Sudan University of Science and Technology

Collage of Graduate Studies

Performance Evaluation of QoS for Real Time Applications Using Multiprotocol Label Switching

تقييم أداء جودة الخدمة في تطبيقات الزمن الحقيقي باستخدام تبديل العلامات متعددة البروتوكول

A Thesis Submitted In Partial Fulfillment for the Requirements of Degree of M.Sc in Electronic Engineering (Computer and Network Engineering)

Prepared By

Duaa Ahmed Mohamed Ahmed

Supervisor

Dr. Fath Elrahman Ismael Khalifa

April 2017

استهلال

قـال تعـالى:

وما أوتيتم من العلم إلا قليلا

سورة الإسراء(85)

إهـــــــــــــــــداء

إلى سندي وعضدي في الحياة .. إلى من أعطوني الحياة وعلموني أسبابها

أمي وأبي ,,,

إلى من منحوني الأمل ومحو عني الألم .. إلى أولئك الذين دعوا لي بخير وتفائل ونجاح

أصدقائي ,,,

إلى من وجهني وعلمني .. إلى العطاء الذي لا ينفذ

أساتذتي الأجلاء ,,,

وقبل ذلك الشكر والحمد حتى يبلغ منتهاه للذي أناجيه سرا وجهرا

إلى ولى نعمتي .. ذو الفضل والمنة

ربـــــي ,,

ACKNOWLEDGEMENT

I would like to express my deep gratitude to my master thesis advisor, Dr. Fath Elrahman Ismael for spending his time to read and guiding me with useful suggestions about this thesis. He does all hard-working professors and I believe their academic achievements will continue to increase.

I would like to extend my appreciation for Dr. Abuaglah Babiker. I have learned a lot of things from him. He spent a lot of time to instructing me how to write a paper, to search for resources and literature and to collect data professionally.

I would like to sincere gratitude to my friends and colleagues whose help me to get resources, whose ask about me usually and always, whose encouraged me when I was weak, guided me when I lost, believe in me.

Last but not the least important, I owe more than thanks to my family members which includes my parents and an elder brother, for their financial support and encouragement throughout my life. Without their support, it is impossible for me to finish my college and graduate education seamlessly.

ABSTRACT

Internet Protocol (IP) network has different problems during packets transmit. Delay and packet drop are famous challenges of developers. The researchers are having many tries to solve those problems. Multi-Protocol Label Switching (MPLS) networks is one of that solutions. Label switching technology is used at the IP core routers to improve the routing mechanism and to make it more efficient. The developed protocol configures the data packets with fixed labels at the start of transmission and at the end of the MPLS domain it's removed. MPLS traffic engineering (MPLS TE) provides better utilization of network recourses. MPLS naturally supports Quality of Service (QoS) by providing classification, marked packet, avoiding congestion, congestion management and Improve traffic. In this research the evaluation of network performance is done. The evaluation is applied on different scenarios with different routing protocols such as Open Shortest Path First (OSPF), MPLS and MPLS with Resource Reservation Protocol (RSVP). OPNET is used to make comparison and view various parameters such as End-to-End delay, delay variation, and throughput. MPLS is faster than OSPF protocols. The delay measurements when MPLS applied with RSVP reduced by 99.7% in light model and four times in heavy model. MPLS with RSVP enhanced video traffic received by 8.64% in light model and 21.2% in heavy model. MPLS provides the reliability of communication while reducing the delays and supporting the speed of the packet transfer specially when applying QoS which is RSVP here.

المستخلص

هناك مشاكل كثيرة في شبكة بروتوكول الإنترنت أثناء إرسال الحزم. من أشهر هذه المشاكل بالنسبة للمطورين التأخير وفقدان الحزمة .قام الباحثون بالعديد من المحاولات لحل تلك المشاكل .وتعد تبديل العلامات متعددة البروتوكول إحدى تلك الحلول .تستخدم تكنولوجيا التبديل في الموجهات الأساسية لتحسين آلية التوجيه وجعلها أكثر كفاءة .ويقوم البروتوكول المطور بتكوين حزم البيانات بتسميات ثابتة في بداية الإرسال وفي نهاية نطاق تبديل العلامات متعددة البروتوكول تتم إزالت هذه التسمية. تبديل العلامات متعددة البروتوكول مع هندسة المرور يوفر أفضل استخدام لموارد الشبكة. صمم تبديل العلامات متعددة البروتوكول ليدعم جودة الخدمة بشكل طبيعي من خلال توفير التصنيف، وضع علامة مميزة، تجنب و إدارة الازدحام، وتحسين حركة المرور .في هذا البحث يتم تقييم أداء الشبكة من خلال سيناريوهات مختلفة مع بروتوكولات توجيه مختلفة مثل المسارالأقصر أولا، تبديل العلامات متعددة البروتوكول و تبديل العلامات متعددة البروتوكول مع بروتوكول حجز الموارد. يستخدم أوبنيت لإجراء المقارنة وعرض مختلف العوامل مثل تأخير نهاية إلى نهاية، وتغير التأخير، والإنتاجية وحركة المرور المستلمة .تبديل العلامات متعددة البروتوكول أسرع من البروتوكولات التقليدية ويهر ذلك من خلال قياسات التأخير حيث نجد أنه باستخدام تبديل العلامات متعددة البروتوكول مع برتوكول حجز الموارد نحصل على تأخير أقل بنسبة 99.7٪ في النموذج الخفيف و أربع مرات في النموذج الثقيلة .حركة الفيديو التي تم استلامها هي أيضا كمية عالية في سيناريو تبديل العلامات متعددة البروتوكول مع برتوكول حجز الموارد حيث كانت مرتفعة بنسبة 8.64٪ في النموذج الخفيف و 21.2٪ في النموذج الثقيل .يوفر تبديل العلامات متعددة البروتوكول موثوقية في الاتصالات مع الحد من التأخير ويدعم سرعة نقل الحزم خصوصا عند تطبيق جودة الخدمة التي كانت هنا برتوكول حجز الموارد.

CONTENTS

LIST OF FIGURES

Figure No. **Title** **Page No.**

LIST OF TABLES

Table No. **Title** **Page No.**

ABBREVIATIONS

AS	Autonomous system
ATM	Asynchronous transfer mode
Bps	Bits per second
CIDR	Class inter domain routing
CoS	Characteristic type of service
DiffServ	Differentiated Services
EGPs	Exterior Gateway Protocols
EIGRP	Enhanced Interior Gateway Protocol
FEC	Forward error correction
FIFO	First In First out
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IGPs	Interior Gateway Protocols
IntServ	Integrated Services
IP	Internet protocol
ISO	International Standards Organization
ISP	Internet Service Providers
LDP	Label Distribution Protocol
LER	Label egress router
LSP	Label Switched Paths
LSR	Label Switch Routers
MPLS	Multi-Protocol Label Switching
OPNET	Optimized Network Engineering Tools
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PDV	Packet delay variation
PQ	Priority queuing
PVC	Permanent virtual circuit
QoS	Quality of service

RIP	Routing information Protocol
RSVP	Resource Reservation Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TE	Traffic Engineering
ToS	Type of service
VJTI	Veermata Jijabai Technological Institute
VoIP	Voice over IP
WFQ	Waited Fair Queuing

CHAPTER ONE

INTRODUCTION

1.1 Preface

A network is a group of devices which are connected together to create small, medium or large network .various devices from various vendors were connected to networks, which make the need for using protocols to make the exchange possible between different devices from different vendors. Internet protocol (IP) is a common protocol, which let the wild world web to be like single network. The rapidly growing of networks and customers requirements for high level of quality and performance cannot be achieved using IP only.

Video conferencing connects people in real time through audio and video communication over broadband networks allowing visual meetings and cooperation on digital documents and shared presentations. In the past, members of meeting connect to central meeting rooms prepared with video conference hardware, but new technologies allow participants to connect remotely over a network through multiple devices like laptops, desktops, smart phones and tablets. To support this type of traffic, we need delay less and reliable technology to transfer data packet quickly[1].

Multi-Protocol Label Switching (MPLS) is appeared to improve some characteristics of IP performance and exit new end to end delivery. IP uses hop-by-hop destination only forwarding paradigm. When forwarding IP packets, each router in the path has to look up the packet's destination IP address in the IP routing table and forward the packet to the next-hop router. MPLS is an advancing technology, which is mainly responsible for high performance packet control and mechanism. It does this by the information contained in the labels attached to the IP packets to forward such packets through a network. It merges the strength of layer 2 switching

and layer 3 routing to form an IP network with a high level of performance. MPLS has evolved into a vital technology which efficiently operates and manages IP networks due to its superior characteristics. The purpose of MPLS is to guarantee speed, traffic engineering, Quality of Service (QoS)[2].

Best effort is a single service model in which an application sends data whenever it must, in any quantity, and without requesting permission or first informing the network. The network delivers data if it can, without any assurance of reliability, delay bounds, or throughput. The real time traffic as mentioned needs guarantee to minimum delay and acceptable throughput[3].

As known, routers using MPLS never look at the IP addresses, but only at the labels, you can encapsulate anything within MPLS and use it for; regardless if the packet was IPv4 or IPv6.

1.2 Problem Statement

In the mluti-service network which contains video as real time application and other different traffics, the packets for real time applications should be delivered with minimum delays under various circumstances.

Packet delivery of video traffic is affected by many factors such as delay, packet loss, and throughput. The network sometimes does not used effectively (many paths are empty when the other paths congested) because of the limitations of routing protocols used.

1.3 Proposed Solution

This research work evaluated the performance of OSPF, MPLS and MPLS_RSVP routing protocols under various circumstances. They are evaluated considering the delays in video, the packets received and the throughput.

1.4 Objectives

The objectives of this research are:

- To simulation OSPF, MPLS and MPLS_RSVP routing protocols using OPNET simulator.
- To compare OSPF, MPLS and MPLS_RSVP protocols considering performance metrics such as delay, packet loss, and throughput.

