ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY

SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

COMMUNICATION ENGINEERING STREAM

Comparative Analysis of QoS in MPLS and IP Network for Broadband Intelsat Internet Using Riverbed Modeler Academic Edition

By: Erena Keno

Advisor: Professor Mohammed Abdo

A Thesis Submitted to Addis Ababa University
Addis Ababa Institute of technology
In Partial Fulfillment of the Requirement for the Degree of Master of Science in Electrical and Computer Engineering

Due Date: 08/22/ 2018 G.C

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY

SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

COMMUNICATION ENGINEERING STREAM

Comparative Analysis of QoS in MPLS and IP Network for Broadband Intelsat Internet Using Riverbed Modeler Academic Edition

By: Erena Keno

Approved by board of Examiners

Dr. ____________ ____________ _________

Chairman Department Signature Date

Graduate committee

Professor Mohammed Abdo ____________ ________

Advisor Signature Date

Internal Examiner

Dr. _____________ ________

Signature Date

Dr. _____________ _________

External Examiner Signature Date

Declaration

I declare that, this thesis represents my own work, except where due acknowledgment is made, and that it has not been previously submitted to this university or to any other Institution for a degree or other qualification**.**

Name: Erena Keno Signature: _______________

Place: Addis Ababa Institute of Technology, Addis Ababa University, Addis Ababa
Date of Submission: ______________________

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

Professor Mohammed Abdo Signature: ______________
Advisor’s Name

Acknowledgment

My first and foremost compliments to Almighty God, who gave me the strength to accomplish my tasks until now including this thesis work. Without His blessings, it is impossible to achieve any success in life. I would like to thank my parents who always encouraged me during the whole course of my study duration. Without their pray, everything is unattainable for me. I am grateful to my thesis **Advisor Professor Mohammed Abdo** for providing me such a great opportunity to work under his respected supervision. Lastly, I would like to thank all my friends from Addis Ababa Institute of Technology and Walkite University, whose love and support provided me such a friendly and peaceful environment to work with. I also like to say best wishes to all of you.

Abstract

Nowadays Multiprotocol Label Switching (MPLS) and Internet Protocol (IP) are widely used technologies in service providers and enterprise networks across the globe. In this thesis, the behavior of traffic in both IP and MPLS are studied since they have more advantageous through all network models. MPLS -enabled infrastructure has the ability to transport any type of payload (Asynchronous Transfer Mode, frame relay, and Ethernet) over it, within the same time providing a multipurpose architecture. An incoming packet is arranged only once as it enters into the MPLS domain and gets assigned label information. Then after all decision processes along a specified path is based upon the attached label rather than assigning destination IP addresses. This work also presents the design and simulation of MPLS and IP network for different applications. These applications used for the performance evaluation including voice, File Transfer Protocol (FTP) and Hyperlink Text Transfer Protocol (HTTP). The parameters used for the analysis are throughput, link utilization, packet delay, jitter, page response time and FTP response time. Comparative analysis of the quality of services is a set of performance models to evaluate the different combination of IP and MPLS network routing topologies have been explained for the proposed network model. The results obtained from this study shows how a service provider can benefit from MPLS services with increasing network performance like throughput, mean opinion score, a packet sent and received. Comparing MPLS queuing delay results with the IP result from the shortest path routing scenario network, the queuing delay keep a much less queuing delay in MPLS configuration with value (Maximum 0.00002 seconds and Minimum 0.00001 seconds) between Http Client and ISP Branch 1. It can be observed that the queuing delay MPLS scenario is more balanced between both paths comparing it with IP scenario.

Keywords: IP, MPLS, LDP, QoS, OSPF, Satellite internet, Riverbed Modeler,

Table Contents

Lists of Figures

List of Tables

Lists of Abbreviations

AS	Autonomous Systems
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CR-LDP	Constraint Routed –Label Distribution Protocol
DVB-S2	Digital Video Broadcast- Satellite number 2
EXP	Experiment
FEC	Forward Equivalence Class
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hyperlink Text Transfer Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
INTELSAT	International Satellite
IP	Internet Protocol
IS-IS	Intermediate System-Intermediate System
ISP	Internet Service Provider
ITU	International Telecommunication Union
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LSP	Label Switch Path

MANET	Mobile Ad hock Network
MPLS	Multi-Protocol Label Switch
MPLS_TE	Multi-Protocol Label Switch Traffic Engineering
NETSim	Network Simulator
NS-2	Network Simulator number 2
OMNET++	Objective Modular Network Tested in C++
OPNET	Optimized Network Engineering Tool
OSPF	Open Shortest Path First
OTCL	Object-oriented Tool Command Language
PSTN	Public Switched Telephone Network
QoS	Quality of Service
QualNET	Quality Network
RAS	Registration, Admission, and Status
REC	Radio Frequency Commission
RIP	Routing Information Protocol
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol-Traffic Engineering
SLA	Service Level Agreement
SIP	Session Initiation Protocol
TCP	Transport Control Protocol
TE	Traffic Engineering
UPD	User Protocol Datagram
VPN	Virtual Private Network

WAN	Wide Area Network
WLAN	Wireless Local Area Network

Chapter 1

Introduction

The Internet today consists of multiple service providers network connected to one another, forming a global network communication infrastructure. This infrastructure enables people around the world to communicate with one another through interconnected network devices. High-speed Internet connectivity has become an essential part of the business, education and healthcare systems that are integral to modern society [1]. Many rural areas have continued to lag behind in developing the broadband access options that allow its community institutions to participate in these networks and remain relevant [2]. These broad systems and networks are the basis for future economic development and healthy communities without them, the overall economic health of rural communities suffers. Broadband satellite Internets have emerged as critical issues for rural communities. Intelsat has had a commitment to excellence in technology and reliability since 1965 [3]. Intelsat operates the world's first Globalized Network, delivering high quality, cost-effective video and broadband services anywhere in the world [4]. Intelsat's Globalized Network combines the world's largest satellite backbone with terrestrial infrastructure, managed services, and an open, interoperable architecture to enable customers to drive revenue and reach through a new generation of network services. Thousands of organizations serving billions of people worldwide rely on Intelsat to provide enough broadband connectivity, multi-format video broadcasting, secure satellite communications, and seamless mobility services. The result is an entirely new world, one that allows us to visualize the impossible, connect without boundaries and transform the ways in which we live. As the service provider begins to scale, their network to accommodate this triple-digit growth, traffic engineering and scalability of the network has been of utmost importance. For this type of service provider, MPLS has the following advantages: scalability, any to any connectivity and built-in support for quality of service. Since MPLS traffic is switched using labels rather than routing the system models have less overhead and latency to deal with switch packet traffic over an MPLS enabled network [5]. Traffic engineering capability extremely flexible and feature-rich controls are available to enable service providers with the ability to engineer a network to meet any type of customer traffic requirements. Controls such as strict routing, loose routing quality of service and bandwidth controls allow for different levels of service.

1.1 Statement of the Problem

Two scaling problems face the internet user today; first, the recent evolutions of Internet Protocol (IP) network are seeing Internet Protocol applications becoming more complex and requiring higher bandwidth consumption. Second, the traffic distribution in both IP and MPLS networks are not uniform for example hosts in all countries of the world access Internet that produced in the few regions of the world. The other problem is in the multi-service network, which contains voice, Hyperlink Text Transfer Protocol (HTTP), and File Transfer Protocol (FTP) as a real-time application is a time delay. The packet sent and received for these real-time applications should be delivered with minimum delays under various conditions.

1.2 Proposed Solution

This research work evaluates the performance of MPLS and IP under various circumstances. They are evaluated considering the delays in voice, voice packets sent and received as well as a packet, sent and received in FTP and HTTP traffic. The thesis proposes the MPLS network as solutions for identifying the quality of services, cost-effective technologies for broadband satellite internet based on MPLS and IP network. Satellite network based on MPLS is one solution to the existing problem. More recently, IP networks are employing multiprotocol label switching over it, which is a technique, used to improve the performance of IP networks. It takes different paths to avoid congestion but also uses label switched technology to efficiently deliver the packets through the MPLS network. The thesis focus on different type of applications that require quality of service guarantee, design, development, and implementation of MPLS networks, architecture, characteristics and effects in comparison to traditional IP networks.

1.3 Objectives of the Thesis

1.3.1 General Objective

- ✓ The main goal of this research is to analyze the Voice, HTTP and FTP traffic that could run over MPLS network within an acceptable range and comparing their traffic with IP traditional network over a broadband satellite network.

1.3.2 Specific Objective

- ✓ To design, two network models for IP and MPLS considering same network topology and analyzing their results by considering the same performance parameters.
- ✓ To choose the performance parameters such as packet sent and received, jitter, MOS, download response and amount of traffic in a label switched paths within each node of the networks and analyzing their results graphically by using Riverbed modeler simulator.
- ✓ To provide suggestions for researchers and organization which are planning to deploy VOIP, FTP, and HTTP application.
- ✓ To analyze, Traffic requirements and Quality of Service design in IP and MPLS network for broadband satellite internet access based on traffic generated in each node of the network model.

1.4 Scope

This thesis report includes the technical issues and factors that need to be considered for implementation of voice over Internet Protocol (VOIP), hypertext transfer protocol (HTTP) and file transfer protocol application (FTP) in both IP and MPLS network and describes the challenging issues that need to be faced by the networks to transmit the HTTP, FTP, and VOIP applications. In short, this work presents the performance of different applications using IP and MPLS network model. This study analyzes and compares by means of modeling and simulation, the performance of multi-protocol switching and Internet Protocol based network model on equal bandwidths for broadband satellite Internet.

1.5 Thesis Methodology

This work involves in-depth literature studies. Most of the information is taken from well-known books and highly recognized research papers. Further, the implementation of different network scenarios to gain a better knowledge of the characteristics of diverse applications is also part of this thesis. Evaluation methods are chosen based on different metrics as mentioned in “objective section”. The theoretical knowledge gained is implemented in the riverbed modeler research simulator.

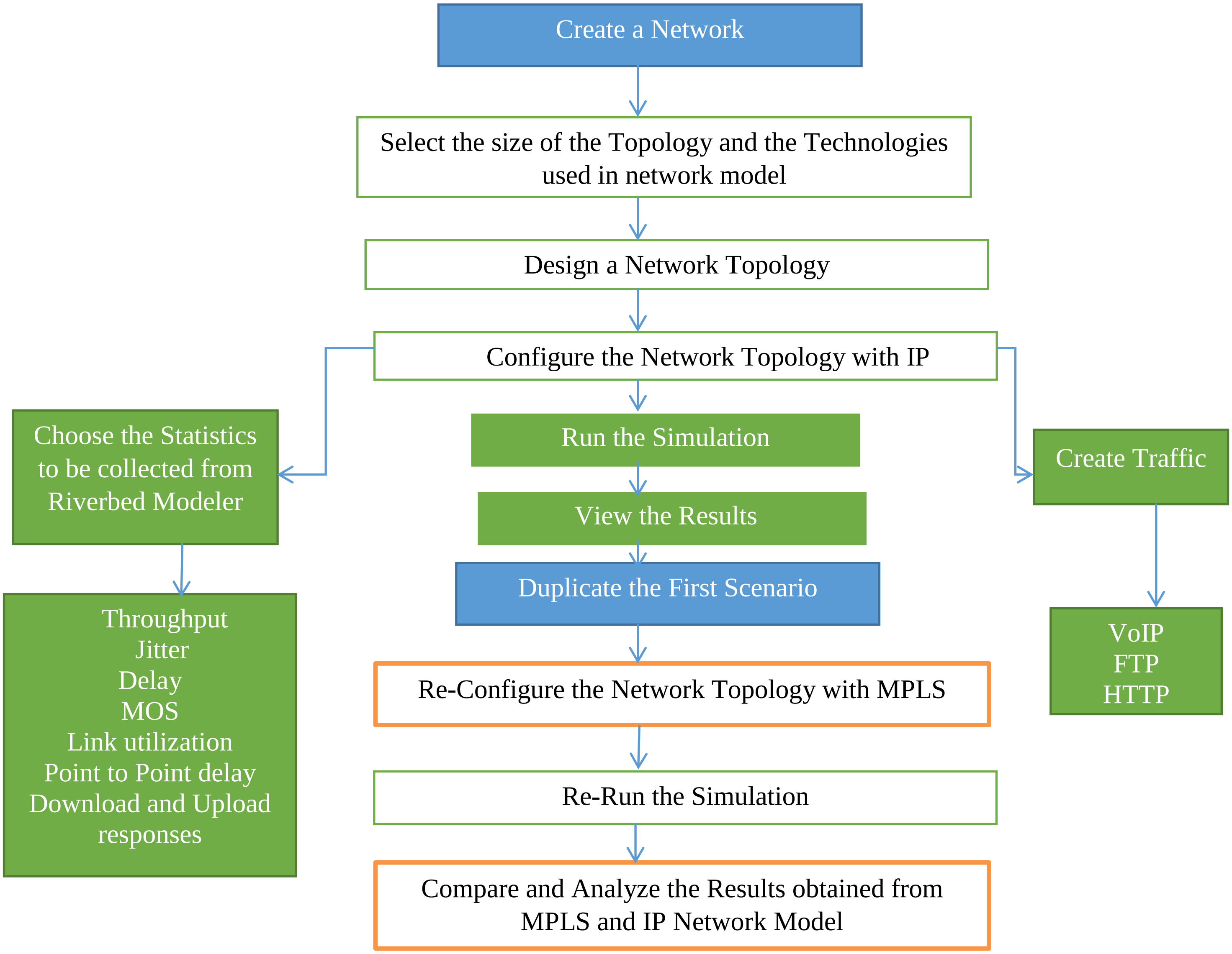


Figure 1.1: Network Model Flow diagram

The network consisting of 15 nodes were created. Out of which, five nodes are assigned as ISP branch nodes. Therefore, to compare the performance of the network, the thesis will initially use only some nodes. All links were set up as a duplex. The MPLS Traffic Engineering simulation topology is similar to the IP topology with the only difference being that all nodes are MPLS capable, which allow label switching. The work is simulated using a network with the following characteristics. Service provider network with a four-provider branch, Router (ISP branch 1-4) and three clients with different application core. IP network model is configured only with open short path first (OSPF) traffic and MPLS network model is configured with OSPF traffic including label switching path and label distribution protocol. The Riverbed Modeler has been used to perform the simulation on MPLS and traditional IP network. The VoIP traffic is sent from source (VoIP Client) to the destination (VoIP Server) in the two networks (MPLS and Traditional IP networks). The main task is to compare the performance of VoIP, HTTP and FTP traffic in both networks by using performance metrics such as voice jitter, voice packet end-to-end delay, packet loss, and throughput. The simulation results obtained are analyzed to determine the efficient technology used for transmitting Voice, file transfer protocol and hypertext transfer protocol traffic.

1.6 Thesis Contribution

The study will provide better understanding concepts for information regarding MPLS importance, uses, and deployment for the businesses. MPLS is a new technology for design and implementation of reliable, secure, efficient and standard QoS services and application classes. This technology will have lasting solutions for traffic engineering and multicasting. The study of IP and MPLS in satellite Internet involves Internet services providers, satellite operators, and network providers.

1.7 Literature Review

In this thesis, different author papers are discussed with their different approaches in IP and MPLS topic. Some authors perform simulation with the different testing environment. These methods are helpful for understanding the concept. Adjusting, analyzing and optimizing voice traffic over data networks have been a major challenge to the network researcher and developer, many techniques have been proposed based on analysis from the real world and simulated traffic. In [6], the main objective of the paper was performed and compared for a multisite office network for G.723 VoIP communication traffic applied on two network infrastructure models, one for IP and the other for MPLS. The authors in [6] have made a comparative analysis of MPLS over Non-MPLS networks and showed that MPLS has a better performance in voice application over IP network for land-based network configuration. Throughout this paper, a comparison study has not been made on signaling protocols like CR-LDP and LDP for MPLS network model and RSVP and OSPF configuration for IP network model in the same router with traffic engineering by explaining their functionality and classification. The simulation of MPLS and IP network by using broadband satellite router has not been done; performance is compared only with consideration of the constraints such as packet loss, throughput, link utilization and end-to-end delay on the designed network traffic. The authors in [7] analyzed two commonly used codecs using the peer-to-peer network scenario. This paper presents OPNET simulator for voice over internet protocol and it considered only latency, jitter and packet loss for the land-based network. The author was able to present from the results that G.711 is an ideal solution for PSTN networks scheme. The authors in [8] calculated the minimum number of voice over internet protocol calls that can be created in an enterprise IP network. The paper presents OPNET simulator designing of the real-world network model. In [9] the author represents the idea of integration of MPLS with Mobile Ad hoc Network and study the effect of performance on quality of services parameters. The idea of this research is to use MPLS in wireless context providing an improvement in the rapid processing of layer 2.5 headers. Layer 2.5 header is a type of data-carrying technique for high-performance telecommunications networks between layer two and layer three headers. Resource reservation protocol operation for mobile satellite communication [10] by Maria Elena Villapol and Jonathan Billington in Cooperative Research Centre for Satellite Systems describes an approach for providing resource reservation protocol services over IP tunnel. It briefly describes the problem, the characteristics of possible solutions, and the design goals. However, this research does not compare the performance of IP with another protocol by using a different application like file transfer protocol and voice. Quality of service over MPLS when using traffic engineering is presented in [11]. This study explains the effect of using traffic trunk to separate transport control protocol from user datagram protocol flows. In [20] the authors Karol Molnar and Martin Vlcek explained the “Evaluation of bandwidth constraint models for MPLS network. It proposed the two basic bandwidth constraint models for MPLS network, called Maximum allocations models and Russian Dolls model from point of view of the quality of service guarantees and introduces the results of performance evaluation of these models in simulation scenarios. However, this work does not evaluate the influence of bandwidth constraint models on the most important transmission parameters such as throughput, packet loss, one-way delay, and jitter. In [12] the authors explained the Simulation of Video Conferencing over IP Network with Quality of Service. The purpose of this study is to simulate the performance of video Using Riverbed Modeler conferencing over IP network with Quality of Services schemes. The analysis was done in terms of delay and its variant for video conferencing, although the other services are present, according to this result the delay is highest for the normal scenario (without QoS) and lowest for (with QoS) scenario. More ever Claire

Liu, Alan Fang and Linda Zhao [13] have made an evaluation to some parameter of quality of services related to video conferencing over three major wireless local area network. It simulated with a different number of applications added along with video conferencing and Standards 802.11a, 802.11b, and 802.11g. In this study, the simulation over different networks, such as Worldwide Interoperability for Microwave Access (WiMAX) and Long Term Evolution (LTE), could not be compared with Ethernet and Wi-Fi networks. N.Absar and A.Wahab [14] have made the Performance Measurement of Open Shortest Path First (OSPF) Protocol in IP Networks with more realistic enterprise modeling and present simulation results using OPNET simulator. Most of the previous work is focused on by comparing performance of network traffic without considering real-time application traffic between both IP and MPLS networks. In this thesis considering the real time application traffic like voice, file transfer and link utilization between MPLS and IP has been done from theoretical analysis. The thesis contribution is for better performance of MPLS over IP from real-time application traffic.

1.8 Thesis Outline

This thesis presents the technical study of Multiprotocol label switching and Internet protocol for satellite internet network design. It discusses the Internet problem and reviews past and current technologies, which have been used as an attempt to provide internet service to the satellite network. Introduction is chapter one that provides statement of the problem; along with the research methodology, objective, and scope of the thesis. Chapter two explains the Multiprotocol label switching (MPLS), an overview of a satellite network and software tools used in network design. Chapter three describes the Internet Protocol and Internet Protocol standard architecture. Chapters four discuss the network model for satellite IP networks and Multiprotocol label switching (MPLS) network. It also describes the implementation requirements and tool used in this thesis with their important features and other applications. Chapter five describes the simulation results. Chapter six concludes the thesis with a recommendation for future work

Chapter 2

Multi-Protocol Label Switching (MPLS) and Overview of Satellite Network

2.1 Overview of Broadband Satellite Internet and Software Tools

2.1.1 Satellite Broadband Internet Connection for Home

Satellite Broadband delivers reliable, high-speed, always-on Internet access to homes without depending on the availability of terrestrial networks. Whether users are in the city or the depths of the countryside or hard to reach areas, users will be able to enjoy broadband connection such as Email, Facebook, Twitter, and other social networking wherever they are. Figure 2.1 shows satellite broadband Internet connection for home.

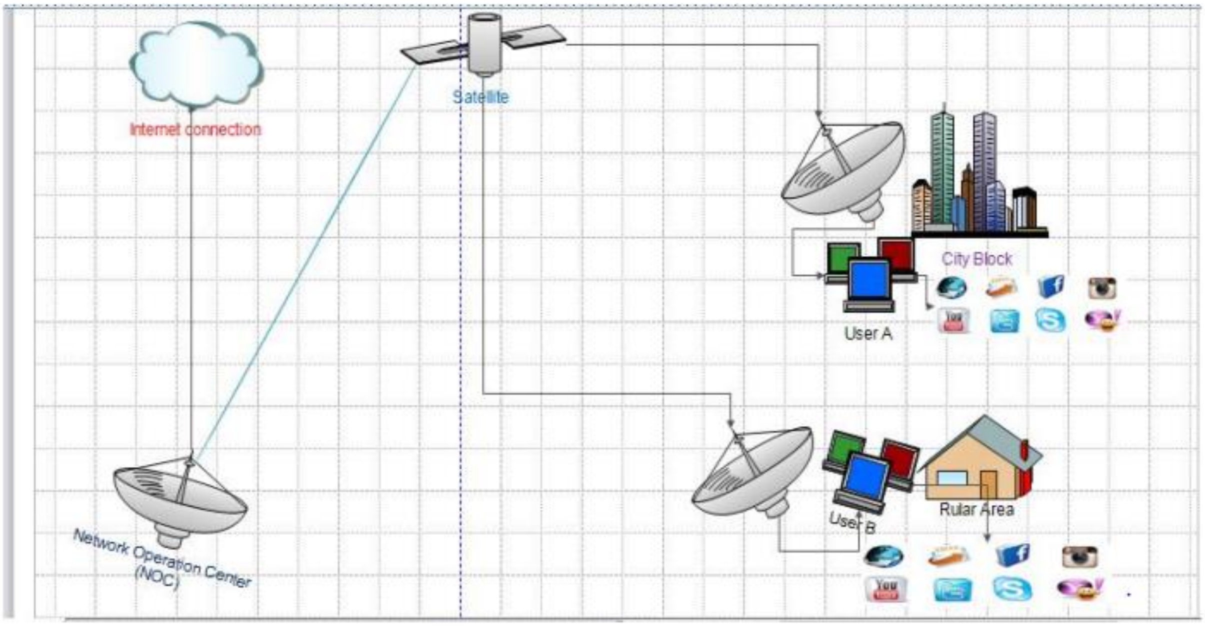


Figure 2.1: Satellite Broadband Internet Connection for Home [4]

2.1.2 Satellite Broadband Internet Connection for Enterprise

Enterprise Broadband offers reliable, secure and efficient broadband solutions via satellite to support their business needs and applications, anytime, anywhere. In our country it will be possible to rapidly deploy Satellite anywhere in the (Finfinne) Addis Ababa archipelago and beyond to delivers key internet applications such as VOIP, web apps, Google apps, e-mails, social networking, and internet surfing. Figure 2.2 shows satellite broadband internet connection for enterprise.

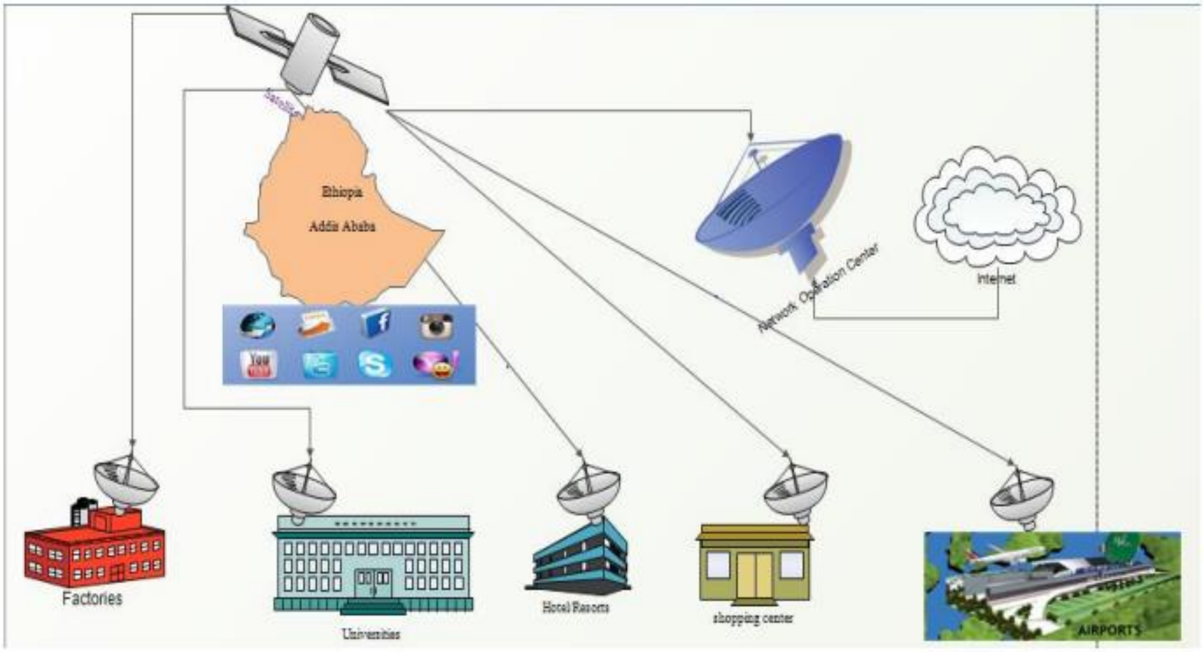


Figure 2.2: Satellite broadband internet for Enterprises [2]

2.1.3 Satellite Broadband for Internet Service Providers (ISP's)

Broadband provides local ISP is the broadband connection they need in order to offer reliable, high-speed and always-on internet access to clients everywhere through wired or wireless (Wi-Fi) connection. Satellite Broadband provides an economic benefit for an ideal solution for small to medium enterprise customers with basic remote networking needs.

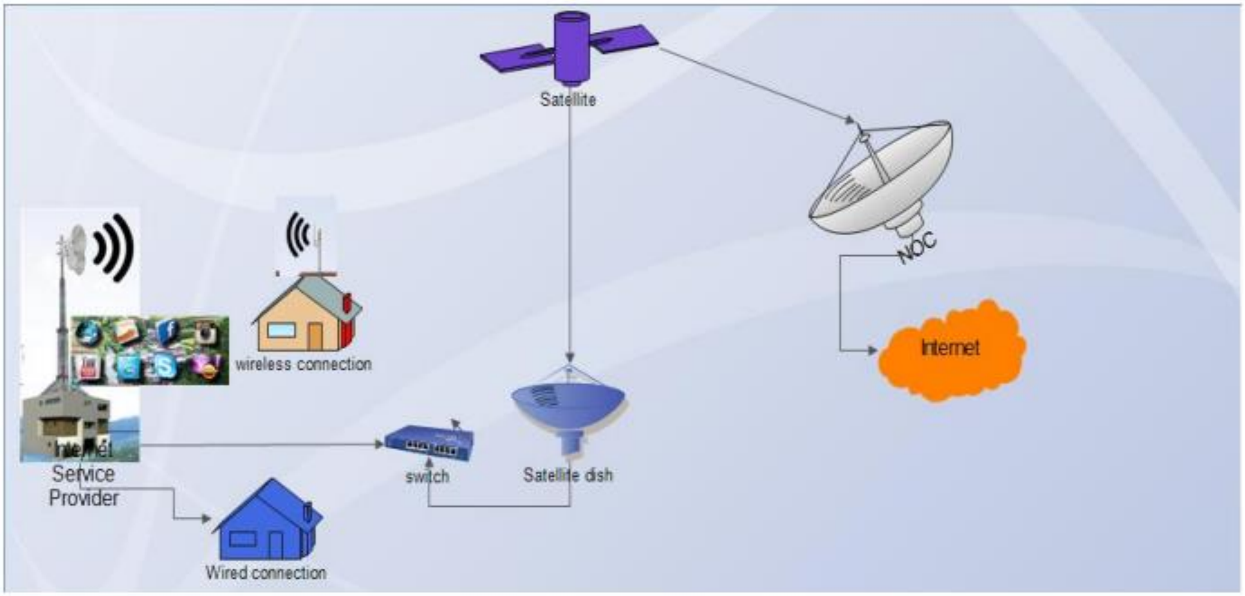


Figure 2.3: Satellite Broadband for Internet Service Providers (ISP's) [4]

2.2 Software Tools

Industry offers a wide range of simulators. Each simulator is designed and used to evaluate or test particular areas of interest. In order to achieve an accurate set of result, the need for good simulator is required. Therefore in this thesis, the following software tools are used.

- ✓ OPNET (Riverbed Modeler Academic Edition 17.5)
- ✓ Packet tracer version 7 (graphical network simulator)
- ✓ Edraw max for designing

I. **OPNET**: Optimized Network Engineering Tool (OPNET) is a discrete event, object-oriented, general-purpose network simulator. It provides a comprehensive development environment for the specification, simulation and performance analysis of computer and data communication networks. OPNET is a commercial network simulation package which is available for supporting both the teaching and research in educational institutions under the OPNET university academic program [15]. OPNET has several modules and tools, including OPNET modeler, planner, model library, and analysis tools [16]. It is widely used in the network industries for performance modeling and evaluation of local and wide-area networks. The main strengths of OPNET include a comprehensive model library, modular model development, a high level of modeling detail, user-friendly GUI, and customizable presentation of simulation results. However, OPNET is a very expensive package (license maintenance fees are also high), and its parameter categorization is not very transparent.

