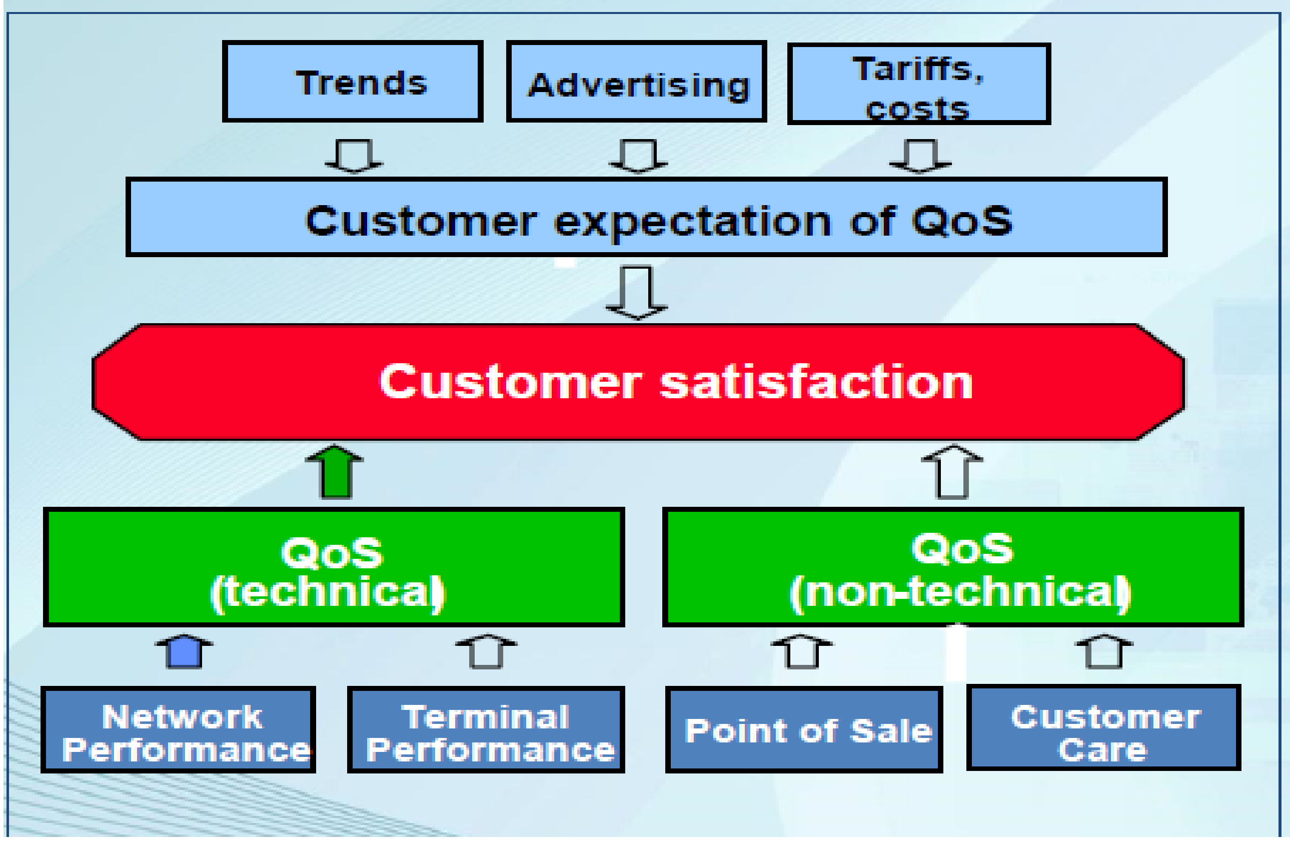


Fig.2.2: User perception of end-to-end QoS delivery framework [64].

User Perception of quality is not limited to the objective characteristics at the man-machine interface. However, the end-users also measure the quality that they experience during their use of a telecommunication service [64].

2.5 QoS framework from Customer's and provider's perspective

ITU-T G.1000 classifies QoS into four from Customer's and provider's viewpoint.

- Customer viewpoints on Requirements and Perception.
- Service provider viewpoints on QoS offered and QoS were achieved.

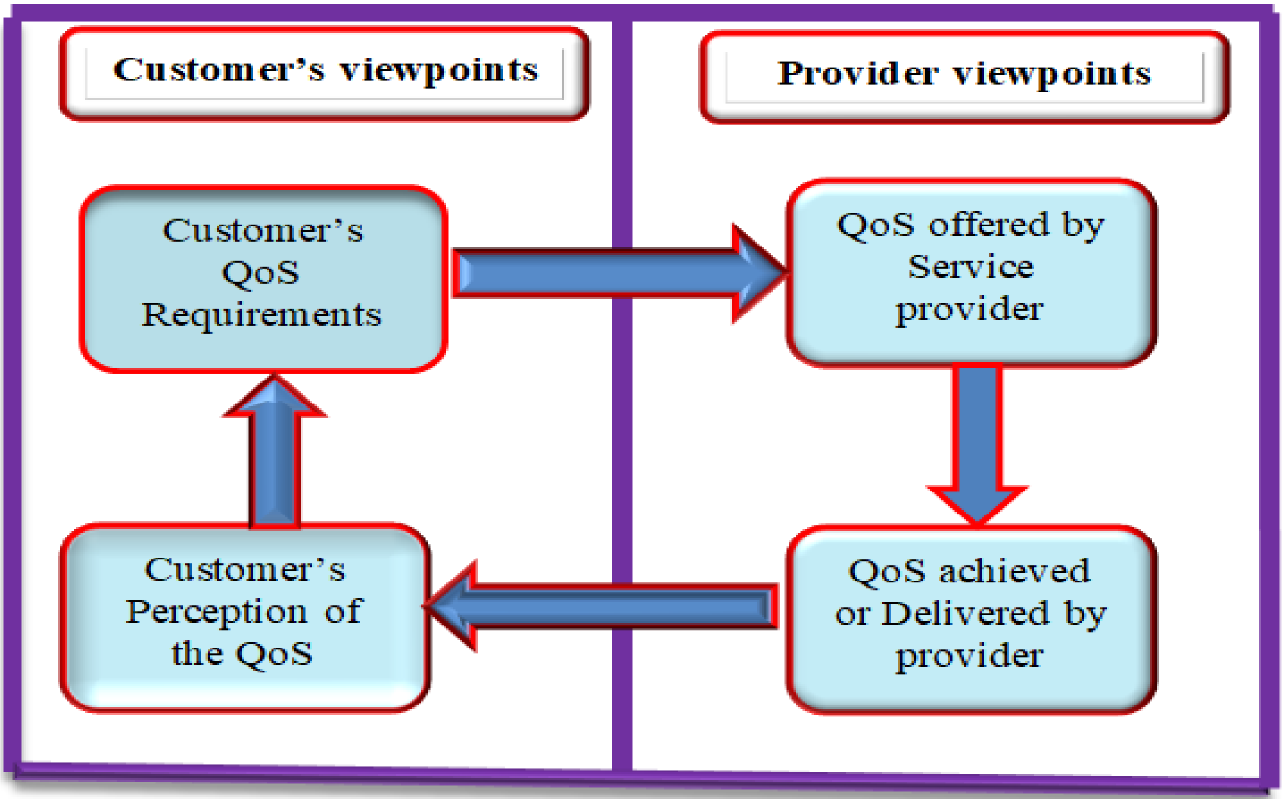

Customer's viewpoints
Provider viewpoints
Customer's QoS Requirements
QoS offered by Service provider
Customer's Perception of the QoS
QoS achieved or Delivered by provider

Fig.2.3: Shows framework for QoS from Customer's and provider's viewpoint [15] [64].

Network QoS is not well defined by itself [64]. It is used with network performance and quality of experience. As a result, the quality of experience impacts QoS and network performance even though end-user subjective [15] [64]. Generally, the researcher concludes that if network performance was well optimized, service provider viewpoints reach a high level and indirectly satisfy the customer QoS requirements or perception. If the Service provider affords quality services to its customers, the customer viewpoint was reached at a high level which increases the quality of user experience.

2.6 ITU-T Y.1541 Recommended QoS Targets

The main goal of this recommendation is to provide direction on the key parameters that affect QoS from the customer perspective. When considering a range of applications involving the media like voice, video, image, and data the parameters that govern end-user satisfaction for these applications and a broad classification of end-user QoS categories are determined [15] [65]. Classification of end-user QoS categories allows for deriving realistic QoS classes and associated QoS control mechanisms for the underlying networks. The user is interested in comparing the same service offered by different providers in terms of universal, user-oriented performance parameters. This implies that performance should be expressed by parameters [15] [65].

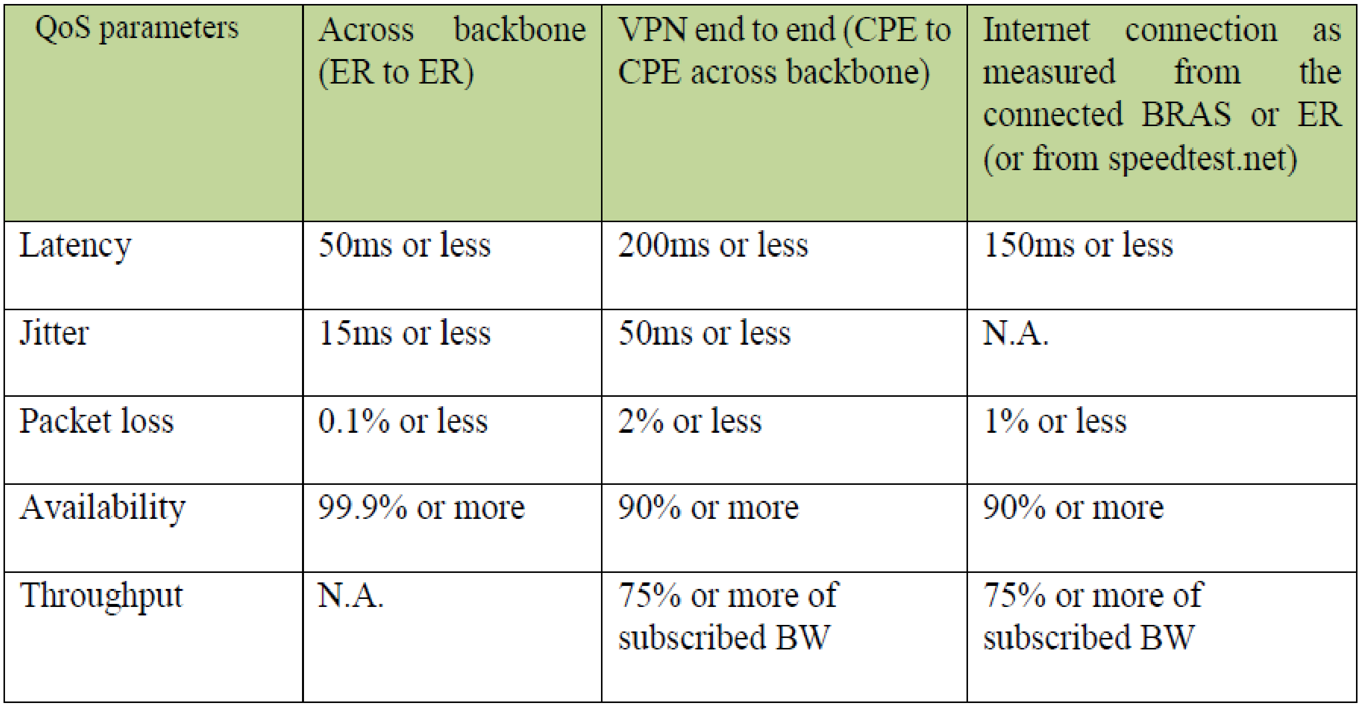
ITU-T G.114 specification of Key QoS requirements and recommendations of VoIP [33], [14] [31] [65]:

- Voice traffic should be marked to DSCP EF per the QoS Baseline and RFC 3246.
- The data packet loss should be no more than 1 %.
- One-way delay (mouth-to-ear) should be no more than 150 ms.
- The average one-way jitter should be targeted at less than 30 ms.
- 21–320 kbps of guaranteed priority bandwidth is required per call (depending on the sampling rate, VoIP codec, and Layer 2 media overhead).

2.7. Recommended IP QoS in Ethio Telecom network

QoS is a configuration that prioritizes data traffic based on a traffic type or destination. So that in the event of congestion on a network, a site's critical traffic has higher priority over other traffic. Currently, in the EthioTelecom network, all packets from all customers are treated equitably, thereby generalized IP network performance targets are recommended as shown in the table below.

Table 2.2: Ethio Telecom recommended QoS targets [66].



QoS parameters	Across backbone (ER to ER)	VPN end to end (CPE to CPE across backbone)	Internet connection as measured from the connected BRAS or ER (or from speedtest.net)
Latency	50ms or less	200ms or less	150ms or less
Jitter	15ms or less	50ms or less	N.A.
Packet loss	0.1% or less	2% or less	1% or less
Availability	99.9% or more	90% or more	90% or more
Throughput	N.A.	75% or more of subscribed BW	75% or more of subscribed BW

To revisit the existing SLA business Model, tariff, and penalty to introduce the class of service to meet customer expectations, improve service availability and QoS and Attract more customers and Sustain our company revenue [67].

2.8 QoS Architectural Framework Recommendation of ITU-T

QoS architectural framework by ITU-T is organized into three planes (Y.1291):

- Control Plane: admission control, QoS routing, and resource reservation.
- Data Plane: buffer management, congestion avoidance, packet marking, queuing, and scheduling, traffic classification, traffic policing, and traffic shaping.
- Management Plane: SLA, traffic restoration, metering and recording, and policy. When very sensitive data (Voice) is sent via an IP network is subject to certain transmission problems such as Packets out of order, delay, jitter, and packet loss [68]. Most of the time Voice quality is directly affected by three QoS parameters: packet loss, latency or delay, and jitter [14] [69].

To overcome these transmission problems, and thus make the IP technology able to support emerging multimedia applications QoS mechanisms should be deployed. For that reason, QoS is considered the most important feature to deploy a successful VoIP system [69].

2.9 Mechanisms of Improving QoS of Voice over Internet Protocol

The main issues that should be addressed by the QoS aspect to adequately transport voice traffic over an IP network are the following: bandwidth, network latency, jitter, and data packet loss [14] [35][70]. In the following section, we inform you how VoIP QoS problems can be addressed to guarantee the required QoS for voice traffic [70].

This problem can be solved and improve VoIP QoS by following multiple Mechanisms [16] [70]:

- Increase link bandwidth or Link capacity increasing: - This is effective but costly.
- Latency-sensitive traffic prioritization: Classify and mark traffic and apply to the queue, Forward important packet first.
- Traffic compression or Use Compression technique:
- Improve the processing process.

To deliver the successful VoIP QoS by increase existing bandwidth and the link, which has a direct impact to improve or ensures QoS of the traffic flow [70]. Additionally, it reduces the transmission delay, jitter, packet loss ratio, and fewer packets are dropped. The other mechanisms used to improve VoIP QoS are Delay sensitive traffic prioritization and traffic. compression, queue scheduling, and congestion avoidance. Improve processing processes such as CPU and memory increase the processing performance and reduce latency and data packet loss [16], [70].

2.10 Quality of Service (QoS)

QoS is a set of techniques to classify and manage network resources with a certain level of packet loss, bit rate, jitter, latency, or delay, etc., which can be guaranteed [71]. QoS is the measure of transmission quality and service availability 99.999 % uptime, with only five minutes of downtime permitted per year of a network (or internetworks). Service availability is a crucial foundation element of QoS. The network infrastructure must be designed to be highly available before you can successfully implement QoS. The transmission quality of the network can determine Voice or video over IP conversation and affected call quality, these factors are Delay variation (Jitter), end-to-end Delay or latency, and packet loss [14] [71]. Real-time applications such as VoIP, online gaming, live broadcasting of video or audio are sensitive to delay and require fixed bitrate. QoS plays an important role in networks where the capacity is a limited resource. It is equally important for applications and consumers to get some level of QoS guarantee for such real-time applications or VoIP to run smoothly [71]. QoS of any service is acceptable when it fulfills SLA and leads to proper customer satisfaction. To guarantee the full throughput, a specific level of assurance is required over the traffic load to reduce losses, jitters, and Delay.

2.10.1 Quality of Service Models

Most Researchers classified QoS into three major levels and few Researchers combine the last two models to add the fourth model called Hybrid models. Classification QoS referred to as service models. These service models describe a set of end-to-end QoS capabilities. Here is the list of QoS models as follows [1], [32], [49] [71]:

1.Best-effort Service Model

2.Integrated Service Model

3.Differentiated Service Model

4.Hybrid Model

2.10.1.1 Best Effort service model

Best Effort is a single service model, no information is provided to and no permission is taken from the network by the application before sending the data. There is no assurance of reliability, throughput, and delay. The First In First Out (FIFO) queue is used as a default for scheduling; it uses drop-tail queue management. First In First Out (FIFO) is a queue mechanism and it means that the new incoming packet is kept at the end of the queue and the packet that comes when the queue is full is discarded [25], [72].
The best Effort service model is also known as the Best Quality Model. Mostly default model in a network. It provides equal service like priority and bandwidth for all types of traffics. It sends the traffic with no guarantees of packet delivery, bandwidth utilization, or traffic prioritization for sensitive services like VoIP. This model is scalable, uses the whole bandwidth of the network, no need to use special QoS, it is simple to implement, all packets are given the same treatment at the same level and there is no separate treatment of different types of sensitive traffics or packets [70] [73]. Know a day’s

Ethio-Telecom uses the Best-effort model and it is realized through the FIFO mechanism. Application programs, without acknowledging the network or obtaining any approval from the network can send any number of packets at any time. For the Best Effort service, the network tries its best to send packets, without ensuring performance such as latency and reliability [70] [73].

2.10.1.2 Integrated Service Model

The integrated service model (IntServ) is a guaranteed service model for some specific levels of traffic in a specific period. It uses RSVP protocol to reserve resources and the path before starts transmission throughout the network, layer 3 routers, or Call Manager Express (CME) routers working in proxy for a non-RSVP-aware device. It also uses a router to reserve the specific bandwidth and requests to the next-hop router for a specific level of services like real-time application or voice and video. Limitation of IntServ: Each router needs to contain a lot of state information that is why it runs on a small-scale network. If the size of the network increases, then it can be challenging to store all traces of all the reservations [74]. Application request services from the network with certain resource requirements such as bandwidth and delay. When the request is processed by the network this information is fed to the application to send the data. Some Service with some delay and bandwidth requirements is requested from the network by the application, later when the network confirms about it, the application sends the data. A network using this model maintains a per-flow state and performs certain operations like policing, classification of packets, and queuing with the help of that state [75].

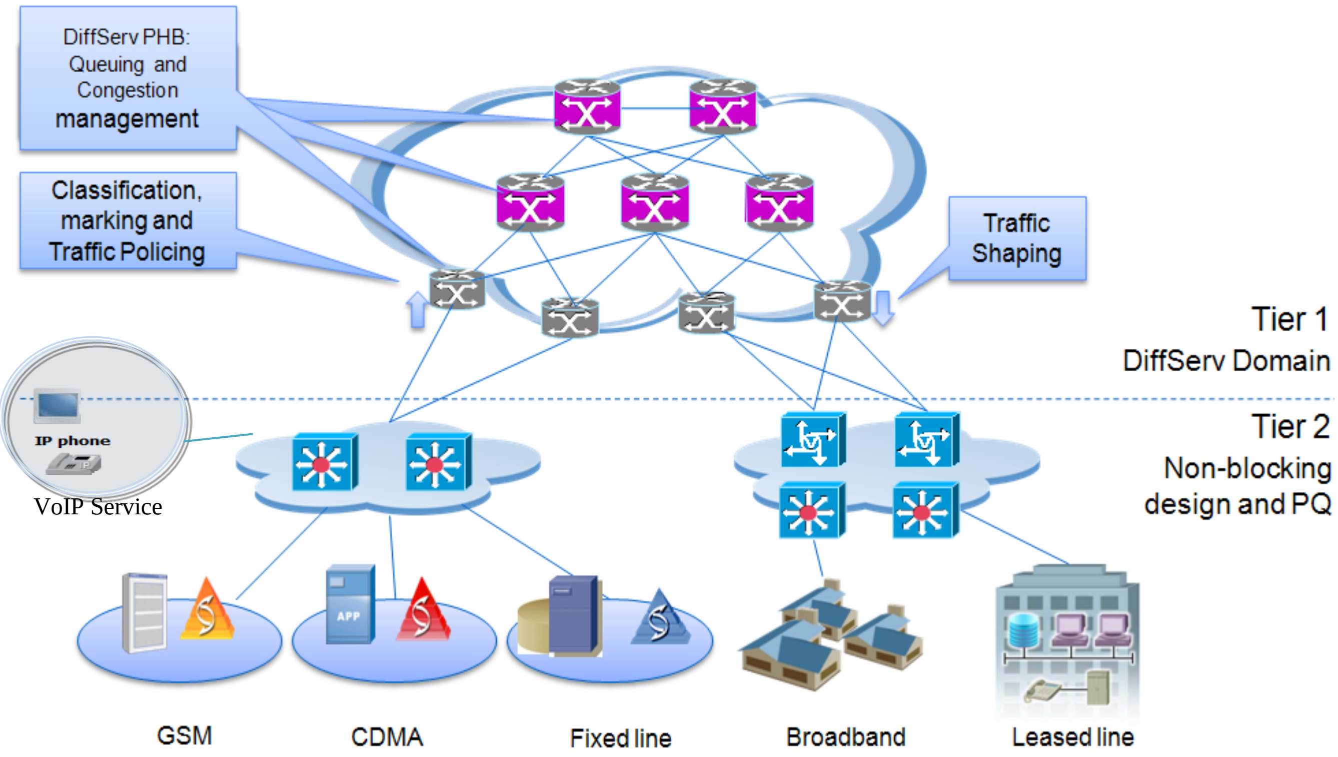
2.10.1.3 Differentiated service Model.