1.5 Methodology

Create environment with different sizes. In the first scenario OSPF protocol is used. The second scenario applied MPLS and the third one deployed QoS addition to MPLS. The main traffic is video conference and various parameters are measured such as received traffic, End-to-End delay, delay variation and throughput. Analysis the result and compare the performance in three scenarios with reasonable justification.

1.6 Thesis Outlines

In general the thesis will be divided into five chapters. Each chapter will discuss on different issues related to the project. The following are the issues discussed.

Chapter One: includes problem statement, proposed solutions and methodology.

Chapter Two: describes the background required to understand the proposed study and some examples of other research.

Chapter Three: define tools and program that used to apply the design.

Chapter Four: analyzing the scenarios that create to make environment study and notice the change in performance parameters in every scenario.

Chapter Five: result and conclusion that have reached by the experience.

CHAPTER TWO

LITERATURE REVIEW

2.1 Background

Computer network consists of two or more computing devices that are connected in order to share the components of your network (its resources) and the information you store there.

The most basic network (which consists of just two connected devices) can be expanded and become more usable with jointing additional devices with their resources to those being shared. Networks can be expanded to cover different areas with different sizes. It can cover the whole world which means there are millions of devices will be connected togather and they need something to make the connection possible.

2.1.1 Open Systems Interconnection (OSI) Model

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the OSI model.

An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software[4, 5].

The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7). As shown in figure 2.1

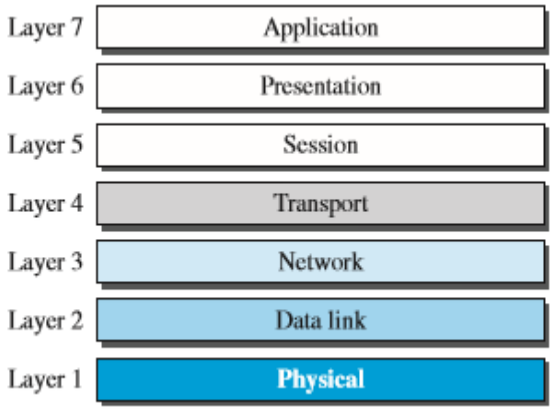

Figure 2-1: OSI Model[4]

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specification of the interface and transmission media. It also defines procedures and functions that physical devices and interfaces have to perform for transmission to occur.

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (link), the network layer ensures that each packet gets from its point of origin to the ultimate destination.

The transport layer is responsible for process-to-process delivery of the entire message. It ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction between communicating systems[4, 5].

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

There is another type of Model which called TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today represent in figure 2-2.

When we compare the two models, we find that two layers, session and presentation, are missing from the TCP/IP protocol suite. These two layers were not added to the TCP/IP protocol suite after the publication of the OSI model. The application layer in the suite is usually considered to be the combination of three layers in the OSI model[4, 5].

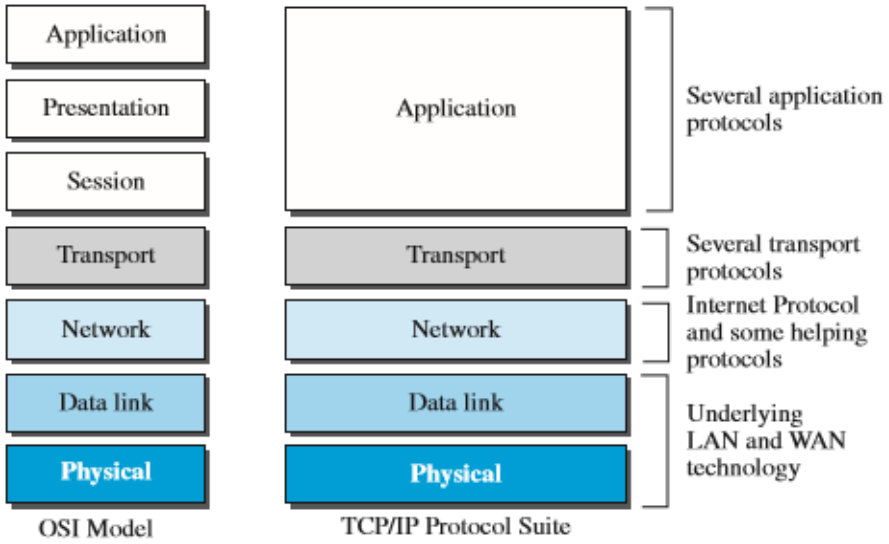

Figure 2-2: OSI Model vs. TCP/IP Suit[4]

2.1.2 Routing Protocol

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 OSPF which forward data based on the information contained in routing tables present in routers.

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. [6].

IP routing protocols have different classifications as following:

2.1.2.1 Static Routing vs. Dynamic Routing

A routing table can be either static or dynamic. A static table is one with manual entries. A dynamic table, on the other hand, is one that is updated automatically when there is a change somewhere in the internet. Today, an internet needs dynamic routing tables. The tables need to be updated as soon as there is a change in the internet. For instance, they need to be updated when a link is down, and they need to be updated whenever a better route has been found [5].

2.1.2.2 Interior Gateway Protocols vs. Exterior Gateway Protocols

All Internets routing protocols fall into one of two categories: Interior Gateway Protocols (IGPs) and Exterior Gateway Protocols (EGPs)

The Internet is divided into a set of autonomous systems; routers within an autonomous system exchange routing information, which is then summarized before being passed to another group to prevent the high traffic would overwhelm the core of the Internet.

The routers within an autonomous system use an IGP to exchange routing information. Several IGPs are available; each autonomous system is free to choose its own IGP. Usually, an IGP is easy to install and operate, but an IGP may limit the size or routing complexity of an autonomous system.RIP, OSPF and IS-IS are examples of IGP.

A router in one autonomous system uses an EGP to exchange routing information with a router in another autonomous system. EGPs are usually more complex to install and operate than IGPs, but EGPs offer more flexibility and lower overhead (i.e., less traffic). To save traffic, an EGP summarizes routing information from an autonomous system before passing it to another autonomous system.BGP is an example of EGP. More important, an EGP implements policy constraints that allow a system manager to determine exactly what information is released outside the organization[7]

2.1.2.3 Distance Vector and Link State

In addition, most routing protocols can be classified into two classes: distance vector and link state. Distance vector routing protocol is based on Bellman – Ford algorithm and Ford – Fulkerson algorithm to calculate paths. A distance vector routing protocol uses a distance calculation and a vector direction of next hop router as reported by neighboring routers to choose the best path. It requires that a router informs its neighbours of topology changes periodically.

Link state routing protocols build a complete topology of the entire network are and then calculating the best path from this topology of all the interconnected networks. It requires more processing power and memory because it has a complete picture of the network[8].

2.1.3 Open Shortest Path First (OSPF) Protocol

The OSPF protocol is based on link state routing which means that every node in the network constructs a map of the network connectivity in the form of a graph. The OSPF protocol is based on the short path first algorithm known as class inter domain routing (CIDR) to address models. There is no concept of hop count in the OSPF protocol as its structure is hierarchical. The procedure for generating shortest path tree is that every router sends local and external link state information to each other. Hence ensuring that every router be able to calculate shortest path within the autonomous system (AS). If any change happens within the AS then a recalculation process starts.

The OSPF uses a shorted path first algorithm in order to build and calculate the shortest path to all known destinations. The shortest path is calculated with the use of the Dijkstra algorithm. The algorithm can be briefly described as follows: Upon initialization or due to any change in routing information, a router generates a link-state advertisement. This advertisement represents the collection of all link-states on that router. All routers exchange link-states by means of flooding. Each router that receives a link-state update should store a copy in its link-state database and then propagate the update to other routers. After the database of each router is completed, the router calculates a Shortest Path Tree to all destinations. The router uses the Dijkstra algorithm in order to calculate the shortest path tree. The destinations, the associated cost and the next hop to reach those destinations form the IP routing table.

In the case that no changes has taken place in the OSPF network, such as cost of a link or a network being added or deleted, the OSPF is then considered to be very quiet. Any changes that occur are communicated through link-state packets, and the Dijkstra algorithm is recalculated in order to find the shortest path[9].

2.1.4 Quality of Service

The Internet was originally designed for best-effort service without guarantee of predictable performance. Best-effort service is often sufficient for a traffic that is not sensitive to delay, such as file transfers and e-mail. Such traffic is called elastic because it can stretch to work under delay conditions; it is also called available bit rate because applications can speed up or slow down according to the available bit rate. The real-time traffic generated by some multimedia applications is delay sensitive and therefore requires guaranteed and predictable performance. Quality of service (QoS) is an internetworking issue that refers to a set of techniques and mechanisms that guarantee the performance of network to deliver predictable service to an application program[3].

2.1.4.1 Flow Control to Improve QoS

Although formal classes of flow are not defined in the Internet, an IP datagram has a type of service (ToS) field that can informally define the type of service required for a set of datagram sent by an application. If we assign a certain type of application a single level of required service, we can then define some provisions for those levels of service. These can be done using several mechanisms. After that scheduling applied using first-in, first-out queuing, priority queuing, and weighted fair queuing. Another way is traffic shaping, which can be achieved using the leaky bucket or the token bucket technique. Resource reservation and admission control can also be used in this case.

2.1.4.2 Differentiated Services (DiffServ)

In this model, also called DiffServ, packets are marked by applications into classes according to their priorities. Routers and switches, using various queuing strategies, route the packets. This model was introduced by the IETF (Internet Engineering Task Force) to handle the shortcomings of Integrated Services. Two fundamental changes were made:

1. The main processing was moved from the core of the network to the edge of the network. This solves the scalability problem. The routers do not have to store information about flows. The applications, or hosts, define the type of service they need each time they send a packet.