II. **NS2**

NS-2 is the simulator targeted at network research. The user interfaces with the simulator by using object-oriented script language OTcl on the UNIX systems (although it is possible to install NS-2 in windows). In order to build the simulation topologies on NS-2, one has to know OTcl language. Moreover, in NS-2 MPLS and RSVP-TE modules are not available as standard libraries these modules are implemented from the third party. The documentation is not available for all modules and it is required by the user to read the source code in order to learn how to interface with it, the generation of results are not automatic [17].

III. **QualNet Developer:** QualNet Developer ('QualNet') is a distributed and parallel network simulator that can be used for modeling and simulation of large networks with heavy traffic. The QualNet consists of QualNet scenario designer, QualNet animator (visualization and analysis tool), QualNet protocol designer (protocol skeleton tool), QualNet analyzer real-time statistical tool), and QualNet packet tracer (visualization and debugging tool). QualNet is a commercial version of the open-source simulator called GloMoSim [5]. The main strength of QualNet is that it supports thousands of nodes and run on a variety of machines and operating systems. It has a comprehensive network relevant parameter sets and allows verification of results through by inspection of code and configuration files. However, QualNet does not have any predefined model constructs.

IV. **NetSim:** NetSim is available both commercial and academic versions, and can be used for modeling and simulation of various network protocols, including WLANs, Ethernet, TCP/IP, and asynchronous transfer mode (ATM) switch NetSim allows a detailed performance study of Ethernet networks, including wireless ethernet [18].

V. **OMNeT++:** It is a modular component-based discrete event simulator. It uses building blocks called modules in the simulator [19]. There are two types of modules used in OMNeT++, namely, simple and compound. Simple modules are used to define algorithms and are active components of OMNeT++ in which events occur and the behavior of the model is defined (generation of events, the reaction on events). Compound modules are a collection of simple modules interacting with one another [20]. The main strengths of OMNeT++ include GUI, object inspectors for zooming into the component level and to display the state of each component during simulation, modular architecture, and abstraction, configurable, and detailed implementation of modules and protocols [21]. However, OMNeT++ is a bit slow due to its long simulation run and high memory consumption. OMNeT++ is also a bit difficult to use.

VI. **Why Riverbed Modeler has been used in the thesis?**

Due to the high cost of setting up laboratory equipment for real-time networking measurements, the use of a network simulator such as riverbed modeler has become effective and realistic. Riverbed is one of the leading network development software introduced in 1986 with the aim of simulating networking and telecommunication environment by modeling system behavior by the user [22]. It is a high-level event-based network level simulator that operates at packet-level, it contains a huge library of accurate models, accurate network behavior and commercially available fixed network hardware and protocols. Its high-level user interface is developed from C and C++ source code and modeling are divided into three main domains: network domain, node domain ad process domain.

2.3 Multi-Protocol Label Switching (MPLS)

(MPLS) technology is an evolving technology for high-performance packet control and forwarding mechanism for the routing of the packets in the networks [23]. It is key to scalable virtual private networks (VPNs) and end-to-end quality of service, enabling efficient utilization of existing networks to meet future growth and rapid fault correction of link and node failure [24].

The technology also helps deliver highly scalable, differentiated end-to-end IP services with a simpler configuration, management, and provisioning for both internet providers and subscribers [25]. MPLS uses labels to advertise between different routers by means of label mapping through label switching mechanism. MPLS also adds the label at the ingress Label Edge Router (LER) of the MPLS network, changes the label value at each LER within MPLS network until it reaches the egress LER, where it completely removes the MPLS label and the data packet is forwarded towards destination IP address [26]. Therefore, Packets in the MPLS network are forwarded based on the Labels. MPLS is not a replacement for the IP but it is an extension of IP architecture by including new functionalities and applications.

2.3.1 MPLS Header

A 32-bit MPLS header consists of a label field, experimental field, stack, and time to live field. The fields present in the MPLS header are shown in Figure 2.4.

Figure 2.4: MPLS Header fields [5]

- ✓ 20 bits (LABEL): the actual label.
- ✓ 3 bits (EXP): Class of Service.
- ✓ 1 bit (Stack): MPLS allows multiple labels to be inserted. This bit is used to determine the last label.
- ✓ 8 bits (TTL): Time to Live.

2.3.2 MPLS Label

MPLS label is inserted between layer two and layer three headers. The location of the MPLS label is shown in Figure 2.5.

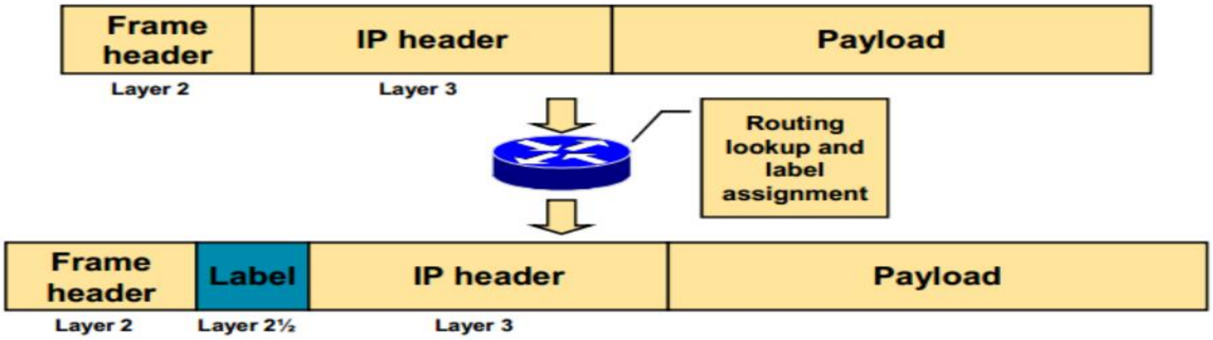


Figure 2.5: MPLS label [27]

2.3.3 MPLS Operation

Entire MPLS network can be divided into two parts namely MPLS edge and core. MPLS edge is the boundary of the MPLS network consisting of ingress and egress routers. MPLS core has intermediate label switching routers, through which label switching paths are formed [5].

Label Edge Router (LER): a router handle layer three lookups and is responsible for adding or removing the labels from the packets when they enter or leave the MPLS domain. Whenever a packet is entering or leaving MPLS domain it has to pass through label edge router.

Label Switch Router (LSR): a router which is located in the MPLS domain and forwarding the packets based on label switching and determines the next hop is called a label switching router. A label is a short fixed entity with no internal structure.

Label Distribution Protocol (LDP): where the label mapping information is exchanged between label switching router. It is responsible for establishing and maintaining labels between switches and routers.

Forward Equivalence Class (FEC): set of packets where they have related characteristics, which are forwarded with the same priority to the same path. This set of packets have the same MPLS label. Each packet in the MPLS network is assigned with FEC only once at the Ingress router. The packets are mapped on to the LSP using Forwarding Equivalence Class (FEC).

Label Switched Path (LSP): the path set by signaling protocols in the MPLS domain. In the MPLS domain there are a number of LSPs that are originated at the Ingress router and traverses one or more core LSRs and terminates at Egress router [28].

2.3.4 MPLS Functionality

MPLS process is performed on two types of routers: Label Edge Router (LER) and Label Switch Router (LSR). Label edge ISP headquarter router (ingress router) shown in Figure 2.6 works at the edge of the MPLS network. Its interfaces are connected to other networks. It routes traffic and works as an interface between the MPLS network and the IP network. For instance, when ISP headquarter router receives a packet from Internet Services Connection or VSAT, it attaches a label and sends the updated packet to the MPLS core network ISP branch 3 and 4. The packet then takes the path called Label Switched Path (LSP), leading to the LER ISP branch 2 (egress router). When the packet is received, the label is removed from the packet and the packet is sent to the respective network. LER that sends the packet to the MPLS core network is called an ingress router while LER that sends the packet to other destination network is called an egress router [28]**.** Both ingress and egress routers participate in the establishment of the LSPs before exchange of packets. The LSR exchange label and forwards the packet. They contribute to establishing the links between two routers (LSPs) and packet forwarding to other MPLS routers. LSRs receive packets from other connected LSRs or LERs, analyze their labels, and then forward the packets according to the label content.

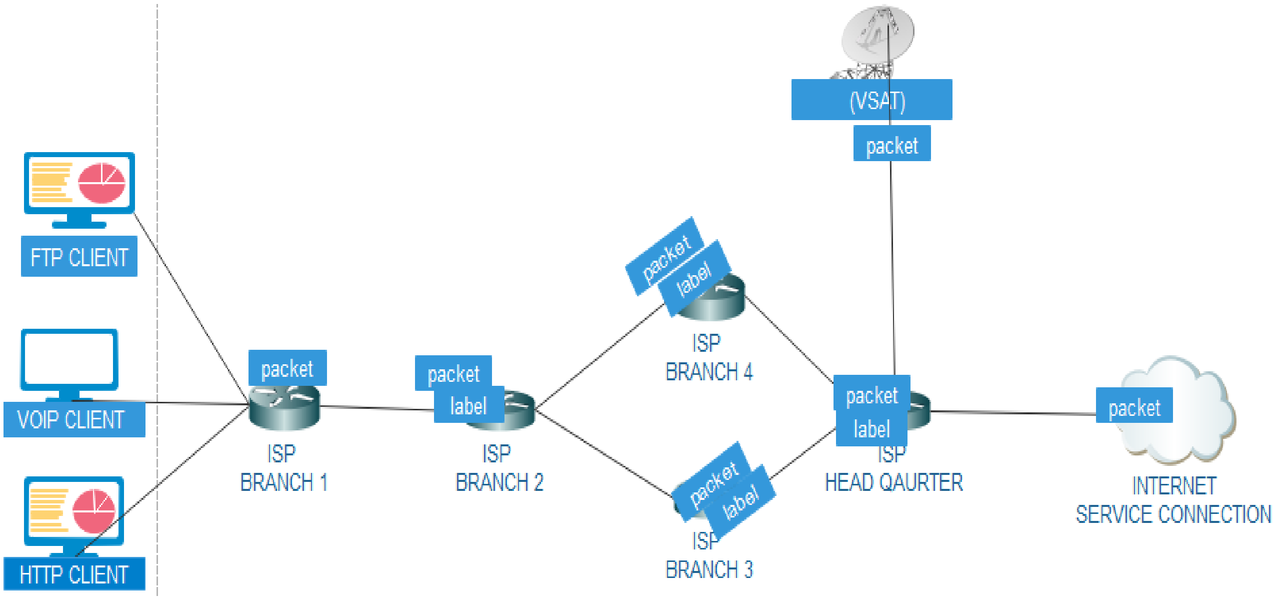


Figure 2.6: MPLS forwarding mechanism

2.3.5 Traffic Engineering in MPLS for Satellite internet

In Multiprotocol label switching traffic engineering, traffic may be forwarded based on other parameters such as QoS, source, or policy. All routers in networks are configured with MPLS enabled and the label distribution protocol (LDP). MPLS-TE tunnels are configured between ISP branch 1 and Internet Service Connection Thus, load sharing across equal paths can be explained in Figure 2.7.

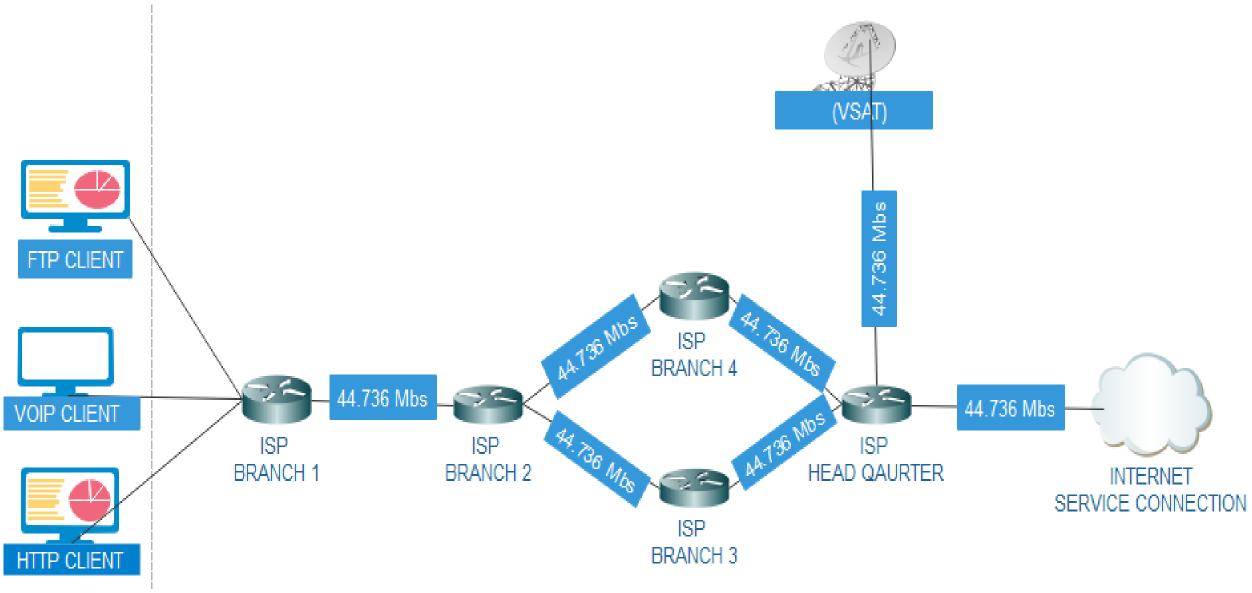


Figure 2.7: MPLS Traffic Engineering

2.3.6 VoIP Performance Metrics in MPLS Network

VoIP performance is measured according to ITU recommendations based on different parameters like (delay, jitter, and packet loss). These parameters can be changed and controlled within the acceptable range to the improved VoIP quality of service [29].

Jitter (Variation of Delay): In order for voice to be intelligible, voice packets must arrive at regular intervals. Jitter describes the degree of fluctuation in packet access, which can be caused by too much traffic on the line [14]. Voice packets can tolerate only about 75 milliseconds (0.075 sec) of jitter delay but are preferred to be 40 milliseconds (0.040 sec) of jitter delay. Jitter delay is calculated as Equation (2.1).

$$\mathbf{J} = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(di-D)^2} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(2.1)}$$

Where D is average of delay, N equals the total number of packets transmitted and di is the sum of all delay in the system. Both average delay and jitter are measured in seconds. Obviously, if all (di) delay values are equal, then D = di and J = 0.

Latency: As a delay sensitive application, voice cannot tolerate too much delay. Latency is the average time it takes for a packet to travel from its source to its destination. A person whose is speaking into the phone is called the source and the destination is the listener at the other end. This is a one-way latency [19]. The Maximum amount of latency that a voice call can tolerate one way is 150 milliseconds (0.15 sec) but is preferred to be 100 milliseconds (0.10 sec). The average delay is calculated by using Equation (2.2).

$$D = \sum_{i=1}^{N} {di}/_{N} \quad \text{………………………………………….. (2.2)}$$

Where di is equal to the sum of all delay, D equals to average delay and N equals the total number of packets transmitted during a specific period.

Packet loss: is the term used to describe the packets that do not arrive at the intended destination. This happened when a device (router, switch, and link) is overloaded and cannot accept any incoming data at a given moment. The Loss packet ratio is given by.

Loss packet ratio = (NL/N) x 100% …………..……. (2.3)

Where NL equals to the number of packets lost during the same time period.

End-to-end Delay: is the total transit time for packets in a data stream to arrive at the endpoint and it is inevitable in a communication system. Delay time is one of the most important factors in determining the quality of a call.

Voice Codec (coder/decoder): is one of the essential components of voice over internet protocol. At the sender side, coder/decoder converts analog voice signals to a digital signal, compresses and encodes to a predetermined format. The International Telecommunication Union introduced and standardized various codecs [30]. Most commonly used ones are G.711, G.722, G.723-1 and G.729 A each working with different bit rate and vary in performance [30]. The features of these standards are as follows.

- ✓ G.711: minimum bandwidth needed is 128kbs and its speech transmission is precise.
- ✓ G.722: different compression is possible.
- ✓ G.726: a version of G.723 and G.721
- ✓ G.723-1: voice quality is high but consumes high processor power.
- ✓ G.729 A: has efficient utilization of bandwidth license required.

H.323 signaling protocol: one of the main key areas of voice over internet protocol system is signaling protocol, which makes different network elements to communicate with each other, establish, and terminate calls. Two commonly used signaling protocol used in the riverbed are H.323 protocol suite introduced by the International Telecommunication Union and session initiation protocol (SIP) by Internet Engineering Task Force (IETF) [24]. H.323 is more standard and operates over a packet switched networks such as the IP network. Registration, Admission, and Status (RAS) signaling protocol also called H.225 signaling is a transaction-oriented protocol which operates between an H.323 terminate or endpoint and gateway. This signaling can also be used for call control/call setup, media control and provide the logical channel. H.323 is considered for signaling protocol of voice in this thesis due to its more advanced as features.

SIP (Session Initiation Protocol): is one of the voices over internet protocols, which is defined in RFC 2543 and standardized by the IETF [31]. This protocol contains initiation, termination and modification standards for user sessions, which consists of a video or audio elements, online games, instant messaging, virtual reality or generally multimedia elements.

Chapter 3

Internet Protocol Networks

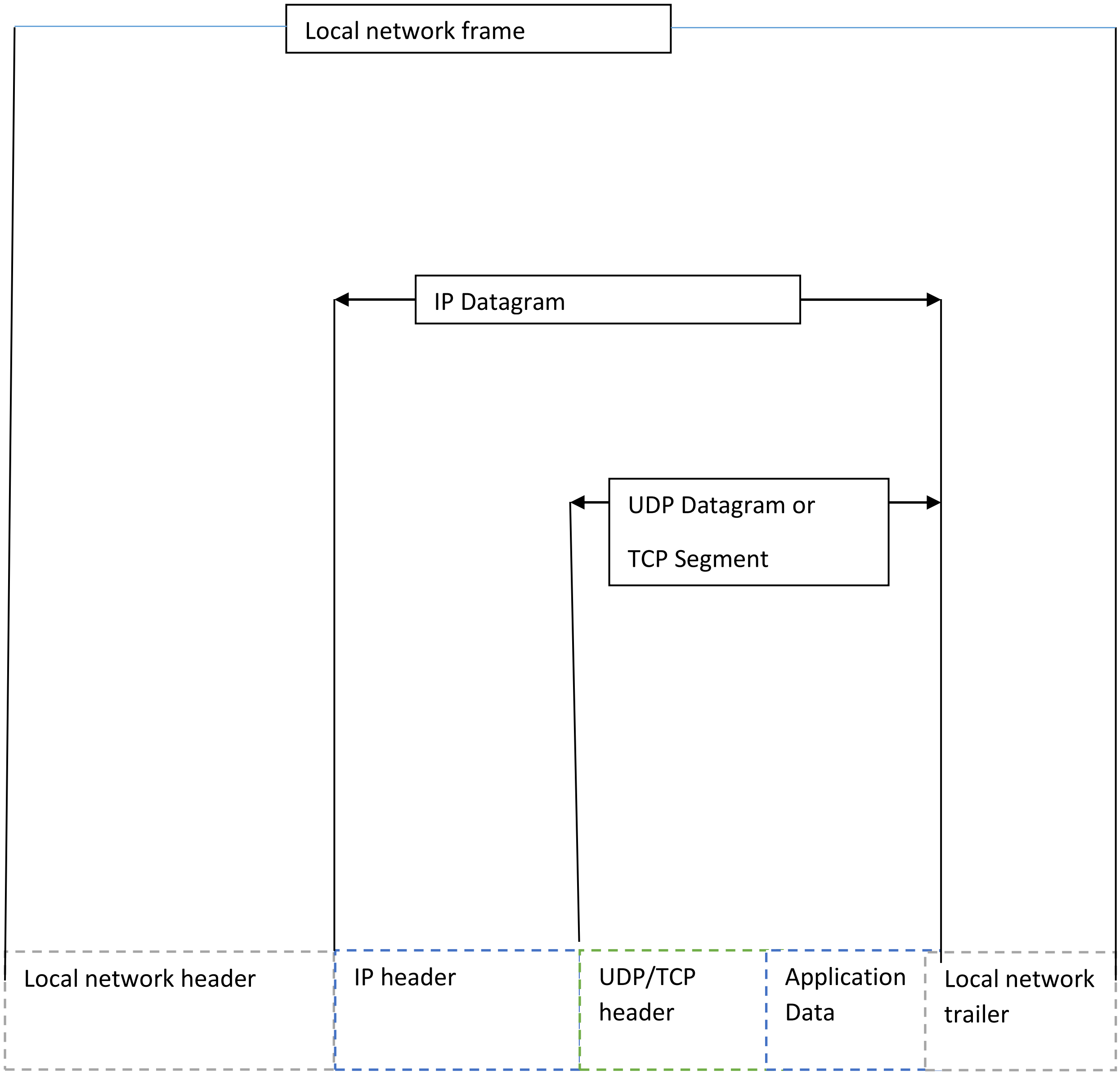
3.1 Internet Protocol

Internet Protocol was developed to transmit internet datagram from source to destination by passing through the interconnected system and network devices. The datagram is a bulk of data transmitting through the connectionless network and its transmission is analogous. An IP datagram of email message consists of datagram length and the addition of information header implemented by TCP or TCP header forwards the packet to the routers along with 802.3 frame header [32]. The Router takes off the frame header and forwards datagram, checks for the destination IP address and forwards the datagram towards the destination IP address. In the case of a virtual circuit connection, a connection-oriented mechanism, the destination address is first concerned and the desired path establishes and performs data transmission [8]. After a change of information, the path is realized by realizing the network resources. Since IP is connectionless protocol while TCP is connection-oriented protocol, by integrating two protocols one can converge between the reliability and unreliability of data transmission.

3.1.1 IP Datagram Fragmentation and Defragmentation

Internet Protocol deals with fragmentation and defragmentation during datagram transmission by IP address to ensure that datagram reached the correct destination address; this is how IP provides address consistency. IP datagram fragmentation and defragmentation is mandatory in some cases when datagram frame sizes are different with respect to LAN or WAN. Table 3.1 shows the structure of IP datagram.

Table 3.1: IP Datagram [33]



3.1.2 IP Header

An IP header contains several types of information as illustrated in Figure 3.1.

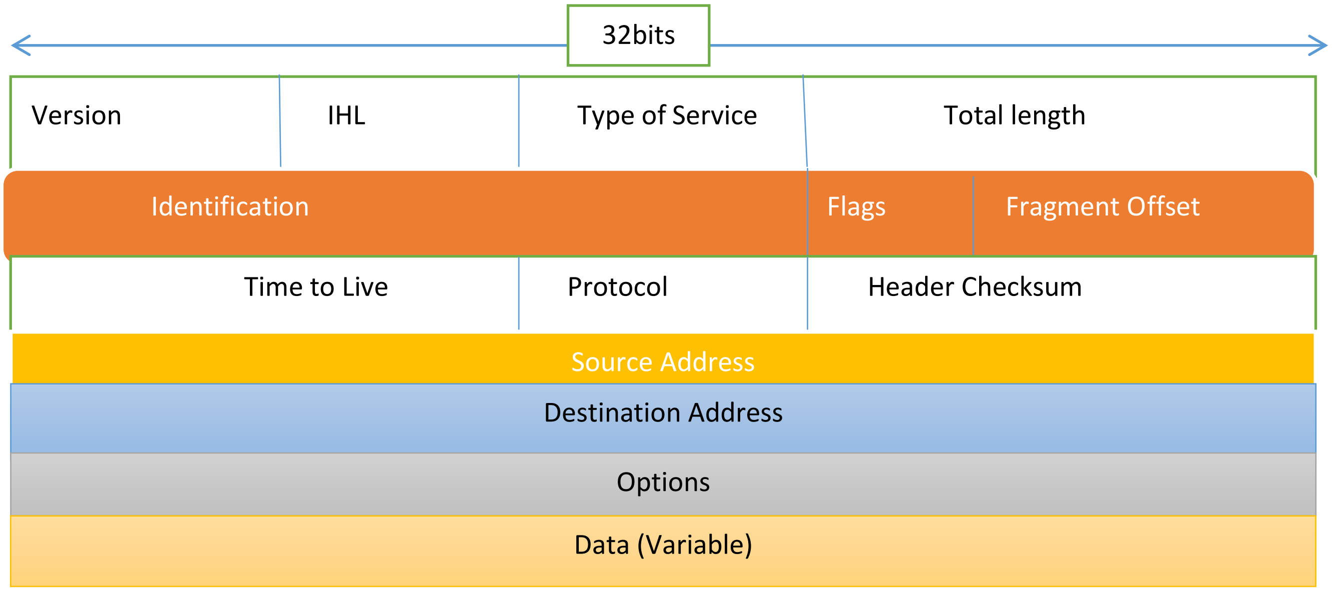


Figure 3.1: IP header structure [33]

Version (4 bits): Indicates the version number to allows the evolution of the protocol.

Internet Header Length (IHL 4 bits): Length of the header in 32-bit words. The minimum value is five for minimum header length of 20 octets [34].

Types of services: The type of service field contains an 8-bit binary value that is used to determine the priority of each packet. This value enables a quality of services (QoS) mechanism to be applied to high priority packet, such as those carrying telephony voice data. The router processing the packets can be configured to decide which packet is to forward first based on the type of service value [35].

Total length: Specifies the length, in bytes, of the entire IP packet, including the data and header.

Identifier (16 bits): A sequence number that, together with the source address, destination address, and user protocol, is intended to uniquely identify a datagram. Thus, the identifier should be unique for the datagram's source address, destination address, and user protocol for a time during which the datagram will remain on the internet [36].

Flags: Consists of a 3-bit field of which the two low-order (least-significant) bits control fragmentation. The low-order bit specifies whether the packet can be fragmented. The middle bit specifies whether the packet is the last fragment in a series of fragmented packets. The third or high-order bit is not used [36].

Fragment Offset: Indicates the position of the fragment's data relative to the beginning of the data in the original datagram, which allows the destination IP process to properly reconstruct the original datagram.

Time-to-Live: The Time-to-Live (TTL) is an 8-bit binary value that indicates the remaining life of the packet. The TTL value is decreased by at least one each time the packet is processed by a router. When the value becomes zero, the router discards or drops the packet and it is removed from the network data flow. This mechanism prevents packets that cannot reach their destination from being forwarded indefinitely between routers in a routing loop. If routing loops were permitted to continue, the network would become congested with data packets that will never reach their destination. Decrementing the TTL value at each hop ensures that it eventually becomes zero and the packet with the expired TTL field will be dropped [34].

Protocol: Indicates which upper-layer protocol receives incoming packets after IP processing is complete.

Header Checksum: Helps ensure IP header integrity.

Source Address: Specifies the sending node

Destination Address: Specifies the receiving node

Options: Allows IP to support various options, such as security.

Data: Contains upper-layer information.

3.2 IP Standard Architecture

Traditional centralized IP network consists of a largely centralized processor connected with two terminals at either sides. The internet contains an infrastructure of core routers connected through Tetra byte fiber optic transmission medium [22]. The core routers provide a link to ISPs or enterprise network through the T3 line of Gigabyte transmission such that ISPs connect common business, homes and other ISPs with local area network or metropolitan area network. LAN consists of a small number of networks nodes connected through ether network and consists of the bus, ring, star and mesh topologies. Bus and token ring topologies form a broadcast network. MAN encircle cities through simple bus topology connected either through ethernet or wireless access; cable television is an example of a MAN network. WAN covers a larger geographic area i.e. countries or continents [30]. Larger ISPs often consisted of WAN networks and involves communication subnet to carry transmission lines and performs switches for end nodes running application programs at the user premises. Transmission lines consist of high-speed channel i.e. fiber optic, copper, radio links, whereas switching is performed through specialized computers which connect these lines across countries/continents. Since there are different types of networks which connect nodes and other networks, in order to perform transmission between nodes of different types of networks gateways are required to connect them and performs hardware software translation. This mechanism is called internet or network as shown in Figure 3.2.

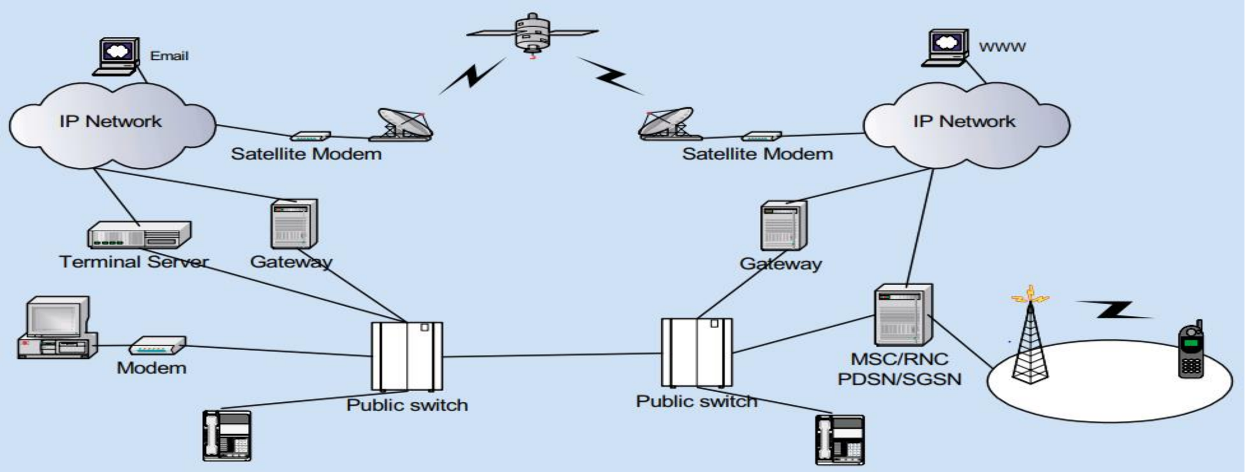


Figure 3.2: Internet protocol Standard Architecture [30].