It was designed by the working group of the IETF (Internet Engineering Task Force, 1998) for specific standards and definitions of services that fall under Differentiated QoS. It is focused on scalability and simple to implement than the IntServ or RSVP model for identifying flows and Technologies that can provide differentiated service for portions of the end-to-end connection [11], [75]. This model solves the scalability issue in IntServ and it classifies packets into different Types of Service (ToS) to treat every packet differently based on service priority. Behavioral aggregate (BA) allows a group of packet flows is aggregated which is a help to make the DiffServ scalable. BA is an activity carried out by using the different routers with different resources; the functionalities of the core and border router are not similar [75]. Core routers cannot exchange packets with other domains since they have only access to internal connections. Hence, if the packet must be exchanged with the other domains then the border router must be handling this communication. The process of routers providing special treatment for packets of different BA’s is termed as Per-Hop Behavior (PHB). Differentiated Service Code Point (DSCP) marked in the DS field is used to identify and classify the packets in the DS [57] [75]. Keeping records of per-flow information and the traffic conditioning is done by the Border routers. There is a profile of certain agreements made for the incoming and outgoing traffic which should not be altered. Hence, for taking care of this and not letting the traffics get off from the boundary, traffic conditioning is needed. The configuration of a border router is carried out by taking a traffic profile with the help of the SLA target. Packet forwarding is performed by core routers examining DSCP and mapping with PHB. IETF standardized two kinds of PHB's, Expedited Forwarding (EF) and Assured Forwarding (AF) [75]. Whether VoIP is implemented using dedicated or shared facilities, QoS is an important consideration. A QoS-enabled network differentiates between different types of traffic and offers different treatments. In analyzing whether an IP network can support VoIP, the effectiveness of its QoS must be evaluated. For the prioritization of data, the Differentiated Services (Diffserv) technique can be used [57] [75]. Packets with the Diffserv feature have information in the packet header about the type of service the packets belong to, which will be used by routers to give packets a corresponding priority now forwarding them to one of the links attached to the router [57] [75].DiffServ includes a set of classification and marking tools, queuing mechanisms, and other components to provide for the differentiated treatment of traffic, based on the marking given to various packets. In the DiffServ model, the edge routers should perform the classification and mark of the various types of traffic traversing the network [76]. Network traffic can be classified by network addresses, protocols, and ports, ingress interfaces, or in a variety of other ways. The differentiated Service Model does not focus on individual flow but the aggregate flow. It provides QoS guarantees for aggregated flow only. It can be used together with Multiprotocol Label Switching (MPLS) [32] [76]. Since VoIP is working on Layer 2 and 3 protocols. As a result, the researcher uses BGP MPLS VPN and Differentiated Services technology to improving VoIP QoS for proper network traffic management, reduce cost, and deploy a performant, reliable, and scalable private network. Connecting enterprises to remote locations, customers, and vendors via the MPLS is a very flexible solution that is being considered by many communication providers [40][76]. MPLS is a relatively new Wide Area Network (WAN) Technology and Many ISPs have already deployed it in their network. Its core technology for next-generation networks, in optical networks and high-speed backbones.it also allows you a hybrid routing or forwarding strategy, streamlining the backbone switching of IP packets between layer 2 and layer 3. MPLS works on small label values. Packets are forwarded based on labels instead of destination IP addresses [12] [40][76].

The problem with differentiated services is that it is very poor for end-to-end QoS guarantees. In differentiated services, the traffic is treated on a per-class basis not on the per-flow basis, and in each service class, the individual flows are aggregated together. In differentiated services networks the DS field replaces the TOS field in the header [14][32] [40][76].

The best-practice QoS design principles include:

- ❖ Classification and Marking Principles
- ❖ Policing and Markdown Principles
- ❖ Queueing and Dropping Principles


DiffServ PHB: Queuing and Congestion management
Classification, marking and Traffic Policing
Traffic Shaping
Tier 1
DiffServ Domain
Tier 2
Non-blocking design and PQ
IP phone
VoIP Service
GSM
CDMA
Fixed line
Broadband
Leased line

❖ Fig. 2.4: Quality of Service of differentiated service model [15].

2.11 Differentiated Services QoS implementation

To improve End to the End Voice quality of service in ISP MPLS VPN environment, it is the most essential way to choose the DiffServ QoS model because it is widely implemented in different telecommunication industries due to its easy scalability [41], [77]. The Differentiated Services (DS) architecture QoS model provides a scalable mechanism to classify packets or classes that have similar QoS requirements. For VoIP service required high-quality voice transmissions and it is extremely bandwidth- and delay-sensitive, voice packets should not be dropped, not excessively delayed, or suffer varying delay (jitter) [77]. VoIP can guarantee high-quality voice transmission only if the voice packets, for both the signaling and audio channel, are given priority over other kinds of network traffic. For VoIP to be deployed so that users receive an acceptable level of voice quality, VoIP traffic must be guaranteed certain compensating bandwidth, latency, and jitter requirements [47] [77]. DiffServ QoS model ensures

VoIP voice packets receive preferential treatment and it uses QoS tools to increase the voice quality on a network by decreasing dropped voice packets during times of network congestion and by minimizing both the fixed and variable delays encountered in voice congestion.DiffServ QoS tools supporting dedicated bandwidth, Traffic classification, marking, queuing, shaping network traffic, Setting traffic priorities across the network, congestion management, and congestion avoidance [76], [77]. Before applying DiffServ QoS, the first provision of sufficient network bandwidth to support real-time voice traffic. After the provision of enough bandwidth for voice traffic, then you can take further steps to guarantee that voice packets have a certain percentage of the total bandwidth and get priority. The DiffServ QoS tools allow you to control network traffic, resource allocation in different ways and allow the system to provide differentiated services [77].

2.11.1 Network Traffic Classification

To guarantee bandwidth for VoIP packets, a network device must be able to identify VoIP packets in all the IP traffic passing through it. The basis for providing any QoS is based on the ability of a network device to identify and group-specific packets [77]. To implement the DiffServ QoS model first step is packet classification or classify the traffic into different classes. Packet classification can be processor-intensive, so it should occur at the edge router. Packet classification at the edge router allows the core network to easily identify marking the type of service (ToS) byte in the IP header [77]. After classification, each class is marked by setting designated bits in the IP header, this process is called marking. After marking, the business policy for each class is configured as per SLA. The total effect of the classification process makes a major impact on end-to-end delay. Here is how to classify [15], [77]: The dial-peer voice VoIP global configuration command: Most of the time VoIP gateways, use voice dial peers to classify the VoIP packets and mark the IP Precedence bits, Access list (standard and extended), Incoming interface, IP precedence, Differentiated service code point (DSCP) and Source or destination IP address and Application and Five Tuple (source and destination IP address, IP protocol number, TCP/UDP source, and destination port numbers). QoS of VoIP packets classification done using access list and then marking the type of service field in the IP packet precedence data stream can be classified based on the different RFC standards [15] [77].

Differentiated Services is described and defined in the following RFCs [20] [15], [77]:

- ❖ RFC 2474, Definition of the Differentiated Service Field (DS Field)
- ❖ RFC 2475, An Architecture for Differentiated Service
- ❖ RFC 2597, Assured Forwarding PHB Group and RFC 2598, An Expedited Forwarding PHB

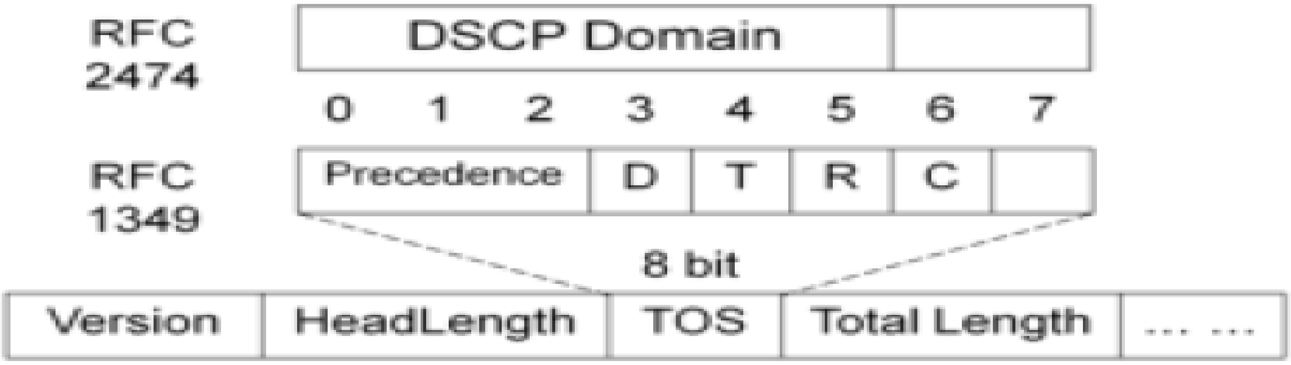


Fig.2.5: VoIP Traffic classification [20], [15] [77].

2.11.2 VoIP Traffic Marking

Traffic Marking is the process of coloring the packet so that it is simply recognized by the next nods. The nodes should mark packets as soon as they have identified and classified the VoIP packets. Marking is to place a value in the DSCP field. With the help of marking, traffic is identified for the next action to achieve QoS [15] [77]. Generally, after every hop in the network can classify and identify the VoIP packets (by port or ToS byte), those hops can then provide each VoIP packet with the required QoS. At that point, you can configure special techniques to provide priority queueing to make sure that large data packets do not interfere with voice transmission and to reduce bandwidth requirements by compressing the 40-byte IP plus UDP plus RTP header to 2 to 4 bytes [77]. In most IP networks, marking IP Precedence or DSCP should be enough to identify traffic as VoIP Traffic. Traffic marking can have done on the data link layer and the network layer [15][77]. Marking is the process of the node setting one of the following [77]:

- Three IP Precedence bits in the IP ToS byte.
- Six DSCP bits in the IP ToS byte.
- Three MPLS Experimental (EXP) bits.
- Three Ethernet 802.1p CoS bits.
- One ATM cell loss probability (CLP) bit

2.11.3 Per-Hop Behavior (PHB)

Per hop behavior (PHB) describes what a DS class should experience in terms of packet loss, delay, and jitter. PHB is a mechanism that is used by the DiffServ model to allocate resources or bandwidth at each node in the path, how traffic is restricted, and how packets are dropped during congestion [13][77]. PHB guarantees 99.999% allocation of the network c (bandwidth, delay, reliability) to a behavior aggregate at each node. These PHBs are building blocks and are grouped to achieve QoS according to SLAs. PHBs are configured at each node in the network in terms of buffer allocation and packet scheduling mechanisms. [76],[77]. IETF defines Three PHBs in DS based on the forwarding behavior required [76],[77]:

- Best-effort class—Class selector bits set to 000
- Assured Forwarding PHB—Class selector bits set to 001, 010, 011, or 100
- Expedited Forwarding PHB—Class selector bits set to 101

The Assured Forwarding (AF) standard specifies four guaranteed bandwidth classes and describes the treatment each should receive. It also specifies drop preference levels, resulting in a total of 12 possible AF classes, as shown in the table below. Most of the time assured Forwarding classes use for data traffic that does not require priority treatment and is largely TCP-based. Expedited Forwarding more closely matches VoIP QoS requirements [77].

2.11.4 Expedited Forwarding PHB (RFC 2598)

Expedited Forwarding (EF) is intended for delay-sensitive applications that require guaranteed bandwidth. An EF marking guarantees priority service by reserving a certain minimum amount of bandwidth that can be used for high-priority traffic. In EF, the egress rate (or configured priority bandwidth) must be greater than or equal to the sum of the ingress rates, so that there is no congestion for packets marked EF [77]. EF implemented by using the strict priority queue in low latency queueing (LLQ). Constant bandwidth is guaranteed for traffic belonging to the EF class, but at the same time, if there is congestion, nonconforming packets exceeding the specified priority rate are dropped to assure that packets in other queues belonging to different classes are not starved of bandwidth [77]. The recommended DSCP value for EF is 101110. The first three bits of this EF value corresponds to IP Precedence 5, which is the recommended IP precedence dial-peer configuration command setting for VoIP traffic. End-to-end QoS is achieved if all IP devices in the network can recognize IP Precedence or DSCP for classification and marking purposes. The DS architecture specifies how to classify, mark, police, and shape traffic entering a DS region and how to treat different classes at every hop in the DS region [77].

2.11.5. Traffic Shaping and Traffic Policing

Traffic shaping and policing are the mechanisms and tools that are used to control the rate of traffic. Most of the time Traffic policing used to drop excess traffic or remark the traffic to control traffic flow within a specific rate limit without introducing any delay to traffic [78]. The other tool used for retains excess traffic in a queue and then schedules such traffic for later transmission over an increment of time is known as Traffic shaping. Traffic in any network was divided into two classes: the voice and others by the network administrator, it is important that LLQ and traffic policing are used to implement the various configurations in the different switches. [60][78].

2.11.6. Congestion Management

Queuing can solve temporary congestion on an interface of a network device by storing the excess packets until there is enough bandwidth to forward the packets. Sometimes some packets are dropped due to the queue depth is full [78]. The most effective way to control data packet loss is Congestion management. Congestion management allows the administrator to control congestion by determining how and when the queue depth is full. There are several ways congestion Management can be implemented [60] [78]:

- Priority Queuing (PQ): This mechanism allows one to give priority to certain traffic while allowing others to be dropped when the queue depths are full.
- Custom Queuing: It allows us to reserve queue space in the router or switch buffer for the traffic type.
- Weighted Fair Queuing (WFQ): This allows the sharing of bandwidth with prioritization given to some traffic.
- Class-based Weighted Fair Queuing (CBWFQ): This extends the functionality of WFQ to provide support for the user-defined class.
- Low Latency Queuing (LLQ): This is a combination of CBWFQ and PQ. It can give traffic that requires low delay the required bandwidth it needs while also giving data the needed bandwidth. It solves the starvation problem associated with PQ.

2.12 Related Works

In this section, notable related works are explained to lay the foundation of this study. There are many authors and researchers had worked on the area of improving the quality of service of VoIP by comparing various VoIP coding Algorithms, Implement DiffServ QoS by integrating BGP MPLS VPN Network with TE, Providing higher priority for voice traffic or packet during configuration of QoS, and Synchronization of time over Network operators. In addition to that, some of them have tried to describe the QoS of VoIP from the customer LAN side, provider edge (PE) to the customer side, network backbone, and other end-to-end QoS perspectives.

Amor L. and Thabet S [79] have made a deep analysis of the Deployment of VoIP Technology and QoS Concerns. Even though VoIP had advantages, they explain VoIP technology suffers different difficulties such as architecture complexity, interoperability issues, QoS concerns, and security issues. Meanwhile, they give higher attention to a QoS issue is the most serious one to improve VoIP QoS from the rest.

They understand that Data packets transmitted via IP network are encountered certain problems such as packet latency, jitter, and data packet loss. To handle these problems, they use strict QoS constraints, QoS mechanisms, and voice clarity. The QoS mechanisms deployment of VoIP helps to achieve bandwidth guarantees while minimizing network latency, jitter, and data packet loss ratio for prioritized traffic like voice traffic. Finally, to transport voice traffic over an IP network, and improve deployment of VoIP system, they are using Network congestion prevention, increase bandwidth and Link capacity, Voice traffic prioritization, Increase traffic compression (Increase processing speed of nodes and transmission speed of links), Packet loss concealment.

Nasser A, and Fayez W. et al. [80] work on Optimizing QoS for Voice and Video Using DiffServ - MPLS because of VOIP and video conference they create massive congestion to the IP networks and require higher bandwidth consumption or QoS assurances has become a critical issue, like end-to-end delay, jitter, and packet loss. These QoS requirements put new challenges on Internet service providers. They have optimized the network by MPLS and Differentiated Services to achieve VoIP quality of service in the IP networks. To meet this VoIP quality of service, they performed an experimental Simulation Model using OPNET Network Simulator with different conditions: The experimental study was divided into two parts, the first part only shows how MPLS improves the overall performance of the network and the second part inserts the DiffServ and the integration of DiffServ and MPLS together. They are using the OSPF routing protocol for voice traffic; the voice encoder scheme is G.711 and selecting the best-effort path. When they perform experiments, they compare the result of tested four scenarios which are: 1) IP _Best effort topology, 2) MPLS topology, and 3) DiffServ topology 4) Integration of MPLS and DiffServ (DiffServ-MPLS). When they compare the result of Best effort topology with MPLS there is load distribution on the MPLS network links using FEC and increase Voice throughput, reduced end-to-end latency, and faster processing rate of the routers as compared to the conventional IP. MPLS - DiffServ improve VoIP QoS mechanism and they recommend other QoS techniques to improve VoIP QoS such as traffic policing, queuing, and congestion avoidance to achieve guaranteed QoS across the IP/MPLS networks.

End-to-End QoS Network Design cisco book [81] explains QoS as the measurement of transmission quality and service availability of a network or internetworks. Service availability is a crucial foundation element of QoS. The network infrastructure must be designed to be highly available before you can successfully implement QoS. The target for High Availability is 99.999 % uptime, with only five minutes of downtime permitted per year. The transmission quality of the network is determined by the following factors: delay, jitter, and packet loss. A communications backbone network transports a multitude of applications, including real-time voice, high-quality video, and delay-sensitive data. As result Networks must provide predictable, measurable, and guaranteed services by managing bandwidth, delay, jitter, and packet loss parameters on a network.

Hardeep S. and M. Mian, [82] work on a Comparative Study and Analysis of various VoIP coding Algorithms to improve VoIP Speech quality. The signal quality of the VoIP system is degraded by different network-layer problems, such as delay, jitter, and packet loss. to optimize this problem by selecting three VoIP Codecs (G.711, G.729, AMR, AMR-WB, etc.). Then VoIP simulations are conducted for G.711, G.729, and AMR-WB speech coders for different network conditions. After the simulations, they had to evaluate results using perceptual evaluation of speech quality (PESQ)/MOS measurement. According to the simulation result, AMR-WB shows better quality than the other two VoIP Codecs. However, if G.711 CODECS is used it can be better to implement the existing infrastructure of Ethio-Telecom equipment or PSTN can be usable access VoIP service easily with good quality of MOS value 4.1 points.

Juan Rendon S.and Thomas P. [83] studies VoIP suppliers with and without QoS and concludes that ‘‘it is an unanswered question how important it is for the customers to have a guarantee for QoS’’. Ioanna D. C. and Yogesh K. D. [84]in an analysis of IP telephony in the Danish market find evidence that price would be more important than the quality of service. However, both studies do not neglect the importance of QoS for the improvement of VoIP service provisioning. Padraig F. [85] Optimize the QoS of VoIP Applications over Wi-Fi and explain the extent to which Network operators synchronized time can be also used to improve the QoS of Real-Time Communications such as Voice over Internet Protocol applications over wired and wireless networks.

Jeevan K. and Deepak A., [86] explain the way how to improve the Performance Voice over Internet Protocol and Implementation of QoS by integrating MPLS Network with TE. MPLS can support Traffic Engineering (TE) which ensures minimizes congestion, load balancing, and management of the network resources. They are using scheduling algorithms for implementing QoS on a network. QoS is implemented on top of the MPLS-TE network using Differentiated Service (DiffServ) architecture. Performance evaluation is done considering the network parameters end-to-end delay, jitter, packet loss. The simulation was done using OPNET modeler 16.0 and the results were analyzed.

The simulation result shows that using Traffic Engineering (TE) along with QoS in the MPLS network decreases the delay, jitter, and packet loss, compared to using TE alone for voice traffic. The above works of literature show direction for the researcher on how to combine different methods and procedures this research proposal tries to combine different methods and procedures that are used as input and works on improving the quality of services of VoIP in Ethio Telecom and satisfying the customer needs by using Multi-Protocol Label Switching-Traffic Engineering and Differentiated Service Model (MPLS VPN and DiffServ Model).

Nadeem U.,_[87] The Author state that to achieve VoIP QoS, the network administrator should have to give higher priority to voice traffic during the configuration of QoS. Explain QoS_as the process of prioritization of a certain type or class of traffic. When an IP network is designed for VoIP service and QoS should be configured so that voice gets priority over other types and classes of traffic.

Mushtaq A. and Abdul B. [88], have explained the way to improve the Internet world or VoIP and provide guaranteed service delivery. To gain their objective, they are using the following mechanisms': by integrating MPLS Traffic Engineering tunneling to optimize the backbone resources in MPLS IP backbone, MPLS VPN QoS for secure communication among two customers.

To meet VoIP quality of service, they performed an experimental Simulation Model using GNS3 Network Simulator. The result shows that when they compare the simulation result of a show that The Data rate of IP MPLS TE based SP network has shown a clear improvement in performance network than Conventional IP network. Similarly, jitter using conventional IP MPLS-based network reduced than the previous Conventional IP network.

Mohammad S.& Syed N. [89]: They have identified VoIP voice quality can be improved by adopting certain Quality of Service (QoS) measures such as classification, marking, or queuing. They also discussed different QoS metrics like delay, packet loss, and jitter could affect the voice quality of VoIP. To reduce these effects, they implement certain QoS mechanisms with some set of configurations. For this purpose, Cisco IP phones have been configured in our topology with routers, switches, traffic generators, end stations, and VoIP quality monitoring software called VQmanager. The two tests had been made with a fixed bandwidth of 70 and a random bandwidth is set with traffic generators unleashing packets of traffic. They include no QoS, Auto QoS, and Customized QoS mechanisms. Results have been indicative of top performance by the Customized QoS mechanism, in both sets of tests, followed by Auto QoS and no QoS mechanisms. It has been observed that a customized scenario could be a particular configuration to any organization's needs and that will have the lowest delay, jitter, and packet loss which are the main QoS metrics that impact the voice quality.