2. The per-flow service is changed to per-class service. The router routes the packet based on the class of service defined in the packet, not the flow. This solves the service-type limitation problem. We can define different types of classes based on the needs of applications, and it out of our study.

2.1.4.3 Integrated Services (IntServ)

Traditional Internet provided only the best-effort delivery service to all users regardless of what was needed. Some applications, however, needed a minimum amount of band width to function (such as real-time audio and video). To provide different QoS for different applications, IETF

developed the IntServ model. In this model, which is a flow-based architecture, resources such as bandwidth are explicitly reserved for a given data flow regardless of the application type (data transfer, or voice over IP, or video-on-demand). What important are the resources the application needs, not what the application is doing. The model is based on three schemes:

- The packets are first classified according to the service they require.
- The model uses scheduling to forward the packets according to their flow characteristics.
- Devices like routers use admission control to determine if the device has the capability (available resources to handle the flow) before making a commitment[3, 4].

For example, if an application requires a very high data rate, but a router in the path cannot provide such a data rate, it denies the admission. We know this model is flow-based, which means that all accommodations need to be made before a flow can start. This implies that we need a connection-oriented service at the network layer. A connection establishment phase is needed to inform all routers of the requirement and get their approval (admission control). However, since IP is currently a connectionless protocol, we need another protocol to be run on top of IP to make it a connection-oriented protocol before we can use this model. This protocol is called RSVP and will be discussed.

2.1.4.4 Receiver-Based Reservation

In RSVP, the receivers, not the sender, make the reservation. This strategy matches the other multicasting protocols. For example, in multicast routing protocols, the receivers, not the sender, make a decision to join or leave a multicast group. RSVP Messages RSVP has several types of messages. However, for our purposes, we discuss only two of them: Path and Resv.

Path Messages Recall that the receivers in a flow make the reservation in RSVP. However, the receivers do not know the path travelled by packets before the reservation is made. The path is needed for the

reservation. To solve the problem, RSVP uses Path messages explain in figure 2-3. A Path message travels from the sender and reaches all receivers in the multicast path. On the way, a Path message stores the necessary information for the receivers. A Path message is sent in a multicast environment; a new message is created when the path diverges[4].

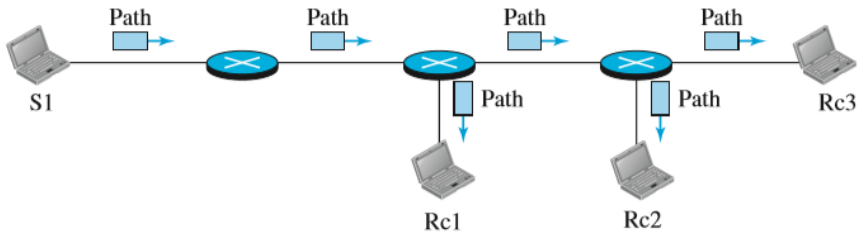

Figure 2-3: Path Message[4]

Revs Messages After a receiver has received a Path message observe in figure 2-4, it sends a Revs message. The Revs message travels toward the sender (upstream) and makes a resource reservation on the routers that support RSVP. If a router on the path does not support RSVP, it routes the packet based on the best-effort delivery methods we discussed before[4].

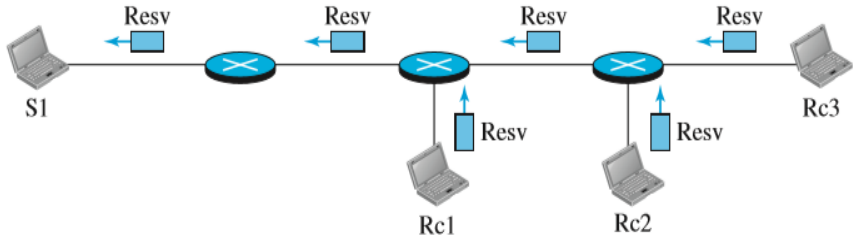

Figure 2-4: Revs Message[4]

A drawback of the present-day Internet is the complete lack of traffic management; all traffic receives best-effort service, and there is no way to predict a priority or guarantee the QoS that will be received by a particular traffic flow. Route selection is based on shortest path computations using simple additive link metrics. This approach is highly distributed and scalable, but flawed. The flaw is that these protocols do not consider the characteristics of offered traffic and network capacity constraints when making routing decisions. This results in subsets of network resources

becoming congested, while other resources along alternate paths remain underutilized. This type of congestion problem is a symptom of poor resource allocation, and is an issue that traffic engineering specifically attempts to rectify through MPLS[10].

2.1.5 Multiprotocol Label Switching (MPLS)

Routing process is slower than the switching. The links in the IP networks can be under-utilized or over-utilized that are caused by the routing process, results in congestion with over-utilized links also TE (Traffic Engineering) is difficult to implement in the IP networks since IP networks are not scalable.

2.1.5.1 MPLS Structure

MPLS can deal with a different payload, recognize layer 2, Ethernet encapsulation, and all dynamic routing protocol, also it is capable of identifying and dealing with IPV4, IPV6, ATM, Frame Relay... etc., this is why it is called multi-protocol.

Additional label added to the packet that runs through the MPLS technology, so forwarding the packet depends on the label that was added which defined the source and destination address. MPLS came as the better and most supported technology for the IP; it has overcome the limitations of other technology like ATM and Frame Relay[11].

MPLS label is placed between the second layer and the third one, and comes as a shim between them, as it is plain in Figure 2-5.

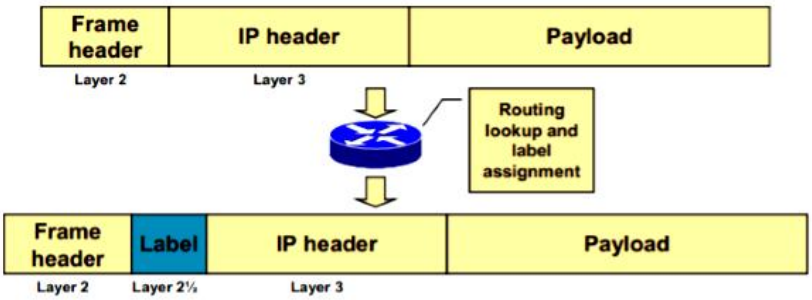

Figure 2-5: MPLS Label[6]

It is a short fixed length identifier which is used to identify FEC (forward error correction). Every label stack entry is a 32-bit length, and it is divided into four fields notice figure 2-6. [11].

Table 2-1: MPLS Header

sequence	Bits No.	Name	The purpose
1	20	label	label
2	3	EXP	Service type (QoS)
3	1	S	'1' if it's last card or '0' for otherwise
4	8	TTL	Time to leave which is used to prevent the Loop

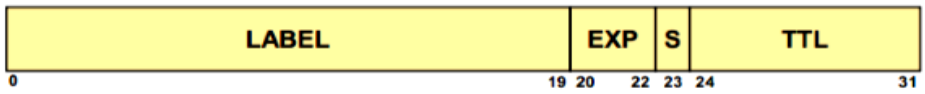

Figure 2-6: MPLS Header[6]

2.1.5.2 MPLS Functionality and Operation Mechanism

General terms associated with MPLS network and their meaning is specified below:

- Label Switching Router (LSR): LSR is a type of MPLS router which operates at the boundary and core of the MPLS network. Ingress and egress router are the two types of edge LSR. The ingress router attaches a new label to every incoming packet and forwards it into MPLS core.
- Label Switched Path (LSP): It is a route established between two edge LSRs which act as a path for forwarding labelled packets over LSPs[12].

In Figure 2-7 MPLS forwarding mechanism represented. When R1 receives a packet from other Layer 2 networks; it attaches a label and sends the updated packet to the MPLS core network. The packet then takes the LSP, leading to the LER R3 (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. Both ingress and egress routers participate in the establishment of the LSPs before exchange of packets. The LSR swaps label and forwards the packet. They contribute in 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 [6].

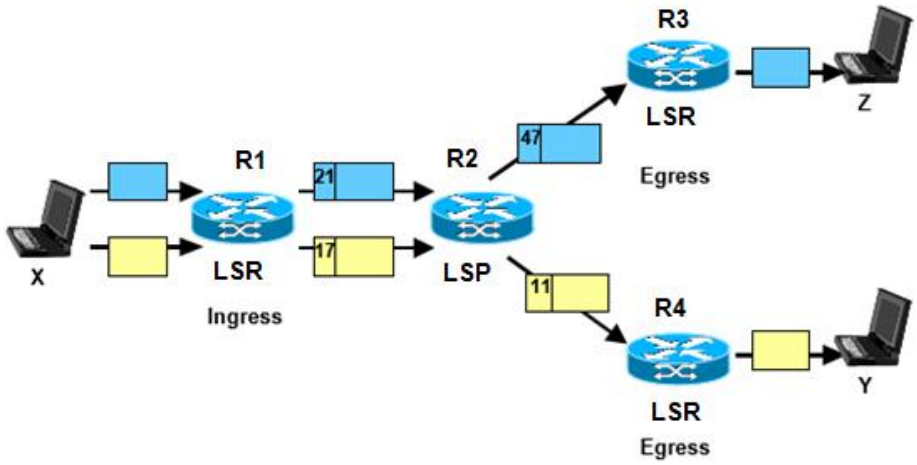

Figure 2-7: Encapsulation in MPLS

2.1.5.3 MPLS Signalling Protocols

The two primary signalling protocols of MPLS are Label Distribution Protocol (LDP) and RSVP.