3.3 Traffic Engineering in IP

Traffic Engineering is a technique to control the flow of data over the network by reserving bandwidth for specific services. TE may be also implemented to accommodate network maintenance [6]. The objective of the traffic engineering technique is to improve the performance of the operational network at the resource level as well as at the traffic level. Parameters such as packet loss, delay, jitter, and throughput are used to measure the network performance. To choose between different routing paths, most IP networks use Interior Gateway Protocols (IGP) based on the Open Shortest Path First (OSPF) algorithm with static link weights. These weights provide the routers with a complete view of the network to populate routing tables. When links have distinct capacities, considering link utilization is more appropriate [2]. Network engineers employ a number of tools to automate the process of monitoring network links and to send alerts when a link is heavily used. These network usage patterns collected over a certain period of time may help manage the flow of data at a particular time instance or for a particular service. The concept of traffic engineering in IP network is shown in Figure 3.3.

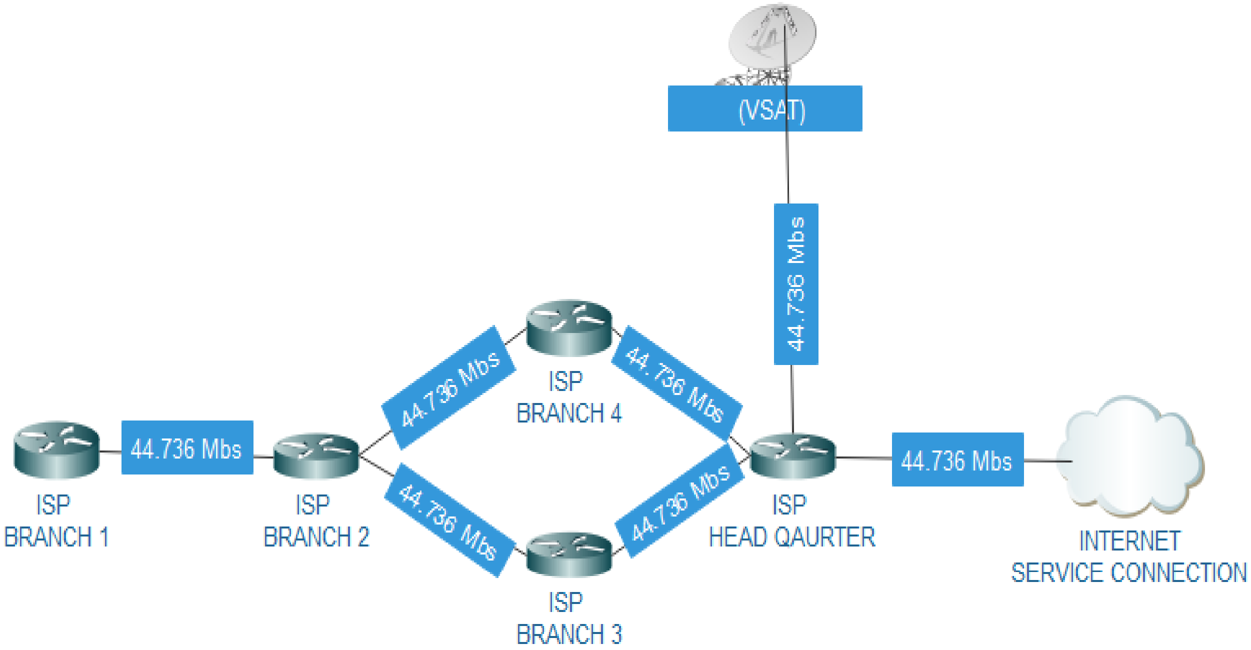


Figure 3.3: Traffic engineering in an IP network

All routers in branches are configured with an Open Shortest Path First (OSPF) algorithm and the networks are advertised between sites. The network shown in Figure 3.3 consists of seven links with the same link capacities. If ISP branch 1 wishes to communicate with ISP headquarter, it can either communicate via branch 3 or 4. By default, a router dynamically selects the link with higher capacity to send the data unless a policy is defined through a static route.

3.3.1 IP Routing

IP routing is able to identify network links and send data to the destination. The total available network bandwidth is shared among all network users without allocating bandwidth for a specific user or service. To send data over different routes, IP routing uses protocols such as the

Open Shortest Path First (OSPF) and the Routing Information Protocol (RIP) [2]. These protocols forward data based on the information contained in routing tables present in routers.

3.3.2 Functionality of IP Routing

In an IP network, a router selects the next router for the destination of the packets based on its routing table. Every router in the path replicates the same process by using its routing table until the packet reaches its destination. IP routing is shown in Figure 3.4.

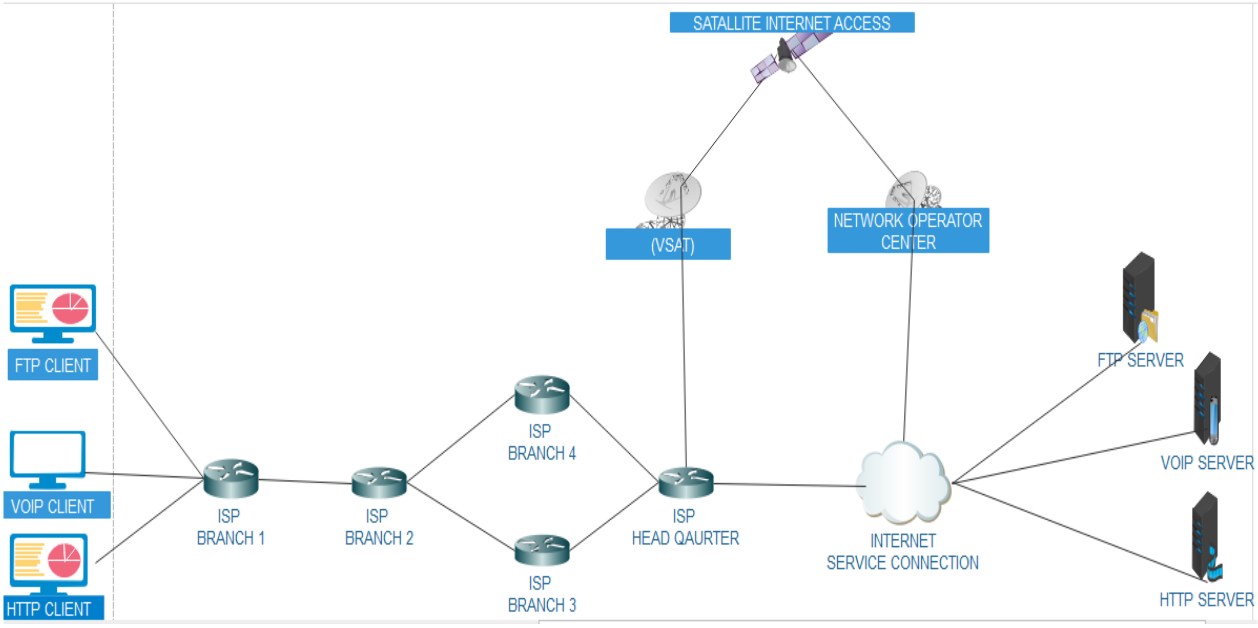


Figure 3.4: IP routing in a simple network

The subnet associated with each router falls under the supernet (parent subnet). If the host with IP address wishes to access the web server, it will send its packet on the path to the connected router via VSAT or Internet Service Connection. Each router will check the destination address of the packet in its routing table. Routing table keeps information about the addresses of the interconnected network and the path that will be followed to send data towards the destination. The routing decision is based on the shortest path available to the destination. Protocols used for the IP routing are Border Gateway Protocol (BGP), Intermediate System-Intermediate System(IS-IS), OSPF(Open Shortest Path First), and Routing Information Protocol (RIP) [2]. RIP keeps track of the closest router for each destination address and is suitable for smaller networks. OSPF keeps track of a complete topological database of all connections in the local network and is suitable for larger networks. The Internet is divided into Autonomous Systems (AS). An AS is a group of routers that are under the control of a single administration. They exchange routing information by using a routing protocol [3]. AS is divided into the following three types:

Stub AS has a single connection to the other autonomous system. Example of a stub network is a small campus network.

Transit AS has multiple links with one or more autonomous systems. It allows data to be forwarded out of the autonomous system. Example of a transit network is the Internet Service Provider (ISP) network.

Multi-homed AS has multiple links with one or more autonomous systems but it does not allow data received on these links to be forwarded out of the autonomous systems. It is similar to a stub autonomous system. Example of multi-homed AS is a large enterprise network.

Chapter 4

Network Model and Design

This chapter describes the model under study and how to implement it in Riverbed Modeler software. The version of OPNET used for this work is Riverbed Modeler 17.5. OPNET is a short form of Optimized Network Engineering Tool and it has its roots in study and research related to computer networks. OPNET Modeler can be used as a platform to develop models of a wide range of systems that includes [5].

- ✓ Standard LAN/WAN performance modeling including satellite internet
- ✓ Internetwork planning
- ✓ Resource sizing
- ✓ Research and development of advanced distributed network environment

In this Thesis, a Riverbed modeler simulation tool is used to model the network design that is being investigated while keeping in mind the final goals as stated in the objective. When the model is in a complete form, built in simulations are run to actually study the system's behavior and performance. However, before running simulations, the user must consider what information is to be obtained from the modeled network. In the case of these thesis simulations, a large number of system variables and metrics are available for evaluation. Each Riverbed modeler module at the node level, as well as a link at the network level, is the source of a significant number of built-in local statistics, and in addition, a simulation can generate large numbers of global and local user-defined statistics. In general, only a small subset of the available data is of particular interest. For collecting the results, Riverbed works as an active network-monitoring tool. The active network monitoring tools send the additional traffic into the network. Active monitoring has done through probes that do not affect the network characteristics in any way. Probes aim to emulate the actual network traffic and are sent among the active network agents (devices). The agents measure the received streams and typically keep a statistical analysis of measured results, which can be obtaining data periodically by the active monitoring device. The active network monitoring is in contrast to passive network monitoring where each network device records statistics on actual network traffic result passing through it as an indication of status at a particular network element. Periodic polling is typically used to gather data residing at different nodes for reporting and analysis. Hence, passive monitoring looks at each device in isolation and by looking at multiple devices an aggregated view of the status of the network is deduced [29]. Once the simulation ends with the desired parameters turned on, this corresponds to specific metrics. The next step is to analyze the results achieved through the Result Browser inside Riverbed modeler. The Results Browser is used to display information in the form of graphs. A graph is the part of the result browser that can contain statistics. With this introduction about the Riverbed modeler, the remaining section deals with the simulated environment regarding this thesis work.

4.1 Assumption

The research aim is to compare the quality of service in IP and MPLS networks for broadband satellite internet. This can help in understanding and in comparing different results achieved through a single model with different scenarios. Quality of service consideration only comes into play when the network gets congested which results in the increased packet, jitter or drops. To better understand IP and MPLS technology in accordance with the QoS, the backbone network links provided here are a smaller factor of the local links, which helps in alleviating the bottleneck links outside the network. This design visualizes the participation of different network application across the core links, and how the backbone nodes handle different application traffic requirements as a prescribed bounded element. It is difficult to predict the behavior of the traffic in the network as the traffic in network varies from source to destination at any time. The simulation of the conventional IP and MPLS models is performed by considering the worst-case scenario in which the minimum number of VoIP calls that a network can support with acceptable quality has been estimated. In the thesis, it is possible to consider the background traffic excluding the VoIP traffic to be like 50% of link capacity. The link capacity is the max-utilization allowed of a link to protect it from bursts as explained in Riverbed Modeler.

Component used for Network Design

Table 4.1 shows the component used in design of proposed network topology for simulation.

Table 4.1: Component used network topology in details

Number of Router including satellite router	8
Number of hosts	3
Number of servers	3
Router Models	Cisco 7200 router
Router Operating System	Cisco’s IOS Operating System
Cloud Interfaces	Internet Gateway

Cisco 7200 router: Router model capable of supporting MPLS and IP network. It leads choice for provider-edge deployment. A wide range of connectivity options and numerous features including service ability and manageability [32]. Increased scalability and flexibility with the new Port Adapter Jacket Card. Increased VPN performance with the new VPN Services Adapter. It is types of Cisco's services that can help to increase operational efficiency, lower support costs, and improve availability risk management. Cisco 7200 Series bundles enable customers to order a Cisco 7200 Series Router with all of its components using just one part number.

This provides enterprise and service provider customers with easy-to-order solutions to meet their WAN and MAN edge services aggregation-networking needs. IP-to-IP Gateway support direct IP interconnections. Table 4.2 shows Cisco 7200 series security bundles.

Table 4.2: Cisco 7200 series security bundles

Bundle part number	Product Description	Availability
7206VXRG2/VSAVPNK9	Cisco 72VXR, VPN services Adapter, 1GB system memory, AC power, Cisco Router, and security device manager (SDM)	Available in OPNET
7206VXRG2/2+VPNK9	Cisco 7206VXR, VPN Acceleration Module 2+(VAM2+), AC power, PA Jacket Card, 1 GB system memory, Cisco SDM	Not Available in OPNET
7206VXRG1/2+VPNK9	Cisco 7206VXR, VAM2+, AC power, 512 MB system memory, Cisco SDM	Not Available in OPNET

4.2 Riverbed Model Configuration

This section will describe which and how different network elements are placed to design the desired network topology inside Riverbed modeler software. To study the characteristics of the intended work, the baseline network topology will remain compliant. Only the configuration on the interacting nodes will differ, according to objectives. The network components used in this thesis are obtained from Riverbed library:

Ethernet_wkstn: ethernet workstation element is used to simulate the network users. It consists of a single ethernet connection at a selected rate, directed by the underlying medium used to connect to an ethernet router of ISP branch 1. In the case of this thesis network model HTTP, FTP and VOIP CLIENT, assign as ethernet_wkstn.

Ethernet server: ethernet server provided in riverbed modeler is used to simulate the service server in the network. It connects to internet connection cloud. In this thesis HTTP server, FTP server and VOIP server are used as ethernet server.

Application Config: This element is used to tell riverbed modeler which application is going to be modeled upon the underlying network. A single Application Configuration is used to instruct riverbed for multiple network applications. Application parameters for different application types being observed are configured in this element.

Profile Config: Profiles describe the activity patterns of a user or group of users in terms of the applications used over a period of (simulation) time [6]. There can be several different profiles running on a given network under observation. User profiles have diverse properties, so configuring a certain profile with a specific application was done here. The configured profiles are then assigned to the network users.

MPLS_config_object: Configuring MPLS FEC and Traffic Trunk is done under this element configuration. The configured specification is used at the ingress edge router to direct the traffic flows and assigns different LSP to different application traffic.

MPLS_E-LSP_STATIC: Static LSP is not signaled during the startup. They allow more routing control.

4.3 Types of Service Levels

Service levels refer to the actual end-to-end quality of services capabilities meaning the ability of the network to deliver service needed by specific network traffic from end to end. These services differ in their level of quality of service requirements, which describes how strongly the service can be guaranteed by specific bandwidth, delay, jitter and loss characteristics.

Best-effort service; also known as lack of QoS. It is the original internet service. Makes best effort to transfer packets, but provides no guarantees. Best-effort service does not employ any prioritization scheme, hence, in the case of congestion, any packet may be dropped.

Differentiated service (DiffServ); also called soft QoS; different priorities are assigned to different applications. Hence, some traffic is treated better than the rest (faster handling, more bandwidth on average, and lower loss rate on average).

Integrated service (IntServ); also called hard QoS; an absolute reservation of network resources for specific traffic. In this class, the devices on the network through signaling can negotiate, request and adjust priority levels for different types of traffic based on the previously agreed values. Table 4.3 shows the type of services used in riverbed modeler software for simulation of voice, file transfer protocol and hypertext transfer protocol for network model.

Table 4.3**:** Types of services used in software for evaluating the performance of the network model

NO	Types of services	Selected code point in the binary	Selected code point in decimal (kbs)
1	Best effort	00011100	28
2	Background	00111100	60
3	Standard	01011100	92
4	Excellent effort	01111100	124
5	Streaming multimedia	10011100	156
6	Interactive multimedia	10111100	188
7	Interactive voice	11011100	220
8	Reserved	11111100	252

In reference to Table 4.3, the interactive voice is used to measure the performance of voice whereas the excellent effort and streaming multimedia used to measure the performance of file transfer and hypertext transfer protocol respectively in the Riverbed Modeler software.

4.4 Simulation Procedure

Since the goal of this thesis is to measure the performance of the network and to evaluate the relationship between IP and MPLS network, Riverbed Modeler Academic Edition is the appropriate simulator for these works. The following sections explain simulation procedure for the network model.

4.4.1 Application Configuration

In order to model an application in Riverbed Modeler, an object is available which is called application definition attribute. Application definition attribute consists of predefined applications, which can be modified as per the user requirements. Some of the predefined applications in application definition attribute are HTTP, FTP, Voice, E-mail, video, and database.

Figure 4.1: Application Configuration

In this thesis, three applications are established which generate the requisite traffic over the network between client and server. Riverbed Modeler Academic Edition makes available an object called Application config, which is used to create the needed applications on the network. The following procedure explains the configurations of applications.

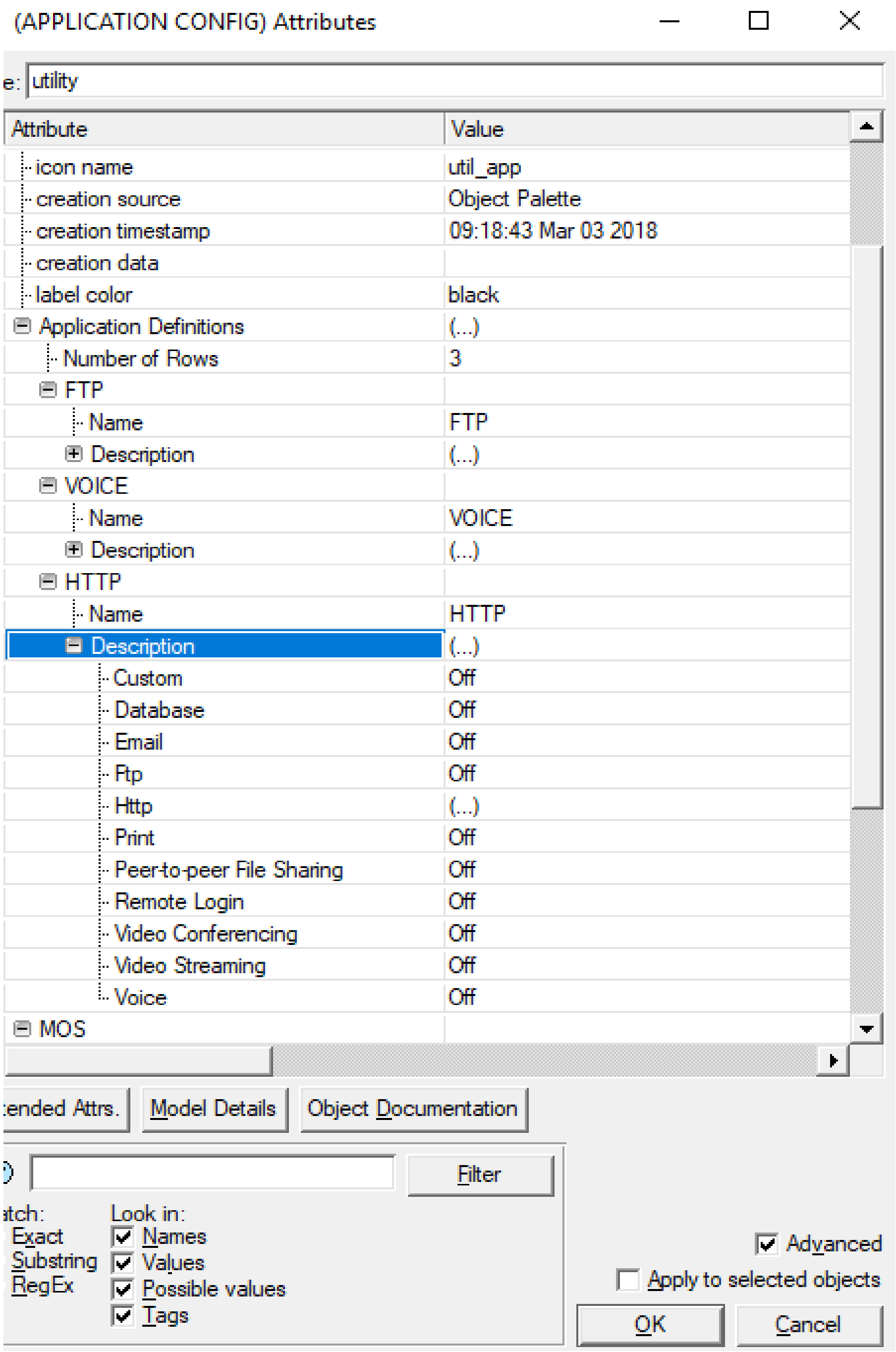
Step 1: Right- click on application Definition object and select edit attributes.

Step 2: Add three rows to the applications definitions table, to enable the creation of three applications.

Step 3: Rename the first row as FTP and select excellent effort against the FTP applications

Step 4: Rename the second row as VOIP application and select interactive voice against voice applications

Step 5: Finally rename HTTP as the third row and select streaming multimedia against HTTP application.



(APPLICATION CONFIG) Attributes

e: utility

Attribute	Value
icon name	util_app
creation source	Object Palette
creation timestamp	09:18:43 Mar 03 2018
creation data	
label color	black
⊟ Application Definitions	(...)
Number of Rows	3
⊟ FTP	
Name	FTP
⊞ Description	(...)
⊟ VOICE	
Name	VOICE
⊞ Description	(...)
⊟ HTTP	
Name	HTTP
⊟ Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	Off
Http	(...)
Print	Off
Peer-to-peer File Sharing	Off
Remote Login	Off
Video Conferencing	Off
Video Streaming	Off
Voice	Off
⊟ MOS	

itch:
Exact
Substring
RegEx

Look in:
☑ Names
☑ Values
☑ Possible values
☑ Tags

☑ Advanced
☐ Apply to selected objects

Figure 4.2: Application Definition attribute used in the simulation model

Figure 4.2 illustrate about the application definition configuration. It is used to tell riverbed which application is going to be modeled upon the underlying network.

4.4.2 Profile Configuration

The application needs to generate traffic over the internet. Riverbed modeler offers a profile configuration object, which is used to generate the necessary traffic. The steps below detail how to configure the profile definition.

Step 1: Right-click on profile configuration object and choose edit attributes.

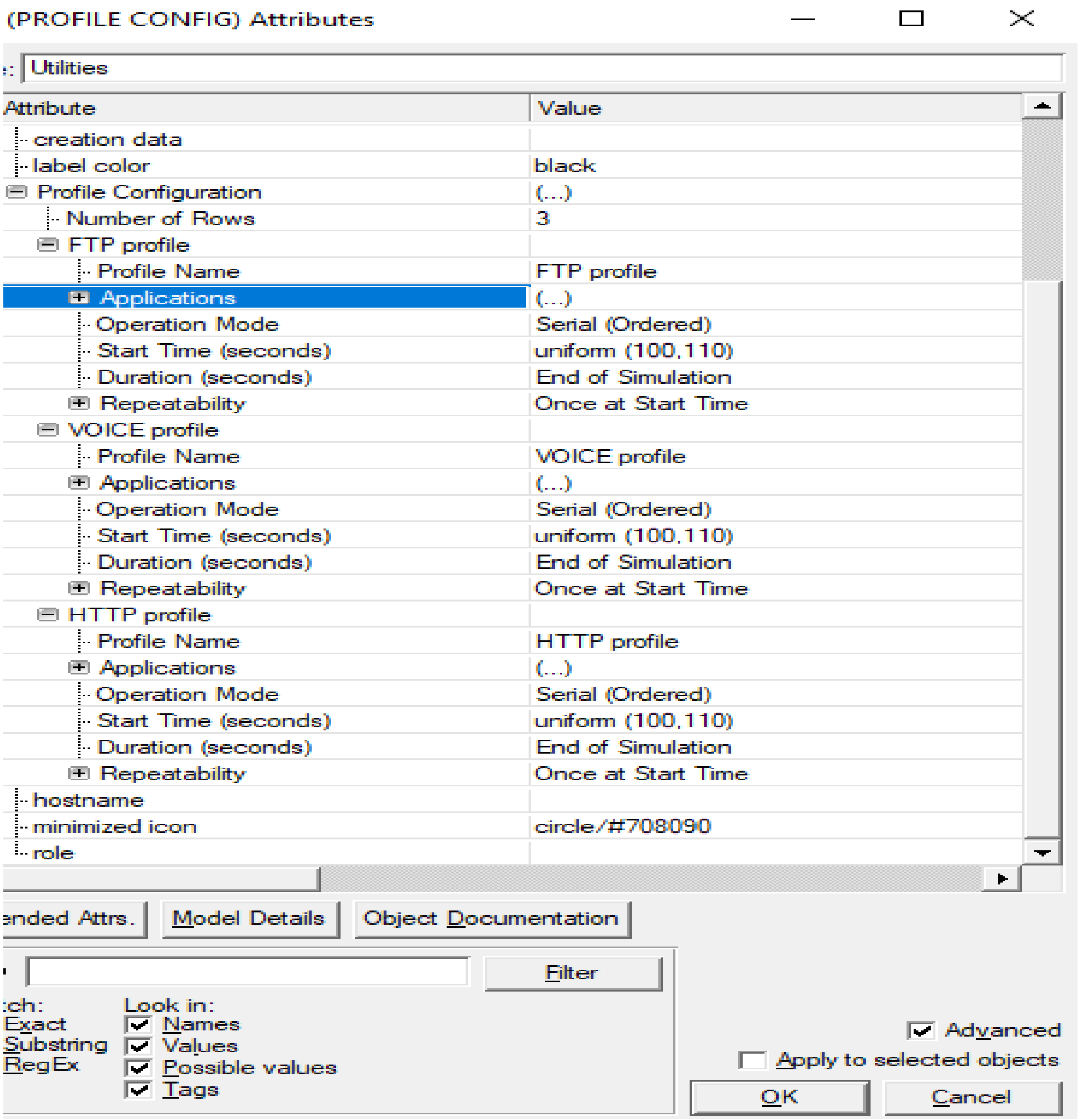
Step 2: Add three rows for configuration

Step 3: Name the first row “FTP Profile” select FTP as its corresponding application.

Step 4: Name the second row as “VOIP Profile” and select voice as its corresponding application.

Step 5: At the end name the last row as “HTTP Profile” as shown in the figure below.

The behavior of the workstation is described by its Profile, which is defined by using the Profile Definition. Figure 4.3 shows the Profile Definition object used in thesis simulation; the start time of the simulation is set to uniform distribution [100,110] seconds and the VoIP application is repeated continuously till the end of the simulation. It means that VoIP calls are established between workstations VoIP client and VoIP server starting at uniform distribution [100,110] seconds and the calls are added continuously until the end of the simulation. In this thesis, the profile configuration use uniform distribution, which consists of a point from the interval [100,110] such that all points are equally likely to be chosen.



Attribute	Value
creation data	
label color	black
⊟ Profile Configuration	(...)
Number of Rows	3
⊟ FTP profile	
Profile Name	FTP profile
⊞ Applications	(...)
Operation Mode	Serial (Ordered)
Start Time (seconds)	uniform (100,110)
Duration (seconds)	End of Simulation
⊞ Repeatability	Once at Start Time
⊟ VOICE profile	
Profile Name	VOICE profile
⊞ Applications	(...)
Operation Mode	Serial (Ordered)
Start Time (seconds)	uniform (100,110)
Duration (seconds)	End of Simulation
⊞ Repeatability	Once at Start Time
⊟ HTTP profile	
Profile Name	HTTP profile
⊞ Applications	(...)
Operation Mode	Serial (Ordered)
Start Time (seconds)	uniform (100,110)
Duration (seconds)	End of Simulation
⊞ Repeatability	Once at Start Time
hostname	
minimized icon	circle/#708090
role	

Figure 4.3: Profile Definition attribute used in the simulation model

4.4.3 Internet Configuration

Riverbed Modeler makes available an IP32 cloud, which performs the function of a simple public internet-based cloud. In this research, the cloud is used to support the three applications from the client to the server over the whole network model. The steps show how to configure the cloud or internet.

Step 1: Right- click on the cloud and select edit attributes

Step 2: Change the packet latency by setting its value to 0.08 seconds

Setting packet latency to 0.08 second implies that the utmost packet delay across the internet as a result of HTTP, FTP and voice is 0.08 seconds. Every packet travels over the cloud within a limited delay of 0.08 seconds.

4.4.4 Router Configuration

The router used in the simulation is the Cisco 7200 router object. The link between them is DS3 and which is used to connect the IP32 cloud and the servers. ISP routers were used for load balancing purposes the following step shows how it was configured in the proposed network models.