J. Jaffar and H. Hashim, et. al. [90] studied the influence of the QoS mechanism via DiffServ-MPLS on network parameters such as packet loss, delay, and throughput for different video resolutions. The comprehensive study showed a general improvement in the throughput and data packet loss particularly of video transmission when using the Diffserv-aware MPLS network as compared to when only MPLS or DiffServ is employed. They do not use the same queuing scheme in the different scenarios so that the results do not compare the different technologies instead compare the different queuing schemes.

Ahmed and Zafar [91] Adopted Graphic Network Simulator (GNS3) to compare traditional IP networks and MPLS-enabled networks without considering any other QoS mechanisms. The comparison analysis is based on the traffic engineering parameters such as delay variation, effective utilization of bandwidth, Jitter, Quality of Service (QoS), packet loss, and congestion. The results of the comparison revealed that traffic engineering through MPLS networks has enhanced reliability, scalability, and other parameters as compared to traditional IP networks.

Naoum and Maswady [92] conducted a simulation study to the multisite office network for G.723 VOIP communication traffic applied on two network infrastructure models: one for IP and the other for MPLS, the results came encouraging for the MPLS model.

Fitsum Tesfaye Belay [93] had worked on VoIP Investigation and Challenges – Case: Ethiopian Telecommunications, in 2014. The researcher recommends the way how to expand the internet Broadband service to improve tremendous communication and reliable internet broadband have a vital role for VOIP service (High-speed web surfing, Online education, Videoconferencing, and Cloud Computing, gaming). There are problems with the quality of service of internet Broadband, regulation issue, and VOIP as part of a service. The problems were poor ICT infrastructure, invisible broadband backbone. Generally, all researchers focus on improving Network QoS parameters like bandwidth guarantees, minimizing network delay, jitter, & packet loss, but do not specifically focus on improving VoIP QoS traffic. Finally, they are not camper their final output result with the ITU standard QoS parameters.

Table 2.3. Shows Summary of related works and research gap to justifies VoIP QoS.

Authors &reference number	**Area of study**	**Routing Technology and QoS used**	**Improvement Achieved**	**Research Gap**
Amor Lazzez and Thabet Slimani [79].	Deep analysis on the Deployment of VoIP Technology and QoS Concerns.	Strict QoS constraints, QoS mechanisms, and voice clarity.	The bandwidth guarantees while somewhat minimizing network delay, jitter, & loss ratio for prioritized voice traffic.	Delay, Jitter & Packet loss are Not fit ITU VoIP QoS Requirement.
Nasser Almofari and Fayez W. Zaki [80].	Enhancing QoS of Voice & Video by Using DiffServ - MPLS.	OSPF, DiffServ - MPLS & Congestion Avoidance	Guaranteed QoS across the IP/MPLS networks, increase Voice throughput, reduced end-to-end delay, and faster processing rate of the routers.	Only granted the to-end delay and router capacity but there are other parameters like packet loss and jitter not included in the study
Hardeep S. & M. Mian [82].	Comparative Study and Analysis of various VoIP Coding Algorithms to improve VoIP Speech Quality.	Use dissimilar speech coders G.711, G.729, AMR-WB) for network conditions & evaluate speech quality by (PESQ)/MOS Measurement.	AMR-WB shows better quality than the other two VoIP Codecs.	The researcher except voice Codecs can only reduce delay, packet loss, jitter, and improve to optimize VoIP QoS.
Juan Rendon S.and Thomas P. [83]	Revise VoIP in the case of providers with and without QoS.	Not use Routing technology and QoS used parameters.	Forward his assumption to guarantee QoS is important for the customers.	It is only assumption and recommendation, rather than showing a solution for the problem.
Jeevan K. and Deepak A. [86]	Improve the Performance Voice over Internet Protocol and Implementation of QoS by combining MPLS and TE.	MPLS VPN-TE & DiffServ Model.	MPLS minimizes the latency, jitter, and packet delay compared to using TE only for voice traffic.	It does not specify the QoS technique and measures the result concerning ITU QoS of network parameters like latency, jitter, packet delay, loss.

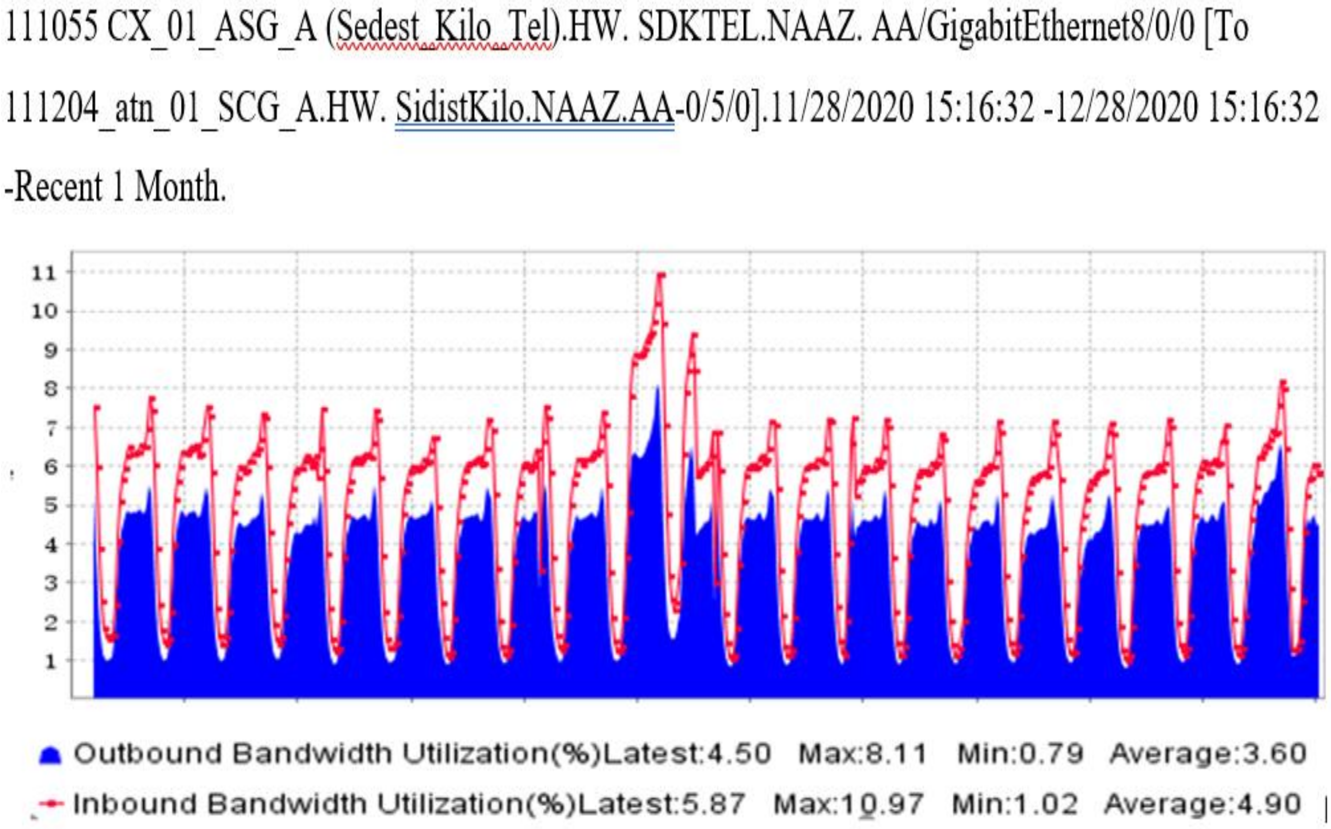
CHAPTER THREE

3.PROPOSED SYSTEM MODEL

Before developing the system model the researcher had collected both and secondary sources of data using questioner and interviews to identify the VoIP Quality of Service problem in Ethio Telecom. In addition to that researcher also Investigation the Existing VoIP QoS problem or network parameters in Ethio Telecom that becomes below ITU target. Finally, the researcher understands the existing problem and proposed artifact to improving the VoIP QoS problem.

3.1. Investigation of Existing VoIP QoS problem in Ethio-telecom and Presentation

As you can see in that preliminary Investigation on Ethio Telecom network sites there is a VoIP QoS problem. VoIP QoS can be measured by network performance like bandwidth utilization, packet loss, delay, jitter, and all parameters are below the International Telecommunication Union target. The existing Arada network sites of maximum Outbound Bandwidth utilization is around 11 mb/s to its SLA Enterprise customer.



111055 CX_01_ASG_A (Sedest_Kilo_Tel).HW. SDKTEL.NAAZ. AA/GigabitEthernet8/0/0 [To 111204_atn_01_SCG_A.HW. SidistKilo.NAAZ.AA-0/5/0].11/28/2020 15:16:32 -12/28/2020 15:16:32 -Recent 1 Month.

Fig.3.1: Shows Existing Arada network site maximum Outbound Bandwidth utilization.

111165 CX_02_ASG_B(Ayat_Tel).HW. AYATA TEL.EAAZ. AA/Eth-Trunk2 [Link to 111089_CX_01_ASG_A.HW. Gerji.EAAZ.AA Eth-Trunk2]. 11/28/2020 15:16:32 -12/28/2020 15:16:32 -Recent 1 Month.

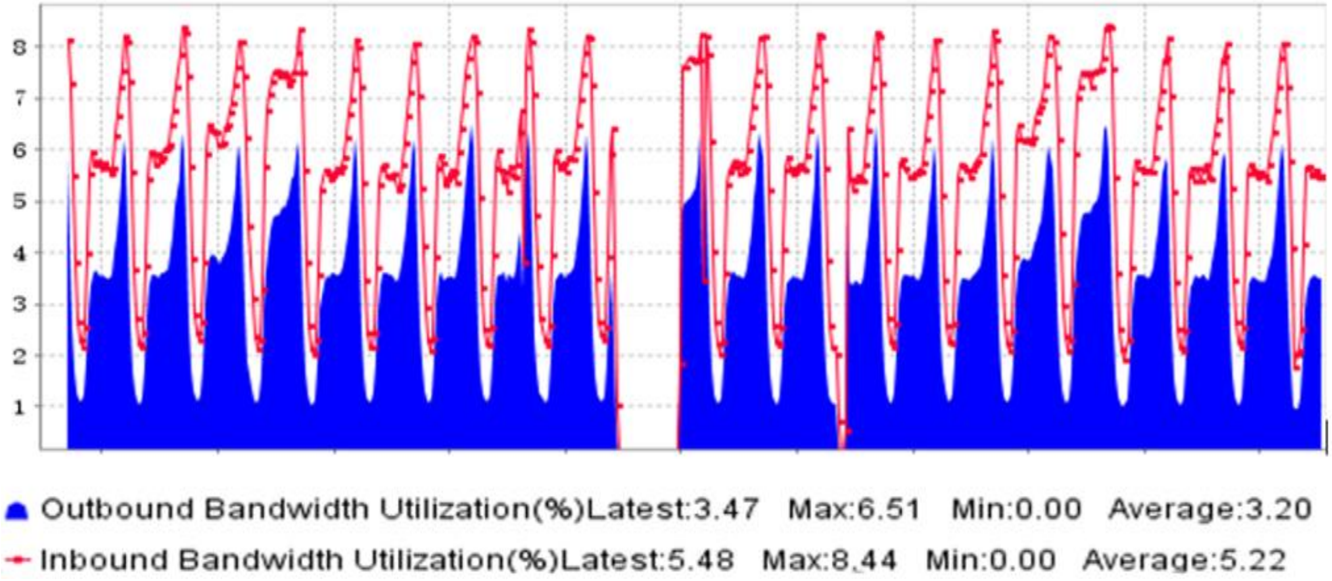


Fig.3.2: Shows Existing Ayata network sites maximum Outbound Bandwidth utilization.

Table 3.1 shows the EthioTelecom network and the degree of data Packet loss and delay.

No	Test path	PLR (%)	Delay (ms)
1	111168_NE_01_HW.Kirkos.SAAZ.AA/Eth-Trunk5(10.1.32.101) - 111055_NE_01_RSG_A.HW.Arada.NAAZ.AA/Eth-Trunk5(10.1.31.101)-20150129162858	46.368	4.131
3	NE40E01.HW.MW.AA/Eth-Trunk5(10.1.29.101) - 111055_NE_01_RSG_A.HW. Arada.NAAZ.AA/Eth-Trunk5(10.1.31.101)-20150129162858	46.476	4.644
4	121290-MK-RSG-B.NR/Eth-Trunk5(10.3.15.9) - 111168_NE40E_02_NE40E_B_HW. Kirkos.SAAZ.AA/Eth-Trunk5(10.1.32.105)-20161212181940	0.87	30.87

3.2. Presentation of Customer Response on Ethio Telecom VoIP QoS Problem

According to the customer response of the survey, there are Network Performance parameters like bandwidth, Delay, Jitter Packet Loss that are highly affected by VoIP quality of service in Ethio Telecom Network.

Table 3.2 shows The Level of Ethio Telecom customer satisfaction of VoIP quality of service.

		Degree of customers satisfaction				
Types of Customer	**Sex**	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
ADSL broadband	Femle	0	0	1	25	5
	Male	1	3	0	8	38
Voice over Internet Protocol	Femle	1	1	2	5	60
	Male	1	1	2	13	93
Ethio Telecom Network Technicians	Femle	0	1	1	3	9
	Male	0	2	1	2	36

Table 3.3 show response of customer on MP-BGP MPLS TE and Diffserv model improve VoIP QoS.

		Degree of customers satisfaction				
Types of Customer	**Sex**	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
ADSL broadband	Femle	20	5	3	2	1
	Male	30	10	1	8	1
Voice over Internet Protocol	Femle	1	1	2	5	60
	Male	90	13	2	1	4
Ethio Telecom Network Technicians	Femle	9	1	1	3	0
	Male	53	1	1	0	0

Generally, the survey shows that customers are not fully satisfied with the VoIP quality of service provided by Ethio Telecom. As a result, the customer expects MP-BGP MPLS TE and Diffserv to improve the network parameters like bandwidth, Delay, Jitter, and Packet Loss, which is indirectly highly affected by VoIP QoS.

3.3. Proposed system model of VoIP QoS Network Architecture

For this research, a simplified VoIP QoS Network Architecture is built as showed (Fig.4.1). It covers the main steps in designing VoIP QoS network architecture. The Generic Network Architecture was chosen according to the requirements for the design of networks with service provisioning and implemented end-to-end VoIP QoS. In the proposed network architecture solution, there are two types of routers, CME, switches, and phones. The routers are P and PE; P routers are the backbone routers. It provides MPLS label forwarding and maintains public network routing information. PE routers are directly connected with CME routers. The functions of PE routers are maintaining and processing VPN route information, forwarding VPN, running MP-BGP, and MPLS protocols. It also has done label popping and imposition. CME is used to configure, evaluate, and maintain VoIP traffic. Switches are used to give dynamic host control protocol (DHCP) IP for phones. Phones are end devices that initiate VoIP traffics.

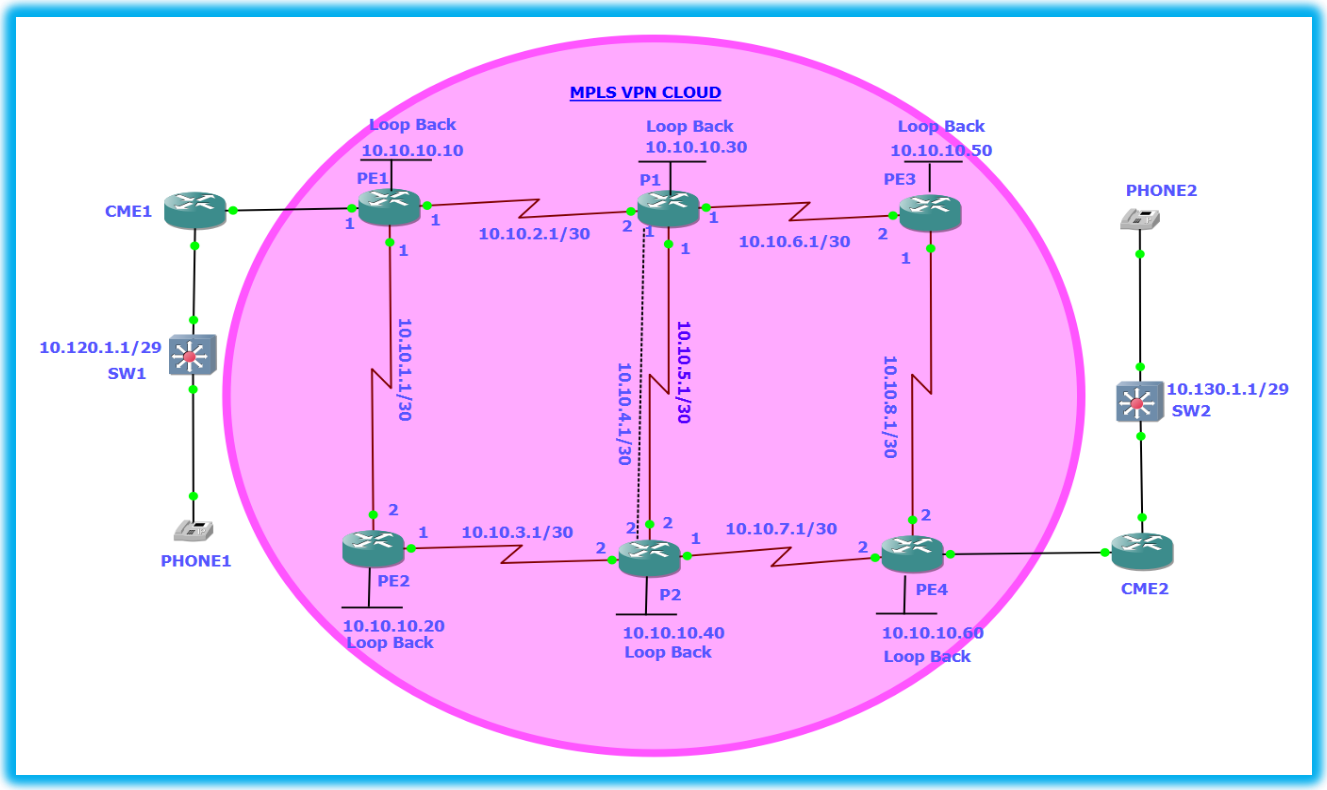


Fig.3.3: Shows the Simplified Proposed VoIP network architecture with end-to-end QoS.

The proposed network model is slightly modified for testing congestion analysis. Phone1 and Phone 2 are traffic generators. In both Phones (Phone 1 and phone 2) traffic was evaluated. The two phones use the same networking protocol and equipment. The links and interfaces are similar in both Phone models.

VoIP QoS applied to the traffic running through the network is similar in both solutions. The core network is realized as a core router and route reflector. The device is logically divided into two logical systems. These systems are acting like separate routers. They have the full functional capabilities of two separate hardware devices. The connections between the two logical systems are made by peering at the interfaces. The links with the other devices in the network are recognized with general Serial interfaces. The access and aggregation networks are made with secure service routers. They are working in multiprotocol label popping and positioning mode instead of the default packet flow, due to the MPLS architecture. The devices are working with Fast Ethernet interfaces. The links with the core networks are through Serial and the links with the end devices are through Fat Ethernet.

The access and aggregation routers apply VoIP QoS to the traffic from the end devices. The two Phones are traffic generators. For testing, the VoIP QoS applied in the traffic flow Wireshark had used. These modules provide functions as random traffic generation, fixed or non-fixed packet size, simultaneous generation of multiple traffic flows. The uniform network entities for both Phone networks of VoIP architectures tested are given in the following description. These units are IP address allocation, interface connections, and configuration, as well as the QoS, applied on the network.

3.4. Designed VoIP Network IP Address Allocation

3.4.1. Network IP Address

There are three types of IP addresses used in this test. The IP address resources are loopback IPs, interconnection IPs, and service IPs. The IP address spaces in the network are described in the following steps. All networks are private from the Internet's point of view and they have just a couple of uplink points connected to the internet. These uplink points are dedicated interfaces, which have public IP addresses and are assumed as external interfaces (the external part of the network).

This allows using private IP address spaces in the internal interfaces in the network. To simplify IP addressing scheme in the proposed network different private IP address spaces are used. Class A IP network is dedicated to the connections between core routers, between core and aggregation routers, between aggregation and aggregation routers, between aggregation and access Phones. Class A IP address is also used to simulate the services.

Loopback IP Address

The loop IP addresses are used to establish a transport control protocol (TCP) peer with neighbors in the MPLS network.

Table 3.4 shows the Loopback IP Addresses.

Device Name	**Loopback IP Address**
P1	10.10.10.30/32
P2	10.10.10.40/32
PE1	10.10.10.10/32
PE2	10.10.10.20/32
PE3	10.10.10.50/32
PE4	10.10.10.60/32

Interconnection IP Address

The interface interconnection IP addresses are used to establish neighbors peering in the MPLS network.