- **Label Distribution Protocol (LDP)**

  LDP is similar to IGPs (OSPF and IS-IS). LDP runs on top of an IGP configuration and it requires that LDP be configured on all routers' interfaces. After LDP is configured on an interface, LDP begins transmitting and receiving LDP messages. LDP sends LDP discovery messages to all LDP enabled interfaces. When an adjacent router receives the discovery message, it establishes a TCP session with the source router. LDP may also setup new paths using LDP messages after a link failure

- **Resource Reservation Protocol (RSVP)**

RSVP offers TE features that are not available with LDP-signalled LSPs. RSVP is a unidirectional path between the ingress edge router and an egress edge router. RSVP offers possibility to specify bandwidth requirements for an LSP. The two main packet types used are a PATH packet (used to establish a path from the source to the destination) and an RESV packet (used to reserve the resources that will be used in an LSP). After being configuring, the ingress edge router sends a path message to the egress edge router. The path message contains the configured information about the resources required for establishing the LSP. After the egress edge router sends back a reservation message, RSVP path is established. The RSVP session terminates after being idle for 3 minutes and the LSP is lost. Unlike other signalling protocols, RSVP-TE is a soft state protocol. Consequently, the sender must periodically resend PATH messages and the receiver must periodically resend RESV messages to maintain reservations [6, 13].

2.1.6 Network Performance Parameters

To evaluate the network during send any type of traffic the network performance parameters are considered. The following list provides definitions for some network performance that can be used to analysis precise requirements:

1. **Capacity (bandwidth):** The network capability of a circuit or network, usually measured in bits per second (bps).
2. **Utilization:** The percent of total available capacity in use.
3. **Throughput:** Quantity of error-free data successfully transferred between nodes per unit of time, usually seconds.
4. **Accuracy:** The amount of useful traffic that is correctly transmitted, relative to total traffic.

5. **Delay (latency):** Time between a frame being ready for transmission from a node and delivery of the frame elsewhere in the network.
6. **Delay variation:** The amount of time average delay varies.
7. **Response time:** The amount of time between a request for some network service and a response to the request [14].

In this work, four parameters are considered received traffic, Delay, Delay variation and Throughput.

2.2 Related Works

There are many works discuss MPLS. It contributed significantly in enhance network performance and the affect of it in the current enterprise and ISP networks .The large number of the researcher focused on compare the MPLS network with non MPLS considering many factors the performance and security in different situations.

Study[15],which was conducted in the University of Khartoum is based on link utilization using Routing information Protocol (RIP), OSPF and MPLS. They studied main concept of MPLS but they didn't test different types of traffic. They find poor link utilization in both of RIP and OSPF and the MPLS network has ability to handle the incoming traffic, flexible routing .It prefers in core network because not all the devices support this kind of technology. The same result had been reached by Eng. Nousyba Hasab Elrasoul from Alneelain Universit who is applied the MPLS over IPv6 and the result was MPLS Routers has performance better than IP routers. As the previous topics mention above the real time application which is a big challenge does not tested[16].

Another study[1], which conducted in King Fahd University of Petroleum and Minerals is compare the MPLS VPN network using two types of protocols namely Enhanced Interior Gateway Protocol (EIGRP) and OSPF to determine which is faster to transfer video traffic. In the same track the other research analysis MPLS network performance parameters and compare it with traditional IP in the ISP network. They make different

scenarios for test different factors but in the last two works there is no Differentiated Services (DiffServ) applied and they figured out this result; Throughput, delay and jitter are better in MPLS. Inversely, the packet loss is increase in MPLS network which is controllable with TCP packet loss avoidance mechanism[17].

Another works take the security as a main point such as S.M. Blair, C.D. Booth and others they care about the security in real time communication they use appropriate data authentication and encryption methods which is make negligible impact on performance and system operation (delay and jitter), it is recover using device to generate Key which is managed automatically over time. The focused on security field and didn't applied QoS to service different traffic[18].

In the same scope the researcher from Veermata Jijabai Technological Institute (VJTI) studied affect of MPLS using different types of traffic and analysis the packet size ,average packet per seconds and average megabit to reach to MPLS network is faster than traditional network[19].

In the same scope many researchers published new type of comparison they test all cases using IPv4, IPv6 and MPLS network and they test packet delay variation (PDV) in real time traffic. The result of their evaluate IPv6 experiences more PDV than their IPv4 counterpart. They were focusing in single parameter of performance which was PDV .[20]

Even if there is a different through using IP over ATM network to transfer multimedia applications and compare it with MPLS plus deploying QoS support to recover connectionless problem and increase scalability of routing and forwarding[21].

The MPLS give solutions for many problems but the looking for low cost and good quality for services is required the different service is a main factor to improve the network utility .There are many studies about apply QoS over MPLS network such as RSVP to get high performance comparison to non MPLS network and MPLS free QoS although the result was valued and it validate the progressive of apply both of MPLS and QoS

but the DiffServ is desired by Enterprise to get completely utility of network resources which is not tested in these research[2].

CAHPTER THREE

SIMULATION CONFIGURATION

In this chapter, the deep details of simulation CONFIGURATIONS for two networks are presented. They are carried different amount of traffic light and heavy. For a network three scenarios with different routing protocols are created and they called as following: OSPF, MPLS and MPLS_RSVP. All scenarios in same network have the same specifications: environment, number of nodes, amount of traffic and other requirements.

To get this aim, Optimized Network Engineering Tools (OPNET) modeler 14.5 is used. It's very powerful software to simulate heterogeneous network with various protocols [22]. It has been used in many high level researches. There are many features of OPNET such as ability to apply fixed network, various protocols and hardware are available, availability of simulating wireless networks, and it's also used for future researches by adding more things in it. End users and researchers found it useful because it is high level research, network planning and optimization tool.

3.1 Selection of Various Network Components

Because there are many scenarios and they have different settings so, the configuration will categorized to sections explain in following sections.

3.1.1 Devices Selection

In this work many devices are used to create the environments study. Routers, switches, workstations and control nodes are used and the brief specifications of these devices are illustrated below.

Ethernet4_slip8_gtwy node model represents an IP-based gateway supporting four Ethernet hub interfaces, and eight serial line interfaces. It Supported Protocols: UDP, IP, Ethernet, RIP, OSPF, SLIP .it has Port

Interface Description: 4 Ethernet 10BaseT/100BaseT connections and 2 Serial Line IP connections at selectable data rates.

Ethernet16_switch_135_upgrade is connecting point with 17 Interface Fast Ethernet Port.

Ethernet_wkstn node model represents a workstation with client-server applications running over TCP/IP and UDP/IP .It Supported Protocols: UDP, IP, Ethernet, Fast Ethernet, Gigabit Ethernet, RIP, TCP, and OSPF. It has 1 Ethernet connection at 10 Mbps, 100 Mbps, or 1000 Mbps as Port Interface.

Sip_proxy_server model represents a server node which supports SIP UAS service. It also supports other standard applications running over TCP/IP and UDP/IP. It has 1 Ethernet connection at 10 Mbps, 100 Mbps, or 1000 Mbps as Port Interface.

Ethernet_server model represents a server node with server applications running over TCP/IP and UDP/IP. This node supports one underlying Ethernet connection at 10 Mbps, 100 Mbps, or 1 Gbps.

Application Config is node can be used for many specifications. One of it is Application Specifications using available application types. You can specify a name and the corresponding description in the process of creating new applications.

Profile Config is node can be used to create user profiles. These user profiles can then be specified on different nodes in the network to generate application layer traffic. You can specify the traffic patterns followed by the applications as well as the configured profiles on this object.

3.1.2 Links Selection

The100BaseT_base duplex link represents as Ethernet connection operating at 100 Mbps. It can connect any combination of the following nodes: Station, Hub, Bridge, Switch and LAN Nodes. It used to connect workstation with switch.

The PPP_DS1_int is connecting two nodes running IP with 1.544 Mbps as data rate. It used to connect switch with edge Router.

The PPP_E1_int is connecting two nodes running IP with 2.048 Mbps as data rate. It used to connect routers together.

3.2 Profile Configurations

It's remaining the same in all networks and scenarios. Figure 3-1 show the three type of profiles video, HTTP and FTP in all of these profiles are attached the same type of applications video, HTTP and FTP respectively.

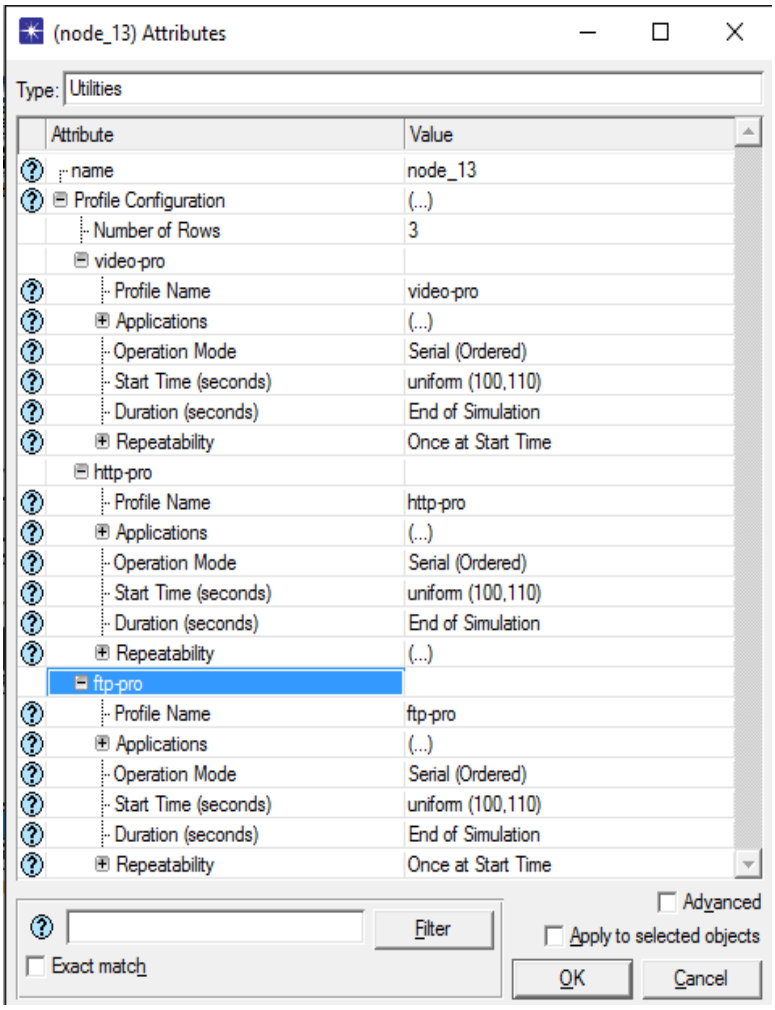

Figure 3-1: Profile Configuration

3.3 Specific Setting for Network Based on Models

Different amounts of traffic are created to initialize various environments. The targeting traffic is video conference and the HTTP and FTP play as background traffic.