Step 1: Click on the discrete event simulation

Step 2: Click on the configuring/ Run DES

Step 3: Click on IP and expand its attributes

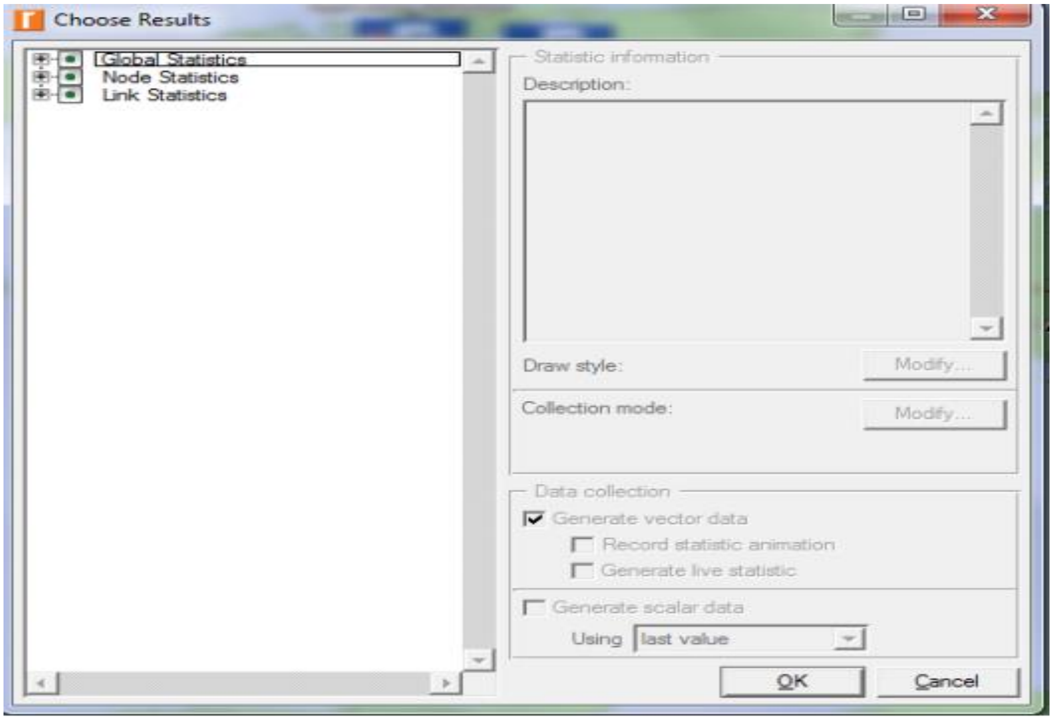
Step 4: change the IP static routing protocol from default to OSPF.

4.4.5 Performance Metrics Configuration

To measure the performance of the cloud against the three applications few parameters are required. Riverbed models provide three levels to measure the performance of a network. These are the global level, node level, and link level. In this research, the global and node, as well as link level, are used to measure the performance of the application on the network. Global level is configured as per the following step.

Step 1: Click on discrete event simulation (DES) menu and select individual statistics.

Step 2: A new window opens with the options to global statistics, node statistics and link statistics as shown in below Figure 4.4.



☑ Generate vector data
☐ Record statistic animation
☐ Generate live statistic
☐ Generate scalar data
Using: last value

Figure 4.4: Performance metrics

The metrics in Figure 4.5 are chosen for performance evaluation of both internet protocol and multi-protocol label switch networks. Figure 4.5 shows global level metrics for performance evaluation expand the HTTP option and choose the page response time, traffic sent and received. In addition, the download and upload response time, traffic sent and received options are checked for FTP options.

At the end global statistics expand the voice options choose the jitter, latency, end-to-end delay and delay variation as shown in Figure 4.5.

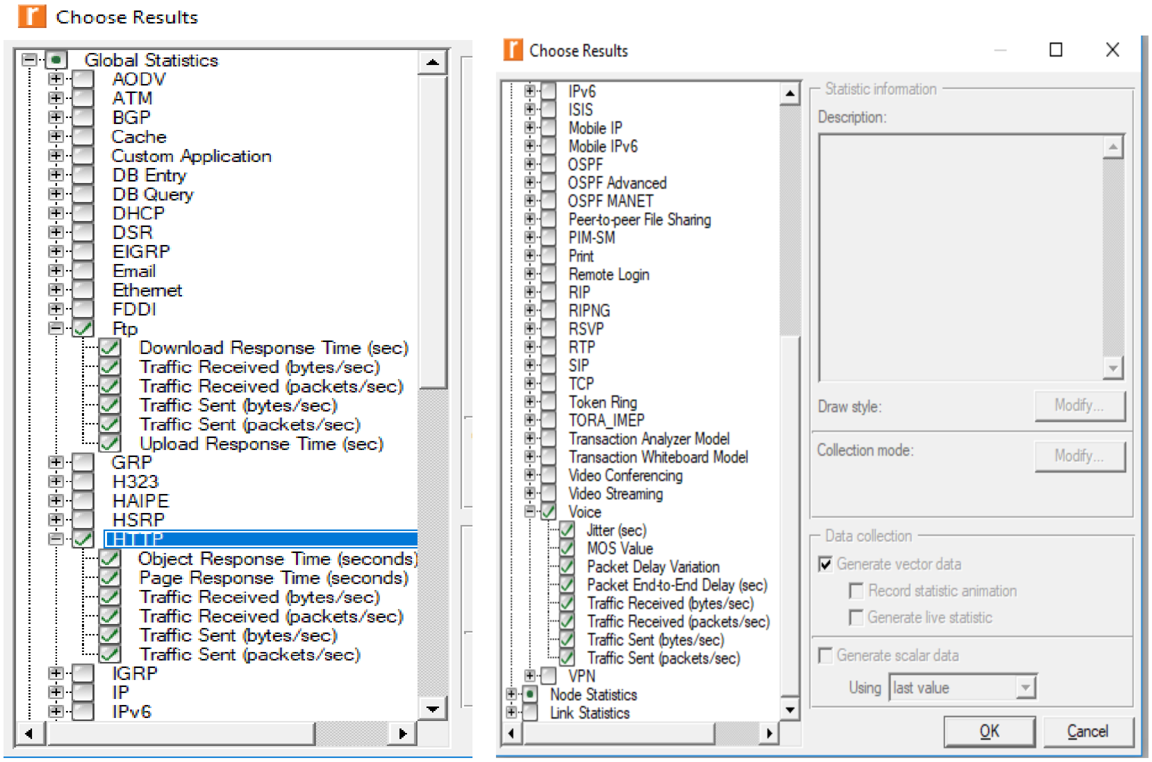


Figure 4.5: Global statistics voice, HTTP and FTP performance metrics

Figure 4.6 shows the link level statistics, the performance metrics are selected from link level statistics. Expand point to point and select inbound and outbound utilization as shown in Figure 4.6.

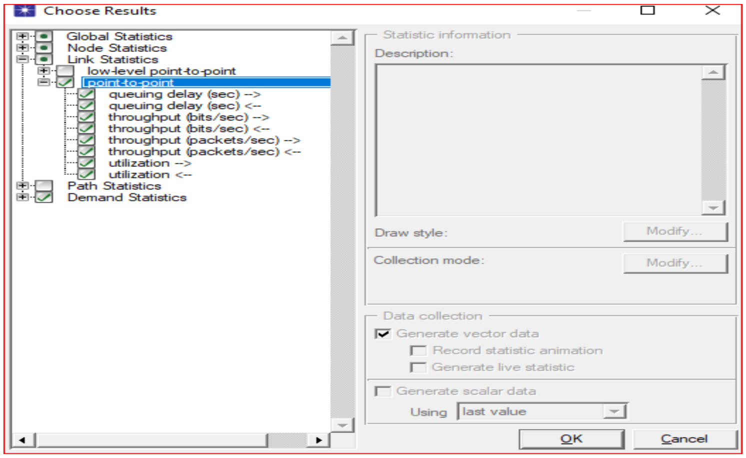


Figure 4.6**:** Link-level point to point performance measurement

4.5 Network Design

The network topology cannot be said to be a realistic operational network. The intention was to create a networking environment, which could represent a part of an overall network topology of an internet service providers network. The model possesses supported application like HTTP, FTP, VOIP client and servers, link models, satellite router, internet cloud, and Cisco 7200 access routers were used at the edge of the network where the traffic was transmitted to or received from the workstations and the servers. The simulation of both IP and MPLS networks are employed in the (Riverbed Modeler). The simulations are set up using two stages.

Stage one: consists of a simulation of the IP network with traffic engineering

Stage two: consists of a simulation of the MPLS network with traffic engineering.

Both the networks are simulated by considering common topology.

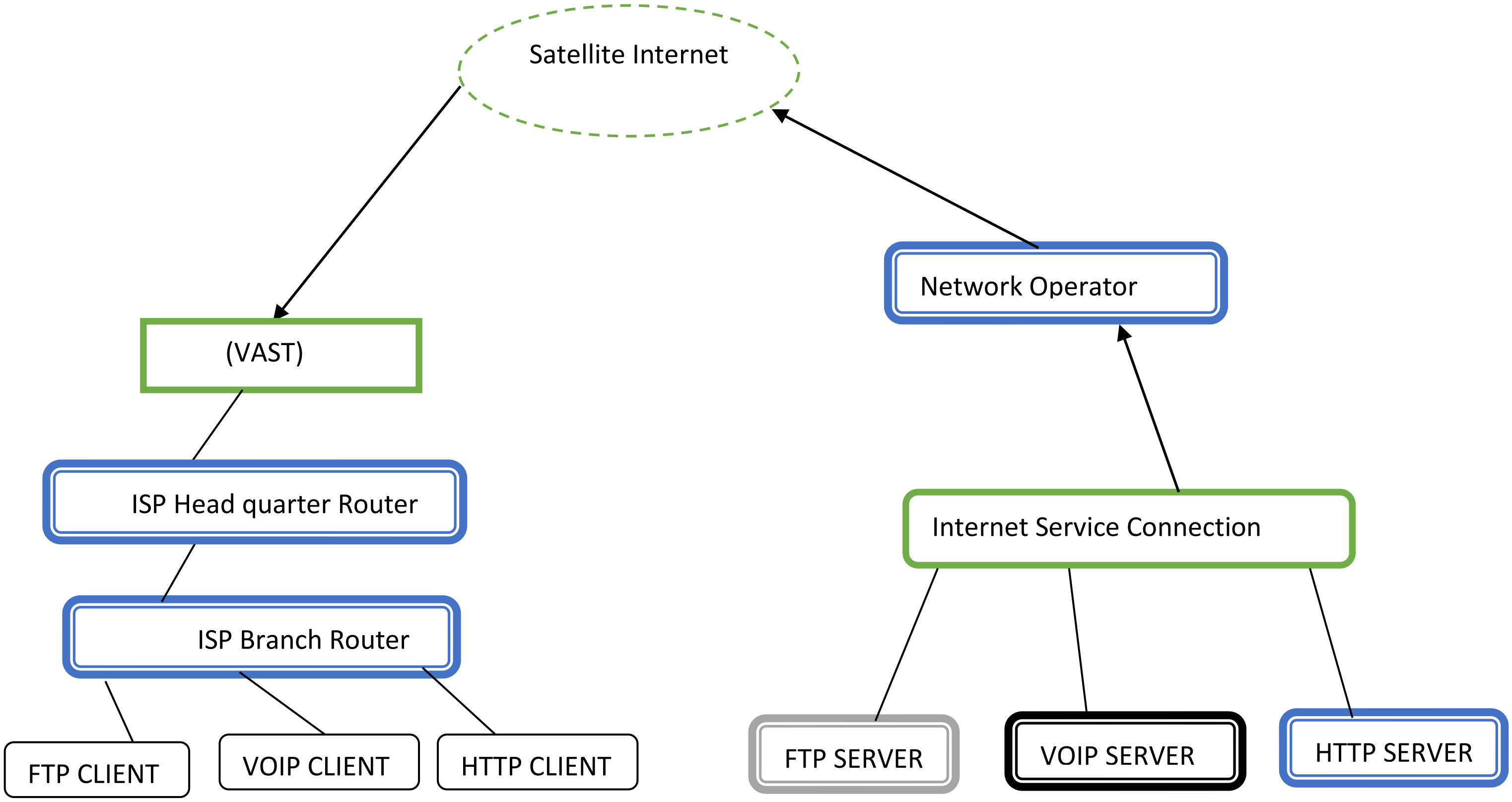


Figure 4.7: Transmitter and Receiver path block diagram

Figure 4.7 shows the general network topology proposed for MPLS and IP network design.

4.5.1 Description of the IP based Network Model

In the proposed network model three applications were configured which used open short path first protocol (OSPF) as their routing protocol. The three application used in network models are voice, file transfer protocol, and hypertext transfer protocol. These three applications are configured on both the client and server side. For the configuration of applications on side, application configuration box and profile, configuration box are used. IP QoS configuration box and IP configuration box are used to configure internet protocol address and quality of services in the network model. All ISP branch router, Internet cloud, clients and servers are connected as shown in the Figure 4.8 topology. In IP Model, all routers including satellite and dish router are replaced with normal internet routers. Open short path first protocol will be used to route all internet protocol traffic, which includes voice, file transfer protocol, and hypertext transfer protocol that is transmitted between client and server. The FTP traffic is transmitted between the FTP Client and FTP Server. The HTTP traffic is transmitted between HTTP Client and HTTP Server. At the end VOIP traffic generated between VoIP Client and VoIP Server. The details over the configuration of the network model with IP nodes and traffic implementations within Riverbed Modeler can be reviewed in Appendix A.

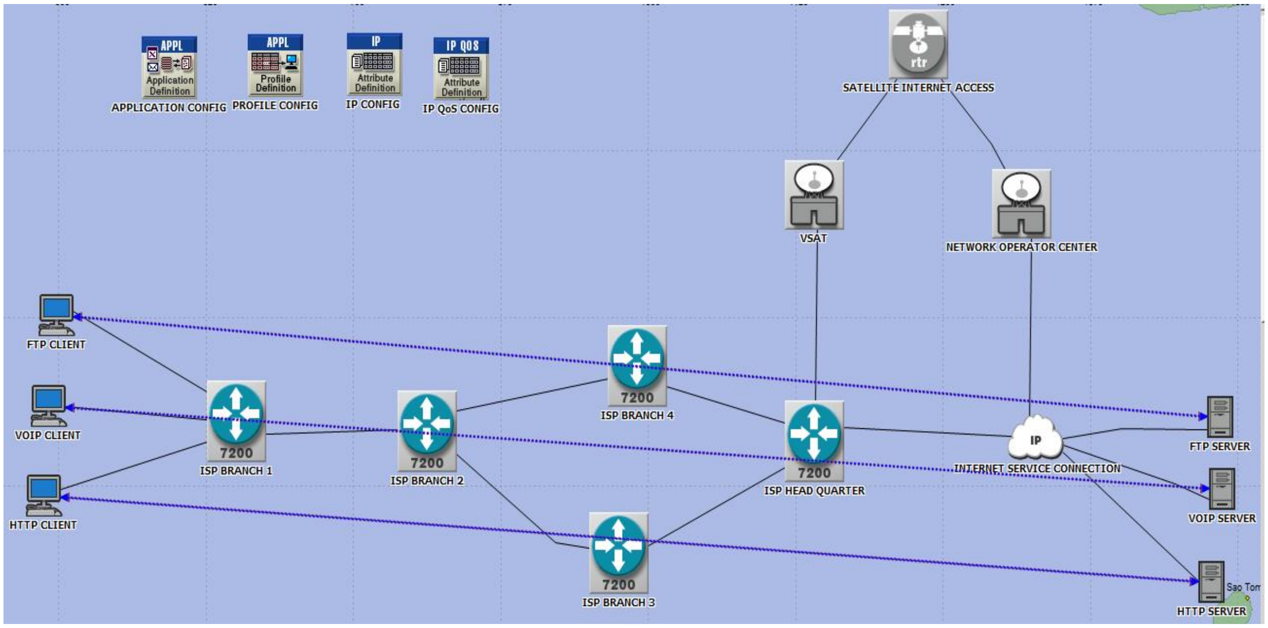


Figure 4.8: Description of the IP based network model

4.5.2 Description of the MPLS based Network Model

In this part of the network model, the voice over internet protocol (VoIP) traffic is sent between VoIP client and VoIP server, the same terminology is followed with file transfer protocol and Hypertext transfer protocol, which are sent between FTP and HTTP client and server respectively. Internet core consists of five routers assigned as ISP router. The routers are connected with digital line subscriber number three (DS3) cable which has a data rate of 44.736Mbs. After connecting all routers with this data rate MPLS is enabled on each router and configuration of MPLS with signaling protocol has been done. The voice client and server, which setup to transfer five frames per packet, use application description with a coding rate of 220Kbs (interactive voice). HTTP client and server used HTTP specification HTTP 1.1, Page inter-arrival time in seconds and types of services with streaming multimedia (156Kbs). While FTP client and server used a file size of 50,000 bytes and excellent effort types of services. The simulation time for the network model is set to 600 seconds. In order to be able to control flows of traffic in MPLS network model, label-switching paths (LSPs) had to be installed. From Riverbed Modeler library static label switching paths were established in order to have a more exact control over the path. Traffic Engineering is implemented in the MPLS simulation model by using constraint route label distribution protocol (CR_LDP) signaling protocol. Traffic engineering is configured in Riverbed Modeler by defining forward equivalence classes (FECs) in MPLS definition attributes and setting the label distribution protocol (LDP) parameters in the routers. The constraint route label-switching path (CR_LSP) which is established can be visible in Figure 4.9 as a blue and red colored link from ISP branch 1 to Internet service connection through ISP branch 3 and 4. When congestion occurs in the network, the traffic is directed along constraint-based routed label switching path so that the traffic at all application is evenly distributed in the MPLS network model. In this thesis dynamic, LSP is not used since the network model was not very large. Instead, static-LSP was interested to have a better control, over the small network design which is not complex.

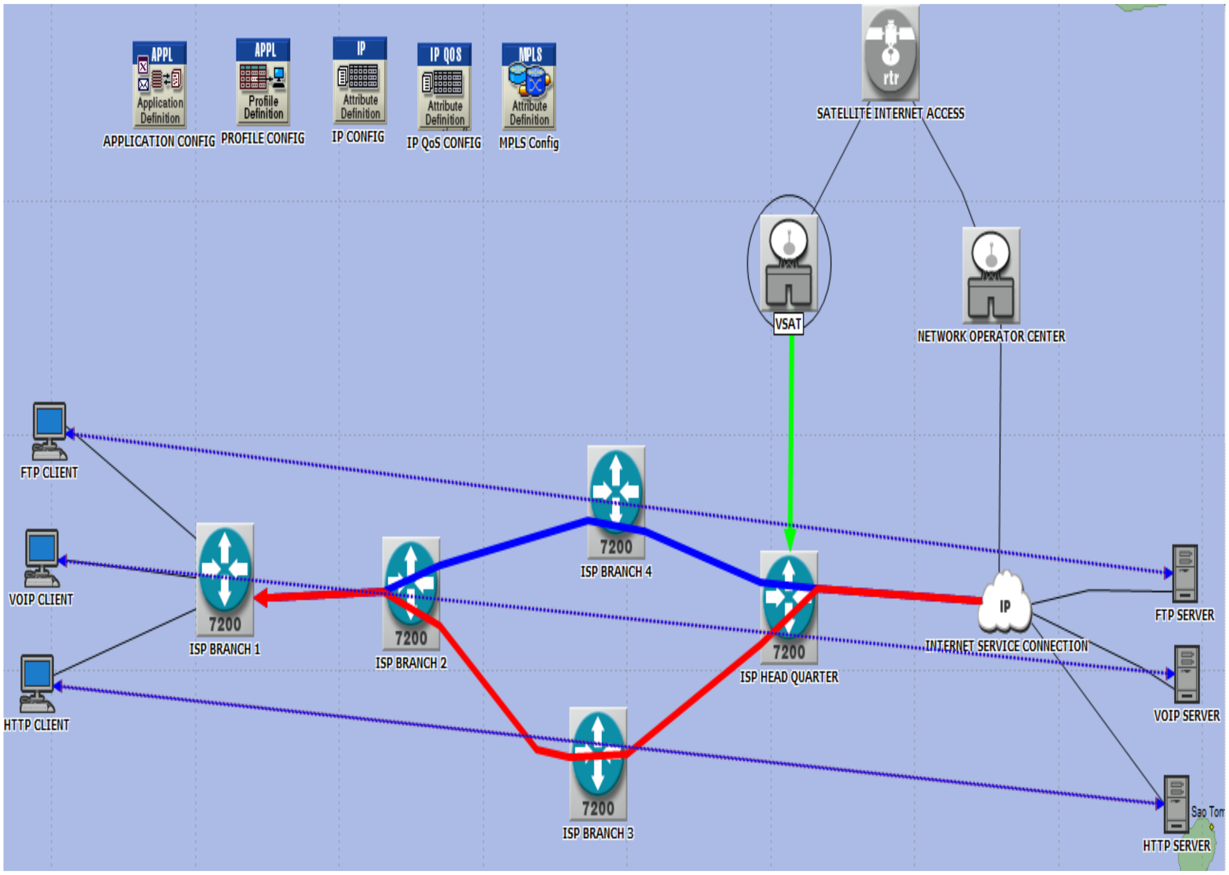
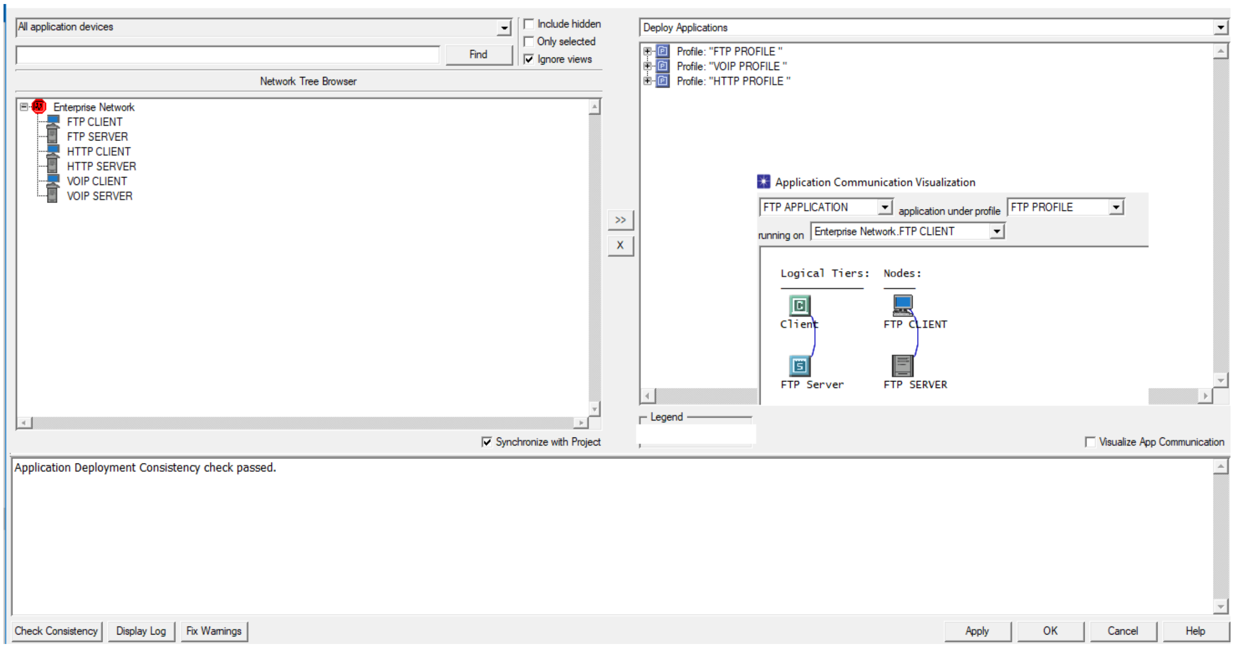


Figure 4.9**:** Description of the MPLS based network model

Four static LSP's were configured from the ingress router ISP Branch 1 and the egress router Internet Service Connection and from Internet Service Connection to ISP Branch 1 as shown in Figure 4.9. ISP Branch 1 ➡ ISP Branch 2 ➡ ISP Branch 4 ➡ ISP Headquarter ➡Internet connection. This path allows FTP traffic from FTP client to the FTP server. Internet Service Connection➡ISP headquarter ➡ISP Branch 4 ➡ISP Branch 2➡ISP Branch 1. This is reverse path allow FTP traffic to follow from FTP server to FTP client. ISP Branch 1➡ ISP Branch 2➡ ISP Branch 3➡ ISP Headquarter ➡Internet connection. This path allows VoIP traffic from VoIP client to the VoIP server. The reverse path allows the VoIP traffic to follow from VoIP server to VoIP client. The path for HTTP traffic is the same as the path configured for FTP traffic. Traffic binding was configured on Internet Service Connection. FEC_FTP was bound to flow through assigned LSP from FTP client to FTP server. Three traffic trunks were specified for the traffic flowing through the LSP's path. Trunk FTP was created to generate the traffic from the FTP client to FTP server. FEC_VoIP was bound to flow through assigned through LSP from VoIP client to VoIP server. Trunk VOIP was created to generate the voice traffic from VoIP client to VoIP server and trunk HTTP was created to generate the HTTP traffic from HTTP client to HTTP server. Three forwarding equivalent classes (FEC) were created, one for FTP traffic based on the types of services excellent effort, VOIP traffic FEC-VOIP with types of services being interactive voices. The same was done with the reverse path. The traffic binding was configured on the Internet Services Connection. After configuration of LSP for MPLS network model on Figure 4.10, the following parameters were set on all routers. LDP was enabled, link discovery hello's were enabled, loopback interfaces were enabled and configured. LDP neighbor's router was set and finally, all the interfaces in the routers were enabled. Details over configurations of MPLS network model and traffic implementations within Riverbed Modeler can be reviewed in Appendix B.

4.6 Deploy Applications



All application devices

Deploy Applications

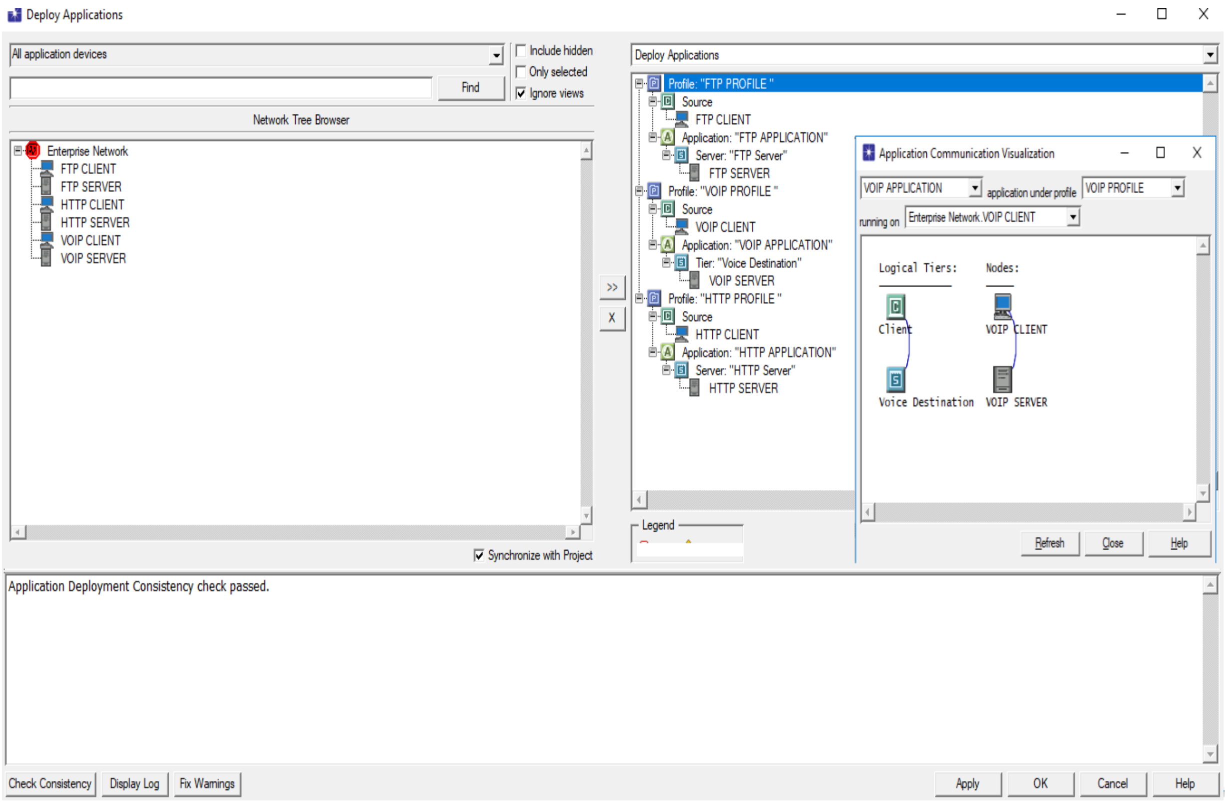
FTP APPLICATION application under profile FTP PROFILE

running on Enterprise Network.FTP CLIENT

Application Deployment Consistency check passed.

Figure 4.10: Before deploying application between client and server

In Figure 4.10 deploying has been taken place when the configuration of three applications in the application definition box and profile definition box has finished. Deploy application means deploying client to server to exchange information with each other to generate traffic proposed for the simulation.



Application Deployment Consistency check passed.

Figure 4.11: After deploying application between client and server

Figure 4.11 shows that the deploying of three applications and application communication visualization.

4.6.1 Voice Codecs Introduced by International Telecommunication Union

A voice codec is employed at the user side to convert the analog voice waves into digital pulses and vice versa. There are various codec's types in riverbed modeler software based on the chosen data rate and sampling rate. The mean opinion score (MOS) was introduced by International Telecommunication Union and represents multimedia quality from users prospective range 1 (poor) and 5 (excellent) [37]. Various codec types are listed in Table 4.4.