Table 3.5. shows Loopback IP Addresses

Local Device	**Remote Device**	**Interconnection IP Address**
PE1	PE2	10.1.1.1/30
PE1	P1	10.1.2.1/30
PE2	P2	10.1.3.1/30
P1	P2	10.1.5.1/30
P1	PE3	10.1.6.1/30
P2	PE4	10.1.7.1/30
PE3	PE4	10.1.8.1/30

Service IP Address

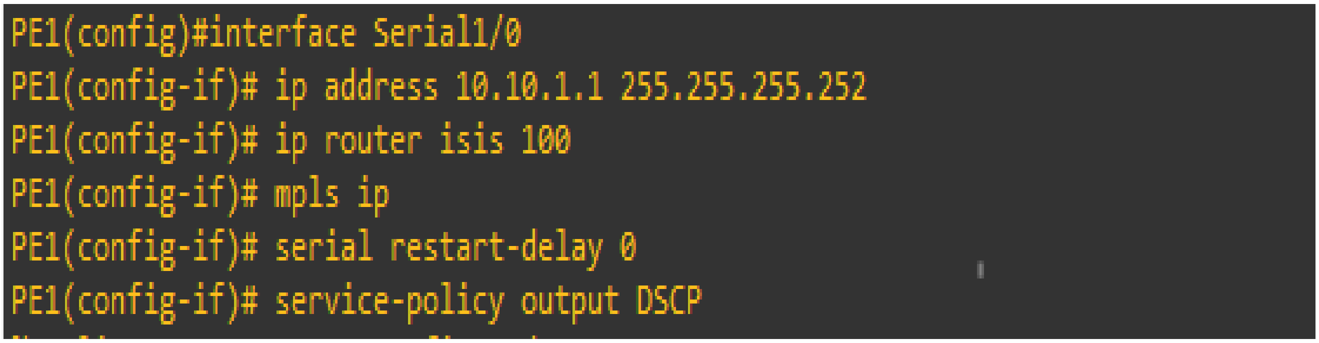
The service IP addresses are used for service provision in the MPLS network.

Table 3.6. Shows the Services IP Addresses

Service Name	Service IP Address
Phone 1	10.120.1.1/29
Phone 2	10.130.1.1/29

3.4.2. Interfaces Configuration in the network architecture

The interfaces peering in the proposed network architecture are established with the following steps. The configuration is almost common for all interfaces. Only loopback has distinct differences in the way of their configuration. The loopback interfaces cannot contain traffic policy configuration. The following command is the most common format to configure given Interfaces:



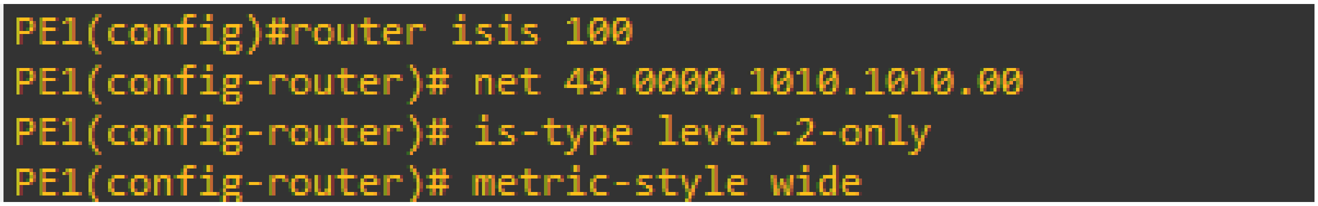
```
PE1(config)#interface Serial1/0
PE1(config-if)# ip address 10.10.1.1 255.255.255.252
PE1(config-if)# ip router isis 100
PE1(config-if)# mpls ip
PE1(config-if)# serial restart-delay 0
PE1(config-if)# service-policy output DSCP
```

Fig.3.4: shows the Interfaces Configuration.

But the interfaces between the core, aggregation, and access routers have shaped depending upon the VoIP QoS policy applied to the interfaces.

3.4.3. Interior Gateway Protocol (IGP) Interconnection

In the proposed network for the interconnection between P and PE routers, the IS-IS protocol has been used. This is because of IS-IS protocol is more convergent. The following command is the most common format to configure the IS-IS protocol.

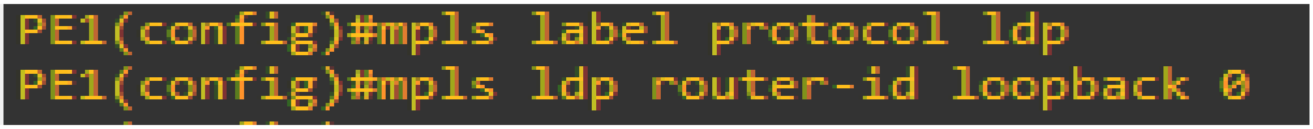


```
PE1(config)#router isis 100
PE1(config-router)# net 49.0000.1010.1010.00
PE1(config-router)# is-type level-2-only
PE1(config-router)# metric-style wide
```

Fig.3.5: shows the configuration of the IS-IS protocol.

4.4.4. MPLS and MP BGP Interconnection

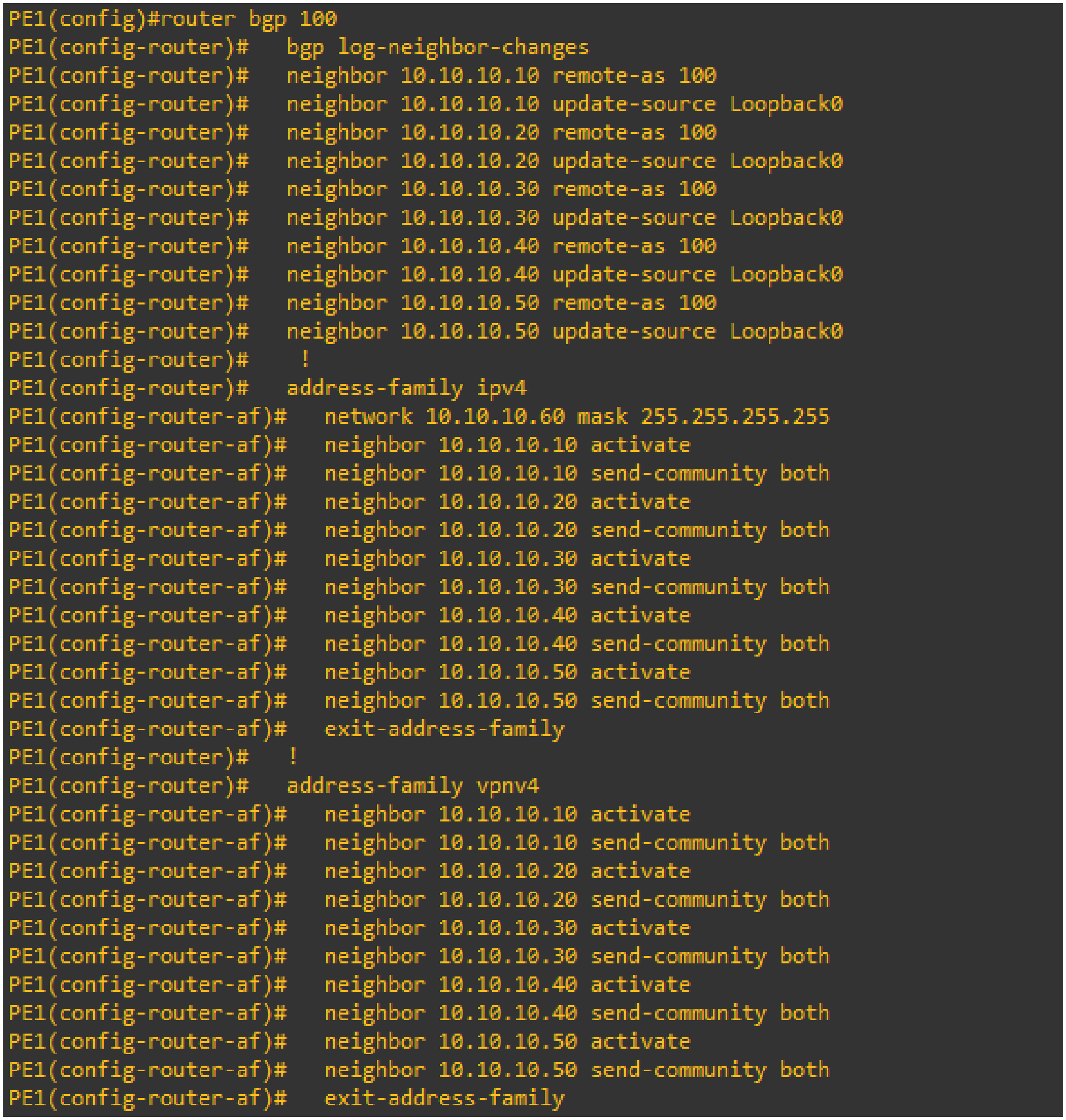
MPLS protocol is used for label switching and distribution. The following command is the most common format to configure MPLS globally.



```
PE1(config)#mpls label protocol ldp
PE1(config)#mpls ldp router-id loopback 0
```

Fig.3.6: shows the configuration of the MPLS protocol.

Multi-Protocol -border getaway protocol (MP BGP) is used to create a peer relationship between different types of routers. The following command is the most common format to configure MP BGP.

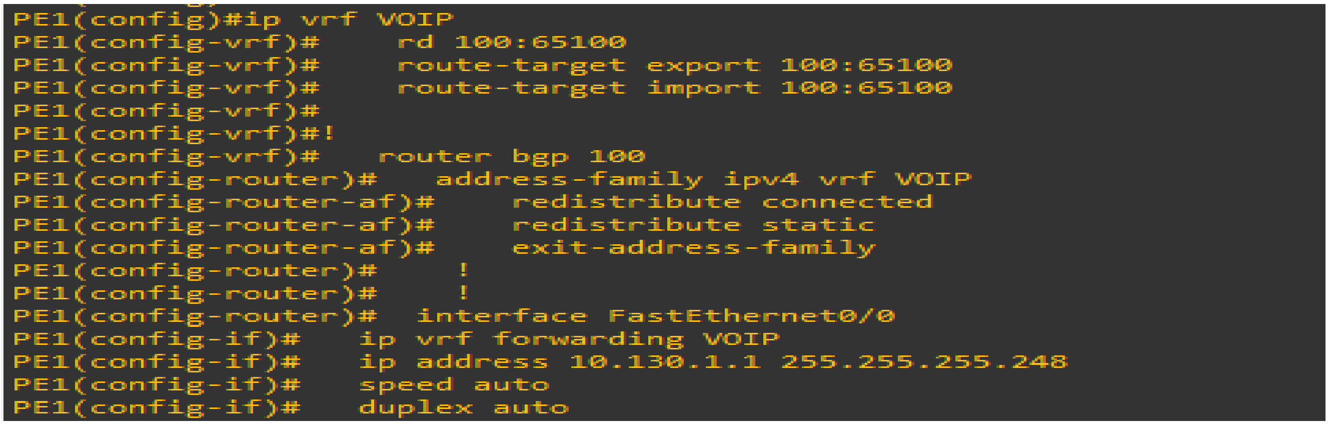


```
PE1(config)#router bgp 100
PE1(config-router)#   bgp log-neighbor-changes
PE1(config-router)#   neighbor 10.10.10.10 remote-as 100
PE1(config-router)#   neighbor 10.10.10.10 update-source Loopback0
PE1(config-router)#   neighbor 10.10.10.20 remote-as 100
PE1(config-router)#   neighbor 10.10.10.20 update-source Loopback0
PE1(config-router)#   neighbor 10.10.10.30 remote-as 100
PE1(config-router)#   neighbor 10.10.10.30 update-source Loopback0
PE1(config-router)#   neighbor 10.10.10.40 remote-as 100
PE1(config-router)#   neighbor 10.10.10.40 update-source Loopback0
PE1(config-router)#   neighbor 10.10.10.50 remote-as 100
PE1(config-router)#   neighbor 10.10.10.50 update-source Loopback0
PE1(config-router)#    !
PE1(config-router)#   address-family ipv4
PE1(config-router-af)#   network 10.10.10.60 mask 255.255.255.255
PE1(config-router-af)#   neighbor 10.10.10.10 activate
PE1(config-router-af)#   neighbor 10.10.10.10 send-community both
PE1(config-router-af)#   neighbor 10.10.10.20 activate
PE1(config-router-af)#   neighbor 10.10.10.20 send-community both
PE1(config-router-af)#   neighbor 10.10.10.30 activate
PE1(config-router-af)#   neighbor 10.10.10.30 send-community both
PE1(config-router-af)#   neighbor 10.10.10.40 activate
PE1(config-router-af)#   neighbor 10.10.10.40 send-community both
PE1(config-router-af)#   neighbor 10.10.10.50 activate
PE1(config-router-af)#   neighbor 10.10.10.50 send-community both
PE1(config-router-af)#   exit-address-family
PE1(config-router)#   !
PE1(config-router)#   address-family vpnv4
PE1(config-router-af)#   neighbor 10.10.10.10 activate
PE1(config-router-af)#   neighbor 10.10.10.10 send-community both
PE1(config-router-af)#   neighbor 10.10.10.20 activate
PE1(config-router-af)#   neighbor 10.10.10.20 send-community both
PE1(config-router-af)#   neighbor 10.10.10.30 activate
PE1(config-router-af)#   neighbor 10.10.10.30 send-community both
PE1(config-router-af)#   neighbor 10.10.10.40 activate
PE1(config-router-af)#   neighbor 10.10.10.40 send-community both
PE1(config-router-af)#   neighbor 10.10.10.50 activate
PE1(config-router-af)#   neighbor 10.10.10.50 send-community both
PE1(config-router-af)#   exit-address-family
```

Fig.3.7: shows the configuration of the MP BGP between different routers.

3.4.5. VoIP Service Configurations

VoIP services are configured as L3VPNs. VPN instances have a VPN name, route distinguisher, and route target. After configuring VoIP VPN instances and bind the instances to the CME interfaces. The following command is the most common format to configure the VPN instance and bind the instance to the interfaces.



```
PE1(config)#ip vrf VOIP
PE1(config-vrf)#    rd 100:65100
PE1(config-vrf)#    route-target export 100:65100
PE1(config-vrf)#    route-target import 100:65100
PE1(config-vrf)#
PE1(config-vrf)#!
PE1(config-vrf)#   router bgp 100
PE1(config-router)#   address-family ipv4 vrf VOIP
PE1(config-router-af)#    redistribute connected
PE1(config-router-af)#    redistribute static
PE1(config-router-af)#    exit-address-family
PE1(config-router)#     !
PE1(config-router)#     !
PE1(config-router)#  interface FastEthernet0/0
PE1(config-if)#   ip vrf forwarding VOIP
PE1(config-if)#   ip address 10.130.1.1 255.255.255.248
PE1(config-if)#   speed auto
PE1(config-if)#   duplex auto
```

Fig.3.8: Shows Configuration of VoIP VPN and bind the instances to the CME router interfaces.

3.4.5.1. Designed QoS of Proposed network architecture.

The designed QoS is to provide different levels of service quality based on different requirements to guarantee SLA targets the quality requirements of different VoIP services. Managing maximum receivable bandwidth, reducing transmission, queueing, and processing delay, managing jitter, and packet loss are the main focuses of the design. The newly designed architecture differs from the existing architecture by separating, classifying Real-time traffic from non-real-time traffics, and prioritize real-time traffics before non-real-time traffics. The detailed explanation has been stated in the following way. In the designed simulation there is real-time (VoIP _traffic) traffic and non-real-time traffic (SMS traffic and DATA traffic). Real-time traffic can have treated differently from non-real-time traffics. The three traffic has been classified and marked. The marked traffic can have used with traffic policing and shaping called class-based marking and policing (CBM and CBP), traffic priority called class-based weighted fair queue (CBWFQ), and congestion control technique called weighted random early discard (WRED).

3.4.5.2. Class-based Traffic Marking, shaping, and Policing using DSCP.

The proposed DSCP differs from the existing architecture by performing traffic classifying based on the Access list, Class map, and policy-map, which was not found on the existing architecture. The three traffic has been classified and marked using a differentiated service code point. The higher DSCP traffic is treated firstly. The configuration steps and the configuration are as follow: Configuration Steps:

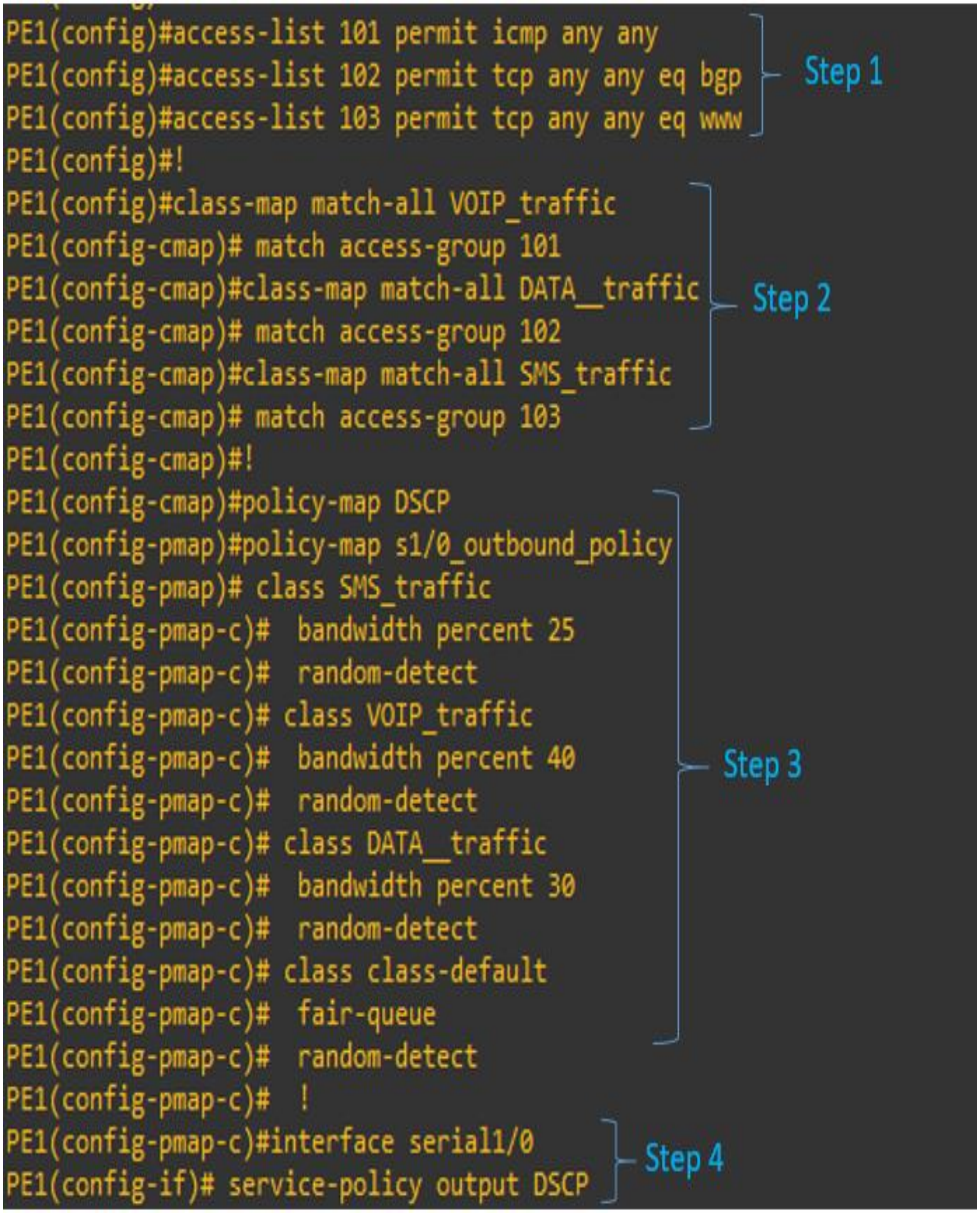
Step1: -Define an Access list

Step2: Define Class map

Step 3: Define a policy map.

Step 4: Apply policy map to the interfaces.

The configuration of Class-based Traffic Marking, shaping, and Policing using DSCP is as below:



```
PE1(config)#access-list 101 permit icmp any any
PE1(config)#access-list 102 permit tcp any any eq bgp
PE1(config)#access-list 103 permit tcp any any eq www
PE1(config)#!
PE1(config)#class-map match-all VOIP_traffic
PE1(config-cmap)# match access-group 101
PE1(config-cmap)#class-map match-all DATA__traffic
PE1(config-cmap)# match access-group 102
PE1(config-cmap)#class-map match-all SMS_traffic
PE1(config-cmap)# match access-group 103
PE1(config-cmap)#!
PE1(config-cmap)#policy-map DSCP
PE1(config-pmap)#policy-map s1/0_outbound_policy
PE1(config-pmap)# class SMS_traffic
PE1(config-pmap-c)#  bandwidth percent 25
PE1(config-pmap-c)#  random-detect
PE1(config-pmap-c)# class VOIP_traffic
PE1(config-pmap-c)#  bandwidth percent 40
PE1(config-pmap-c)#  random-detect
PE1(config-pmap-c)# class DATA__traffic
PE1(config-pmap-c)#  bandwidth percent 30
PE1(config-pmap-c)#  random-detect
PE1(config-pmap-c)# class class-default
PE1(config-pmap-c)#  fair-queue
PE1(config-pmap-c)#  random-detect
PE1(config-pmap-c)#  !
PE1(config-pmap-c)#interface serial1/0
PE1(config-if)# service-policy output DSCP
```

Fig.3.9: Shows Access list, Class-based Traffic Marking, shaping, and Policing configuration using DSCP.