3.3.1 Light Network Model

Figure 3-2 shows the light network model which contained 17 nodes.

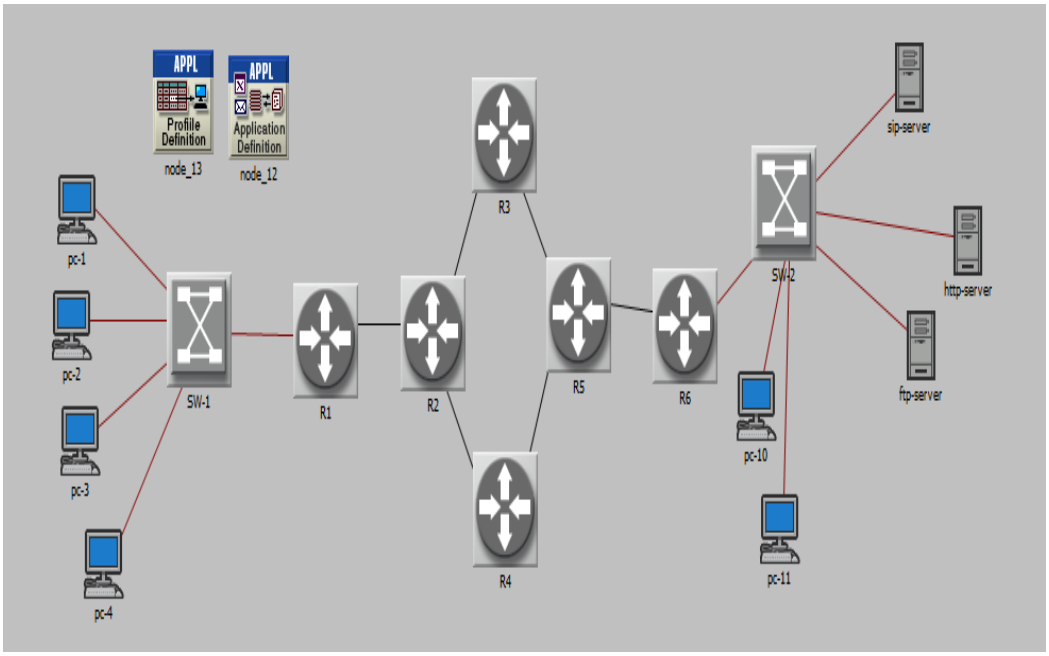

Figure 3-2: Light Network Model

The all types of traffic (video conference, HTTP and FTP) set as light traffic and the settings illustrated in figure 3-3.The name of each type of traffic is assigned and the traffic specifications is set to match the light amount of traffic. And the quantities of traffic will remain the same in all scenarios in the same network.

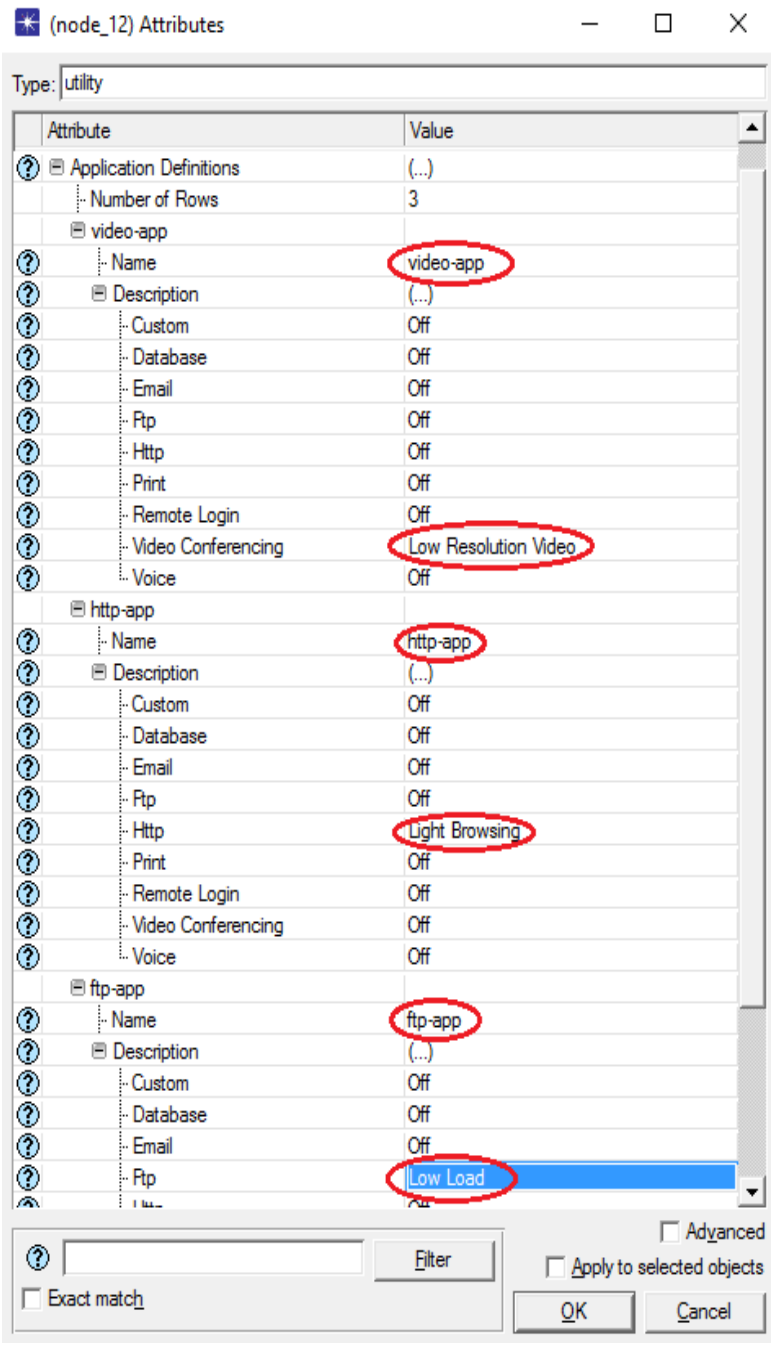

Figure 3-3: Application Definitions for Light Model

3.3.2 Heavy Network Model

Figure 3-4 shows the heavy network model which contained 25 nodes and different setting explain later. The numbers of nodes are raised and the traffic also increased at the application level.

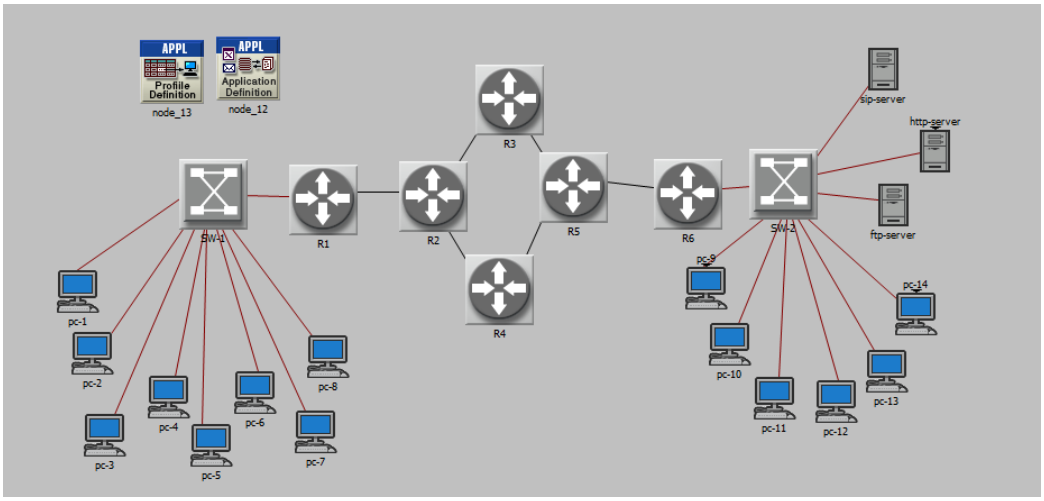

Figure 3-4: Heavy Network Model

Video conference (main traffic) is set as high resolution and its defined setting in OPNET as show in figure 3-5 (a).