Table 4.4: various codec's types [37]

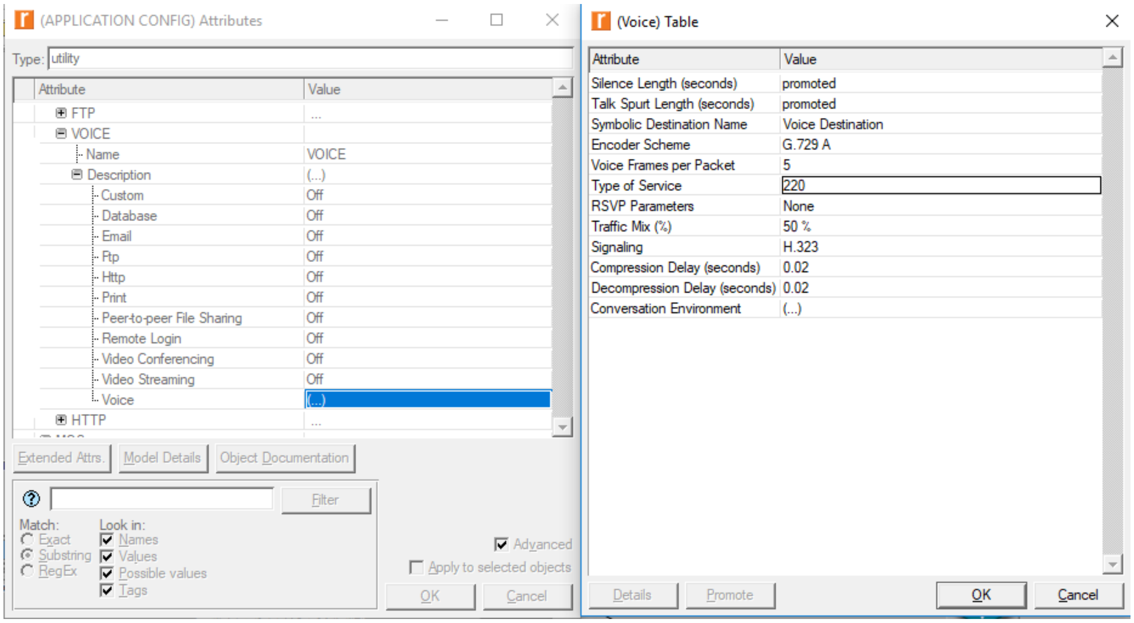
Codec Type	Coding rate in (Kbps)	MOS
G.711	64	4.4
G.722	48	3.87
G.723	5.3 and 6.4	3.9
G.726	16 to 24	3.85
G.727	16 to 40	3.71
G.728	16	3.61
G.729	8	3.92

As shown in the above Table 4.4, the mean opinion score (MOS), which is speech quality, is decreasing in a non-linear manner with their data rate.

4.6.2 Modeling of VOIP Traffic in Riverbed Modeler

As shown in Table 4.5 silence length specifies the time spent in seconds by the called and calling party in silence mode for a speech silence cycle. Voice frames per packet attribute determine the number of encoded voice frames grouped into, voice packet before being sent by the application to the lower layers. Compression delay and Decompression delay attributes specify the delay in compressing and decompressing a voice packet is 0.02 seconds as shown in Table 4.5.

Table 4.5: Riverbed Modeler voice traffic specification



Type: utility

Attribute	Value
FTP	...
VOICE	
Name	VOICE
Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	Off
Http	Off
Print	Off
Peer-to-peer File Sharing	Off
Remote Login	Off
Video Conferencing	Off
Video Streaming	Off
Voice	(...)
HTTP	...

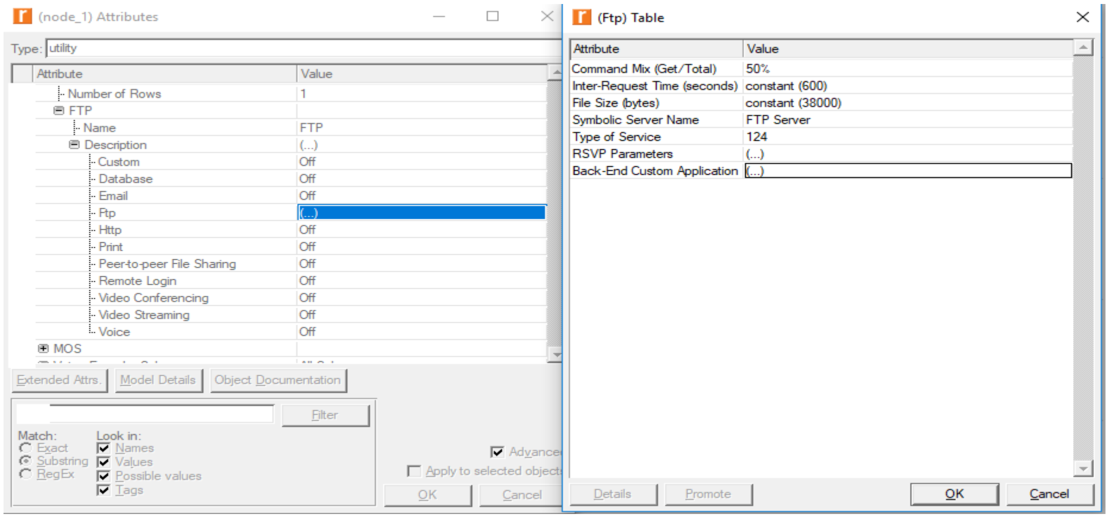
Attribute	Value
Silence Length (seconds)	promoted
Talk Spurt Length (seconds)	promoted
Symbolic Destination Name	Voice Destination
Encoder Scheme	G.729 A
Voice Frames per Packet	5
Type of Service	220
RSVP Parameters	None
Traffic Mix (%)	50 %
Signaling	H.323
Compression Delay (seconds)	0.02
Decompression Delay (seconds)	0.02
Conversation Environment	(...)

The VoIP application uses G.729A encoder scheme and Interactive Voice as the type of service, which has a value of a 220-code point for establishing the VoIP calls. After configuring the VoIP application in Application Definition there is a necessity to define, which workstation will be using this VoIP application. In the case of this thesis, VoIP Client and VoIP Server will run the VoIP application. G.729A codec was chosen in the simulation of voice application because besides its low bandwidth requirements. It has mean of opinion score 3.92, which is very related to G.723. The G.729A has the following character optimized for high performance on digital signal processing architecture, multichannel implementation, multitasking environment, compatible common compressed speech frame stream interface to support systems with multiple speech coders, dynamic speech coders selection if multiple speech codec is available. The detailed configuration of how to set up the voice traffic is explained in Appendix A.

4.6.3 Modeling of FTP Traffic in Riverbed Modeler

FTP is used to generate traffic flow from the FTP server towards the FTP client, thus simulating file downloading based upon the request from the client. The file transfer protocol traffic characteristics are provided in Table 4.6. For modeling FTP, the thesis used exponential distribution for packet arrival, constant packet size and excellent-effort types of services. File transfer was a good choice in this simulation due to the fact that it was able to define how large the file or packet size, which was going to be uploaded or downloaded from the server.

Table 4.6: Riverbed Modeler FTP Traffic Specification



Type: utility

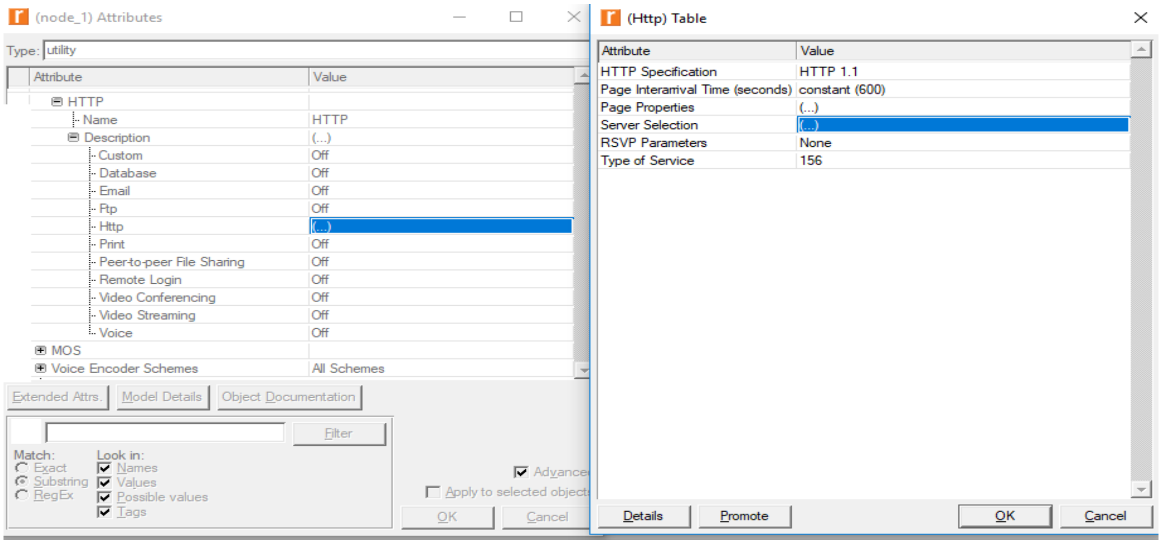
Attribute	Value
Number of Rows	1
FTP	
Name	FTP
Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	(...)
Http	Off
Print	Off
Peer-to-peer File Sharing	Off
Remote Login	Off
Video Conferencing	Off
Video Streaming	Off
Voice	Off
MOS	

Attribute	Value
Command Mix (Get/Total)	50%
Inter-Request Time (seconds)	constant (600)
File Size (bytes)	constant (38000)
Symbolic Server Name	FTP Server
Type of Service	124
RSVP Parameters	(...)
Back-End Custom Application	(...)

4.6.4 Modeling of HTTP Traffic in Riverbed Modeler

Hyperlink text Transfer Protocol is used to simulate the web-browsing case, with the proposed network design. In the Table 4.7 HTTP request and reply, characteristics are mentioned. HTTP Specification HTTP 1.1, Page Interarrival time (seconds) which is constant and type of service with streaming multimedia is used in HTTP modeling.

Table 4.7: Riverbed Modeler HTTP Traffic Specification



(node_1) Attributes

Type: utility

Attribute	Value
HTTP	
Name	HTTP
Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	Off
Http	(...)
Print	Off
Peer-to-peer File Sharing	Off
Remote Login	Off
Video Conferencing	Off
Video Streaming	Off
Voice	Off
MOS	
Voice Encoder Schemes	All Schemes

(Http) Table

Attribute	Value
HTTP Specification	HTTP 1.1
Page Interarrival Time (seconds)	constant (600)
Page Properties	(...)
Server Selection	(...)
RSVP Parameters	None
Type of Service	156

Chapter 5

Simulation Results and Evaluation

In this part of the simulation the VoIP traffic is sent from source (VoIP CLIENT) to destination (VoIP SERVER) in the two networks using G.729A encoding. The main goal is to compare the performance of VoIP traffic in both IP and MPLS networks by using performance metrics throughput. For each scenario, the duration of the simulation is 600 seconds. In the simulation, the traffic starts at 100th second and end after 600 seconds. 100 second is considered because, in the simulation, the start time of traffic application from source to destination is in 100 seconds.

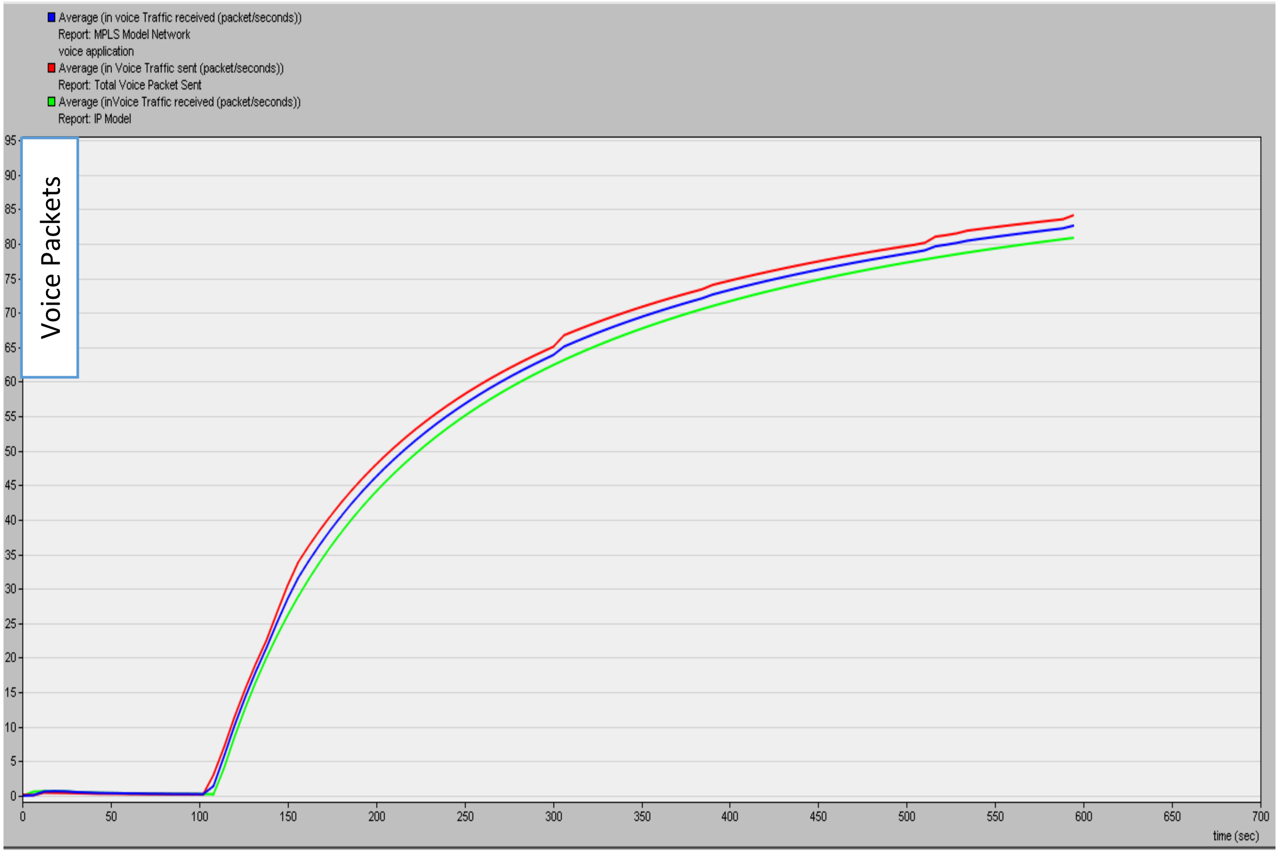


Figure 5.1: Average voice traffic sent and received versus simulation time

Figure 5.1 gives the average number of packet sent and received in both MPLS and IP network. At the end of the simulation, it is observed that the MPLS model which is blue in color, gives more throughput than IP models. The simulation of MPLS and IP models are done considering voice traffic sent. It is observed from Figure 5.1 that voice packet received start to increase from 100 seconds in both models. After 100 seconds MPLS voice traffic received increases more than traditional IP model. The voice traffic received increased in MPLS because MPLS delivers the packet with high transmission speed with low delay. This is due to packet labeled and traffic engineering in the MPLS network, which reduce congestion.

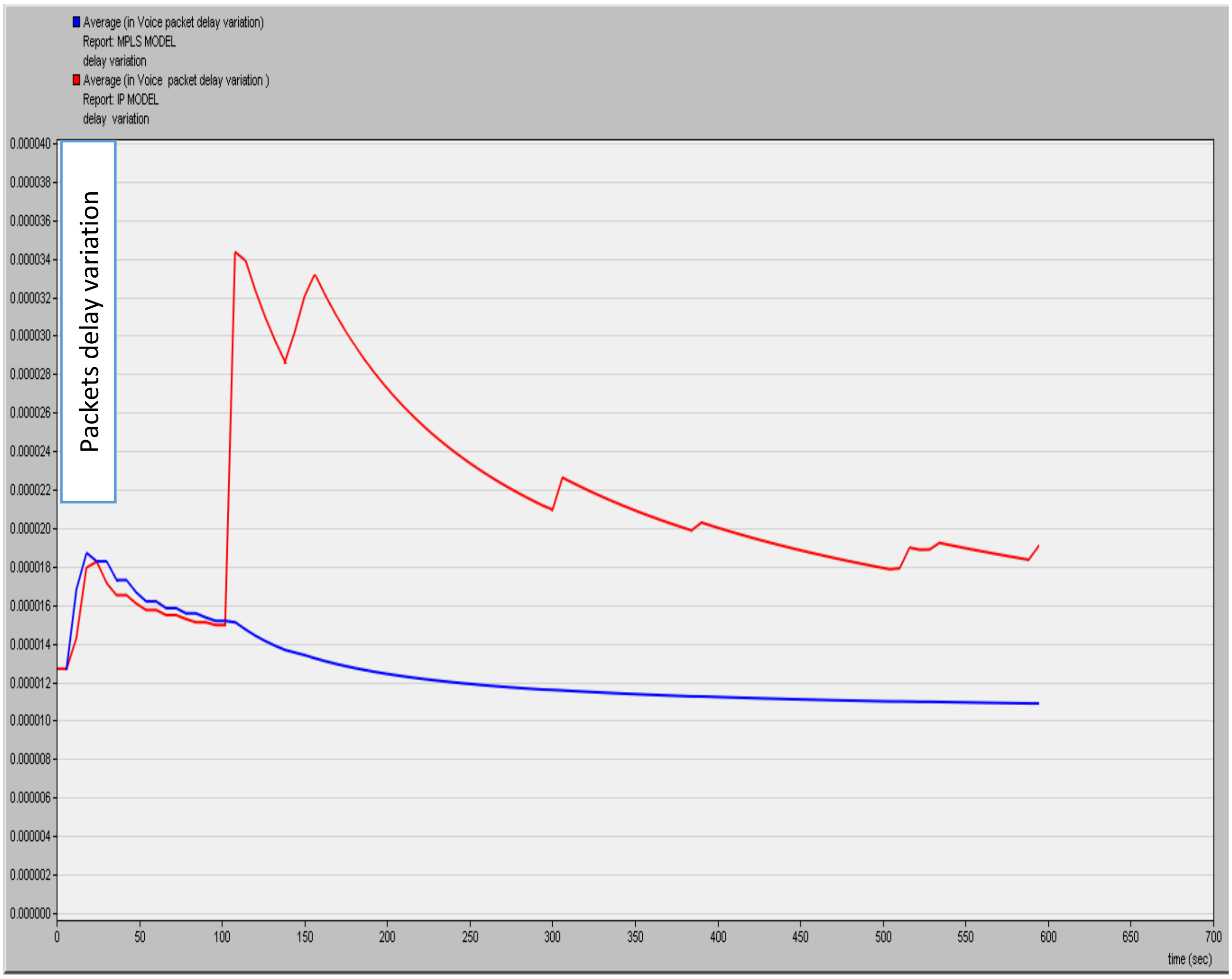


Figure 5.2: voice packet delay variation versus simulation time

The voice packet end-to-end delay of MPLS and IP network model is shown in Figure 5.2. It is noticed from Figure 5.2 that end-to-end delay in IP network exceeds the threshold between 100 sec and 150 sec and the MPLS network reaches the end-to-end delay threshold at between 100 and 150 seconds with low value than IP network. The IP network reaches the threshold earlier than MPLS network, because traffic engineering is implemented in the MPLS network.

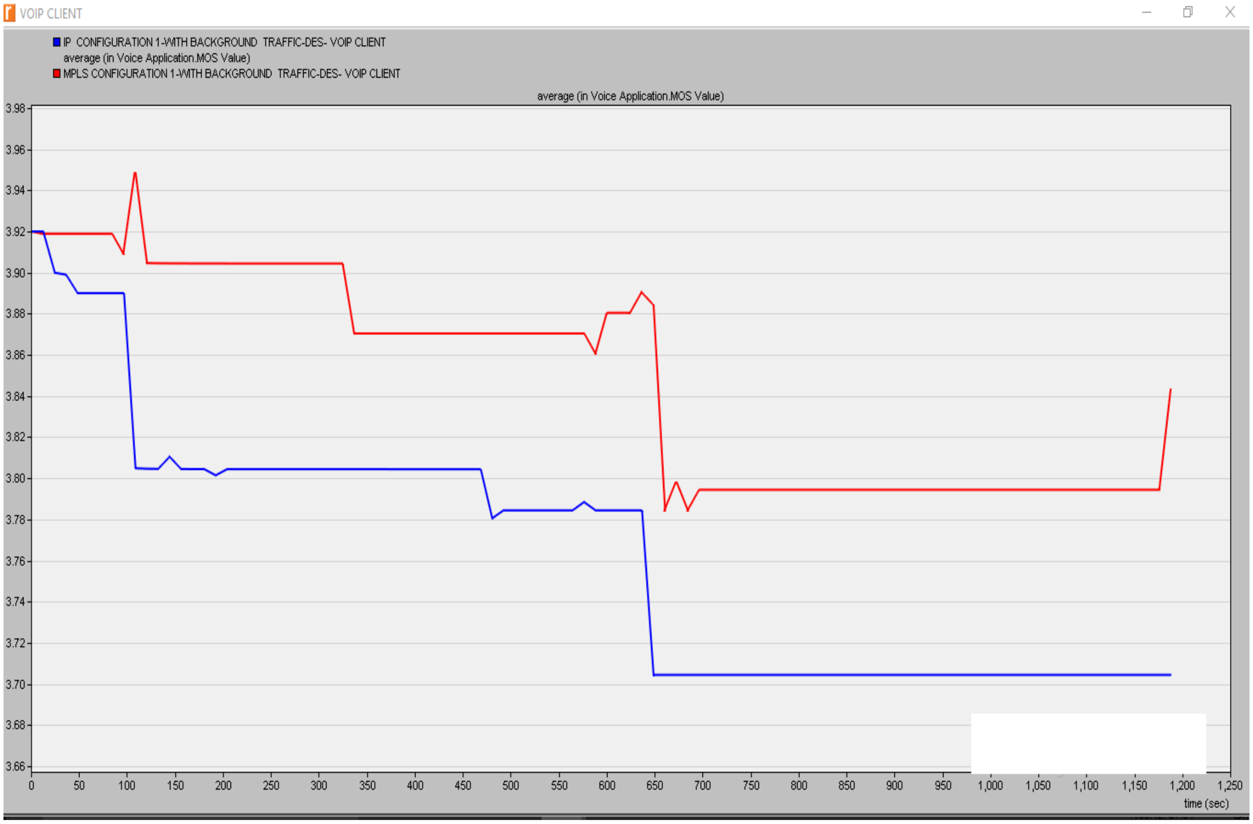


Figure 5.3: Mean Opinion Score value versus simulation time

The MOS (Mean Opinion Score) is the term, which is given to the network based on all the quality of service parameters. This can also be termed as the rating score. The MOS value will be with limits of 1(poor) to 5(excellent). Figure 5.3 shows the MOS value of MPLS and IP. From the graphs, MPLS has the more MOS value, indicating that is more efficient.

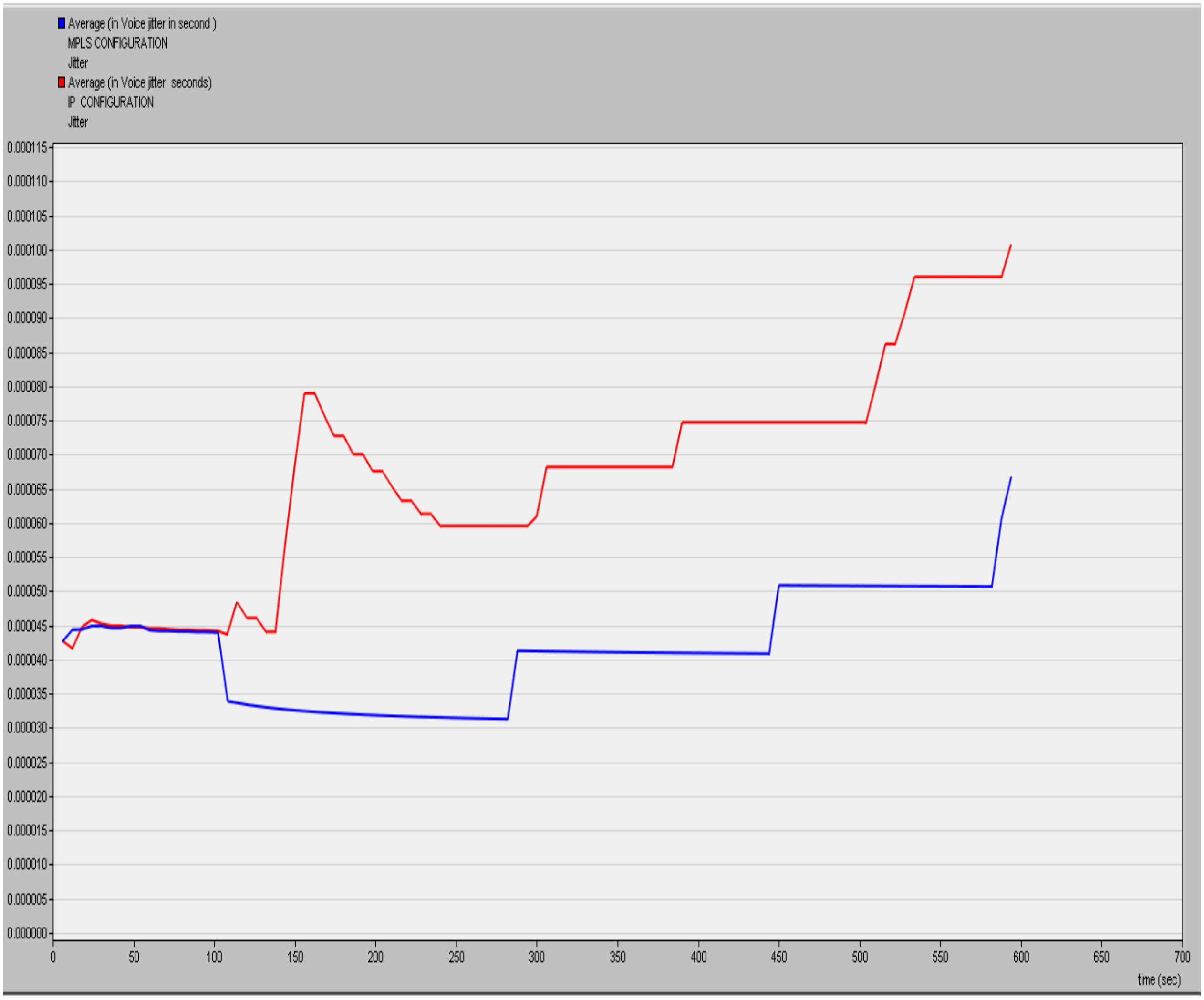


Figure 5.4: Voice Packet Jitter versus simulation time

The graph in Figure 5.4 shows the Voice packet jitter of MPLS and IP network model. It is noticed that Voice Jitter starts to increase after 100 seconds in the IP network and for MPLS network it starts to increase at 300 seconds; this increases the throughput in the MPLS network. The difference is due to the high delay in IP network model.

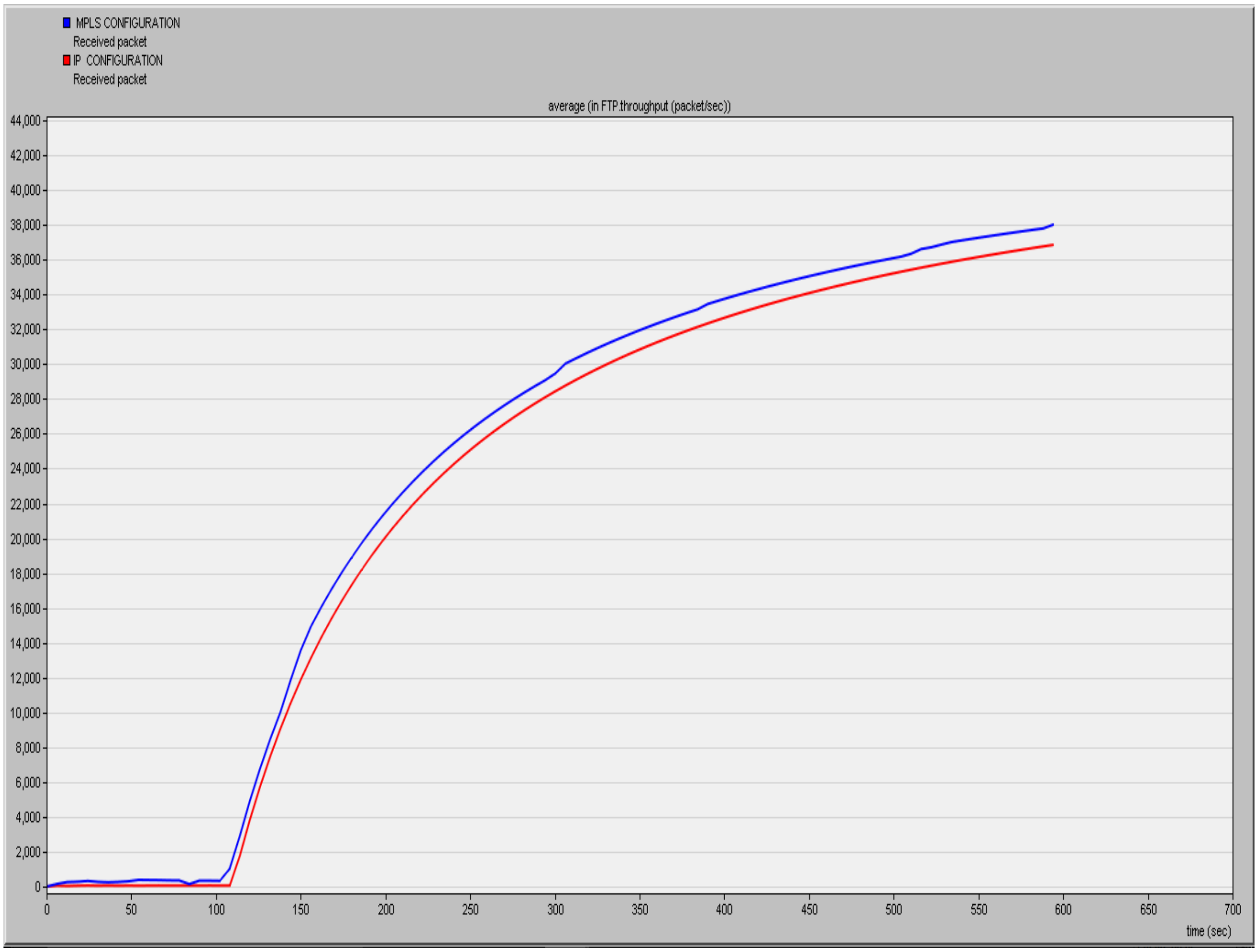


Figure 5.5: FTP packet received versus simulation time

Throughput depends on link speed and nature of the component being used to transmit the data. It is clear that from the Figure 5.5 the packet received increase linearly with time until the channel gets saturated. Afterward, it almost remains constant with high value in cases of MPLS but there is an observable low value in case of IP as compared to MPLS. This is due to both its random path detection nature and heavy packet drop because of congestion. Moreover, IP does produce relatively less packet received. MPLS based network, which is responsible for the reduction of delay factor, which assigns a label path for routing of packet results in the high performance of packet received.