CHAPTER FOUR

4.SIMULATION RESULT AND DISCUSSIONS

4.1. Simulation Results

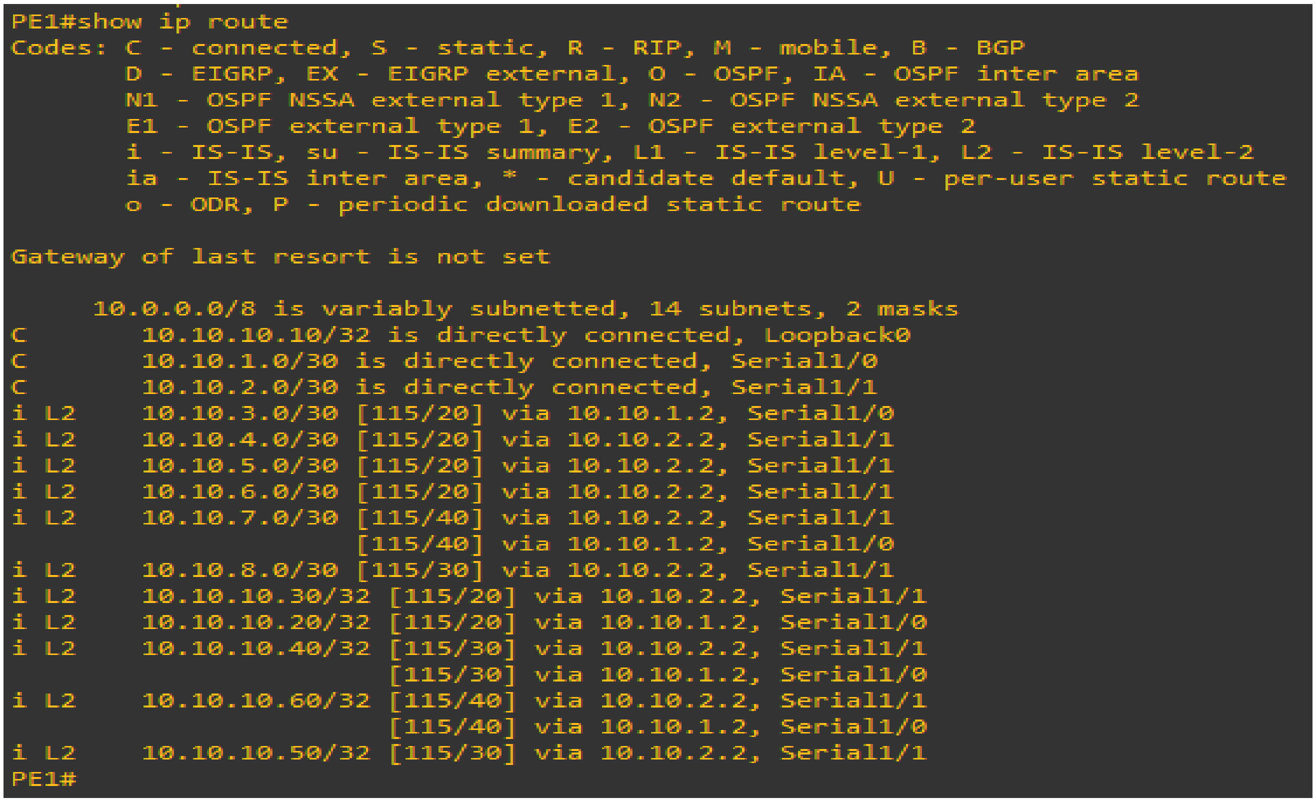
The proper functioning of the designed VoIP QoS network architectures includes:

- ❖ All protocols are fully operating and Proper implementation of the designed VoIP QoS.
- ❖ Provisioning of the necessary services ensuring L3VPN VoIP operation and
- ❖ Redundancy of network resources, which includes rerouting in case of link or node failure.

The necessities for fulfilling these requirements have been discussed with the relevant tests for each of them. To be entrusted with the proper working of the network, first, the basic components have been checked.

4.1.1. IGP protocol (IS-IS)

In the proposed architectures first, the IS-IS operation is checked. Since it is one of the basic components of the designed models. Checking IS-IS routing protocol involves testing its routing information, established neighbors, link-state database, and interface enabled with IS-IS. To check the IS-IS routing information “show IP route” command is used. It checks whether routes are learned by other routers. Route information includes all direct routes and the routes to loopback interfaces.



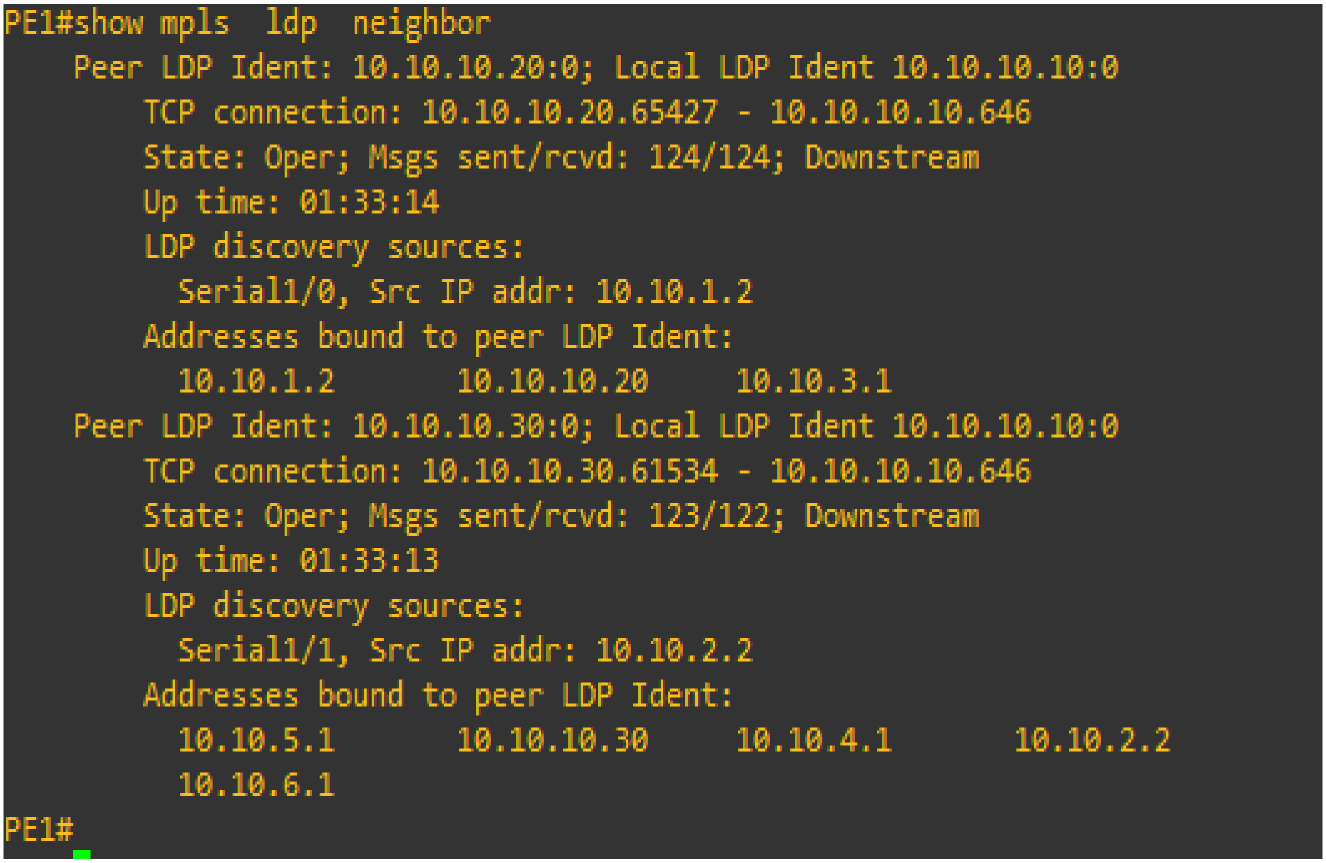
```
PE1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
C       10.10.10.10/32 is directly connected, Loopback0
C       10.10.1.0/30 is directly connected, Serial1/0
C       10.10.2.0/30 is directly connected, Serial1/1
i L2    10.10.3.0/30 [115/20] via 10.10.1.2, Serial1/0
i L2    10.10.4.0/30 [115/20] via 10.10.2.2, Serial1/1
i L2    10.10.5.0/30 [115/20] via 10.10.2.2, Serial1/1
i L2    10.10.6.0/30 [115/20] via 10.10.2.2, Serial1/1
i L2    10.10.7.0/30 [115/40] via 10.10.2.2, Serial1/1
                     [115/40] via 10.10.1.2, Serial1/0
i L2    10.10.8.0/30 [115/30] via 10.10.2.2, Serial1/1
i L2    10.10.10.30/32 [115/20] via 10.10.2.2, Serial1/1
i L2    10.10.10.20/32 [115/20] via 10.10.1.2, Serial1/0
i L2    10.10.10.40/32 [115/30] via 10.10.2.2, Serial1/1
                       [115/30] via 10.10.1.2, Serial1/0
i L2    10.10.10.60/32 [115/40] via 10.10.2.2, Serial1/1
                       [115/40] via 10.10.1.2, Serial1/0
i L2    10.10.10.50/32 [115/30] via 10.10.2.2, Serial1/1
PE1#
```

Fig.4.1: This shows the IS-IS route information.

From the output of these commands, each router is connected to the other device's loopback addresses which is an important prerequisite for the proper functioning of the other components of the proposed network. The outcome of the routers in Fig.3.5 means that the IS-IS protocol successfully established its link-state database of the network and built its routing table.

4.1.2. MPLS LDP Operation

Checking the operation of MPLS involves testing its routing information, MPLS link-state protocol, and MPLS adjacency. To check the MPLS routing information "show MPLS LDP neighbor" command is used.



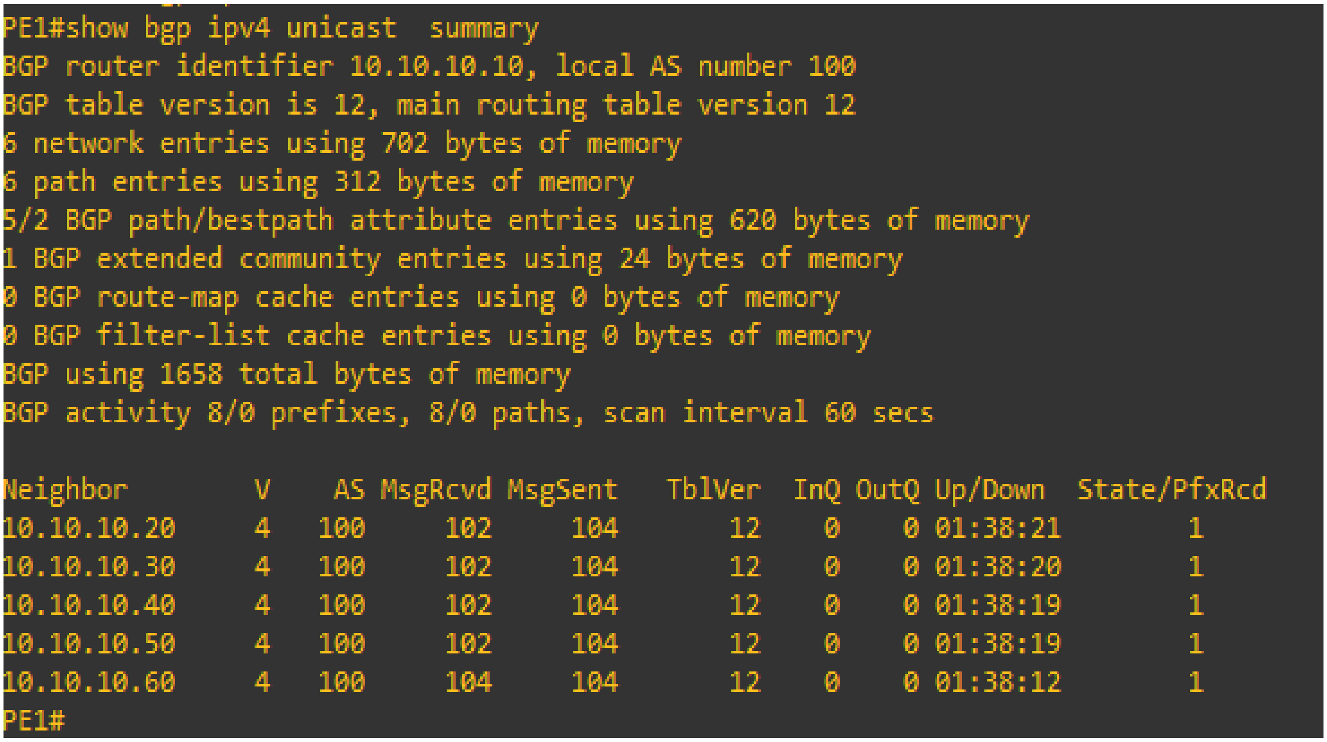
```
PE1#show mpls  ldp  neighbor
    Peer LDP Ident: 10.10.10.20:0; Local LDP Ident 10.10.10.10:0
        TCP connection: 10.10.10.20.65427 - 10.10.10.10.646
        State: Oper; Msgs sent/rcvd: 124/124; Downstream
        Up time: 01:33:14
        LDP discovery sources:
          Serial1/0, Src IP addr: 10.10.1.2
        Addresses bound to peer LDP Ident:
          10.10.1.2       10.10.10.20     10.10.3.1
    Peer LDP Ident: 10.10.10.30:0; Local LDP Ident 10.10.10.10:0
        TCP connection: 10.10.10.30.61534 - 10.10.10.10.646
        State: Oper; Msgs sent/rcvd: 123/122; Downstream
        Up time: 01:33:13
        LDP discovery sources:
          Serial1/1, Src IP addr: 10.10.2.2
        Addresses bound to peer LDP Ident:
          10.10.5.1       10.10.10.30     10.10.4.1       10.10.2.2
          10.10.6.1
PE1#
```

Fig.4.2: This shows the MPLS adjacency information.

The router is configured to send the information explicitly on the path established. Fig.3.4 shows that the interfaces of the routers are fully functional. From. To provide Layer 3 VPN VoIP service MPLS creates a separate routing table. The paths have different labels assigned for forwarding data. LSP configured to create their entries in the routing table that contain information about the metrics of the different paths.

4.1.3. BGP Protocol Operation

Checking the operation of BGP involves testing its routing information. To check the BGP neighbor relationship information “show ipv4 unicast summary” command is used.



```
PE1#show bgp ipv4 unicast  summary
BGP router identifier 10.10.10.10, local AS number 100
BGP table version is 12, main routing table version 12
6 network entries using 702 bytes of memory
6 path entries using 312 bytes of memory
5/2 BGP path/bestpath attribute entries using 620 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1658 total bytes of memory
BGP activity 8/0 prefixes, 8/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.20     4   100     102     104       12    0    0 01:38:21        1
10.10.10.30     4   100     102     104       12    0    0 01:38:20        1
10.10.10.40     4   100     102     104       12    0    0 01:38:19        1
10.10.10.50     4   100     102     104       12    0    0 01:38:19        1
10.10.10.60     4   100     104     104       12    0    0 01:38:12        1
PE1#
```

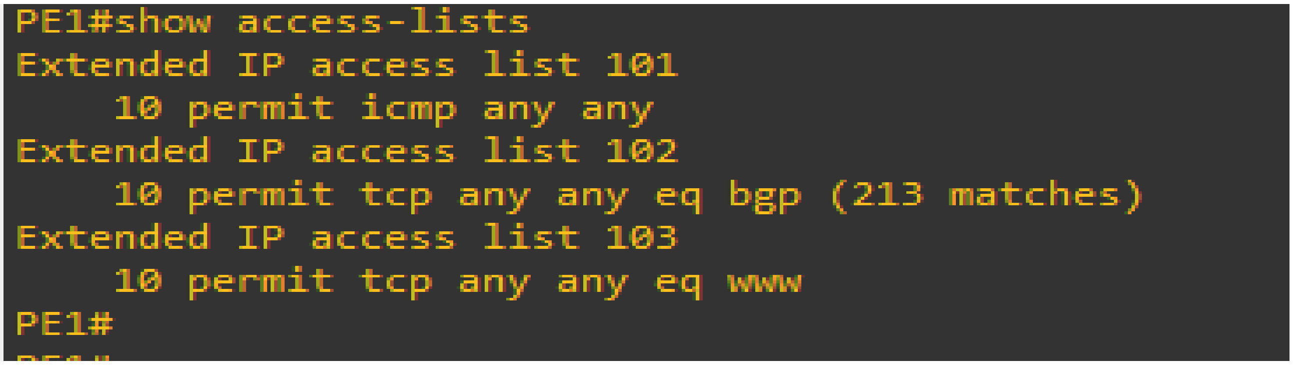
Fig.4.3: Shows BGP neighbor relationship.

Fig.3.6 shows that BGP is fully operational and has established a neighbor relationship. BGP sessions are established. The VoIP L3VPN groups are properly signaled. The end router traffic is properly forwarded and there is communication between the routers in the L3VPN services.

4.1.4. VoIP QoS Operation

To check VoIP QoS operation different parameters are using different methods. Here are the basic VoIP QoS operation confirmation methods.

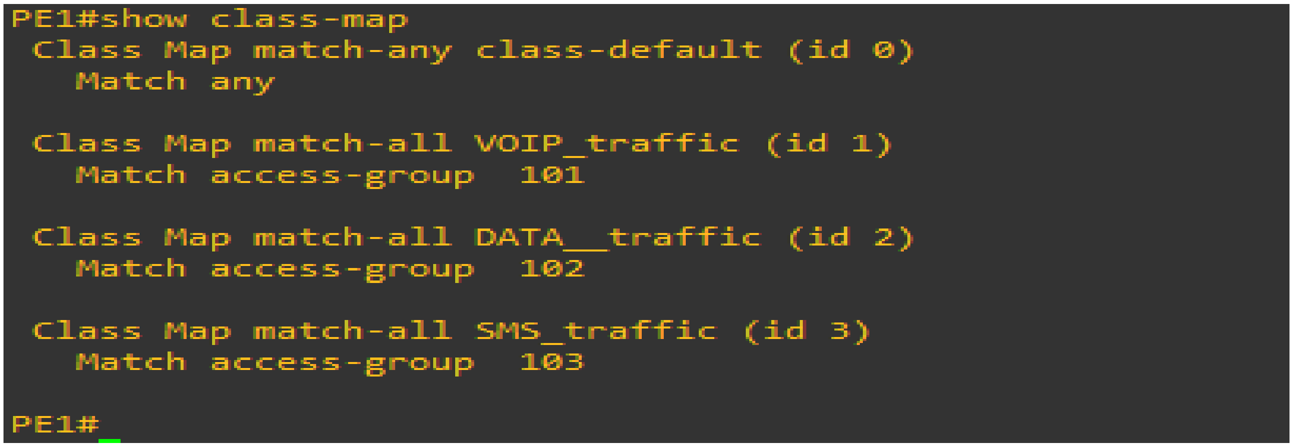
✓ To check the operation access list defined “show access-list” command is used.



```
PE1#show access-lists
Extended IP access list 101
    10 permit icmp any any
Extended IP access list 102
    10 permit tcp any any eq bgp (213 matches)
Extended IP access list 103
    10 permit tcp any any eq www
PE1#
```

Fig.4.4: This shows the Access-list operation.

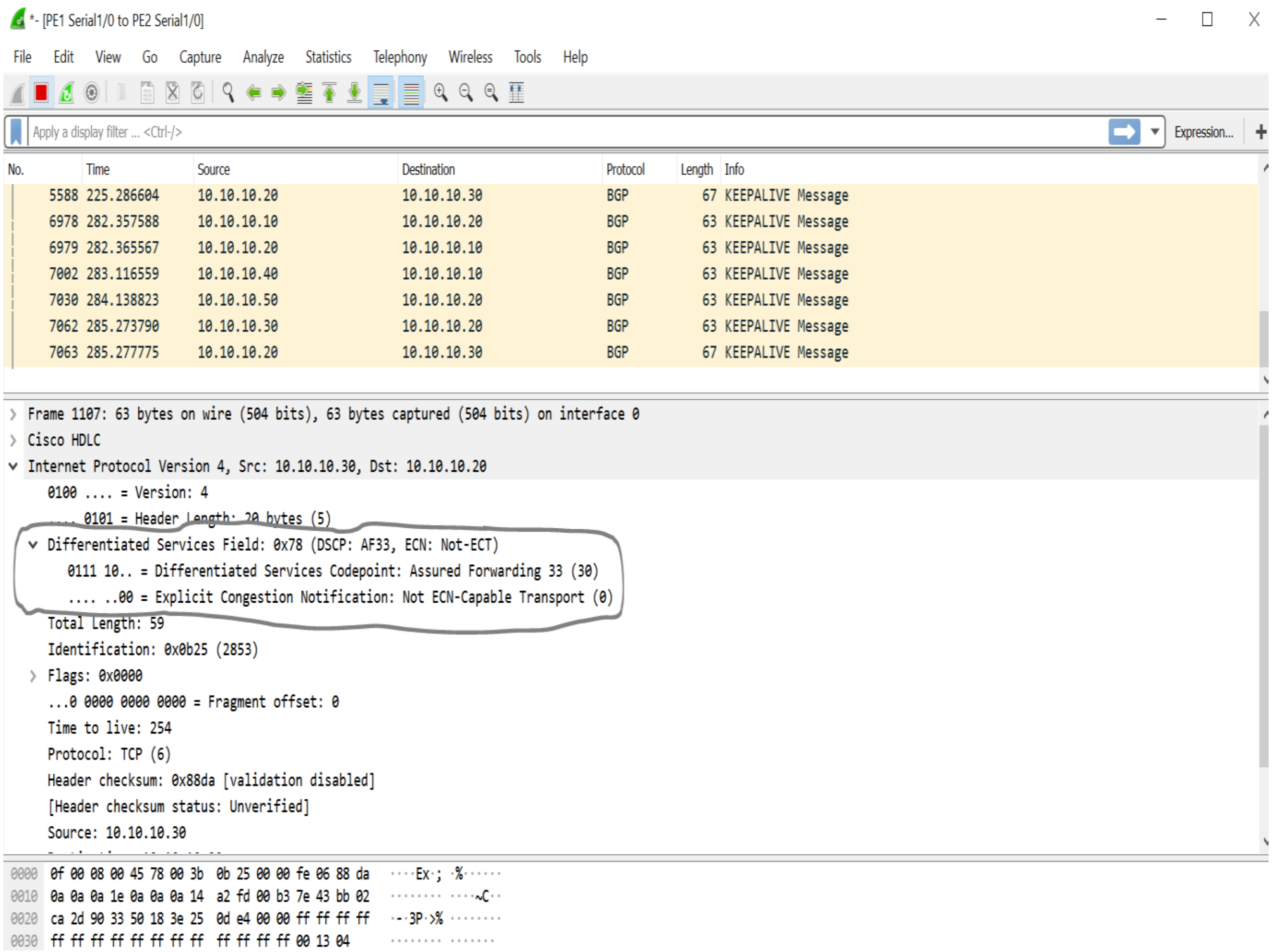
✓ To check the class-map “show class-map” command is used.



```
PE1#show class-map
 Class Map match-any class-default (id 0)
   Match any

 Class Map match-all VOIP_traffic (id 1)
   Match access-group  101

 Class Map match-all DATA__traffic (id 2)
   Match access-group  102

 Class Map match-all SMS_traffic (id 3)
   Match access-group  103

PE1#
```

Fig.4.5: This shows the Class map operation.