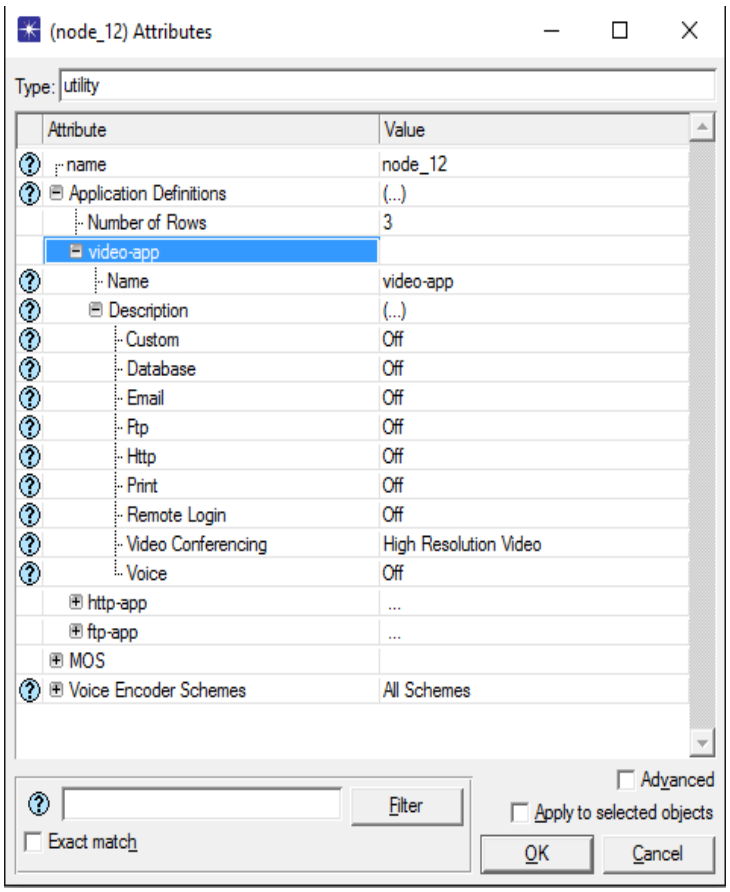

Figure 3-5 (a): Application Definitions for Heavy Model

HTTP traffic (background traffic) is set as heavy browsing. Using small interval and large size of packet the high traffic of HTTP is generated illustrate in figure 3-4(b).

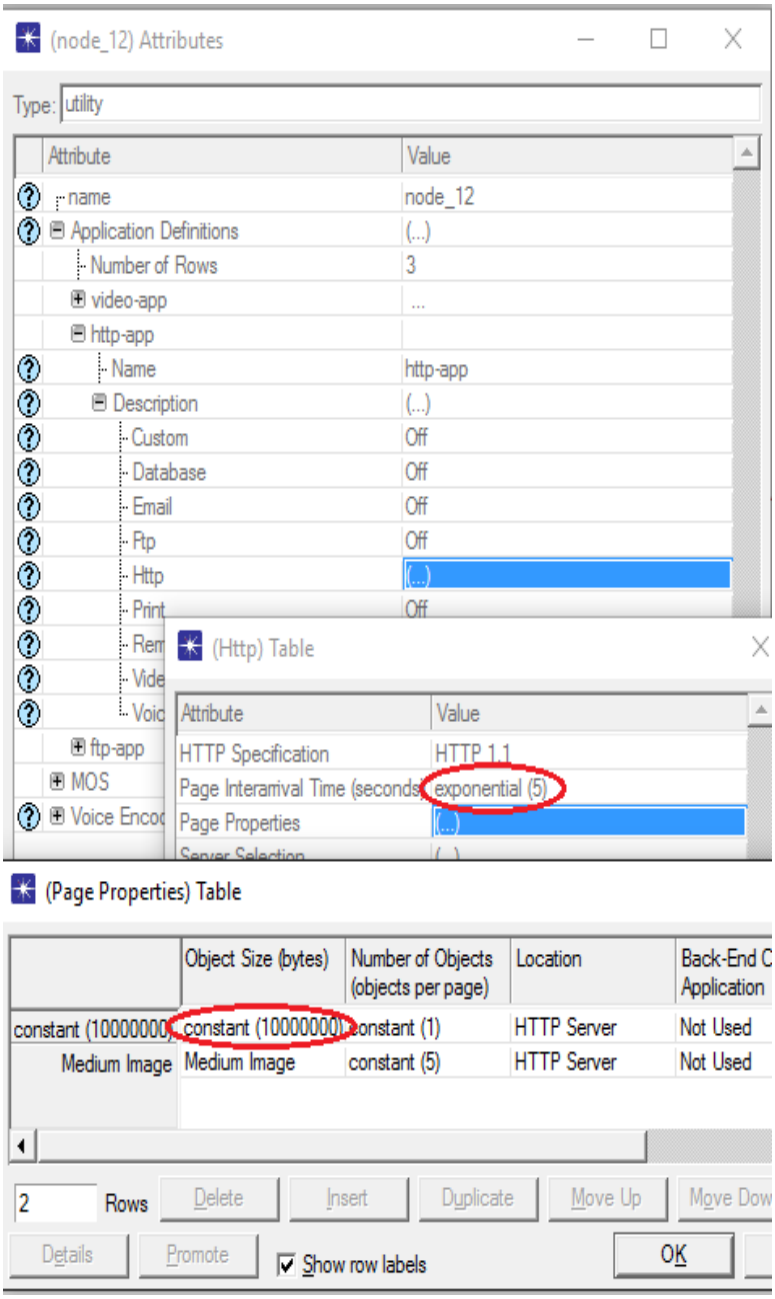

Figure 3-5 (b): Application Definitions for Heavy Model

Figure 3-5(c) represents FTP traffic (background traffic) which is set to be high. The small interval and large size of packet are used to generate heavy load.

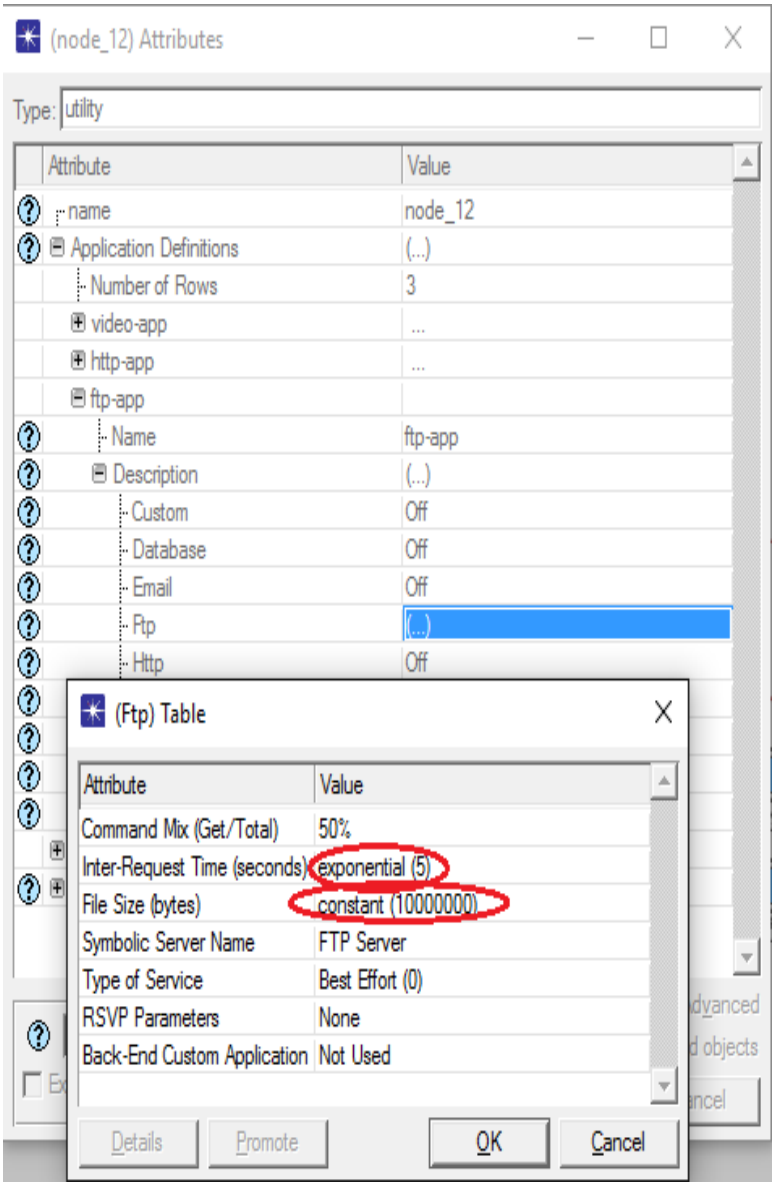

Figure 3-5 (c): Application Definitions for Heavy Model

3.4 Workstation Configurations

Based on applications types the workstation configurations divide on three groups:

3.4.1Group One

The workstations sent all types of traffic. The configuration shows in figure 3-6.Destination preferences and supported profiles are assigned to make these Workstations sending all types of traffics.