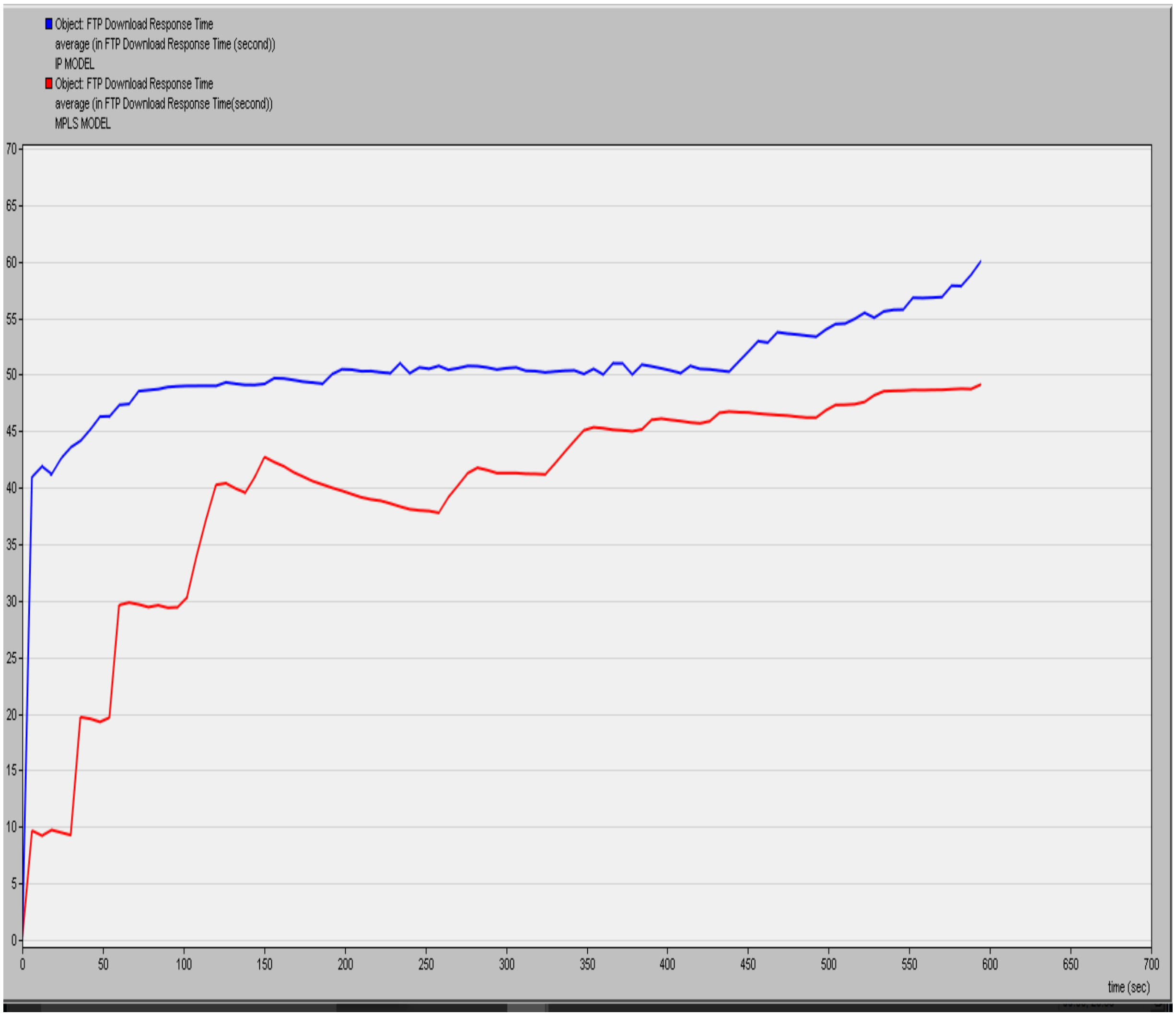


Figure 5.6: FTP downloads response time for MPLS and IP network versus simulation time

MPLS gives best download response to all kinds of traffic. It means that there is little delay required to initiate the conversation and to let the FTP Client start sending its data. As shown in the Figure 5.6 FTP download response time of MPLS is considerably less compared to IP technologies. IP based core shows the worst behavior of FTP download response time because of its random path detection. This directly leads one to the conclusion that MPLS gives better performance for real-time traffic as far as any type of delay is concerned.

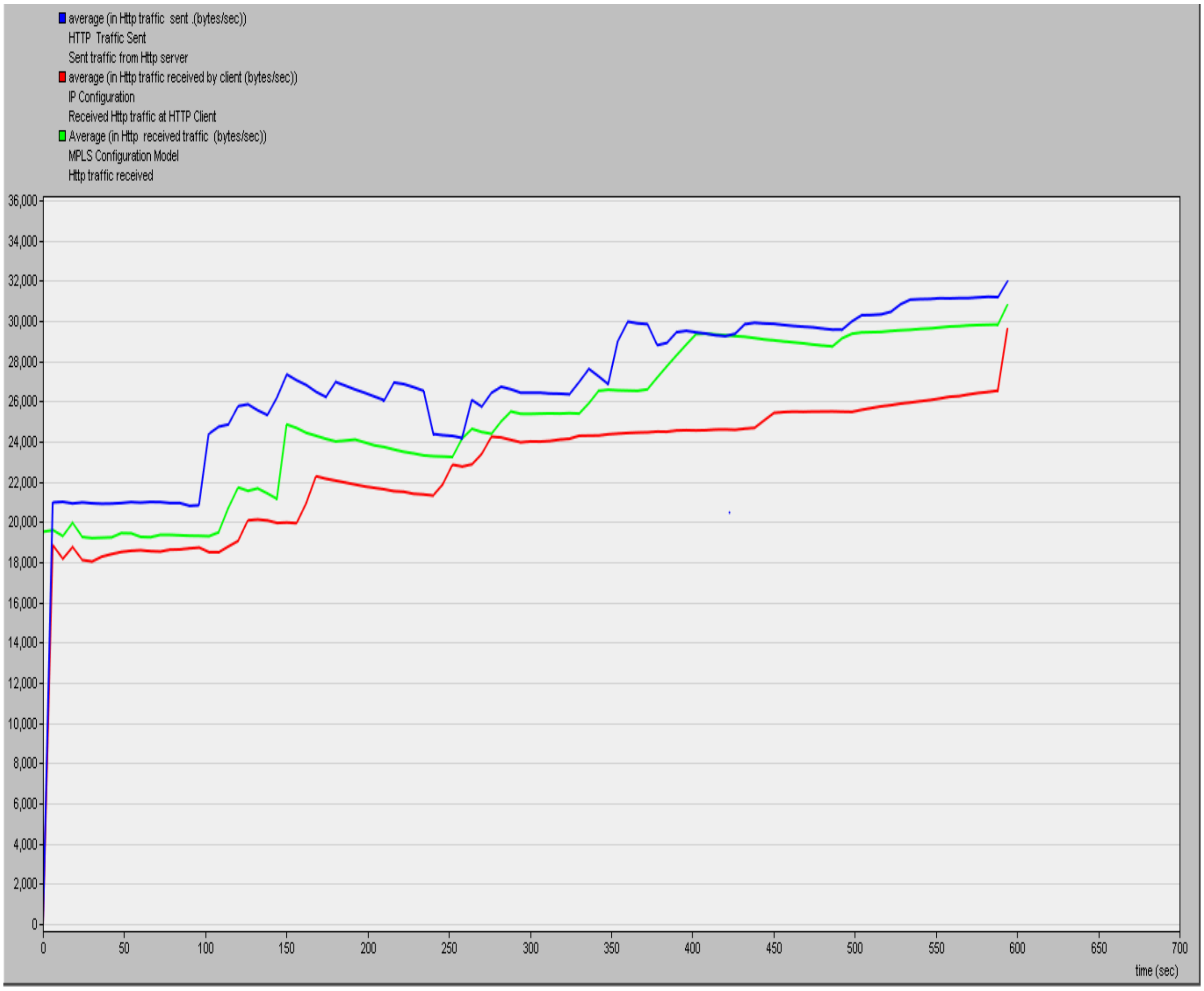


Figure 5.7: average number of transmitted and received HTTP packets versus simulation time

Figure 5.7 shows the average number of transmitted and received HTTP packets versus simulation time when the HTTP client communicates with the HTTP server. Here the MPLS network with label switch path and constraint-routed label distribution protocol is better than IP network only with open short path first protocol.

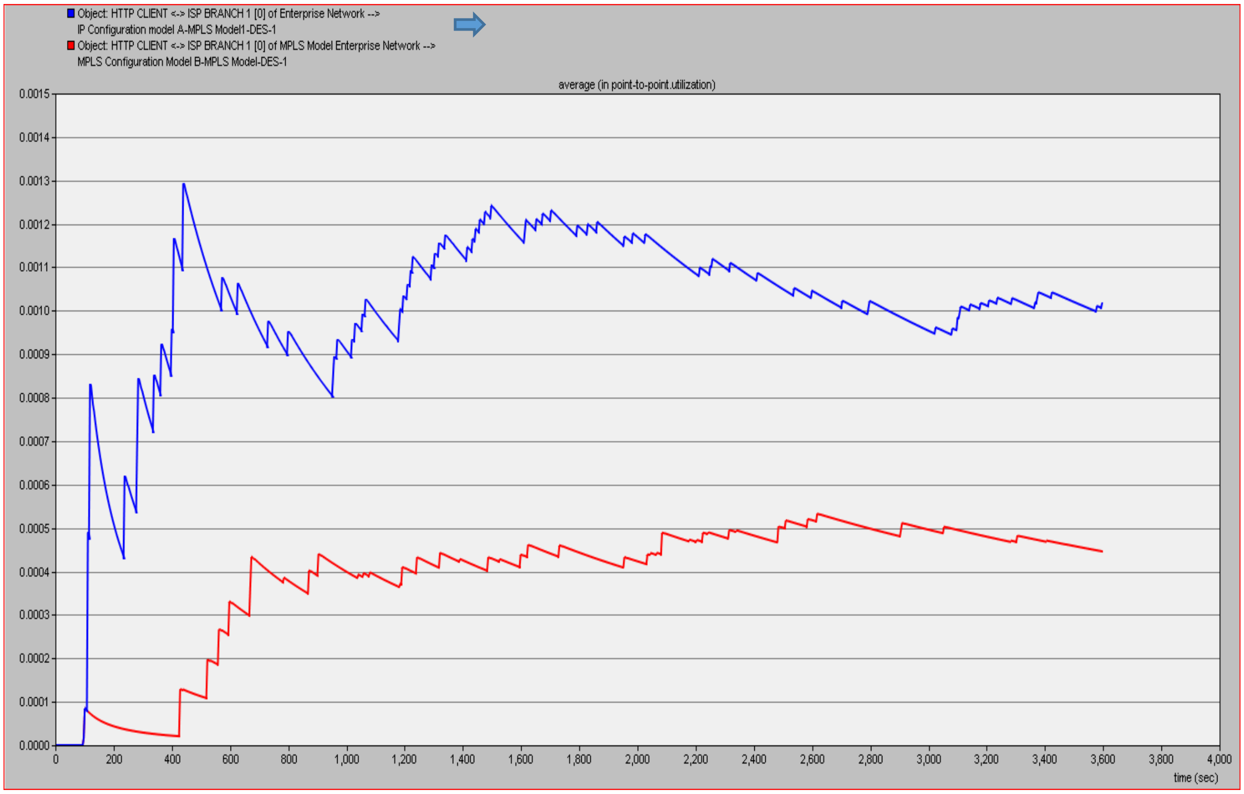


Figure 5.8: Average point-to-point link utilization in seconds from Http Client to ISP Branch 1

Figure 5.8 illustrate the point-to-point link utilization from Http client to ISP Branch 1 with respect to IP and MPLS network configuration. The maximum average point-to-point link utilization in IP is 0.0013 seconds whereas the maximum average point-to-point link utilization in MPLS configuration is 0.0005 seconds. Less link utilization more efficiency in MPLS configuration model. This is due to the added features like Traffic engineering and MPLS mechanism of forwarding packets makes MPLS less link utilization in transferring the VoIP communication, FTP and HTTP.

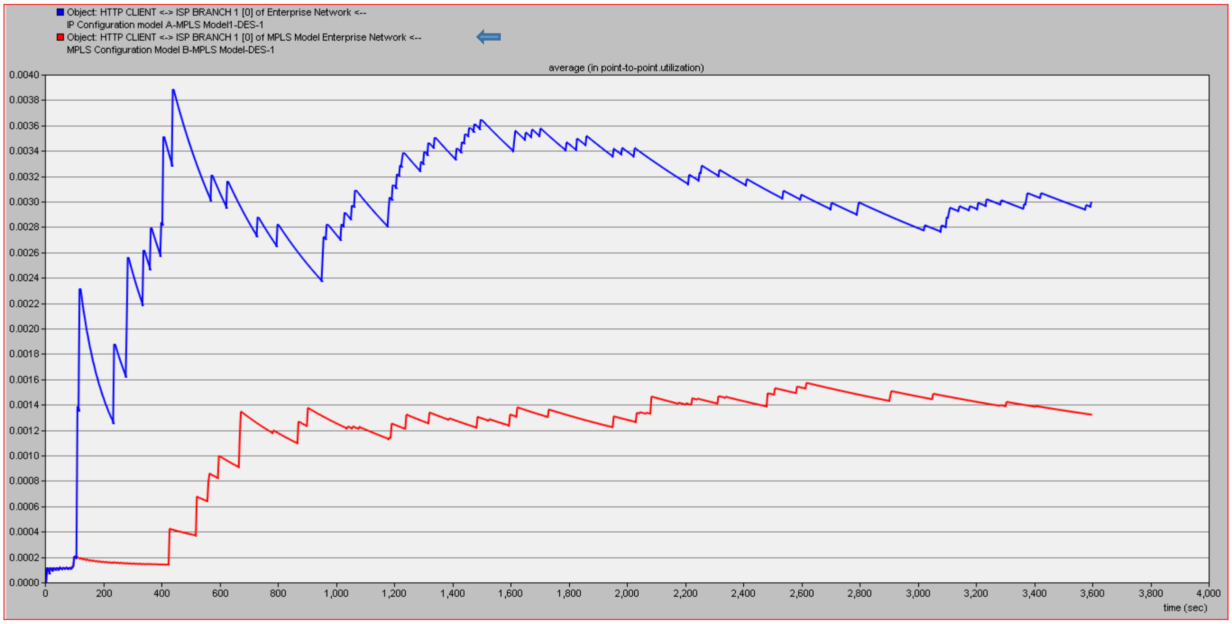


Figure 5.9: Average point-to-point link utilization in seconds from ISP Branch 1 to HTTP Client.

Figure 5.9 illustrates the point-to-point link utilization from ISP Branch 1 to Http Client with respect to IP and MPLS network configuration, which was reverse direction. The maximum average point-to-point link utilization in IP is 0.0040 seconds whereas the maximum average point-to-point link utilization in MPLS configuration is 0.0016 seconds. Less link utilization more efficiency in MPLS configuration model.

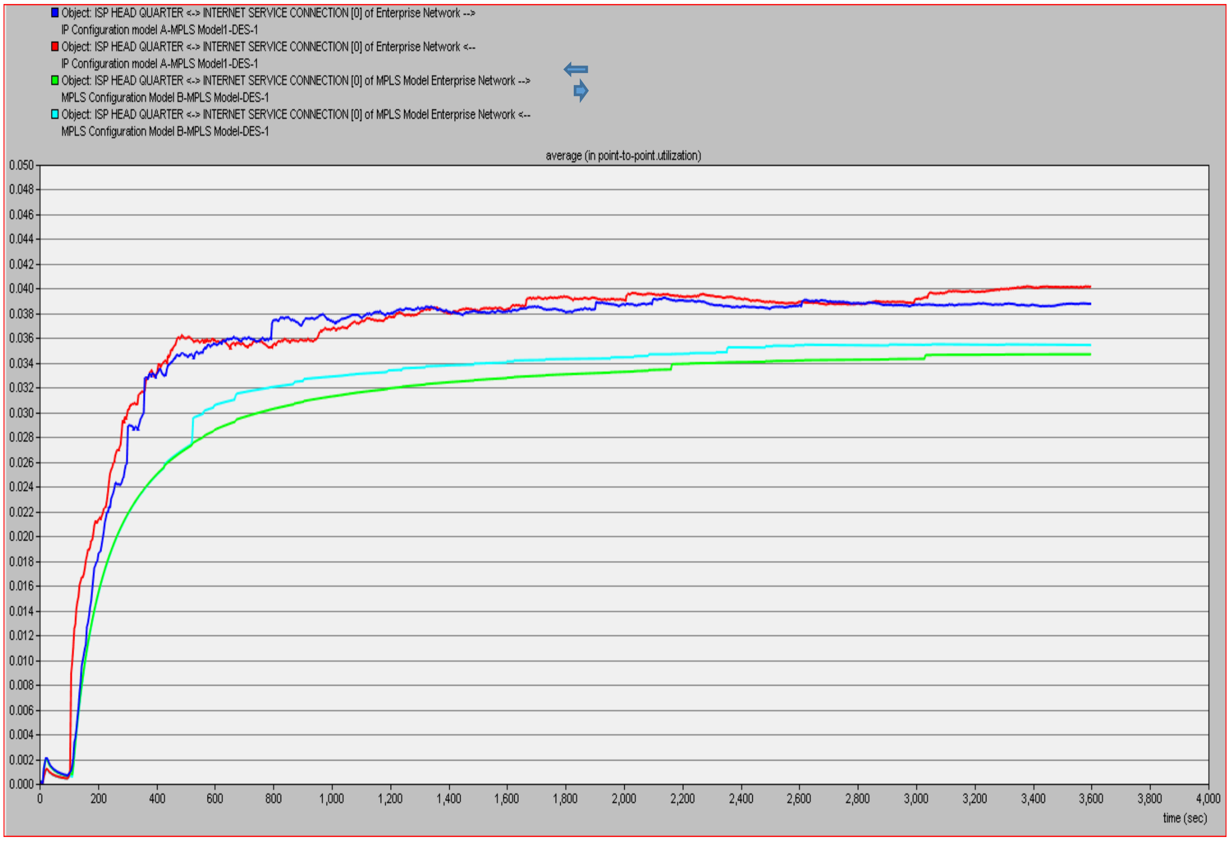


Figure 5.10: Average point-to-point link utilization between ISP Head Quarter and Internet Connection

Figure 5.10 illustrates the point-to-point link utilization from ISP Head quarter to Internet Service Connection with respect to IP and MPLS network configuration. The maximum average point-to-point link utilization in IP is 0.040 seconds whereas the maximum average point-to-point link utilization in MPLS configuration is 0.034 seconds. Less link utilization more efficiency in MPLS configuration model.

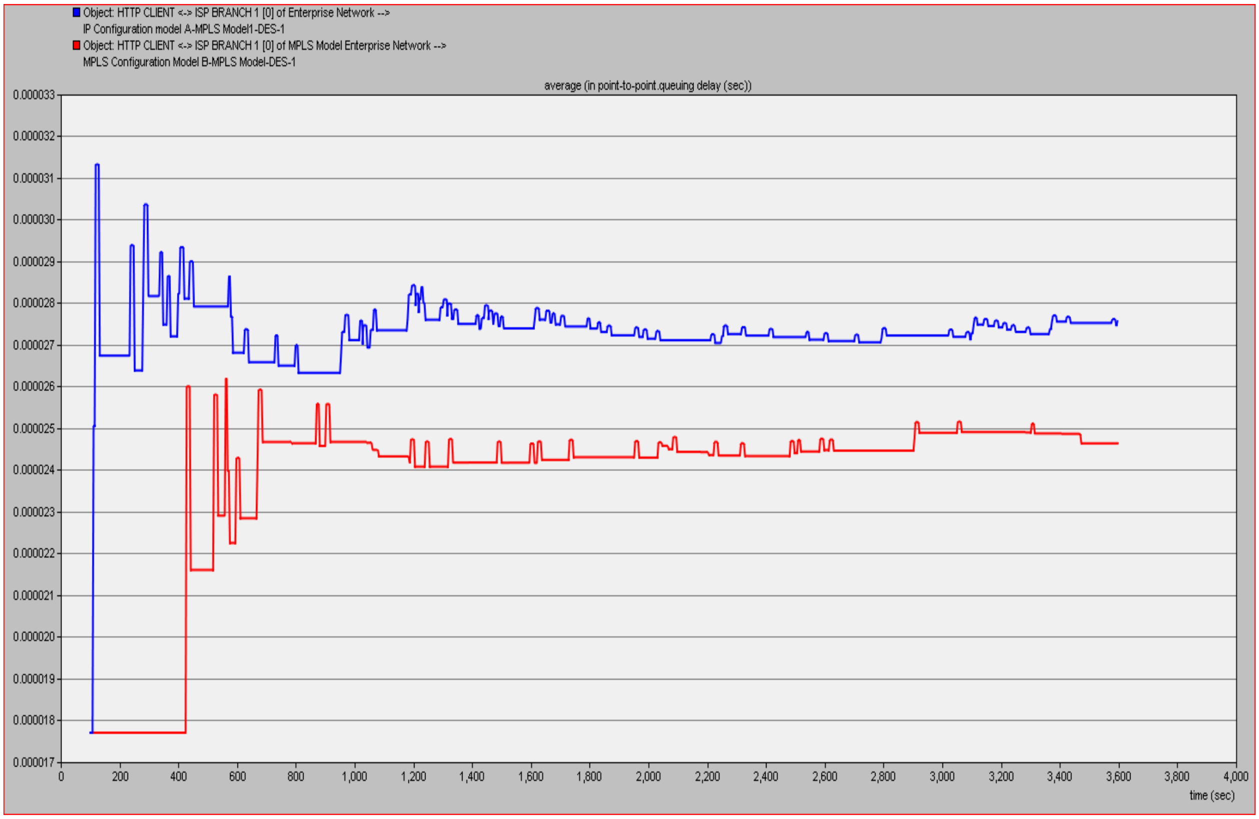


Figure 5.11: Average in Http Client to ISP Branch 1 queuing delay

Figure 5.11 illustrate the queuing delay between Http client and ISP Branch 1 with respect to IP and MPLS network configuration. The maximum average point-to-point queuing delay in IP is 0.000031seconds whereas the maximum average point-to-point queuing delay in MPLS configuration is 0.000026 seconds. Comparing MPLS queuing delay results with the IP result from the shortest path routing scenario network, the queuing delay keep a much less queuing delay in MPLS configuration with value (Maximum 0.000026 seconds and Minimum 0.000018 seconds) between Http Client and ISP Branch 1. It can be observed that the queuing delay MPLS scenario is more balanced between both paths comparing it with IP scenario.

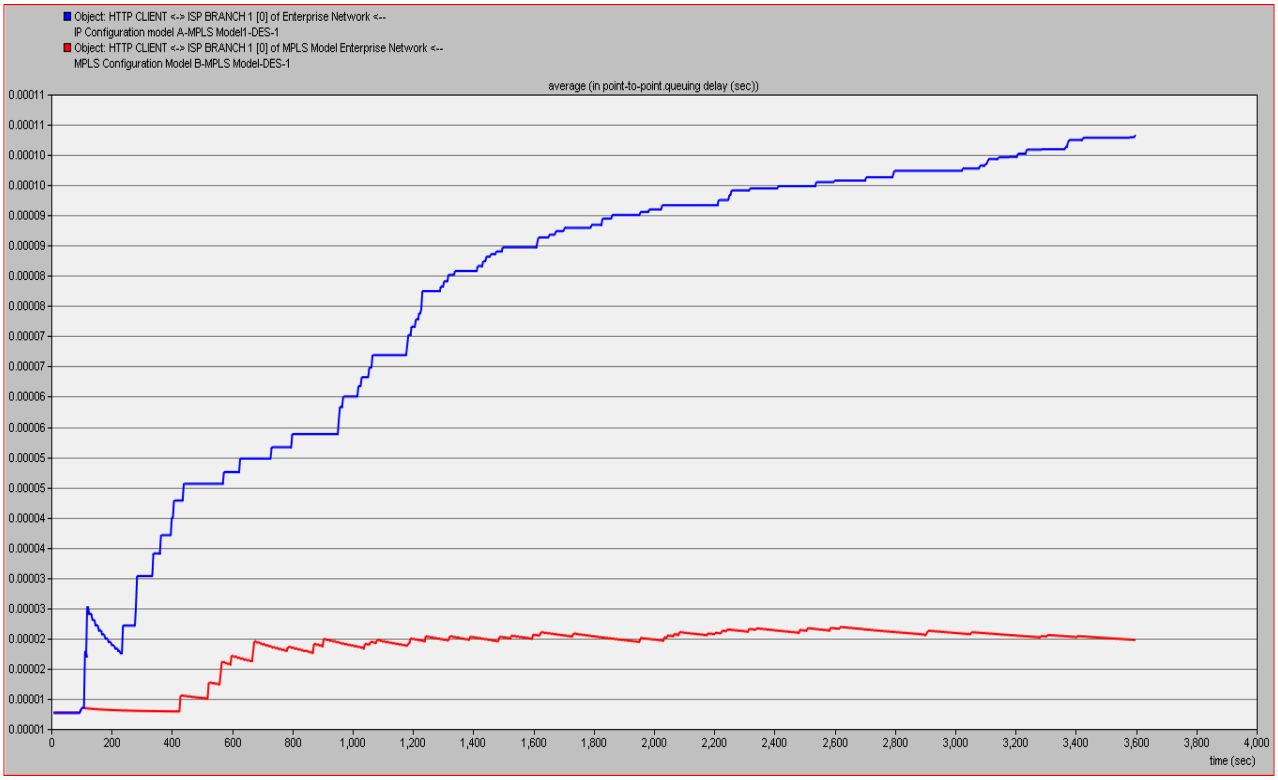


Figure 5.12: Average in ISP Branch 1 to Http Client queuing delay

Figure 5.12 illustrates the queuing delay between Http client and ISP Branch 1 with respect to IP and MPLS network configuration. The maximum average point-to-point queuing delay in IP is 0.00011 seconds whereas the maximum average point-to-point queuing delay in MPLS configuration is 0.00002 seconds. Comparing MPLS queuing delay results with the IP result from the shortest path routing scenario network, the queuing delay keep a much less queuing delay in MPLS configuration with value (Maximum 0.00002 seconds and Minimum 0.00001 seconds) between Http Client and ISP Branch 1. It can be observed that the queuing delay MPLS scenario is more balanced between both paths comparing it with IP scenario.

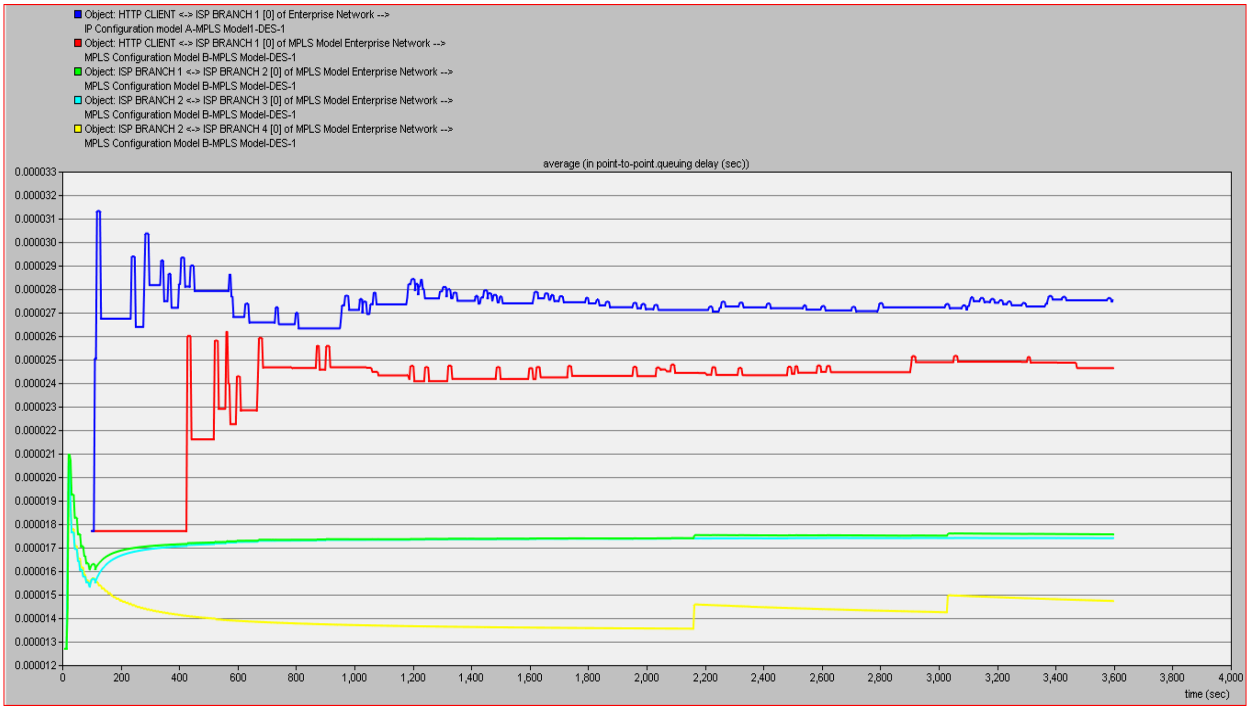


Figure 5.13: Average in ISP Branch 1 to Http Client and ISP Branch 2 to ISP Branch 4 and ISP Branch 3 queuing delay

Figure 5.13 shows the average point-to-point delay for MPLS network model in ISP Branch 1 to Http Client, ISP Branch 2 to ISP Branch 4 and ISP Branch 3 is less than that of IP network model. This is due to the added features like Traffic engineering and MPLS mechanisms of forwarding packets make MPLS a better choice in transferring the VoIP communication and file transfer in ISP Branch routers.