✓ To check policy-map differentiated service code point (DSCP) the traffic captured using Wireshark on bound Interfaces.



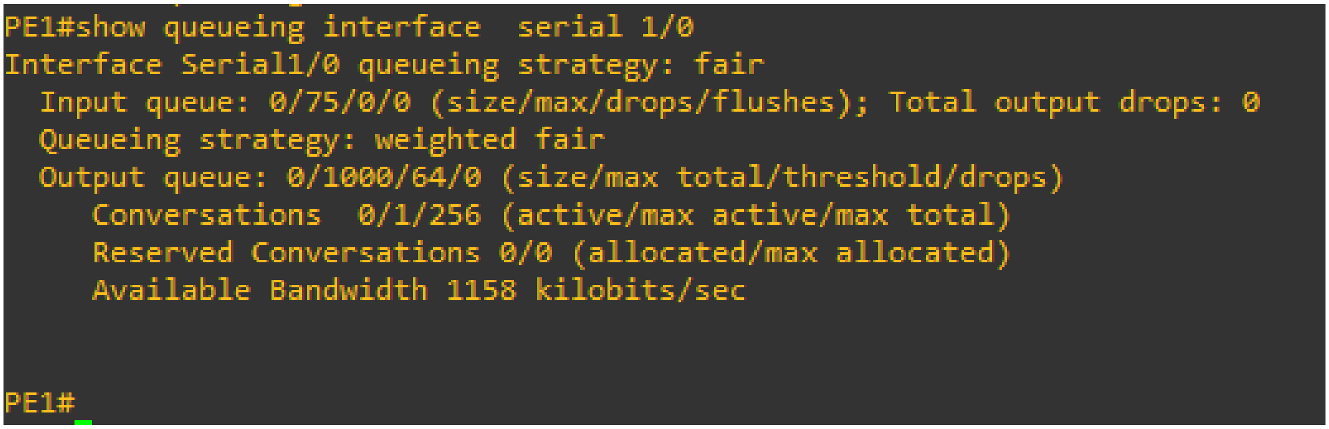
```
No.   Time        Source       Destination  Protocol Length Info
 5588 225.286604  10.10.10.20  10.10.10.30  BGP        67 KEEPALIVE Message
 6978 282.357588  10.10.10.10  10.10.10.20  BGP        63 KEEPALIVE Message
 6979 282.365567  10.10.10.20  10.10.10.10  BGP        63 KEEPALIVE Message
 7002 283.116559  10.10.10.40  10.10.10.10  BGP        63 KEEPALIVE Message
 7030 284.138823  10.10.10.50  10.10.10.20  BGP        63 KEEPALIVE Message
 7062 285.273790  10.10.10.30  10.10.10.20  BGP        63 KEEPALIVE Message
 7063 285.277775  10.10.10.20  10.10.10.30  BGP        67 KEEPALIVE Message
```

```
> Frame 1107: 63 bytes on wire (504 bits), 63 bytes captured (504 bits) on interface 0
> Cisco HDLC
v Internet Protocol Version 4, Src: 10.10.10.30, Dst: 10.10.10.20
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  v Differentiated Services Field: 0x78 (DSCP: AF33, ECN: Not-ECT)
      0111 10.. = Differentiated Services Codepoint: Assured Forwarding 33 (30)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 59
    Identification: 0x0b25 (2853)
  > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 254
    Protocol: TCP (6)
    Header checksum: 0x88da [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.30
```

```
0000  0f 00 08 00 45 78 00 3b  0b 25 00 00 fe 06 88 da   ····Ex·; ·%······
0010  0a 0a 0a 1e 0a 0a 0a 14  a2 fd 00 b3 7e 43 bb 02   ········ ····~C··
0020  ca 2d 90 33 50 18 3e 25  0d e4 00 00 ff ff ff ff   ·-·3P·>% ········
0030  ff ff ff ff ff ff ff ff  ff ff ff ff 00 13 04      ········ ·······
```

Fig.4.6: Shows How differentiated service code point (DSCP) operation.

✓ To check traffic queueing on interfaces “show queueing interface serial 1/0” command used.

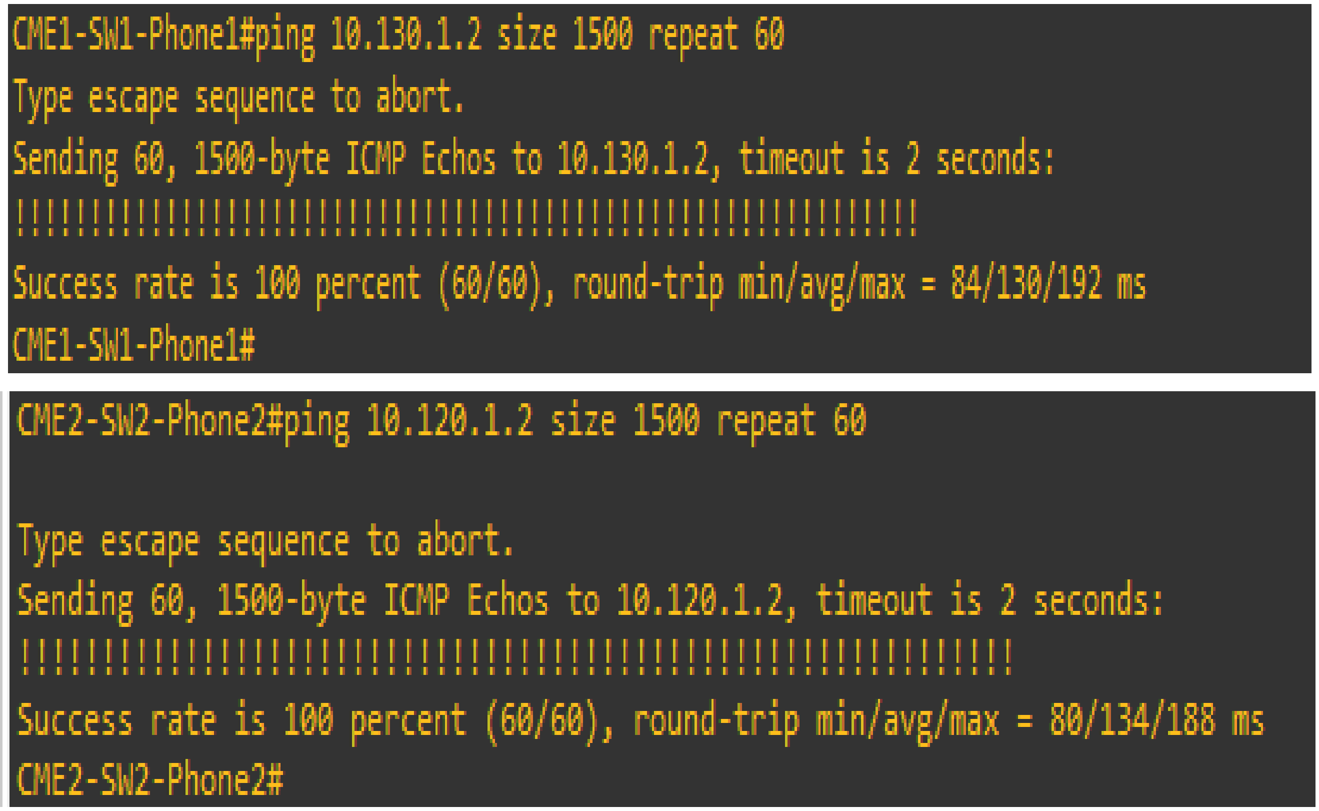


```
PE1#show queueing interface  serial 1/0
Interface Serial1/0 queueing strategy: fair
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec


PE1#
```

Fig.4.7: Shows the Traffic queueing operation.

4.1.5. Performance among VOIP L3VPN Service

The two VoIP L3VPN services are fully functional. To check detail routing information of them ping reachability is checked.



```
CME1-SW1-Phone1#ping 10.130.1.2 size 1500 repeat 60
Type escape sequence to abort.
Sending 60, 1500-byte ICMP Echos to 10.130.1.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (60/60), round-trip min/avg/max = 84/130/192 ms
CME1-SW1-Phone1#
```

```
CME2-SW2-Phone2#ping 10.120.1.2 size 1500 repeat 60

Type escape sequence to abort.
Sending 60, 1500-byte ICMP Echos to 10.120.1.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (60/60), round-trip min/avg/max = 80/134/188 ms
CME2-SW2-Phone2#
```

Fig.4.8: Shows VoIP call service operation.

Generally, when the VoIP QoS of the proposed network architecture was verified using Wireshark, different parameters such as an MP-BGP MPLS, VPN, TE, and Diffserv traffic classification, policing, and shaping are fully functional.

4.2. Representation of Experimental Discussions with Table and Graph

The existing and proposed VOIP architectures are the same in devices used and physical interconnection. But they have differences, especially in VoIP QoS designing like or service classification class mapping Access listing, and traffic prioritization.

Table 4.1. Shows the similarities and differences between the existing and proposed VoIP QoS architecture in a detailed manner.

Mechanisms Used	**Exiting VoIP Architecture Without QoS**	**Proposed VoIP Architecture With QoS**
Traffic Transport through	BGP MPLS VPN	BGP MPLS VPN
VOIP QoS Model	Best effort model	Differentiated services model
Congestion Management	FIFO	Weighted fair queueing
Congestion Avoidance	Tail Drop	Weighted random early detection

VoIP QoS in the proposed network architectures is tested with the Wireshark tool. A couple of scenarios (Fig.3.7) are tested with different traffic streams with different parameters and speeds. The proposed network architecture uses DiffServ QoS Model. The traffic has different priorities. Traffic with a higher priority has been processed first than the others. In the case of traffic Engineering, it uses different mechanisms or algorithms than the older architecture. The proposed architecture uses a weighted fair queueing algorithm for congestion management and a weighted random early detection algorithm for congestion avoidance. In this case, the traffics was classified and priority is given to them depending on their SLA levels. Then traffic policies were defined and applied on an aggregation router outbound interface. In this case, the generated traffic consists of two VoIP VPN instance application traffic streams. The two VPN instance traffic flows emulate two end nodes connected to the CME routers. The traffic streams use TCP with a speed of 10 Mbps and 12 Mbps respectively. The first test is made between CME1 and CME2 and the second test is made between CME2 and CE1 routers. The results of this experiment are given in Fig.4.8.

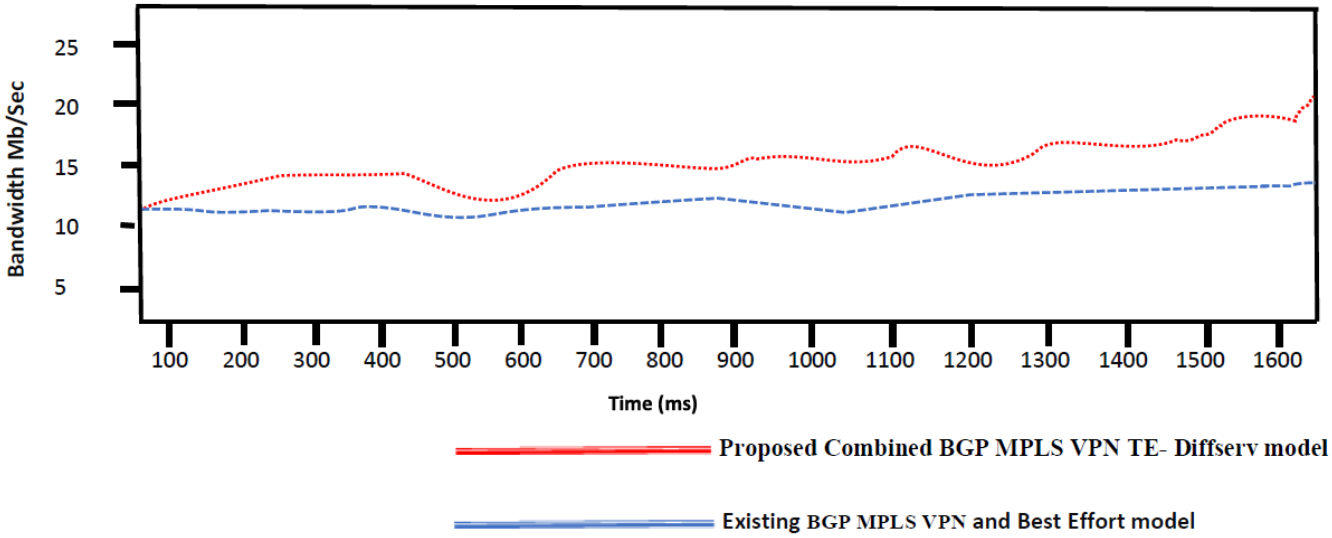


Fig.4.9: Shows the Bandwidth Utilization Measurement Comparison.

After combining BGP MPLS TE VPN -Diffserv Model shows improvement on bandwidth utilization of the proposed VoIP architecture becomes very good. In this case, the network uses the DiffServ QoS model which isolated the network at each aggregation. The isolated aggregate is guaranteed to transmit the maximum number of traffics. So, real-time traffic is transmitted firstly depending on their priorities.

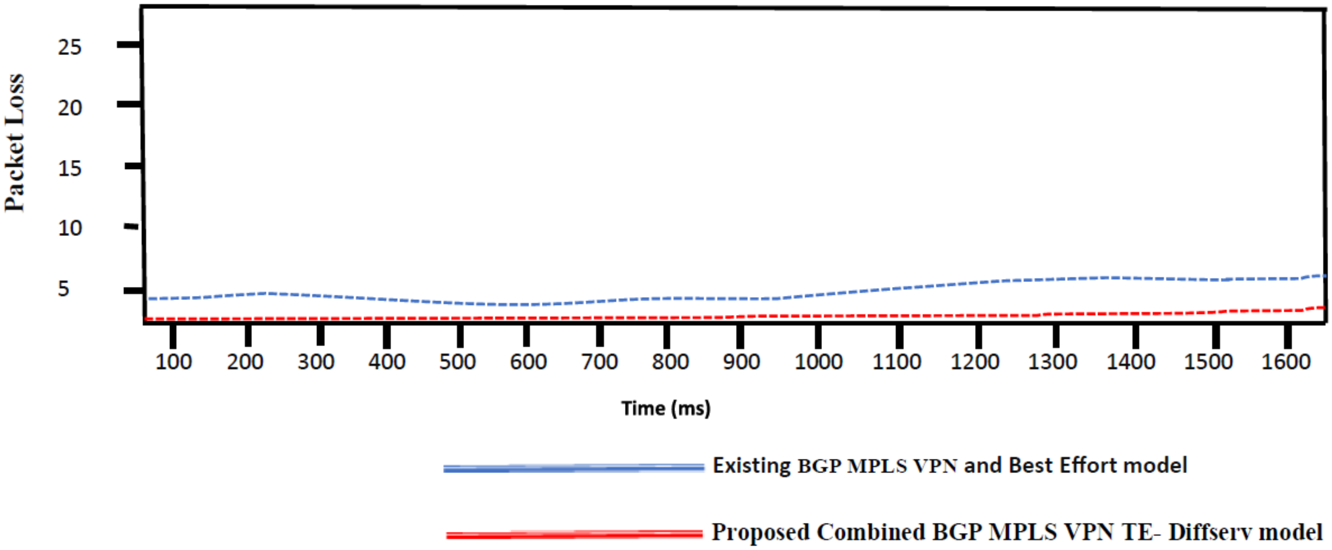


Fig.4.10: Shows the Packet Loss Comparison.

As it can be seen from the evaluation testing of Fig.4.9 the DiffServ QoS model has advantages to minimize or avoid data packet loss. In case of congestion, this model classifies the traffic depending on its priority. The classified traffics is marked and shaped depending on the router's maximum data transfer rate. Some traffic is transmitted, whereas the excess traffics is remarked and transmit later. This decreases the packet loss ratio in the proposed VoIP architecture the packet loss is almost near to zero.

The latency is the time that a packet waits before being transmitted. In the proposed VoIP architecture, the delay and jitter are acceptable, this is because the DiffServ model can guarantee VoIP traffic per aggregation.

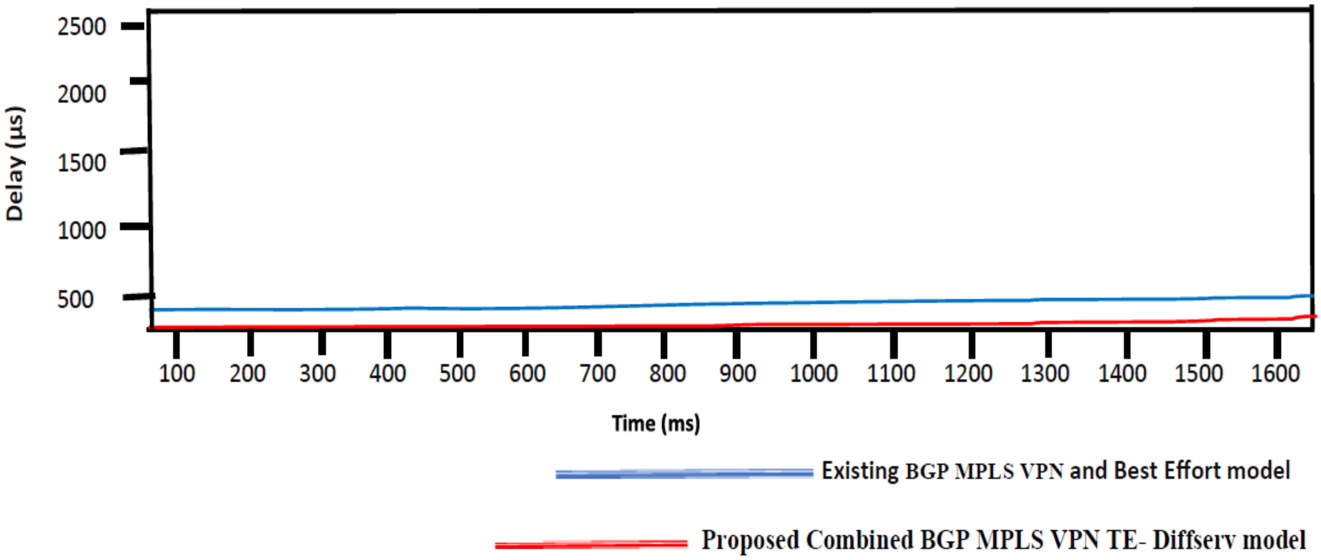


Fig.4.11: Shows the Delay Comparison.

The delay is the time that a packet waits before being transmitted. It can be seen from Fig.4.10; the proposed network architecture shows lower latency compared to the existing network architecture. The reason for this is that the DiffServ model can guarantee the traffic per aggregation.

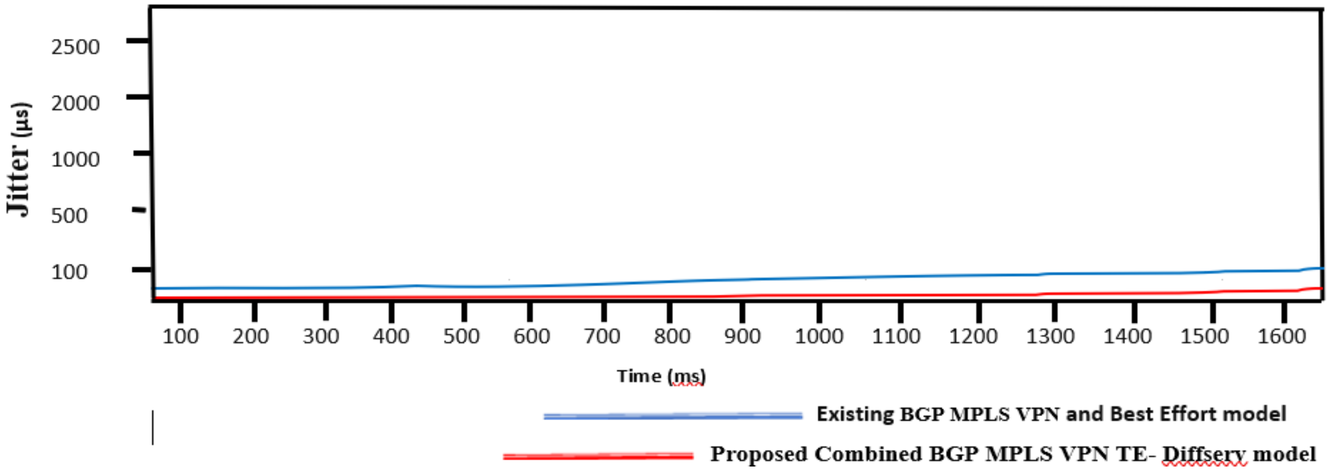


Fig.4.12: Shows the Jitter Comparison.

The jitter is the variation in the delay of received packets. It can be seen from Fig.4.11; the proposed network architecture shows lower jitter compared to the existing network architecture. The reason for this is that the DiffServ model can avoid network congestion. Table 4.2. Shows the Evaluation result and Comparison of existing versus proposed VoIP network performance QoS parameter.

Table 4.2. Shows the numerical result of comparison in between the existing and proposed VoIP QoS architecture.