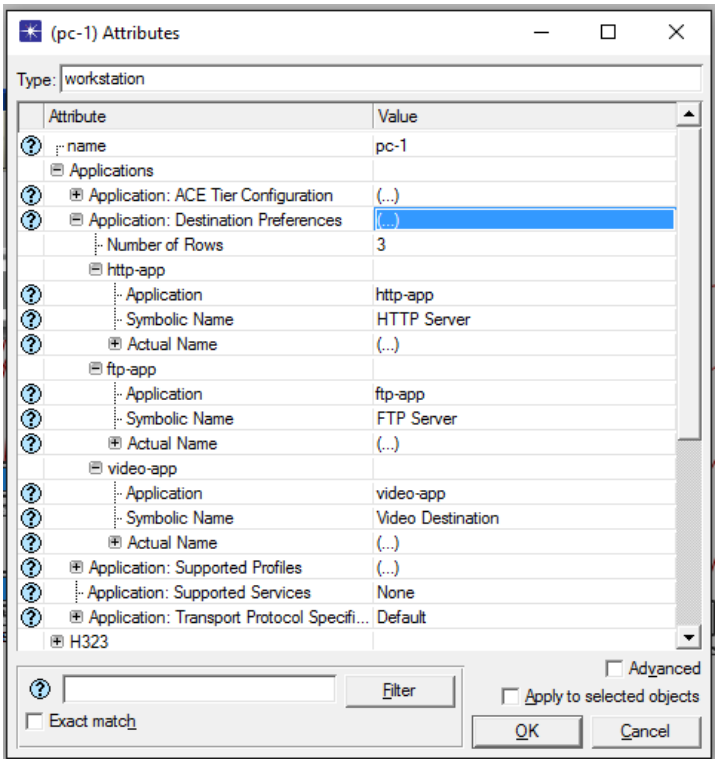

Figure 3-6 (a): Configuration of Workstation to Send all Applications

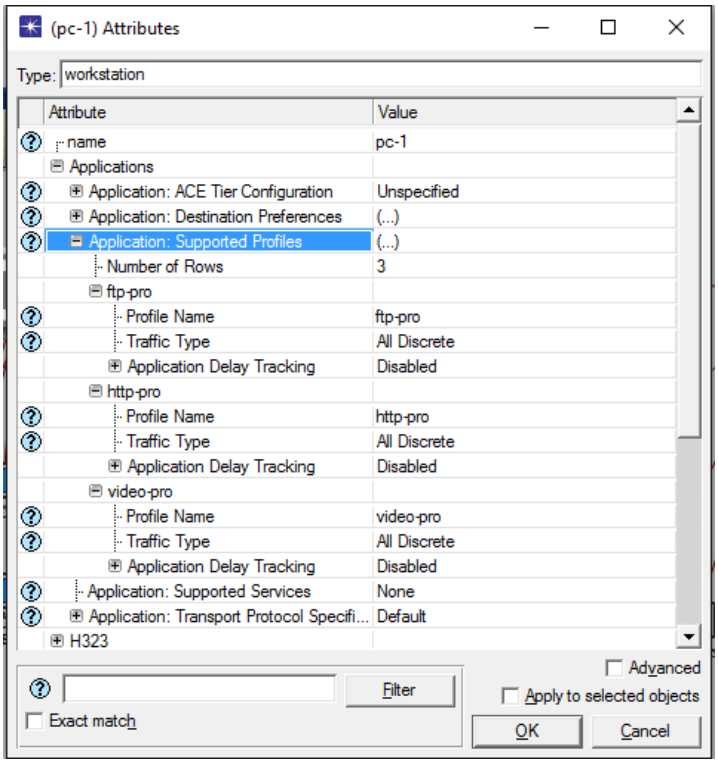

Figure 3-6 (b): Configuration of Workstation to Send all Applications

3.4.2 Group Two

In addition to sending FTP and HTTP traffic the workstations are configure to receive video traffic only .Figure 3-7 represents that configurations where video service is added to be supported.

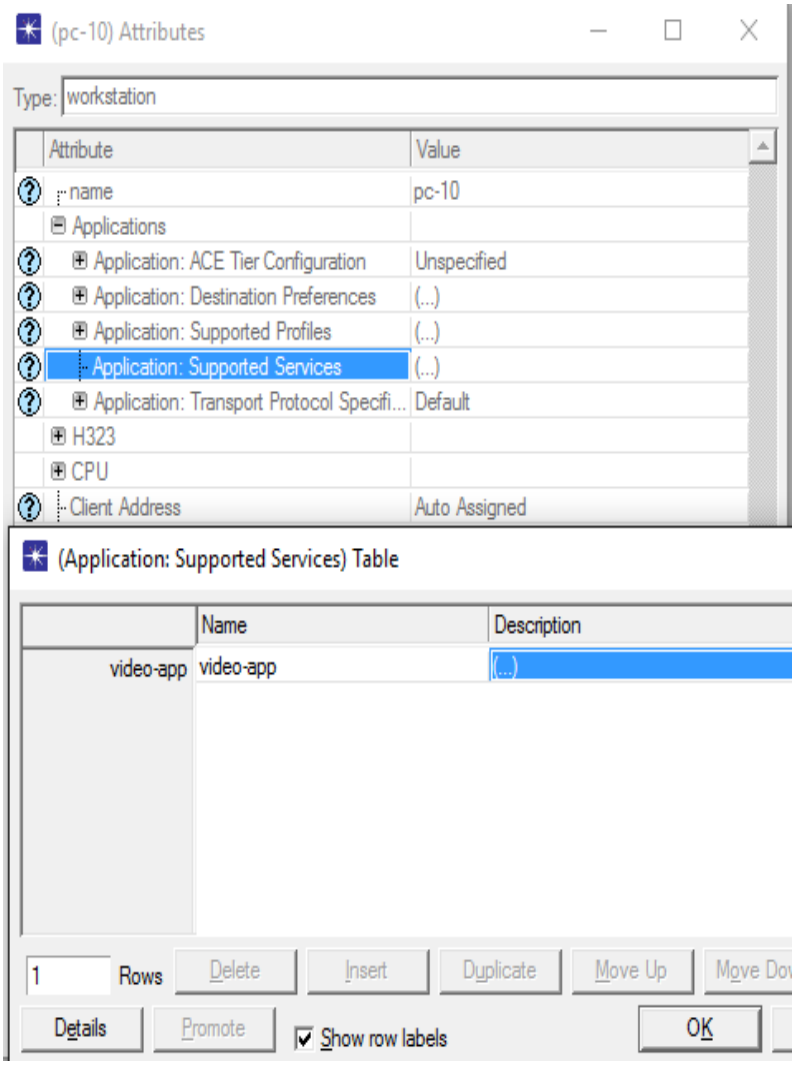

Figure 3-7: Configuration of Workstation to Receive Video

3.4.3 Third Group

The Workstations send HTTP and FTP (Background) traffic only to their servers. No video traffic sending here. Figure 3-8 represents destination preferences and supported profiles where are assigned to make these Workstations sending HTTP and FTP traffic.

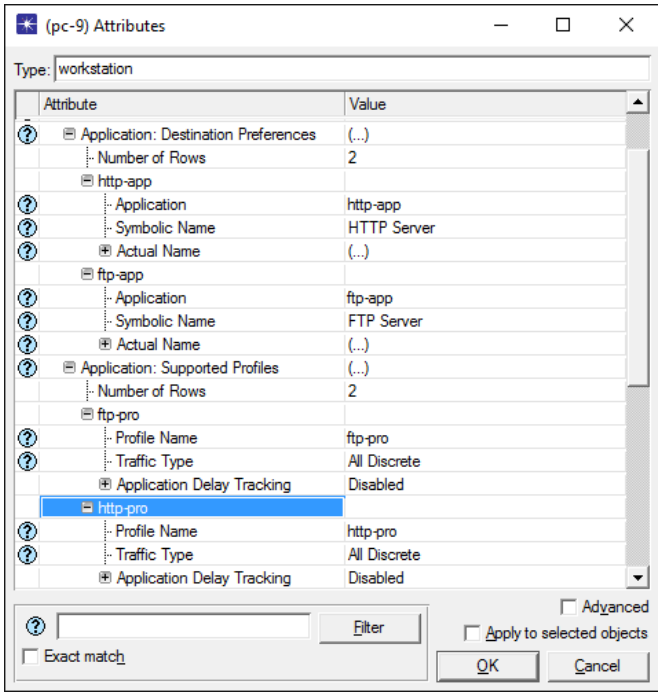

Figure 3-8: Configuration of Workstation to Send HTTP and FTP

3.5 Protocols Configurations

In this work there are three scenarios and they are required different configurations displaying in the next lines.

3.5.1 OSPF Scenario Setting

The IP routing protocol is chosen as OSPF for all connected interface. See figure 3-9.

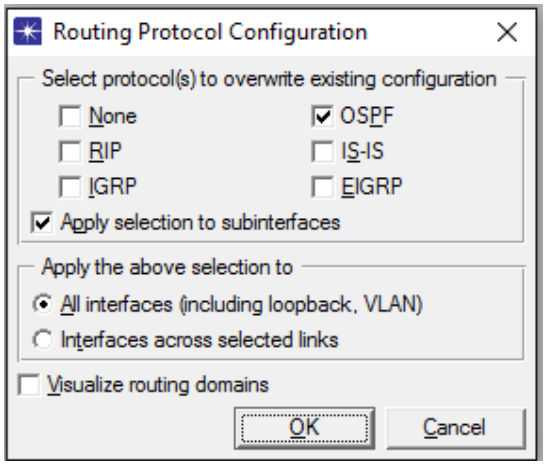

Figure 3-9: OSPF Configuration

3.5.2 MPLS Setting

The Routers are replaced with others that supports MPLS protocol .The **ethernet2_slip8_lsr** node model represents an IP-based gateway running MPLS and supporting up to two Ethernet interfaces and up to 8 serial line interfaces at a selectable data rate.

3.5.3 MPLS-RSVP Settings

QoS applied using **attribute configuration** .It defines details for protocols supported at the IP layer. These specifications can be referenced by the individual nodes using symbolic names. It uses for multiple things .we used it to defines queuing profile Weighted Fair Queuing (WFQ) among different types of queuing profiles.