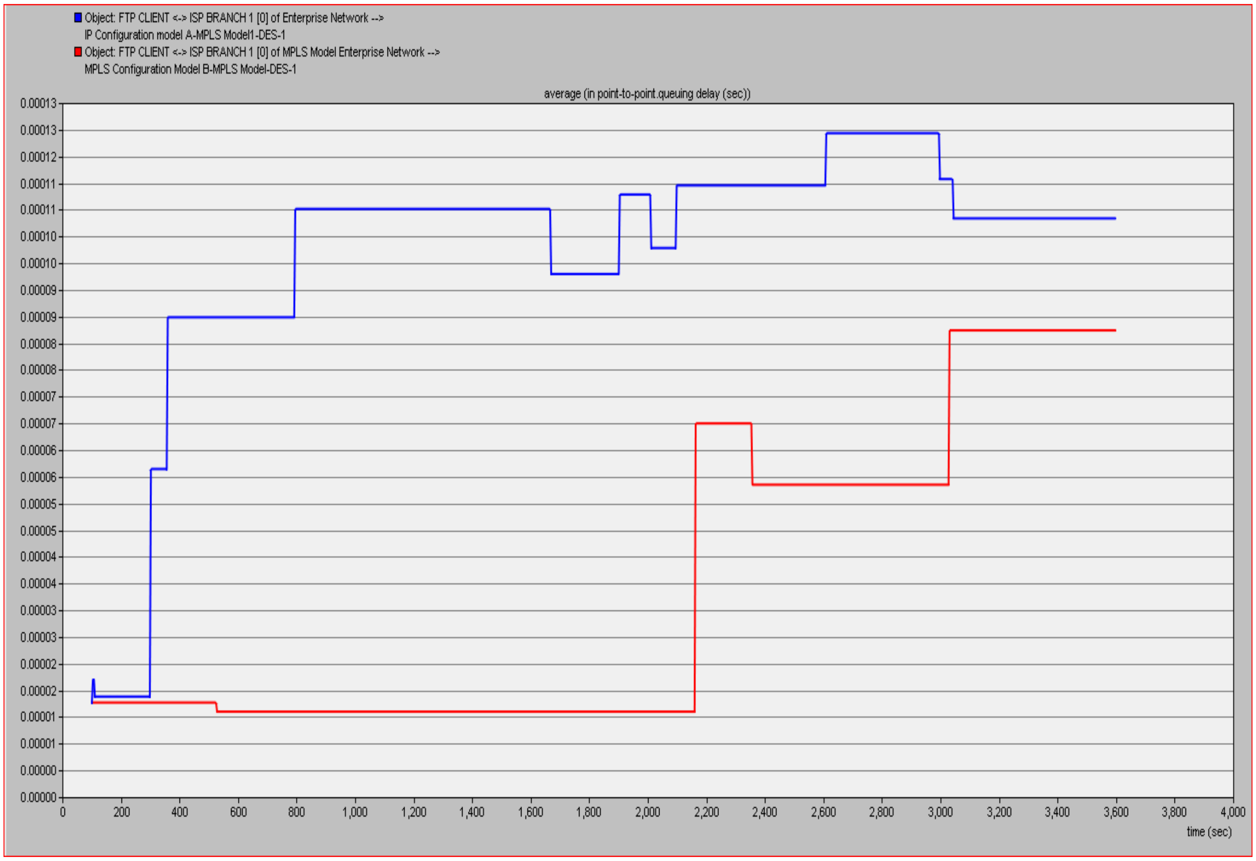


Figure 5.14 : Average in Ftp Client to ISP Branch 1 queuing delay

Figure 5.14 illustrate the queuing delay between Ftp client and ISP Branch 1 with respect to IP and MPLS network configuration. The maximum average point-to-point queuing delay in IP is 0.0013seconds whereas the maximum average point-to-point queuing delay in MPLS configuration is 0.0009 seconds. Comparing MPLS queuing delay results with the IP result from the shortest path routing scenario network, the queuing delay keep a much less queuing delay in MPLS configuration with value (Maximum 0.0009 seconds and Minimum 0.0001 seconds) between Ftp Client and ISP Branch 1. It can be observed that the queuing delay MPLS scenario is more balanced between both paths comparing it with IP scenario.

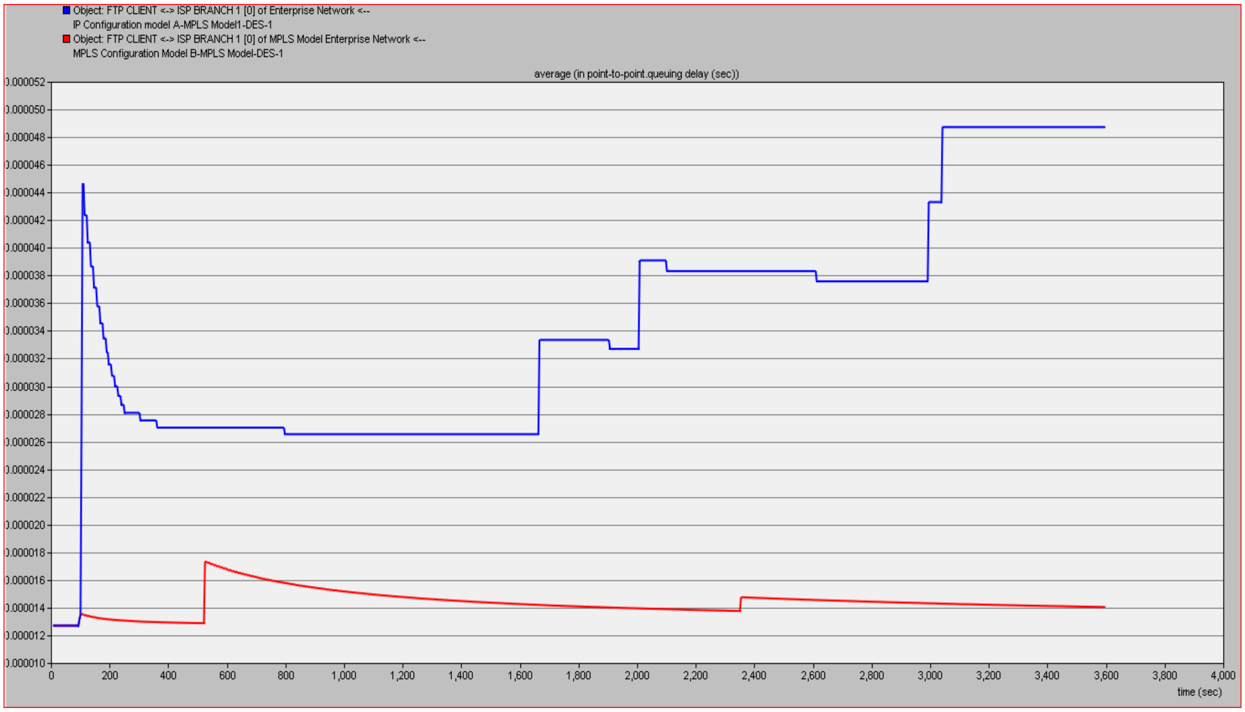


Figure 5.15: Average in ISP Branch 1 to Ftp Client queuing delay

Figure 5.15 illustrate the queuing delay between ISP Branch 1 and Ftp Client with respect to IP and MPLS network configuration. The maximum average point-to-point queuing delay in IP is 0.000050 seconds whereas the maximum average point-to-point queuing delay in MPLS configuration is 0.000018 seconds. Comparing MPLS queuing delay results with the IP result from the shortest path routing scenario network, the queuing delay keep a much less queuing delay in MPLS configuration with value (Maximum 0.000018 seconds and Minimum 0.000012 seconds) between Ftp Client and ISP Branch 1. It can be observed that the queuing delay MPLS scenario is more balanced between both paths comparing it with IP scenario. Generally, the results shown in the Figure 5.12, Figure 5.13, Figure 5.14, Figure 5.15 and Figure 5.16 are the average point-to-point queuing delay obtained for MPLS and IP networks. From the graphs, it is observed that there is a decrease in the average point-to-point delay when voice, file and hypertext are transmitted using MPLS technology. This is due to the added features like TE and MPLS mechanism of forwarding packets make MPLS a better choice in transferring the VoIP communication and file transfer for proposed network model.

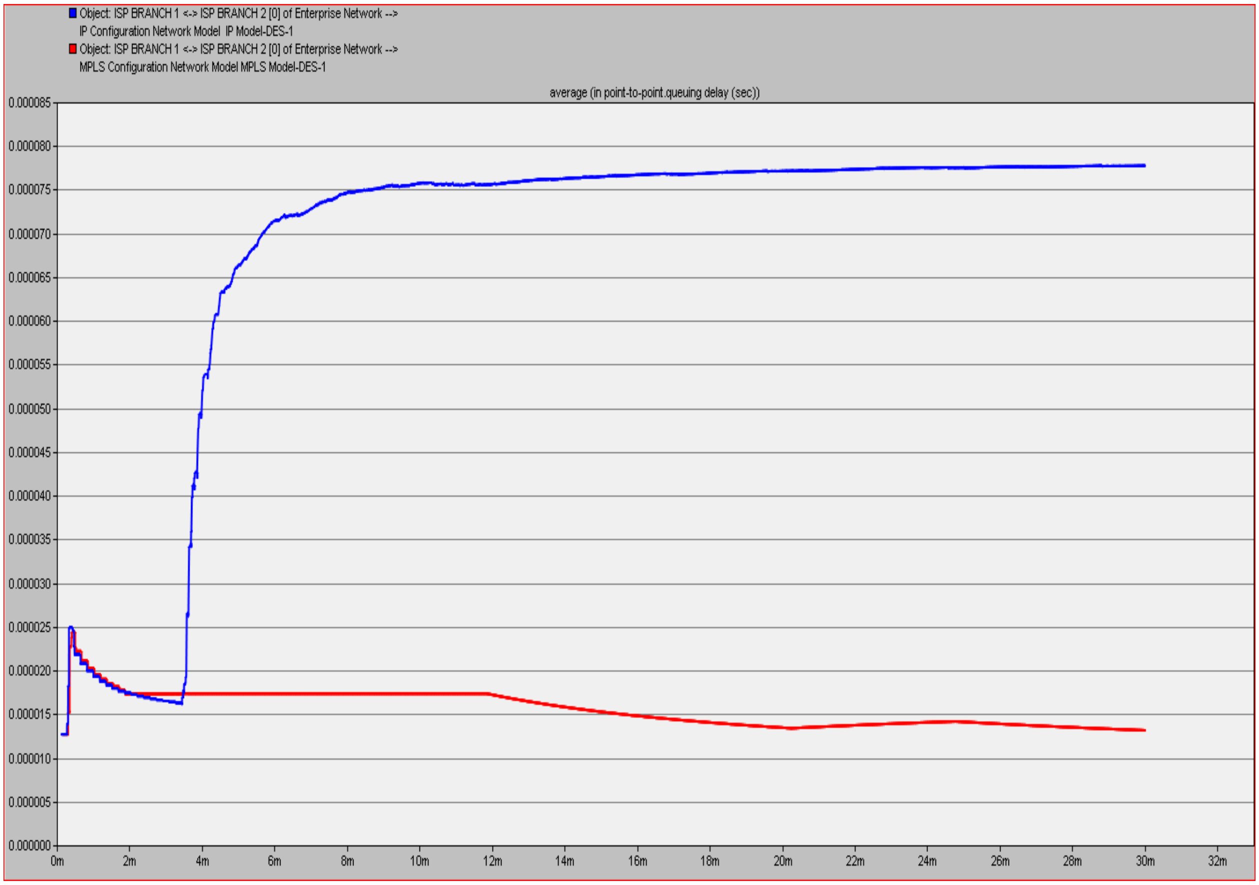


Figure 5.16: Average in ISP Branch 1 to ISP Branch 2 queuing delay

Figure 5.16 illustrate the queuing delay between ISP Branch1 and ISP Branch 2 with respect to IP and MPLS network configuration. The maximum average point-to-point queuing delay in IP is 0.00008 seconds whereas the maximum average point-to-point queuing delay in MPLS configuration is 0.000025 seconds.

Chapter 6

Conclusions and Recommendation for Future Work

6.1 Conclusions:

The main objective of the thesis is to compare the performance of internet protocol network with multi-protocol label switch network with respect to different applications like that of voice, file transfer protocol and hypertext transfer protocol. The performance analysis is followed by presenting an approach in Riverbed modeler to estimate the quality of file transfer protocol, voice over internet protocol and hypertext transfer protocol that can be maintained in MPLS and IP networks. The performance analysis in both networks is made on focusing on the performance metrics such as voice packet sent and received, voice jitter, mean opinion score, voice packet delay variation, ftp packet sent and received, ftp download response time, and HTTP packet sent and received. Based on the simulation results it can be concluded that MPLS provides the best solution in implementing file transfer, voice over internet protocol and hypertext transfer protocol compare to IP network model. The reason is that the routers in MPLS are capable of taking less processing time in forwarding the packets. This makes it more suitable for the application like voice, ftp, and HTTP, which has less tolerance for network delays. Another reason is implementing MPLS with traffic engineering minimizes the congestion in the network. Traffic engineering in MPLS is implemented by using signaling protocols such as CR-LDP and LSP. When considering similar network topology and designing parameters for the MPLS and IP network, the problem is to identify which technology provides more number of VoIP class and file transfer in the network. To solve this problem an approach made in riverbed modeler to know maximum number of voice and file that can be maintained in MPLS and IP networks. During the study of this thesis, network MPLS with IP QoS influences delay in the VoIP, FTP and HTTP. This is due to the added features like TE and MPLS mechanism of forwarding packets make MPLS a better choice in transferring the VoIP communication, HTTP and file transfer.

6.2 Recommendation for Future work

This thesis work mainly focuses on the performance comparison of FTP, HTTP and VOIP traffic between IP and MPLS network including traffic engineering. The Future work of the thesis can be carried to study the performance of MPLS traffic engineering signaling protocols CR-LDP, EIGRP and RSVP when VoIP application is implemented in them. It would be interesting if one considers different codecs while establishing a VoIP application. The work can be further extended to study the performance of video and database applications on CR-LDP, EIGRP and RSVP signaling protocol. Future study will be QoS enabled VoIP or Video over MPLS with IGRP and QoS enabled VoIP or Video over MPLS with EIGRP. IPv6 consists of many features and it can be used with MPLS to improve packet transmission and increase the flexibility of payload. Based on the result of this thesis work, it is strongly recommended that network designers have to consider traffic in both MPLS and IP for all their routes in a different direction in the area of network expansion from time to time.

Reference

[1] B. Miller, “Satellites Free for the Mobile Phone,” IEEE Spectrum, pp. 26-35, March 1998.

[2] P. Chitre and F Yegenoglu, “Next-Generation Satellite Networks: Architecture and Implementations,” IEEE Communications Magazine, pp. 30-36, March 1999.

[3] M. Koyuncu, “Comparison of Scheduling Algorithms for Multimedia Applications in IPv4 and IPv6,” Thesis for the degree of Master of Science in Information Systems Engineering, Atilim University Ankara, Turkey, March 2015.

[4] D. P. Connors, B. Ryu, and S. Dao, “Modeling and Simulation of Broadband Satellite Networks Part I: Medium Access Control for QoS Provisioning,” IEEE Communications Magazine, pp. 72-79. March 1999.

[5] K. Jannu and R. Deekonda, “OPNET simulation of voice over MPLS,” Master thesis in Electrical Engineering, Thesis no: MSE-2010-5311, Blekinge Institute of Technology, Sweden, June 2010.

[6] O. Akinsipe et al. “Comparison of IP, MPLS and MPLS RSVP-TE Networks using OPNET”, International Journal of Computer Applications (0975 – 8887), Volume 58, No.2, November 2012.

[7] Y. Ravikumar, “A Case Study on MANET Routing Protocols Performance over TCP and HTTP,” Thesis for the degree of Master of Science in Electrical Engineering, Blekinge Institute of Technology, no. June 2010.

[8] S. Ahmad and W. A. Hamdani, “Performance Evaluation of IPv4 and IPv6 over MPLS using OPNET,” *Mohsin Hassan Magray Comput. Sci. Eng. Dep. Univ. Kashmir, Srinagar (J&K), India 190006 Abstr.*, vol. 125, no. 3, pp. 34–38, 2015.

[9] M. H. Baig, “Performance Evaluation of MANET Using MPLS,” thesis for the degree of Master of Science in Electrical Engineering, Blekinge Institute of Technology, November 2010.

[10] Maria Elena Villapol and Jonathan Billington, "Resource Reservation Protocol for Mobile Satellite Communication," Cooperative Research Centre for Satellite Systems, Institute for Telecommunications Research, University of South Australia, pp. 18– 124, October 2002.

[11] Raj Jain and Wei Sun "Quality of service over MPLS when using traffic engineering," Department of Computer and Information Science, Ohio State University, Columbus, OH 43210-1277.

[12] M. I. Abouseda, K. A. Bozed, and A. R. Zerek, "Simulation of Video Conferencing over IP Network with QoS Using Riverbed Modeler," Proceedings of Engineering & Technology (PET), Libyan academy School of Engineering, Electrical and Computer Eng. Department, Tripoli -Libya, pp. 238-246, 2016

[13] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture," IETF RFC 3031, January 2001.

[14] N. Absar, A. Wahab, and K. U. Sikder, "Performance Measurement of Open Shortest Path First (OSPF) Protocol in IP Networks," IEEE Communications Magazine, vol. 6890, no. 6, pp. 110–115, 2017.

[15] T. Svensson and A. Popescu, "OPNET Modeler Development of laboratory exercises based on OPNET Modeler," OPNET Modeler Development of laboratory , no. June 2003.

[16] Xipeng Xiao, Alan Hannan, and Brook Bailey, Global Center Inc. Lionel M, NI, Michigan State University. "Traffic Engineering with MPLS in the Internet," pp.10-12 September 2008

[17] Nader F.Mir., Albert Chien, "Simulation of Voice over MPLS communications Networks," IEEE ICSS- 02, conference.

[18] "R. Ioan, "An Empirical Analysis of Internet Protocol version 6 (IPv6), MSc Thesis", Wayne State University, Detroit, Michigan, 2002."

[19] D. Garc and A. Group, "Présentation on OMNET ++ Introduction to simulation with OMNET ++."

[20] Karol Molnar and Martin Vlcek," Evaluation of Bandwidth Constraint Models for

MPLS Networks, " Annual Journal of Electronics, 2009, ISSN 1313-1842.

[21] M. Atif Qureshi et al, “Comparative study of VoIP over WiMAX and Wi-Fi, ”International Journal of Computer Science Issues (IJCSI), vol. 8, no. 3, pp. 433–437, May 2011.

[22] Anupkumar. M. Bongale and Nithin. N, “Analysis of Link Utilization in MPLS Enabled Network using OPNET IT Guru”, International Journal of Computer Applications (0975 – 8887), Volume 41– No.14, March 2012.

[23] B. Boudani, B. Cousin, C. Jawhar, and M. Doughan, “Multicast routing simulator over MPLS networks”, Proceedings of the 36th Annual Simulation Symposium (ANSS’03), Orlando, Florida, March 2003, pp. 327–334.

[24] J. Aggarwal and A. Dhall, “Simulation-Based Comparative Analysis of Voice over Internet Protocol over MPLS and Traditional IP Network,” *IJSETR,* vol. 4, no. 6, pp. 2283–2287, 2015.

[25] D. Sharma and R. Singla, “Performance Measure of MPLS and traditional IP network through VoIP traffic,” *IJSETR*, vol. 4, no. 6, pp. 2118–2122, 2015.

[26] P. Eugen, “An MPLS Simulation for Use in Design Networking for Multi-Site Businesses,” vol. XVII, no. 1, pp. 373–378, 2017.

[27] Ahmed Sameh, Sherif Wagih, Qusay Salama, “Dealing with Quality of Service in Hybrid Wired-Wireless Networks”, Proc of Second International Conference on Network Applications, Protocols and Services, Kedah, pp. 105-109, 2010

[28] A.-B. R. Sulaiman and O. K. Salih Alhafidh, “Performance Analysis of Multimedia Traffic over MPLS Communication Networks with Traffic Engineering,” *Int. J. Comput. Networks Commun. Secur. Multiprotocol Label Switch. (MPLS), Traffic Eng.*, vol. 2, no. 3, pp. 93–101, 2014.

[29] M. H. Miraz, M. A. Ganie, S. A. Molvi, M. Ali, and A. H. Hussein, “Simulation and Analysis of Quality of Service (QoS) Parameters of Voice over IP (VoIP) Traffic

through Heterogeneous Networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 7, pp. 242–248, 2017.

[30] D. O. Awduche and B. Jabbari, "Internet traffic engineering using multi-protocol label switching (MPLS)," vol. 40, pp. 111–129, 2002.

[31] B. Rong, J. Lebeau, M. Bennani, A. K. Elhakeem, and M. Kadoch, "OPNET Simulation of SIP-Based IP Telephony over MPLS Network."

[32] Daniel O. Aweduche, "MPLS and Traffic Engineering in IP Networks," IEEE Communication Magazine December 1999, UUNET (MCI WorldCom).

[33] C. Science and S. Engineering, "Performance Analysis of Voice over Multiprotocol Label Switching Communication Networks with Traffic Engineering," vol. 2, no. 7, pp. 195–199, 2012.

[34] Aruna Kapoor, Sunila Godara, Sanjeev Khambra, "Comparative Analysis of Signaling Protocols in Mpls-Traffic Engineering," Amandeep Deptt. of CSE, GJUS&T, Hisar, India,2011.

[35] Ian F. Akyildiz, Seong-Ho Jeong, "Satellite ATM Networks," A Survey," IEEE Communications Magazine, Vol 5.35. No. 7, July 1997.

[36] L.D. Dhomeja, S.Abbasi1, A. A. Shaikh1 and Y.A. Malkani, "Performance Analysis Of WLAN Standards for Video Conferencing Applications," International Journal of Wireless & Mobile Networks (IJWMN), pp. 59-69,(2011).

[37] M. M. Al-quzwini and S. K. Ibrahim, "Performance Evaluation of Traffic Engineering Signal Protocols in IPV6 MPLS Networks," vol. 2012, no. November, pp. 298–305, 2012.

Appendix

Appendix A: procedure for modeling the OSPF experiment in IP network model

I. Creating network

1. Add the following objects from the object palette to the thesis workspace: Application Config, Profile Config, QoS attributes, MPLS config, three ethernet client, three servers, five cisco 7200 routers model, one satellite router, and two dish routers.
2. Connect the cisco7200 routers together with digital subscriber number three (DS3) links from the link model palette as per the diagram.
3. Connect the workstations to the ISP router one and the server to Internet Service Connection with DS3 links.
4. Select the following application from the menu protocols/IP/Routing/select routing protocols, the open short path first was selected and applied to all subinterfaces and all interfaces including a look back, virtual local area networks.

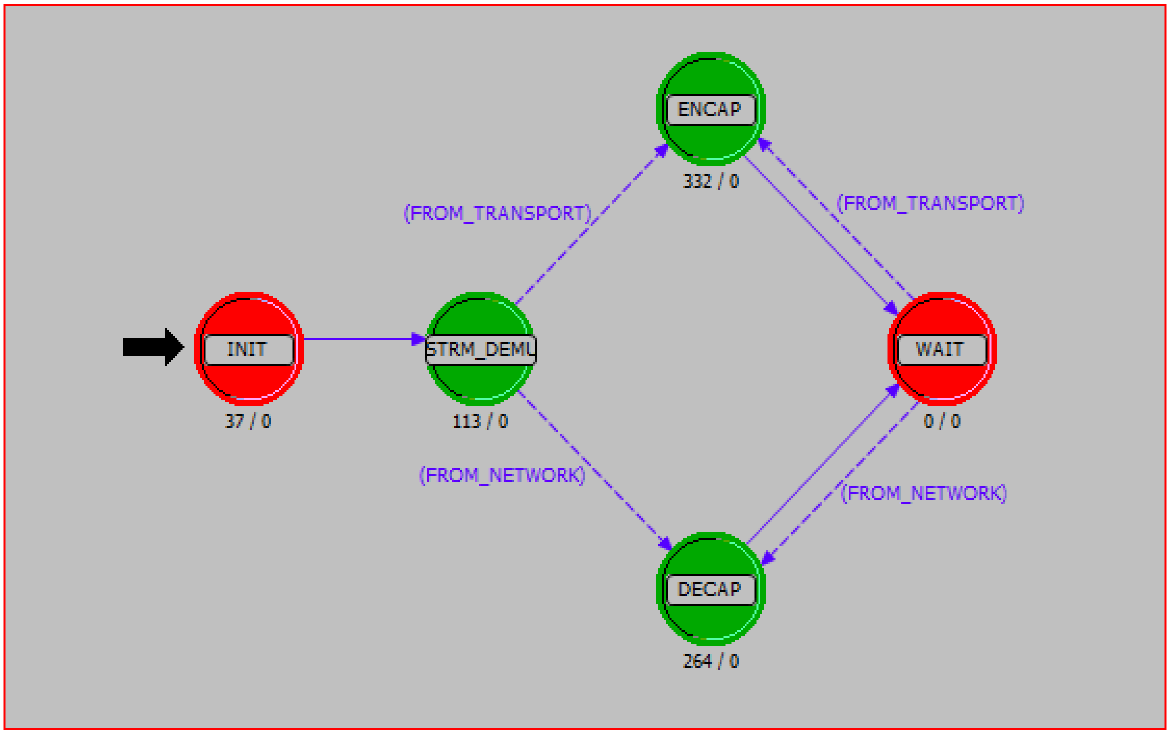


Figure A.0.1: IP process model on each router

5. Select all routers then protocols/OSPF/configure area, insert area 0 in the box then click ok.
6. Select all WAN links from ISP router 1 to ISP headquarter router then select OSPF/ to configure interface costs explicitly for all selected links to 100.

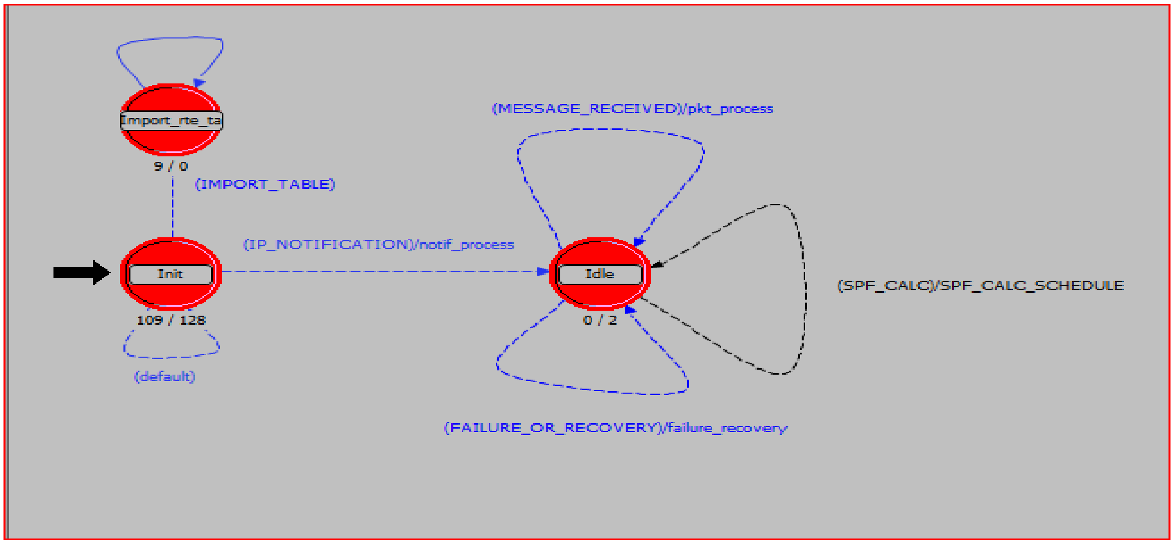


Figure A.0.2 Process model of open short path first configuration on each router

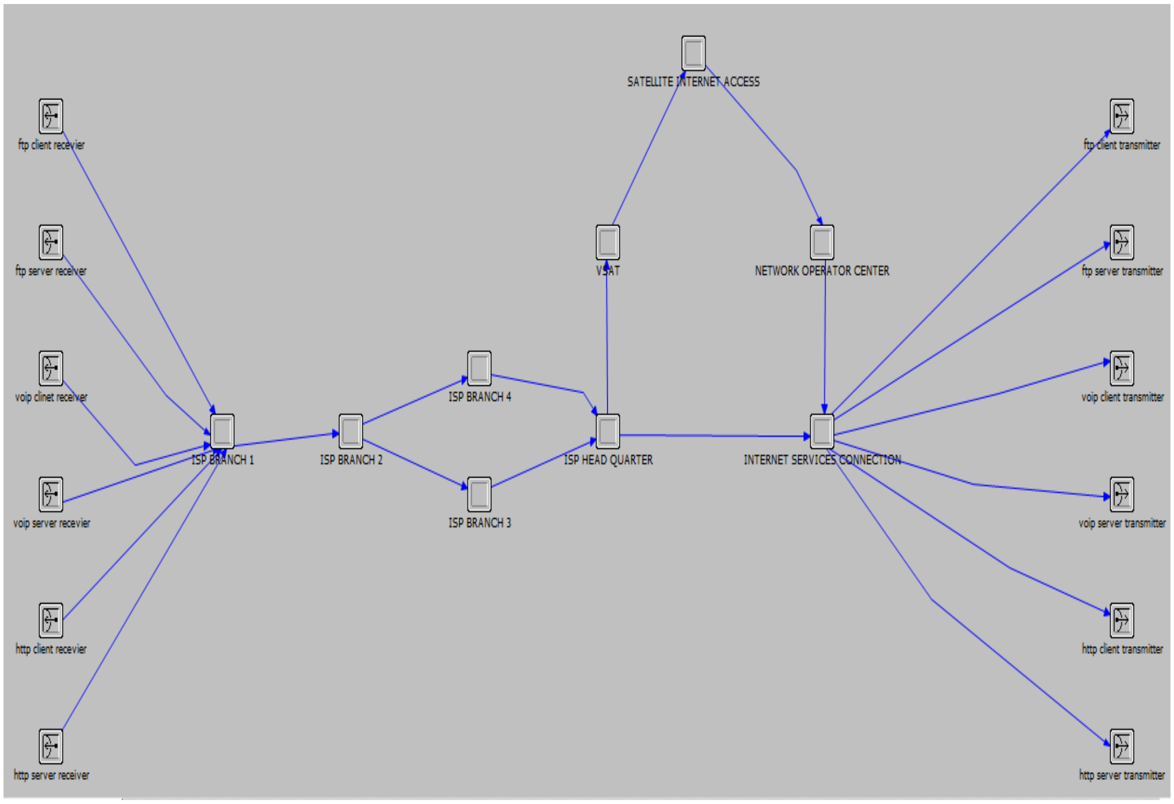


Figure A.0.3: Node network model

II. Configuring the Application

In this case, the applications and file sizes to be used on the network model are defined.