	Existing (Best Effort) with BGP MPLS VPN VoIP QoS				**Proposed (BGP MPLS VPN DiffServ) VoIP QoS**		
Evaluation parameters	**Exp. Result**	**Ethio Telecom VoIP QoS SLA Targets**	**ITU specification of VoIP QoS Gevin Value**	**ITU Threshold**	**Exp. Result**	**Ethio Telecom VoIP QoS SLA Targets**	**ITU Threshold Value**
Packet loss (%)	1.897	Out off Range	Not > 1	Out off Range	0.526	Within Range & highly improved	Successful & Under Range
Delay(m/sec)	4.644	Within Range	150	Out off Range	0.14	Within Range & highly improved	Successful & Under Range
One-way jitter(m/sec)	45.04	Out off Range	30	Out off Range	30	Within Range & somewhat improved	Successful & Under Range
Bandwidth per call (bit/sec)	14068	Out off Range	20+ kbps	Out off Range	20100	Within Range & highly improved	Successful & Under Range

Generally, I have compared both existing and proposed network topology concerning network performance parameters, most of the results were as expected. The difference between packet loss and bandwidth in existing and on the proposed network architecture there is a visible improvement at all network performance parameters. Also, the difference between end-to-end delay and jitter was visible and meet the VoIP quality of service target of Ethio Telecom SLA and ITU.

If the researcher used more than ten routers on both network architectures. The result of the current output would be increased because of the transmission, serialization, queueing, and processing delay. Generally, if the number of routers (nodes) increased the difference was surly visible in all evaluated VoIP QoS Network performance parameters.

CHAPTER FIVE

5.CONCLUSIONS, RECOMMENDATIONS, AND FUTURE WORKS

5.1 Conclusions

The simulations result of VoIP QoS shows that Voice packet QoS depends on Differentiate of Service (DiffServ) carried through the BGP MPLS VPN TE network with a full configuration of QoS and that make an integrated mechanism that allows MPLS in fast-forwarding of packets plus the specification of DiffServ to decide voice packet served first and which is very useful in the current network traffics like VoIP, Video conference and other multimedia applications are sensitive to delay, jitter and bandwidth. BGP MPLS VPN TE is an optimal choice to service providers in their backbone network to forward packets from source to destination using Traffic Engineering with guaranteed delivery, assured bandwidth, and minimum or no jitter and finally making two end communicating users feel as if they are on the same local area network (Virtual Private Network). This thesis work presents the different QoS available that can support the customers of service level agreements. Also proposes and implements Simplified end-to-end VoIP QoS architecture in the IP network. In the IP network recognize and treat packets belonging to real-time traffic with priority. This involves an access list, traffic marking such packets, classifying the packets based on the markings so that they are given differential treatment, and allowing the scheduling mechanisms to transmit the packets on time. GNS3 free software is used to design and simulate an end-to-end VoIP QoS. Wireshark is used for analyzing the packet loss, delay, jitter, and bandwidth utilization in a designed network. Finally, the simulation result shows that in the proposed VoIP architecture the packet loss reduced from1.897% to 0.526%, bandwidth utilization increased from 14068bit/sec to 20100 bit/sec, delay reduced from 14.644 m/sec to 0.14m/sec, and jitter reduced from 45.04 m/sec to 30m/sec which are acceptable with the ITU threshold values. This is the result that can be achieved because the DiffServ model can guarantee VoIP traffic per aggregation.

5.2 Recommendations

Ethio Telecom should have to combine BGP MPLS VPN TE and Diffserv Model to improve Voice over Internet Protocol Quality of Service. To balance and satisfy the customer expectation of VoIP Quality of service afforded by Ethio Telecom by Integrating a Unified communication system must be implemented in addition to improving VoIP Quality of service provided to the customer. Ethio Telecom should have worked hard on the VoIP QoS sector because, this technology creates greater potential for huge revenue collection, cost savings, or lowers operational costs and increases organizational productivity. Ethio Telecom should have fully implemented VoIP QoS, which allows the company the converging various systems into one. these means With IP telephony the user can gate voice, data, video, and multimedia technologies into one unified system that is digital-based. Ethio Telecom should have Hosted VoIP Qos Solution monitored from a 24/7/365 Network Operation Center. In addition to Best Effort QoS, Ethio Telecom can improve VoIP QoS by implementing Differentiated Services, Multiprotocol Label Switching, Resource Reservation Protocol, and Subnet Bandwidth Manager (SBM). To provide the SLA target signed with the customer Ethio Telecom should have also integrated VoIP QoS network Monitoring tools and applications like Embedded VoIP monitoring software. e.g MyVoIP, VoIP Spear web service, VoIP monitor. MyVoIP Speed online VoIP connection test: that reports jitter, packet loss, bandwidth quality. VoIP Spear web service that monitors your VoIP quality 24x7x365. VoIP monitor is an open-source live network packet sniffer which analyzes SIP and RTP protocol. VoIP monitor also capable of Predicts MOS-LQE score according to ITU-T G.107 E-model, Detailed delay/loss/MOS statistics stored to MySQL, and Each call is saved as a standalone file. Ethio Telecom should have also Monitor Ethernet Traffic and Debugging displays from a VOIP program. Ethio Telecom should have Implementing Diynamic and predictive network monitoring like
Software-Defined Network.

5.3 Future Works

In future work, there will need to generate real traffics or high traffic to show the effects of DiffServ and, we need an application tool that generates more results than Wireshark to analyze more things which is a lack of graphics results. The other researcher can apply Integration of Voice mail Advanced IVR capability, Automated wake up and alarm, Voice Activity Detection (VAD)to enhance VoIP QoS. One of the most open areas of this study that is not covered in this study was VoIP QoS Integration with security systems concerns which will be answered by other researchers in the future. There is also the interest in Integrating a Unified communication system to all VoIP and which helps for the implementation of fruitful VoIP QoS. In addition to using the MPLS DiffServ mechanism to improve VoIP QoS by classifying, prioritizing, and transmit voice traffic in the Ethio Telecom network, there is also another efficient way to improve VoIP QoS by Perform Evaluation of Voice call quality using standard Evaluation tools and improving VoIP Voice call quality. voice quality is one the main measurement VoIP QoS, which have a major impact on the deployment of a guaranteed communication of VoIP QoS system. As a result, in the coming researchers can work on VoIP Call quality evaluation using E-model. I hope researchers also need to include different call quality factors like fidelity, echo, and sidetone, and background noise to improve VoIP QoS provide to SLA customers. Multiple connectivity options (E1/T1, ISDN. Analogue, GSM, VOIP, and Radio) and Support for multiple user terminals from different vendors is also an open area of study for the future. The researcher can also work on Hosted VoIP Qos Solution monitored from a 24/7/365 NOC.

References

[1]. M. Shahidul & S.Nasir, "How Different QoS Mechanisms Affect VoIP QoS Metrics", *M.S thesis, University of Halmstad, Sweden*, PP.1-11, June 2010.

[2] Y.Wang and Ch.Huang" QoSaaS: Quality of Service as a Service ", *International Journal of Modern Engineering Sciences, Yale University*, March 2011

[3].I.Lopetegui Cincunegui, *"*Quality of Service for VoIP in Wireless Communications *"*, *Ph.D. , Thesis of Newcastle University* March 2011

[4]. Sh. Jadhav and H. Zhang, et. l, "Performance Evaluation of Quality of VoIP in WiMAX and UMTS "*on 12th Proc. IEEE International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), pp. 375 – 380,*22 October 2011.

[5]. K. Kumar and V. Mahadevan et al. ''Voice over IP (VoIP)" Nov 25, 2020

[6]. F. Tesfaye, *"VoIP Investigation and Challenges – Case: Ethiopian Telecommunications", Bachelor´s. thesis, University of Turku, pp.1-3,* 2014.

[7]. Ethio Telecom, *"QoS Document" MPLS VPN Services Quality and Customer Experience Related Issues and Complaint Analysis",* Version 02, 2017.

[8]. Ing. F. BOI., "QoS-based Playout Control in IP Telephony over NGNs", *Ph.D. University of Cagliari, Italy, pp 8-10,* March 2010.

[9].Nadeem U., ''How to Improve Your VoIP Network", PP 1-22, Jan.31, 2019.

[10]. Sruti Gan Ch., "Design and Implementation of a Differentiated Service-Based QoS Model for Real-Time Interactive Traffic on Constrained Bandwidth IP Networks", *MS. Thesis, Kharagpur University*, February 2010.

[11]. A. Agarwal, *"Quality of Service (QoS) in the New Public Network Architecture*", pp. 22 -25, 2000.

[12]. Mahmoud Ahmed A. Al-Asri, and Ammar T. A. Zahary, et al. "MPLS Network Optimization for VoIP Using DiffServ with Multiple ER-LSP". *Computational and Applied Mathematics Journal. Vol. 1, No. 5, pp. 249-260,* 2015.

[13]. P.Ó Flaithearta, "Optimizing the QoS of VoIP Applications over WiFi through use of Synchronized Time", *Ph.D. Thesis, University of Ireland Galway, Ireland,* Jan. 2015.

[14]. M. Daka "Traffic Analysis of IP Core Networks: The Case of Ethio Telecom." *MB. thesis, Addis Ababa, University, Ethiopia,* May 2017.

[15]. Sh. Asrat, , "Improving Quality of Service of Border Gateway Protocol Multiprotocol Label Switching Virtual Private Network of EthioTelecom Service Level Agreements", *MS. thesis, St. Mary's University, Addis Ababa, Ethiopia, PP.6-8,* June 2018.

[16]. K. Lee**,** MS. Thesis, "Global QoS model in the ISP networks: DiffServ-aware MPLS Traffic Engineering",7 Nov 2006.

[17]. H. Assem and D. Malone, "Monitoring VoIP Call Quality Using Improved Simplified E-model*"*, *MS.Thesis, National University of Ireland,* 2012.

[18]. Cisco Unified Communications Manager Architecture, Chapter 1,

[19]. Huawei Technologies, "How to configure MPLS VPN" *MPLS with BGP, May 2017.*

[20] B. Feyissa "SLA for Enterprise Customer with Class of Service*", EthioTelecom Marketing Division SLA Service Level Agreement Circular and Minute of meeting Service*", July 2019.

[21]. Shahid Ali and Bilal Zahid Rana, "OPNET Analysis of VoIP over MPLS VPN with IP QoS", *MS. Thesis, Karlskrona University, Sweden, March 2011.*

[22]. Spirent Communications, *"Voice over IP (VoIP)", Vol.1, pub., pp.1-52,* 2001.

[23]. Ing. F. BOI, "QoS-based Playout Control in IP Telephony over NGNs", Ph.D. University of Cagliari, Italy, March 2010.

[24]. Cisco Press, “MPLS VPN QoS Design”, *End-to-End QoS Network Design, volume 3, March* 2017.

[25]. J.Kharel and D.Adhikari, “Performance Evaluation of Voice Traffic over MPLS Network with TE and QoS Implementation”, *MS. Thesis University of Karlskrona, Sweden,* PP 16-21,November 2011.

[26]. Comrex, “An Overview of VoIP Technology, How It Works, and How to Use It.”, internet: https://www.comrex.com/wp-content/uploads/2016/07/VoIP-and-SIP-Primer.pdf., Dec. 12, 2019 [Nov.10, 2020].

[27]. B. Enache and I. Gina, “Method for implementing, simulating and analysis of VoIP Network*”, presented at 6th Int. Conf. on Modern Power system (MPS), Cluj-Napoca, Romania, pp109- 110,* May 2015.

[28]. James Yu and Imad Al-Ajarmeh, "Call Admission Control and Traffic Engineering of VoIP, Proceedings *of The Second IEEE International Conference on Digital Telecommunications " (ICDT 2007), San Jose, California, USA, pp. 11-16,* July 2007.

[29]. R. Shankar & Dr. E. Karthikeyan, "VoIP Packet Delay Techniques: A Survey," *Global Journal of Computer Science and Technology: E,* vol. Volume 14, no. Issue 3, 2014.

[30]. U. R. ALO and N. Henry Firday, “Voice over Internet Protocol (VOIP): Overview, Direction, and Challenges”, *Journal of Information Engineering and Applications, Vol.3, No.4, pp.19-24,*2013.

[31]. Dr. Bur Goode, “Voice over Internet Protocol (VoIP)”, *Proc. on the IEEE, Vol. 90, No. 9, pp.1-23,* Sept,2002.

[32]. G**.** H. Sabri**,** “QoS in MPLS and IP Networks” *M.B. Thesis, University of Karlskrona, Sweden, 9th November* 2009.

[33]. A. Lazzez and T. Slimani, *“Deployment of VoIP Technology: QoS Concerns*”, Vol. 2. Issue 9, pp. 1-3, Dec 2013.

[34]. F. Alsoubaie “Voice over Internet Protocol (VoIP) Best Service Provider Decision Making with Using Hierarchical Decision Model (HDM)” *BS.Degree project paper, Portland State University,* Dec 2018.

[35] Paul J. Fong, Eric Knipp, and David Gray., *Configuring Cisco Voice Over IP, 2nd Edi,* Syngress Publishing, Inc., 800 Hingham Street, Rockland, pp-167-342, 2002.

[36]. R. Alexander, "An Analysis of the MOS under Conditions of Delay, Jitter and Packet Loss and an Analysis of the Impact of Introducing Piggybacking and Reed Solomon FEC for VOIP", *M.S. Thesis, University of Georgia State,* 2007.

[37]. A. M. Alsahlany and H. S. Rashid, "Audio Codecs Impact on Quality of VoIP Based on IEEE802.16e Considering Mobile IP Handover.", *American Journal of Networks and Communications. Vol. 4, No. 3, pp. 59*-*66*, 2015.

[38]. I.A. Almerhag and N. Aboalgasm, "The Effect of Mobility on the Performance of VoIP Application in WiMAX Networks.", *In Proc.,1st Conference of Industrial Technology*,2017.

[39]. N. H. Almofary*, H. S. Moustafa, F. W. Zaki, *"Optimizing QoS for Voice and Video Using DiffServ-MPLS", International Journal of Modern Computer Science & Engineering, Vol.1 Issue 9, pp 1-15,* December 2012.

[40]. P. Eugen *"An MPLS Simulation for Use in Design Networking for Multi-Site Businesses",* Vol. XVII. Issue 1, pp 1-7, 2017.

[41]. Huawei Technologies, "How to configure MPLS VPN" *MPLS with BGP, May 2017.*

[42] N. H. Almofaria, and H. S. Moustafa, et. l"Study of Voice and Video Performance on IP and MPLS Networks", *International Journal of Modern Science & Engineering, Mansoura University, Yemen, Vol.1, No.1, pp 1-9,* 2013.

[43]. R. Zhang and M. Bartell, "*BGP Design and Implementation*", Indianapolis, Cisco Press,2004.

[44] Ph. Smith & B.Greene "BGP Best Current Practices" *Cisco ISP/IXP Workshop, Last updated 4th September 2016 Last updated 7th* December 2018.

[45]. J. Lawrence, *"*Designing Multiprotocol Label Switching Networks*", Communications Magazine, IEEE,* July 2012.

[46]. M. C. Castro, N. A. Nassif etal., “QoS Performance Evaluation in BGP/MPLS VPN”, University of Campinas, Brazil, Tech.Report.,2003.

[47]. M. Nasr Alhady, “Improve the QoS by Applying Differentiated Service over MPLS Network”, International *Journal of Computer Science and Mobile Computing, Vol.4 Issue.9, pg. 84-91,* September 2015.

[48] Raman and S.Baghla *et al.,* “Method & Implementation Of Data Flow To Improve QoS In MPLS Network”, *Journal of Applied Engineering Letters Vol. 1, No 4, PP.105-110,* December 2016.

[49] I.Pepelnjak and J.Guichard et al., “MPLS and VPN Architectures”, *Cisco Press , Vol. 1, No 4, PP 25-49,May 23,* 2002.

[50]. V. Alwayn,” Advanced MPLS Design and Implementation”, *Cisco Systems*, Cisco press 201, 2011.

[51] A. Albdoor and G.Kannan “Analysis of MPLS and IP Networks Performance to Improve the Qos using Opnet Simulator ”, *Journal of Emerging Trends in Computing and Information Sciences, Vol. 8 No. 1, pp,* January 2017.

[52] A. Albdoor and G.Kannan “Analysis of MPLS and IP Networks Performance to Improve the Qos using Opnet Simulator ”, *Journal of Emerging Trends in Computing and Information Sciences, Vol. 8 No. 1, pp 1-56,* January 2017.

[53]. R.Chakravorty and S.Kar, et al. “End-to-End Internet Quality of Service (QoS): An Overview of Issues, Architectures and Frameworks. *Proc. of ICIT, December*., 2000.

[54] Cisco Press Systems “Virtual Route Forwarding Design Guide for VRF-Aware Cisco Unified Communications Manager Express”,2008.

[55]. PCCW Global’s, “MPLS VPN Service”, Oct 29, 2013.

[56]. EthioTelecom, *“*EthioTelecom, Citizen’s Charter Document*”, Tech.Report pp. 1-36, issued.1, August 31,* 2014.

[57]. Huawei technologies co. ltd, "Configuration Guide VPN", *Huawei technologies- Cloud Engine 12800 Series Switches,* volume 06, pp 5-7., Sept. 2017.

[58]. E.Osborne and A.Simha "Traffic Engineering with MPLS" July 17, 2002.

[59]. Cisco press "MPLS Traffic Engineering DiffServ Configuration Guide" Cisco Systems, Inc 2011.

[60] D.Egbenyon, "Implementing QoS for VoIP in a Local Area Network (LAN)'', *BS. Degree, Turku University,* Nov 2011.

[61] A. Albdoor and G.Kannan "Analysis of MPLS and IP Networks Performance to Improve the Qos using Opnet Simulator ", *Journal of Emerging Trends in Computing and Information Sciences, Vol. 8 No. 1, pp 26- 39,* January 2017.

[62]. A. Ranjbar, "CCNP Certification Guide", First *Edition, Cisco Press 800* USA, 2013.

[63] A. Shabbir Khan & B.Afzal, "MPLS VPNs with DiffServ – A QoS Performance Study" *MS. thesis, Halmstad University, Sweden,* February 2011.

[64]. Prof. Dr. T. Janevski "QoS and QoE frameworks for converged services and applications", *Regional Workshop for Europe, Methodius University in Skopje, Bologna, pp 25-26,* Nov, 2015.

[65]. ITU, "QoS Parameters", *ITU-T Y.1541 Recommended QoS Target,* June 2012.

[66]. Sh. Asrat, , "Improving Quality of Service of Border Gateway Protocol Multiprotocol Label Switching Virtual Private Network of EthioTelecom Service Level Agreements", *M.S Thesis ,St. Mary's University, Addis Ababa, Ethiopia, PP21-22* June 2018.

[67] B. Feyissa "SLA for Enterprise Customer with Class of Service", *EthioTelecom Marketing Division SLA Service Level Agreement Circular and Minute of meeting Service",* July 2019.

[68]. K. Lee**,** M.Thesis, "Global QoS model in the ISP networks: DiffServ aware MPLS Traffic Engineering", pp. 7-15, Nov 2006

[69]. A. Lazzez and T. Slimani, *"Deployment of VoIP Technology: QoS Concerns*", Vol. 2. Issue 9, pp. 7-11, Dec 2013.

[70]. Sh. Asrat, “Improving Quality of Service of Border Gateway Protocol Multiprotocol Label Switching Virtual Private Network of EthioTelecom Service Level Agreements”, M.*S Thesis, St. Mary’s University, Addis Ababa, Ethiopia, Vol. 1 No. 1, pp.20-29,* June 2018.

[71]. J.Kharel and D.Adhikari, M.S. Thesis, “Performance Evaluation of Voice Traffic over MPLS Network with TE and QoS Implementation”, University of Karlskrona, Sweden, Vol. 1. Issue 1, pp. 1-16, November 2011.

[72]. Sh. Asrat, “Improving Quality of Service of Border Gateway Protocol Multiprotocol Label Switching Virtual Private Network of EthioTelecom Service Level Agreements”, *M.S Thesis, St. Mary’s University, Addis Ababa, Ethiopia, Vol. 1. Issue 1, pp. 26-31,* June 2018.

[73]. M. Shahidul & S.Nasir, “How Different QoS Mechanisms Affect VoIP QoS Metrics”, *M.S thesis, University of Halmstad, Sweden, Vol. 1. Issue 1, pp. 27-30,* June 2010.

[74]. G**.** H. Sabri**,** “QoS in MPLS and IP Networks” M.B. Thesis, University of Karlskrona, Sweden, Vol. 1. Issue 1, pp. 54-56, November 2009.

[75]. J.Kharel and D.Adhikari, “Performance Evaluation of Voice Traffic over MPLS Network with TE and QoS Implementation”, *M. Thesis University of Karlskrona, Sweden, Vol. 1. Issue 1, pp. 15-21,* Nov 2011.

[76]. Cisco Systems and Telecommunications et al. ‘‘Voice & Data Convergence’’, January 11, 2001.

[77] cisco press “Quality of Service for Voice over IP’’, Vol. 1. Issue 1, pp. 1-30, April 13, 2011.

[78] K. Muhhin, “QoS Implementation on Network Devices*”, Master Thesis, Tallinn University, Tallinn Estonia,* May 31, 2010.

[79]. A. Lazzez and T. Slimani, *“Deployment of VoIP Technology: QoS Concerns*”, Vol. 2. Issue 9, pp. 1-32, Dec 2013.

[14]. M. Daka “Traffic Analysis of IP Core Networks: The Case of Ethio Telecom.” M.B. thesis, Ethiopia, pp. 1-40, May 2017.

[80]. N. H. Almofary*, H. S. Moustafa, F. W. Zaki, *“Optimizing QoS for Voice and Video Using DiffServ-MPLS”, International Journal of Modern Computer Science & Engineering, Vol.1* Issue 9, pp.1-32, December 2012.

[81]. M. Daka “Traffic Analysis of IP Core Networks: The Case of Ethio Telecom.” *M.B. thesis, Ethiopia, Vol.1 Issue 9, pp.18-32*, May 2017.