1. Select the edit attributes from the application node: set application definition to three because there are three applications used to generate traffic at all links in the network models: name the rows as FTP Application, HTTP Application, and VoIP Application.
2. From the FTP Application description row, set the value of FTP to high load. Change the value in the ftp table for a size of 38,000 and an inter-request time of exponential (600) to continue to request files of 50,000 bytes. Set the types of services field to the excellent effort.
3. From the HTTP Application description row, set the value of HTTP to web browsing change the value in the HTTP table for streaming multimedia.
4. From voice application service description row, set the value of the encoder scheme to G.729 A and voice frames per packet to five. Set the types of services field to interactive voice.

III. Configuring profiles

1. From the profiles nodes, select edit attributes; set profile definition to three because there are three profiles. The rows are named ftp profile, http profile and voice profile.
2. Name and set the attributes of the row as shown below with the ftp traffic starting 100 seconds after the start of the simulation.
3. Set the voice to start 100 seconds after the start of the simulation.
4. Set http to start at 100 seconds after the start of the simulation.

IV. Configuring the clients and servers

1. Right-click the FTP client, from edit attributes: application, supported profiles, set the rows to one and named profile to ftp profile then click ok twice.
2. Right-click the voice client, from edit attributes: application, supported profiles set the rows to one and named it as voice profile then clicks ok twice.
3. Right-click the http client, from edit attributes: application, supported profiles set the rows to one, the application was edited and set services named to http application ok twice.

4. Server: right-click the ftp server, edit attributes application; supported services and set rows to one, set services name to ftp application then ok twice.
5. Right-click the voice server: edit attributes application, supported services and set rows to one, set services name to voice application then ok twice.
6. Right-click the http server: edit attributes application, supported services and set rows to one, set services name to http application ok twice.

V. Traffic and flows

1. Set OSPF to run on all routers with an area of 0
2. Run discrete event simulation for 600 seconds and quantify the different traffic flows after choosing the appropriate statistics.

Appendix B: Procedure for Modeling MPLS Network Experiment:

In this model, Trunk Profiles are created. For traffic forward equivalence classes (FECs) are assigned and then bound to the static label switching protocols at label edge router ISP branch 1 and Internet Service Connection. Voice traffic will be made to flow along the route ISP branch 1 → ISP branch3 → ISP headquarter → Internet Services Connection. Two unidirectional paths are made one originating at each label edge router from ISP branch 1 to Internet Service Connection or vice versa. On the other hand FTP and HTTP traffic flow between the label edge router, ISP Branch 1 to ISP headquarter through ISP branch 4 router. Two unidirectional paths will be made between two label edge of ISP router.

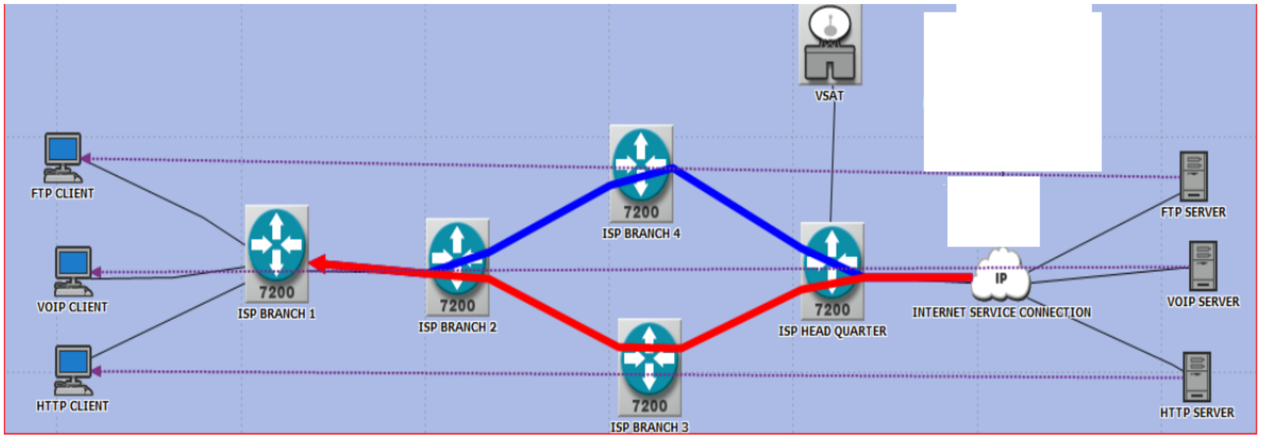
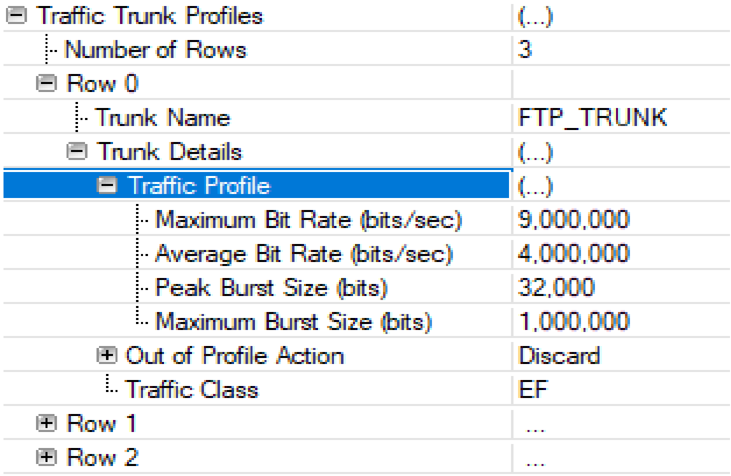


Figure B.1**:** Two unidirectional paths will be made between two-label edge of ISP router

I. Creation of Traffic Trunk Profiles

Three traffic flows need to be defined for three different DSCP classes as follows. Right click on the MPLS configuration object and select edit attributes. Select Traffic Trunk Profiles, edit the fields, enter three rows for each row adds the trunk name, and enter the traffic profiles for each traffic flow. Trunk FTP is added then Trunk HTTP finally Trunk voice is added with the following configurations as shown below.

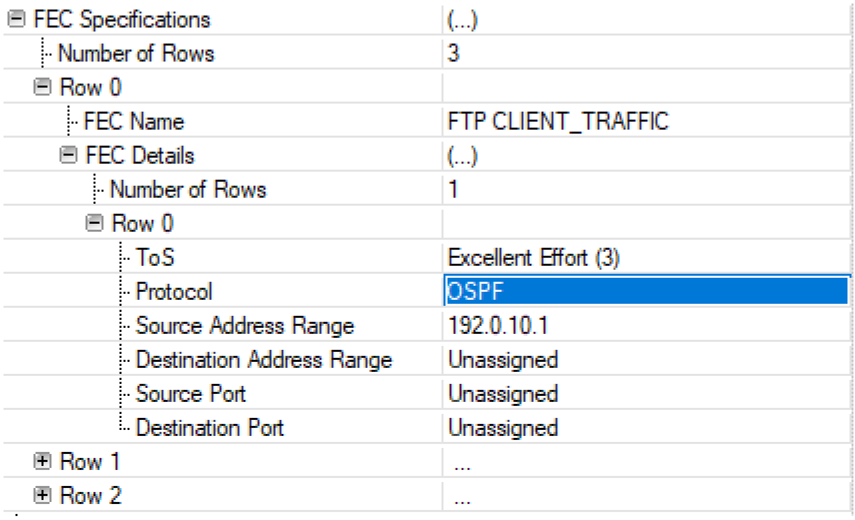


⊟ Traffic Trunk Profiles	(...)
Number of Rows	3
⊟ Row 0	
Trunk Name	FTP_TRUNK
⊟ Trunk Details	(...)
⊟ Traffic Profile	(...)
Maximum Bit Rate (bits/sec)	9,000,000
Average Bit Rate (bits/sec)	4,000,000
Peak Burst Size (bits)	32,000
Maximum Burst Size (bits)	1,000,000
⊞ Out of Profile Action	Discard
Traffic Class	EF
⊞ Row 1	...
⊞ Row 2	...

Figure B.2: Creation of trunk profiles

II. Creation of Forward Equivalence Classes (FECs)

Here three forward equivalence classes are created. One for voice and the other two will be for HTTP and FTP traffic. This three traffic would be managed in the network model. Right click on MPLS configuration object and select edit attributes, select FEC specification and edit the fields enter three rows. For each row add an FEC name voice, HTTP and FTP traffic as shown below. Assign types of service code point for voice, HTTP and FTP in the model. Details for FEC_FTP are as shown below:



⊟ FEC Specifications	(...)
Number of Rows	3
⊟ Row 0	
FEC Name	FTP CLIENT_TRAFFIC
⊟ FEC Details	(...)
Number of Rows	1
⊟ Row 0	
ToS	Excellent Effort (3)
Protocol	OSPF
Source Address Range	192.0.10.1
Destination Address Range	Unassigned
Source Port	Unassigned
Destination Port	Unassigned
⊞ Row 1	...
⊞ Row 2	...

Figure B.3: Creation of Forward Equivalence Classes

III. Configure of Static Label Switching Path (LSP) between ISP branch 1 up to Internet Services Connection Router through ISP branch 4

Using the MPLS-E-LSP static object configure a unidirectional static route from ISP branch 1 to Internet Services Connection. Click on the MPLS-E-LSP static object in the MPLS object palette. From the riverbed workspace, click on the LSP's ingress ISP branch 2 router, click on the next link or ISP branch 4 in the LSP's route. The tooltips indicate which links and routes can be added to the route. Hold the cursor over a link or router for details about adding it to the label switching. Continue clicking on each link or router in the route until all have been added. Right click on the thesis workspace and select the finish path definition to finish drawing the LSP.

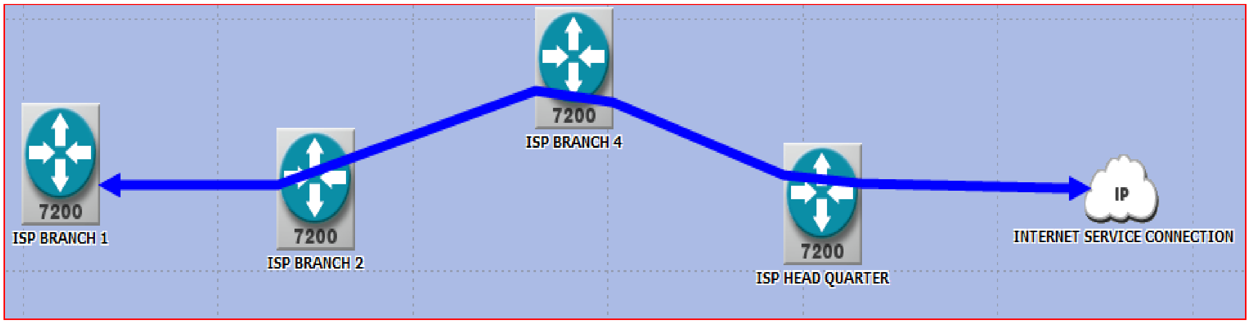


Figure B.4: Configure of Static Label Switching Path (LSP) between ISP branch 1 up to Internet Services Connection Router through ISP branch 4

IV. Configure a static LSP between ISP branch 1→ISP branch 3→Internet Service Connection.

The same as Figure B.4 but from ISP branch 1 to Internet Service Connection on the bottom path. When creation of LSPs is finished, right-click in the workspace and select abort path definition, otherwise draw the next static LSP.

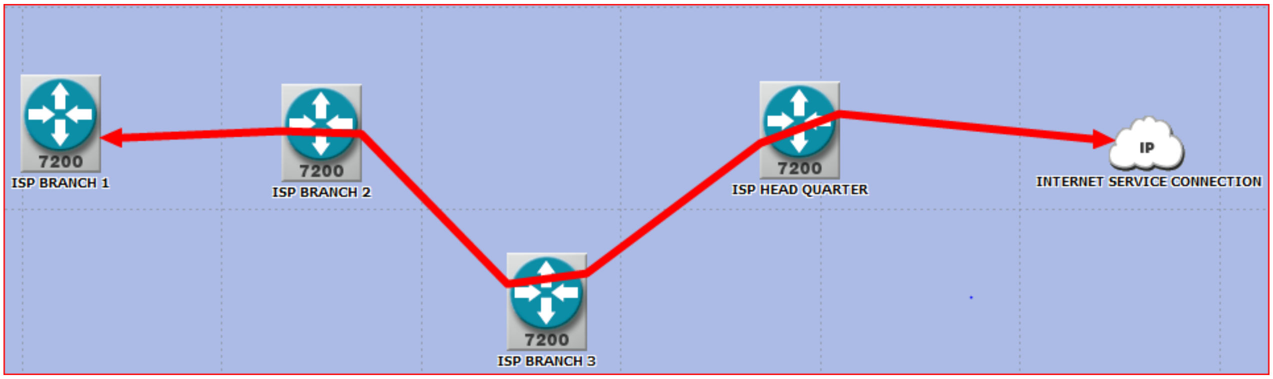


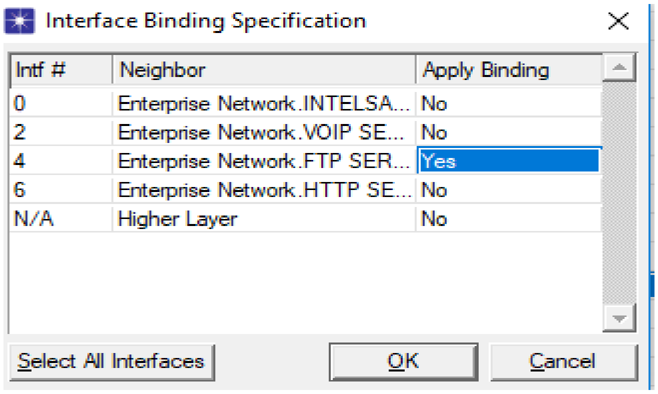
Figure B.5**:** Configure a static LSP between ISP branch 1, ISP branch 3 and Internet Service Connection

V. Update the LSP Details

From the protocols/MPLS menu, choose to update LSP details to configure label switching information to LSPs. Choose protocol/MPLS/ show all LSPs to show the paths on the topology diagram. Right click on the link between ISP branch 1 and Internet Service Connection to reveal the path names. Click on path details and examines the path details to see the labels being used to determine the path between the routers.

VI. Configure Traffic Mapping Configuration on Internet Service Connection and ISP branch 2

Here I am going to bind the FEC-voice profile to voice trunk and map this onto one or more label switching paths. Then both FEC-ftp profile is bound to ftp trunk and mapped onto a different LSP. The same is true for the FEC-HTTP profile. On ISP branch 2 router choose the edit attributes/ MPLS/MPLS parameters/Traffic mapping configuration attributes and enter three rows.



Interface Binding Specification

Intf #	Neighbor	Apply Binding
0	Enterprise Network.INTELSA...	No
2	Enterprise Network.VOIP SE...	No
4	Enterprise Network.FTP SER...	Yes
6	Enterprise Network.HTTP SE...	No
N/A	Higher Layer	No

Figure B.6: Configure Traffic Mapping Configuration on Internet Service Connection and ISP branch 2

Configure the FEC/destination prefix as FEC-voice with the traffic trunk to trunk-voice, the primary LSP from ISP branch to head quarter and backup LSP to ISP branch to head quarter. Configure the next two rows as the voice for the same FEC and LSP except set the traffic Trunk to Trunk-HTTP and Trunk-ftp as shown below.

I. Configure Link Discovery Protocols on the Routers

Select the ISP branch 1 router and right click select edit attributes/MPLS/LDP parameters. Set the status to enabled; the discovery configuration link enabled and the loopback interface to be enabled then select the route’s loopback address (LB0). Set the neighbor configuration, number of row to one and add name the neighbors as ISP branch 4 click ok to save parameters. At the least ensuring that the appropriate interfaces between the MPLS routers have been enabled. A similar process should be done on all the other ISP routers.

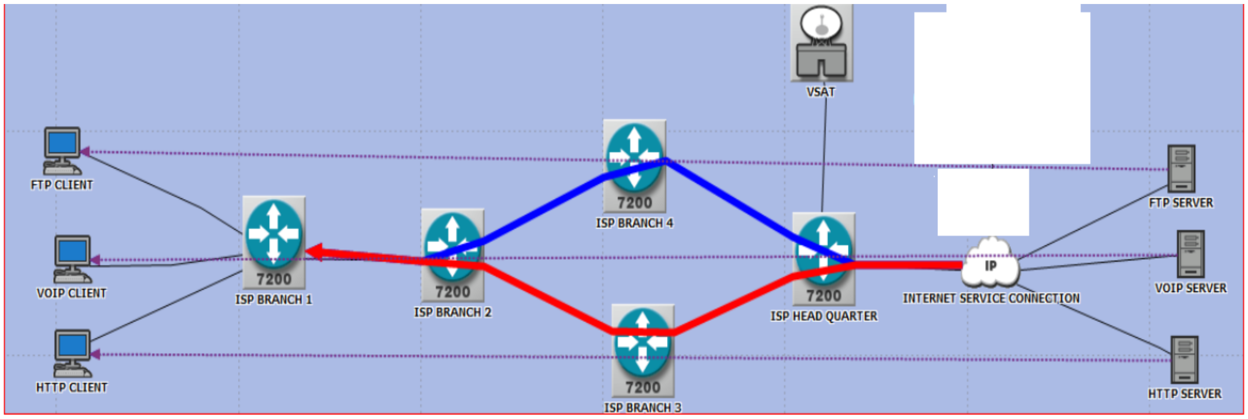
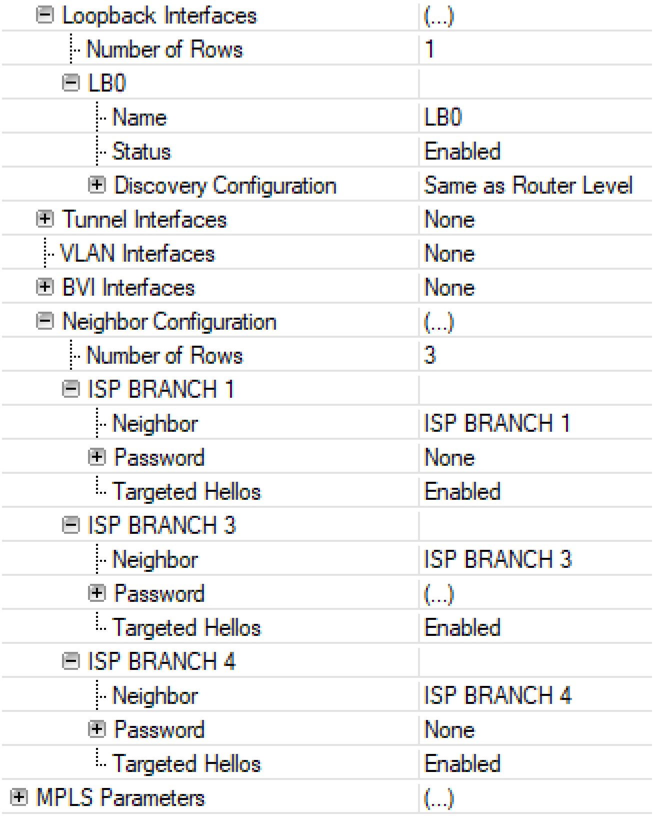
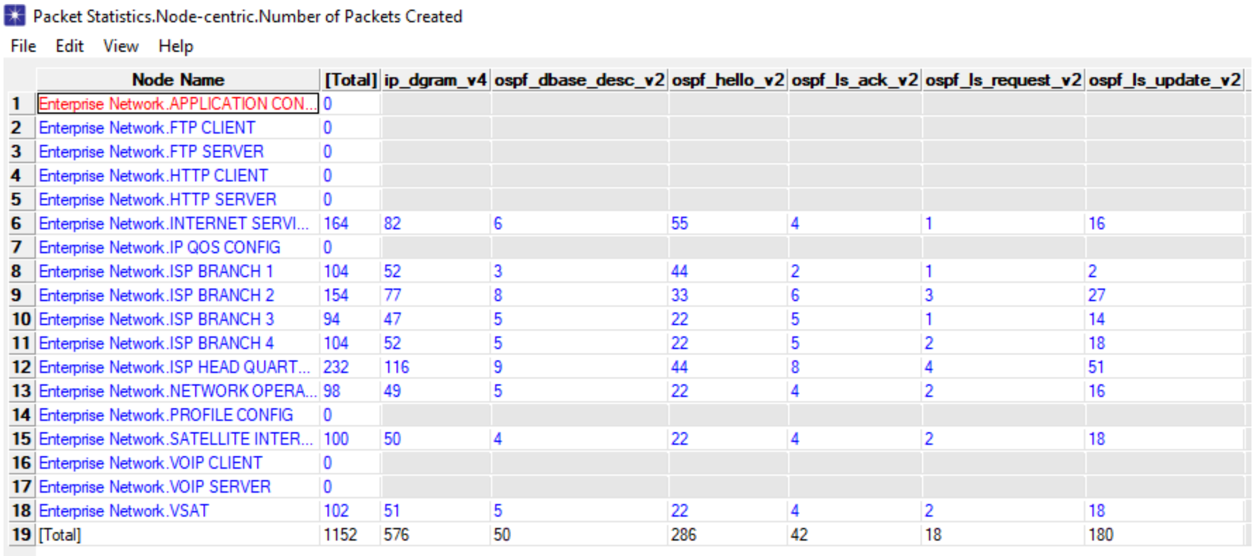


Figure B.7: Configure Link Discovery Protocols on the Routers



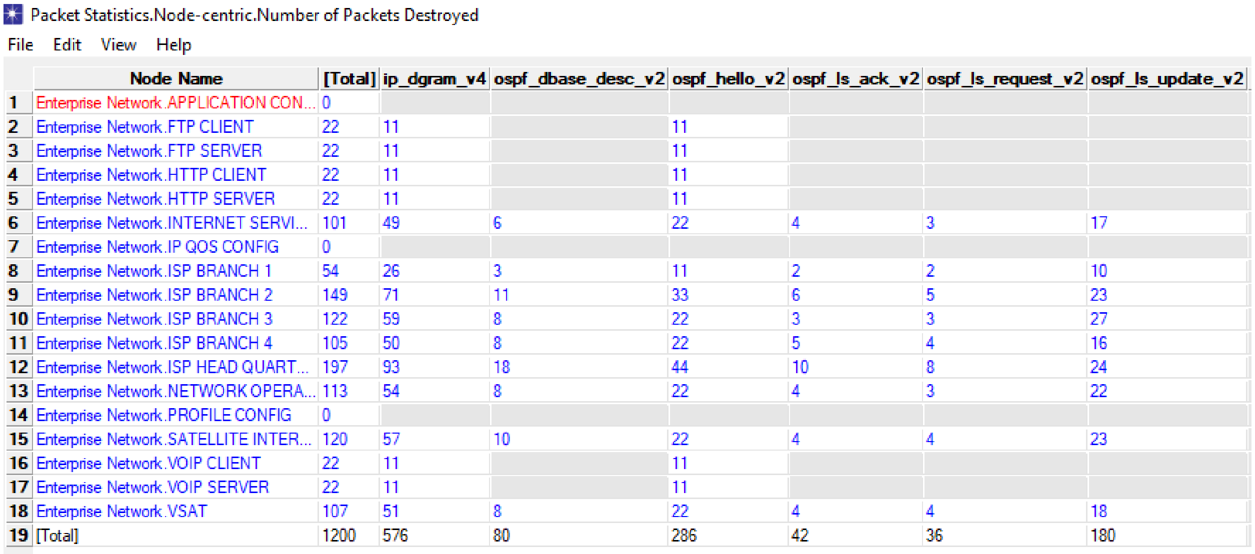
⊟ Loopback Interfaces	(...)
Number of Rows	1
⊟ LB0	
Name	LB0
Status	Enabled
⊞ Discovery Configuration	Same as Router Level
⊞ Tunnel Interfaces	None
VLAN Interfaces	None
⊞ BVI Interfaces	None
⊟ Neighbor Configuration	(...)
Number of Rows	3
⊟ ISP BRANCH 1	
Neighbor	ISP BRANCH 1
⊞ Password	None
Targeted Hellos	Enabled
⊟ ISP BRANCH 3	
Neighbor	ISP BRANCH 3
⊞ Password	(...)
Targeted Hellos	Enabled
⊟ ISP BRANCH 4	
Neighbor	ISP BRANCH 4
⊞ Password	None
Targeted Hellos	Enabled
⊞ MPLS Parameters	(...)

Figure B.8: Configure Link Discovery Protocols and Neighbor Configuration on the Routers



	Node Name	[Total]	ip_dgram_v4	ospf_dbase_desc_v2	ospf_hello_v2	ospf_ls_ack_v2	ospf_ls_request_v2	ospf_ls_update_v2
1	Enterprise Network.APPLICATION CON...	0						
2	Enterprise Network.FTP CLIENT	0						
3	Enterprise Network.FTP SERVER	0						
4	Enterprise Network.HTTP CLIENT	0						
5	Enterprise Network.HTTP SERVER	0						
6	Enterprise Network.INTERNET SERVI...	164	82	6	55	4	1	16
7	Enterprise Network.IP QOS CONFIG	0						
8	Enterprise Network.ISP BRANCH 1	104	52	3	44	2	1	2
9	Enterprise Network.ISP BRANCH 2	154	77	8	33	6	3	27
10	Enterprise Network.ISP BRANCH 3	94	47	5	22	5	1	14
11	Enterprise Network.ISP BRANCH 4	104	52	5	22	5	2	18
12	Enterprise Network.ISP HEAD QUART...	232	116	9	44	8	4	51
13	Enterprise Network.NETWORK OPERA...	98	49	5	22	4	2	16
14	Enterprise Network.PROFILE CONFIG	0						
15	Enterprise Network.SATELLITE INTER...	100	50	4	22	4	2	18
16	Enterprise Network.VOIP CLIENT	0						
17	Enterprise Network.VOIP SERVER	0						
18	Enterprise Network.VSAT	102	51	5	22	4	2	18
19	[Total]	1152	576	50	286	42	18	180

Figure B.9: Number of packet created on each node of the router during routing processing using OSPF



	Node Name	[Total]	ip_dgram_v4	ospf_dbase_desc_v2	ospf_hello_v2	ospf_ls_ack_v2	ospf_ls_request_v2	ospf_ls_update_v2
1	Enterprise Network.APPLICATION CON...	0						
2	Enterprise Network.FTP CLIENT	22	11		11			
3	Enterprise Network.FTP SERVER	22	11		11			
4	Enterprise Network.HTTP CLIENT	22	11		11			
5	Enterprise Network.HTTP SERVER	22	11		11			
6	Enterprise Network.INTERNET SERVI...	101	49	6	22	4	3	17
7	Enterprise Network.IP QOS CONFIG	0						
8	Enterprise Network.ISP BRANCH 1	54	26	3	11	2	2	10
9	Enterprise Network.ISP BRANCH 2	149	71	11	33	6	5	23
10	Enterprise Network.ISP BRANCH 3	122	59	8	22	3	3	27
11	Enterprise Network.ISP BRANCH 4	105	50	8	22	5	4	16
12	Enterprise Network.ISP HEAD QUART...	197	93	18	44	10	8	24
13	Enterprise Network.NETWORK OPERA...	113	54	8	22	4	3	22
14	Enterprise Network.PROFILE CONFIG	0						
15	Enterprise Network.SATELLITE INTER...	120	57	10	22	4	4	23
16	Enterprise Network.VOIP CLIENT	22	11		11			
17	Enterprise Network.VOIP SERVER	22	11		11			
18	Enterprise Network.VSAT	107	51	8	22	4	4	18
19	[Total]	1200	576	80	286	42	36	180

Figure B.10: The number of packets destroyed on each node router during routing processing using OSPF