[82]. H. Singh and M. Mian, (May 2016.) *“Comparative Study and Analysis of various VoIP coding Algorithms”,* Vol. 141.Issue 2. PP.975-8880, Jan 30, 2019.

[83]. J. R. Schneir and T. Plu¨Ckebaum, *“VoIP network architectures and impacts on costing”*., Vol. 12 Issue. 3, pp. 59-72, May 2010

[84] I. D. Constantiou and Y. K. Dwivedi, *“*The Diffusion of IP-Telephony and The Vendors’ Commercialization Strategies*”,* June 2010.

[85]. P.Ó Flaithearta, “Optimizing the QoS of VoIP Applications over WiFi through use of Synchronized Time”, *Ph.D. Thesis, University of Ireland Galway, Ireland, PP.86 -90,* Jan. 2015.

[86]. J.Kharel and D.Adhikari, “Performance Evaluation of Voice Traffic over MPLS Network with TE and QoS Implementation”, *MS. Thesis University of Karlskrona, Sweden, PP 1-44,*November 2011.

[87]. Nadeem U., ‘‘How to Improve Your VoIP Network”, PP 1-27, Jan.31, 2019.

[88]. U. R. ALO and N. Henry Firday, “Voice over Internet Protocol (VOIP): Overview, Direction, and Challenges”, *Journal of Information Engineering and Applications, Vol.3, No.4, pp.1-28,*2013.

[89]. M. Shahidul & S.Nasir, “How Different QoS Mechanisms Affect VoIP QoS Metrics”, *M.S thesis, University of Halmstad, Sweden*, *PP.1-47,* June., 2010.

[90]. A. Lazzez and T. Slimani, *“Deployment of VoIP Technology: QoS Concerns”, Vol. 2. Issue 9, pp. 1-8, Dec* 2013.

[91]. N. H. Almofary*, H. S. Moustafa, F. W. Zaki, *“Optimizing QoS for Voice and Video Using DiffServ-MPLS”, International Journal of Modern Computer Science & Engineering, Vol.1* Issue 9, pp.1-32, December 2012.

[92]. Huawei technologies co. ltd, “Configuration Guide VPN”, *Huawei technologies- Cloud Engine 12800 Series Switches, volume 06, pp 1-7.,* Sept. 2017.

[93]. F. Tesfaye, *“VoIP Investigation and Challenges – Case: Ethiopian Telecommunications”, Bachelor´s. thesis, University of Turku, pp.20-35,* 2014.

[94]. EthioTelecom, *“*EthioTelecom, Citizen’s Charter Document*”, Tech. Report pp. 1-36, issued.1, August 31,* 2014.

[95]. E. Osborne and A.Simha, *Design, configure and manage MPLS TE to optimize network performance.* United States of America, Indianapolis, Cisco Press, July 17, 2002.

[96]. B. Enache and I. Gina, “Method for implementing, simulating and analysis of VoIP Network*”, presented at 6th Int. Conf. on Modern Power system (MPS), Cluj-Napoca, Romania, pp 110-112,* May 2015.

[97]. M. Shahidul & S.Nasir, “How Different QoS Mechanisms Affect VoIP QoS Metrics”, *M.S thesis, University of Halmstad, Sweden, PP.1-47,* June 2010.

Appendices

P1 Configuration

```
hostname P1
!
no ip domain lookup
mpls label protocol ldp
!
ip tcp synwait-time 5
!
interface Loopback0
 ip address 10.10.10.30 255.255.255.255
 ip router isis 100
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial1/0
 ip address 10.10.5.1 255.255.255.252
 ip router isis 100
 mpls ip
 serial restart-delay 0
```

P2 Configuration

```
hostname P2
!
no ip domain lookup
mpls label protocol ldp
!
interface Loopback0
 ip address 10.10.10.40 255.255.255.255
 ip router isis 100
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 ip address 10.10.7.1 255.255.255.252
 ip router isis 100
 mpls ip
 clock rate 1000000
!
interface Serial1/0
 ip address 10.10.5.2 255.255.255.252
 ip router isis 100
 mpls ip
 serial restart-delay 0
 clock rate 1008000
 clock rate 100800
!
interface Serial1/0.10
 ip address 10.10.4.1 255.255.255.252
 ip router isis 100
 mpls ip
!
interface Serial1/1
 ip address 10.10.2.2 255.255.255.252
 ip router isis 100
 mpls ip
 serial restart-delay 0
 clock rate 100800
!
interface Serial1/2
 ip address 10.10.6.1 255.255.255.252
 ip router isis 100
 mpls ip
 serial restart-delay 0
 clock rate 1008000
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
router isis 100
 net 49.0000.1010.1030.00
 is-type level-2-only
 metric-style wide
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 10.10.10.10 remote-as 100
 neighbor 10.10.10.10 update-source Loopback0
 neighbor 10.10.10.20 remote-as 100
 neighbor 10.10.10.20 update-source Loopback0
 neighbor 10.10.10.40 remote-as 100
 neighbor 10.10.10.40 update-source Loopback0
 neighbor 10.10.10.50 remote-as 100
 neighbor 10.10.10.50 update-source Loopback0
 neighbor 10.10.10.60 remote-as 100
 neighbor 10.10.10.60 update-source Loopback0
```

```
!
interface Serial1/0.10
 ip address 10.10.4.2 255.255.255.252
 ip router isis 100
 mpls ip
!
interface Serial1/1
 ip address 10.10.3.2 255.255.255.252
 ip router isis 100
 mpls ip
 serial restart-delay 0
 clock rate 1008000
!
interface Serial1/2
 ip address 10.10.7.1 255.255.255.252
 ip router isis 100
 serial restart-delay 0
 clock rate 1008000
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
router isis 100
 net 49.0000.1010.1040.00
 is-type level-2-only
 metric-style wide
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 10.10.10.10 remote-as 100
 neighbor 10.10.10.10 update-source Loopback0
 neighbor 10.10.10.20 remote-as 100
 neighbor 10.10.10.20 update-source Loopback0
 neighbor 10.10.10.30 remote-as 100
 neighbor 10.10.10.30 update-source Loopback0
 neighbor 10.10.10.50 remote-as 100
 neighbor 10.10.10.50 update-source Loopback0
 neighbor 10.10.10.60 remote-as 100
 neighbor 10.10.10.60 update-source Loopback0
 !
 address-family ipv4
 !
 address-family ipv4
 neighbor 10.10.10.10 activate
 neighbor 10.10.10.10 send-community both
 neighbor 10.10.10.20 activate
 neighbor 10.10.10.20 send-community both
 neighbor 10.10.10.40 activate
 neighbor 10.10.10.40 send-community both
 neighbor 10.10.10.50 activate
 neighbor 10.10.10.50 send-community both
 neighbor 10.10.10.60 activate
 neighbor 10.10.10.60 send-community both
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.10.10.10 activate
 neighbor 10.10.10.10 send-community both
 neighbor 10.10.10.20 activate
 neighbor 10.10.10.20 send-community both
 neighbor 10.10.10.40 activate
 neighbor 10.10.10.40 send-community both
 neighbor 10.10.10.50 activate
 neighbor 10.10.10.50 send-community both
 neighbor 10.10.10.60 activate
 neighbor 10.10.10.60 send-community both
!
mpls ldp router-id Loopback0
!
control-plane
!
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
```

PE1 Configuration

```
hostname PE1
!
no aaa new-model
```

```
 neighbor 10.10.10.10 activate
 neighbor 10.10.10.10 send-community both
 neighbor 10.10.10.20 activate
 neighbor 10.10.10.20 send-community both
 neighbor 10.10.10.30 activate
 neighbor 10.10.10.30 send-community both
 neighbor 10.10.10.50 activate
 neighbor 10.10.10.50 send-community both
 neighbor 10.10.10.60 activate
 neighbor 10.10.10.60 send-community both
 no auto-summary
 no synchronization
 network 10.10.10.40 mask 255.255.255.255
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.10.10.10 activate
 neighbor 10.10.10.10 send-community both
 neighbor 10.10.10.20 activate
 neighbor 10.10.10.20 send-community both
 neighbor 10.10.10.30 activate
 neighbor 10.10.10.30 send-community both
 neighbor 10.10.10.50 activate
 neighbor 10.10.10.50 send-community both
 neighbor 10.10.10.60 activate
 neighbor 10.10.10.60 send-community both
 exit-address-family
!
mpls ldp router-id Loopback0
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
```

PE4 Configuration

```
hostname PE4
!
no aaa new-model
memory-size iomem 5
```

```
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
ip vrf VOIP
 rd 100:65100
 route-target export 100:65100
 route-target import 100:65100
!
no ip domain lookup
mpls label protocol ldp
!
ip tcp synwait-time 5
!
class-map match-all VOIP_traffic
 match access-group 101
class-map match-all DATA__traffic
 match access-group 102
class-map match-all SMS_traffic
 match access-group 103
!
policy-map DSCP
 class VOIP_traffic
  set ip dscp af11
 class DATA__traffic
  set ip dscp af33
policy-map s1/0_outbound_policy
 class SMS_traffic
  bandwidth percent 25
  random-detect
 class VOIP_traffic
  bandwidth percent 40
  random-detect
 class DATA__traffic
  bandwidth percent 30
  random-detect
 class class-default
  fair-queue
  random-detect
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
 ip router isis 100
!
interface FastEthernet0/0
 bandwidth 10240
 ip vrf forwarding VOIP
 ip address 10.120.1.1 255.255.255.248
```

```
no ip icmp rate-limit unreachable
ip cef
!
ip vrf VOIP
 rd 100:65100
 route-target export 100:65100
 route-target import 100:65100
!
no ip domain lookup
mpls label protocol ldp
!
ip tcp synwait-time 5
!
class-map match-all VOIP_traffic
 match access-group 101
class-map match-all DATA__traffic
 match access-group 102
class-map match-all SMS_traffic
 match access-group 103
!
!
policy-map DSCP
 class VOIP_traffic
  set ip dscp af11
 class DATA__traffic
  set ip dscp af33
policy-map s1/0_outbound_policy
 class SMS_traffic
  bandwidth percent 25
  random-detect
 class VOIP_traffic
  bandwidth percent 40
  random-detect
 class DATA__traffic
  bandwidth percent 30
  random-detect
 class class-default
  fair-queue
  random-detect
!
interface Loopback0
 ip address 10.10.10.60 255.255.255.255
 ip router isis 100
!
interface FastEthernet0/0
 bandwidth 12288
 ip vrf forwarding VOIP
 ip address 10.130.1.1 255.255.255.248
 speed auto
 full-duplex
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial1/0
 ip address 10.10.1.1 255.255.255.252
 ip router isis 100
 mpls ip
 serial restart-delay 0
 service-policy output DSCP
!
interface Serial1/1
 ip address 10.10.2.1 255.255.255.252
 ip router isis 100
 mpls ip
 serial restart-delay 0
 service-policy output DSCP
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
```

```
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 ip address 10.10.7.2 255.255.255.252
 ip router isis 100
 mpls ip
 clock rate 1000000
!
interface Serial1/0
 ip address 10.10.8.2 255.255.255.252
 ip router isis 100
 mpls ip
 serial restart-delay 0
 clock rate 1008000
 service-policy output DSCP
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 serial restart-delay 0
 clock rate 1008000
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
```

```
router isis 100
 net 49.0000.1010.1010.00
 is-type level-2-only
 metric-style wide
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 10.10.10.20 remote-as 100
 neighbor 10.10.10.20 update-source
Loopback0
 neighbor 10.10.10.30 remote-as 100
 neighbor 10.10.10.30 update-source
Loopback0
 neighbor 10.10.10.40 remote-as 100
 neighbor 10.10.10.40 update-source
Loopback0
 neighbor 10.10.10.50 remote-as 100
 neighbor 10.10.10.50 update-source
Loopback0
 neighbor 10.10.10.60 remote-as 100
 neighbor 10.10.10.60 update-source
Loopback0
 !
 address-family ipv4
 neighbor 10.10.10.20 activate
 neighbor 10.10.10.20 send-community both
 neighbor 10.10.10.30 activate
 neighbor 10.10.10.30 send-community both
 neighbor 10.10.10.40 activate
 neighbor 10.10.10.40 send-community both
 neighbor 10.10.10.50 activate
 neighbor 10.10.10.50 send-community both
 neighbor 10.10.10.60 activate
 neighbor 10.10.10.60 send-community both
 no auto-summary
 no synchronization
 network 10.10.10.10 mask 255.255.255.255
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.10.10.20 activate
 neighbor 10.10.10.20 send-community both
 neighbor 10.10.10.30 activate
 neighbor 10.10.10.30 send-community both
 neighbor 10.10.10.40 activate
 neighbor 10.10.10.40 send-community both
 neighbor 10.10.10.50 activate
 neighbor 10.10.10.50 send-community both
```

```
router isis 100
 net 49.0000.1010.1060.00
 is-type level-2-only
 metric-style wide
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 10.10.10.10 remote-as 100
 neighbor 10.10.10.10 update-source
Loopback0
 neighbor 10.10.10.20 remote-as 100
 neighbor 10.10.10.20 update-source
Loopback0
 neighbor 10.10.10.30 remote-as 100
 neighbor 10.10.10.30 update-source
Loopback0
 neighbor 10.10.10.40 remote-as 100
 neighbor 10.10.10.40 update-source
Loopback0
 neighbor 10.10.10.50 remote-as 100
 neighbor 10.10.10.50 update-source
Loopback0
 !
 address-family ipv4
 neighbor 10.10.10.10 activate
 neighbor 10.10.10.10 send-community both
 neighbor 10.10.10.20 activate
 neighbor 10.10.10.20 send-community both
 neighbor 10.10.10.30 activate
 neighbor 10.10.10.30 send-community both
 neighbor 10.10.10.40 activate
 neighbor 10.10.10.40 send-community both
 neighbor 10.10.10.50 activate
 neighbor 10.10.10.50 send-community both
 no auto-summary
 no synchronization
 network 10.10.10.60 mask 255.255.255.255
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.10.10.10 activate
 neighbor 10.10.10.10 send-community both
 neighbor 10.10.10.20 activate
 neighbor 10.10.10.20 send-community both
 neighbor 10.10.10.30 activate
 neighbor 10.10.10.30 send-community both
 neighbor 10.10.10.40 activate
 neighbor 10.10.10.40 send-community both
 neighbor 10.10.10.60 activate
 neighbor 10.10.10.60 send-community both
 exit-address-family
 !
 address-family ipv4 vrf VOIP
 redistribute connected
 redistribute static
 no synchronization
 exit-address-family
!
ip route vrf VOIP 0.0.0.0 0.0.0.0 10.120.1.2
!
access-list 101 permit icmp any any
access-list 102 permit tcp any any eq bgp
access-list 103 permit tcp any any eq www
no cdp log mismatch duplex
!
mpls ldp router-id Loopback0
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
```

PE2 Configuration

```
hostname PE2
!
no ip domain lookup
mpls label protocol ldp
!
interface Loopback0
 ip address 10.10.10.20 255.255.255.255
 ip router isis 100
!
interface FastEthernet0/0
 no ip address
```

```
 neighbor 10.10.10.50 activate
 neighbor 10.10.10.50 send-community both
 exit-address-family
 !
 address-family ipv4 vrf VOIP
 redistribute connected
 redistribute static
 no synchronization
 exit-address-family
!
ip route vrf VOIP 0.0.0.0 0.0.0.0 10.130.1.2
!
no ip http server
no ip http secure-server
!
access-list 101 permit icmp any any
access-list 102 permit tcp any any eq bgp
access-list 103 permit tcp any any eq www
no cdp log mismatch duplex
!
mpls ldp router-id Loopback0
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
```

PE4 Configuration

```
hostname PE3
!
no ip domain lookup
mpls label protocol ldp
!
interface Loopback0
 ip address 10.10.10.50 255.255.255.255
 ip router isis 100
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial1/0
 ip address 10.10.1.2 255.255.255.252
 ip router isis 100
 mpls ip
 serial restart-delay 0
 clock rate 1008000
!
interface Serial1/1
 ip address 10.10.3.1 255.255.255.252
 ip router isis 100
 mpls ip
 serial restart-delay 0
 clock rate 1008000
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
```

```
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/2
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial1/0
 ip address 10.10.8.1 255.255.255.252
 ip router isis 100
 mpls ip
 serial restart-delay 0
 clock rate 1008000
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 ip address 10.10.6.2 255.255.255.252
 ip router isis 100
 mpls ip
 serial restart-delay 0
 clock rate 1008000
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
```

```
!
router isis 100
 net 49.0000.1010.1020.00
 is-type level-2-only
 metric-style wide
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 10.10.10.10 remote-as 100
 neighbor 10.10.10.10 update-source
Loopback0
 neighbor 10.10.10.30 remote-as 100
 neighbor 10.10.10.30 update-source
Loopback0
 neighbor 10.10.10.40 remote-as 100
 neighbor 10.10.10.40 update-source
Loopback0
 neighbor 10.10.10.50 remote-as 100
 neighbor 10.10.10.50 update-source
Loopback0
 neighbor 10.10.10.60 remote-as 100
 neighbor 10.10.10.60 update-source
Loopback0
 !
 address-family ipv4
 neighbor 10.10.10.10 activate
 neighbor 10.10.10.10 send-community both
 neighbor 10.10.10.30 activate
 neighbor 10.10.10.30 send-community both
 neighbor 10.10.10.40 activate
 neighbor 10.10.10.40 send-community both
 neighbor 10.10.10.50 activate
 neighbor 10.10.10.50 send-community both
 neighbor 10.10.10.60 activate
 neighbor 10.10.10.60 send-community both
 no auto-summary
 no synchronization
 network 10.10.10.20 mask 255.255.255.255
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.10.10.10 activate
 neighbor 10.10.10.10 send-community both
 neighbor 10.10.10.30 activate
 neighbor 10.10.10.30 send-community both
 neighbor 10.10.10.40 activate
 neighbor 10.10.10.40 send-community both
 neighbor 10.10.10.50 activate
```

```
!
router ospf 100
 log-adjacency-changes
 network 10.10.0.0 0.0.0.0 area 0
!
router isis 100
 net 49.0000.1010.1050.00
 is-type level-2-only
 metric-style wide
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 10.10.10.10 remote-as 100
 neighbor 10.10.10.10 update-source
Loopback0
 neighbor 10.10.10.20 remote-as 100
 neighbor 10.10.10.20 update-source
Loopback0
 neighbor 10.10.10.30 remote-as 100
 neighbor 10.10.10.30 update-source
Loopback0
 neighbor 10.10.10.40 remote-as 100
 neighbor 10.10.10.40 update-source
Loopback0
 neighbor 10.10.10.60 remote-as 100
 neighbor 10.10.10.60 update-source
Loopback0
 !
 address-family ipv4
 neighbor 10.10.10.10 activate
 neighbor 10.10.10.10 send-community both
 neighbor 10.10.10.20 activate
 neighbor 10.10.10.20 send-community both
 neighbor 10.10.10.30 activate
 neighbor 10.10.10.30 send-community both
 neighbor 10.10.10.40 activate
 neighbor 10.10.10.40 send-community both
 neighbor 10.10.10.60 activate
 neighbor 10.10.10.60 send-community both
 no auto-summary
 no synchronization
 network 10.10.10.50 mask 255.255.255.255
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.10.10.10 activate
 neighbor 10.10.10.10 send-community both
 neighbor 10.10.10.20 activate
 neighbor 10.10.10.50 send-community both
 neighbor 10.10.10.60 activate
 neighbor 10.10.10.60 send-community both
 exit-address-family
!
mpls ldp router-id Loopback0
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
```

CME1-SW1-Phone1 Configuration

```
hostname CME1-SW1-Phone1
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
ip dhcp excluded-address 192.168.1.1
!
ip dhcp pool VOIP
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 192.168.1.1
 domain-name VOIP.com
 lease infinite
!
interface FastEthernet0/0
 ip address 10.120.1.2 255.255.255.248
 duplex half
!
interface FastEthernet1/0
 no ip address
 shutdown
 speed auto
 duplex auto
```

```
 neighbor 10.10.10.20 send-community both
 neighbor 10.10.10.30 activate
 neighbor 10.10.10.30 send-community both
 neighbor 10.10.10.40 activate
 neighbor 10.10.10.40 send-community both
 neighbor 10.10.10.60 activate
 neighbor 10.10.10.60 send-community both
 exit-address-family
!
mpls ldp router-id Loopback0
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
```

CME2-SW2-Phone2 Configuration

```
hostname CME2-SW2-Phone2
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
ip dhcp excluded-address 192.168.2.1
!
ip dhcp pool VOIP
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 192.168.2.1
 domain-name VOIP.com
 lease infinite
!
interface FastEthernet0/0
 ip address 10.130.1.2 255.255.255.248
 duplex half
!
interface FastEthernet1/0
 no ip address
 shutdown
 speed auto
 duplex auto
```

```
!
interface FastEthernet1/1
 no ip address
 shutdown
 speed auto
 duplex auto
!
interface Ethernet2/0
 no ip address
 shutdown
 duplex full
!
interface Ethernet2/1
 no ip address
 shutdown
 duplex full
!
interface Ethernet2/2
 no ip address
 shutdown
 duplex full
!
interface Ethernet2/3
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.120.1.1
ip route 192.168.1.0 255.255.255.0 10.120.1.1
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
```

```
!
interface FastEthernet1/1
 no ip address
 shutdown
 speed auto
 duplex auto
!
interface Ethernet2/0
 no ip address
 shutdown
 duplex full
!
interface Ethernet2/1
 no ip address
 shutdown
 duplex full
!
interface Ethernet2/2
 no ip address
 shutdown
 duplex full
!
interface Ethernet2/3
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.130.1.1
ip route 192.168.2.0 255.255.255.0 10.130.1.1
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
```

```
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
```