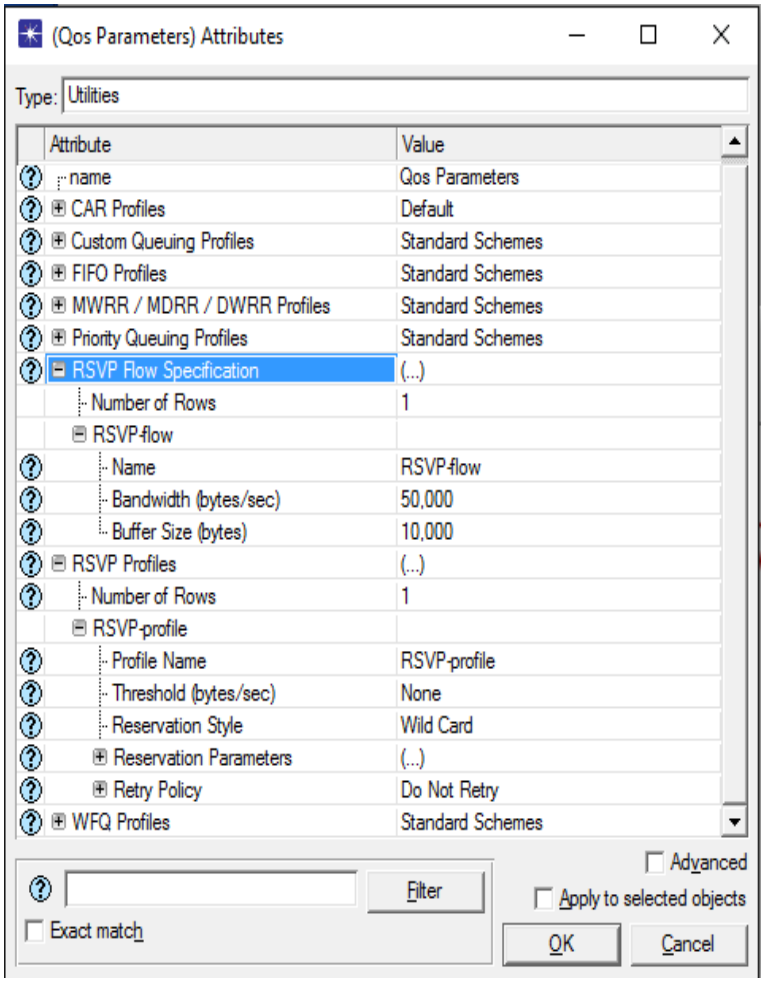

Figure 3-10: QoS Configuration

In the previous figure 3-10, the setting will be in two levels the first one on QoS parameters. The flow name is assigned and buffer size and bandwidth are set. Secondly, the connected interfaces on Routers are set with WFQ as QoS scheme as show in figure 3-11.

Queuing algorithm is a control mechanism used to congestion management and sort the traffic. First In First out (FIFO), Priority queuing (PQ) and WFQ are examples of queuing algorithm.

WFQ applies priority to identify and classify traffic into conversations then determine how much bandwidth each conversation is allowed relative to other conversations. WFQ classifies traffic into different flows based on such characteristics as source and destination address, protocol, and port and socket of the session.

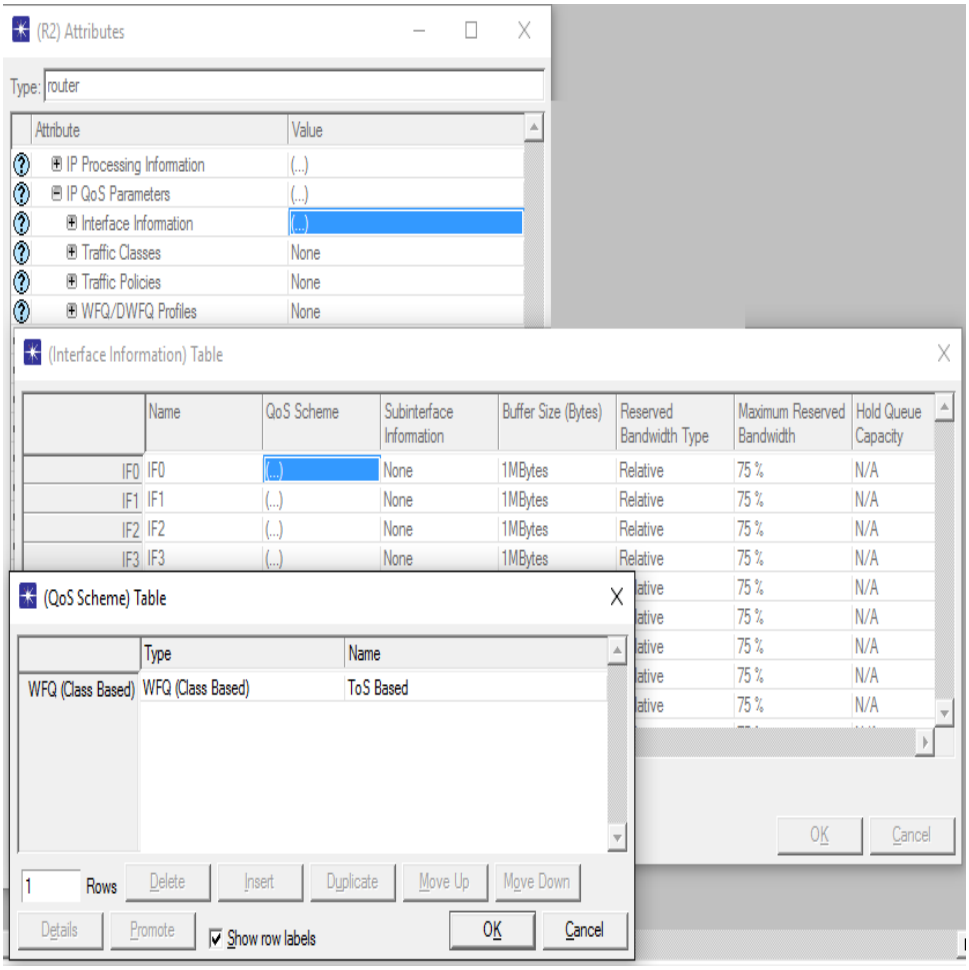

Figure 3-11: Configuration of QoS on Routers

Finally, all interfaces used (connected) are set to enable RSVP as show in figure 3-12.

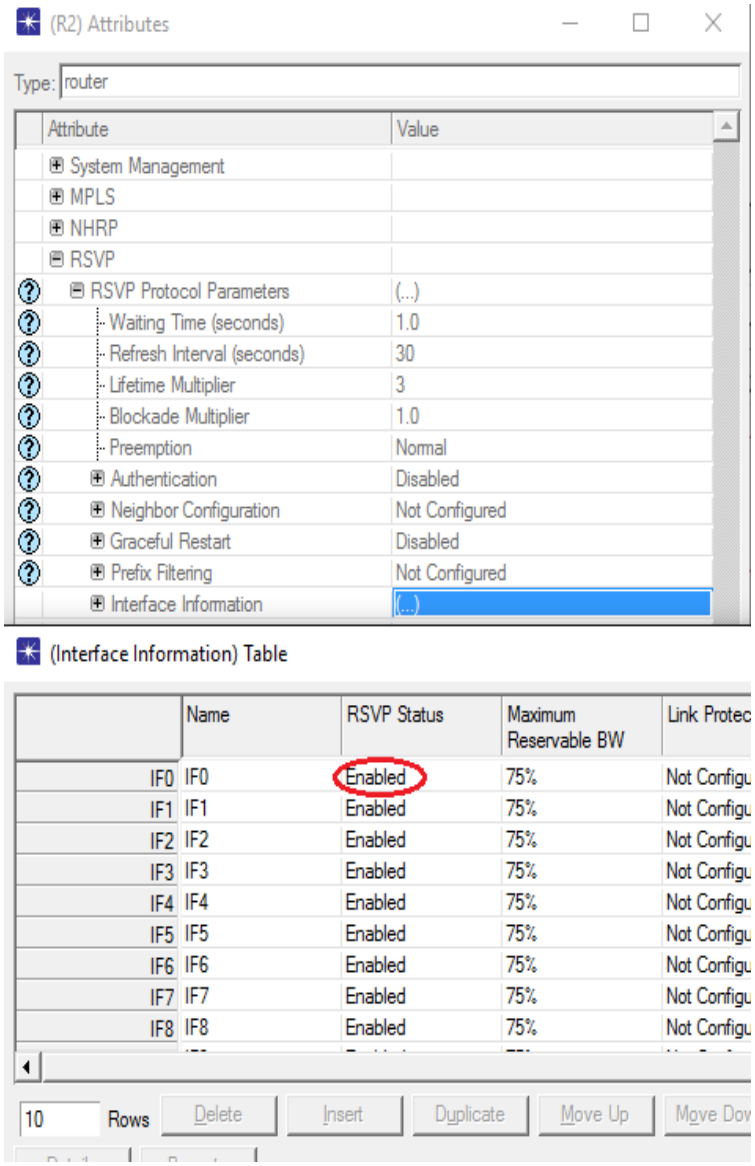

Figure 3-12: Configuration RSVP on Routers

To run RSVP, the additional setting is done to enable RSVP on network level see figure 3-13.

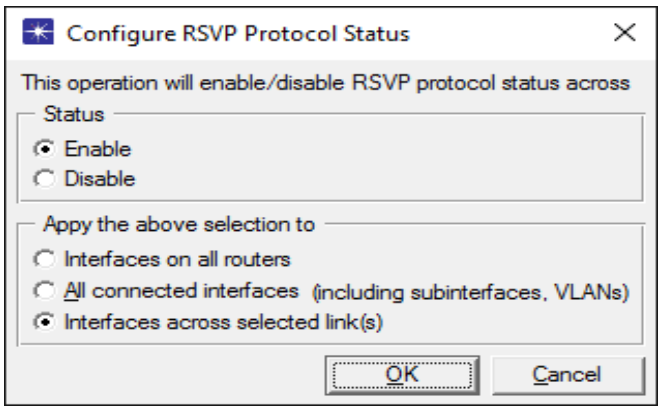

Figure 3-13: Apply RSVP on Network

CHAPTER FOUR

RESULT AND DISCUTION

In this chapter the result of simulation is presented for both design (light and heavy).before that, I am going to explain view points about OPNET as general and our design. The OPNET modeler includes huge number of parameters can measured during simulation run, among these we will chose specific parameters related to our work. Video conference is the main traffic so ,all parameters related to it (traffic sent and receive, delay variation and End-to-End delay), HTTP and FTP are play as background traffic so we view the traffic sent only to ensure there is traffic transmitted across network and throughput of network. Simulation run will work for 30 minutes for all scenarios. The result is displayed as average value for measurements that collected during 30 minutes.

4.1 Light Network Model

The simulation had run for 30 minutes and the result was collected through parameters measurements for various scenarios.

4.1.1 Light Background Traffic

Figure4-1 displays FTP traffic when the setting was low load traffic. Figure 4-2 displays HTTP traffic when the setting was light browser. Those two types of traffic out of study scoop and they are represented only to ensure the design close to real life situation.

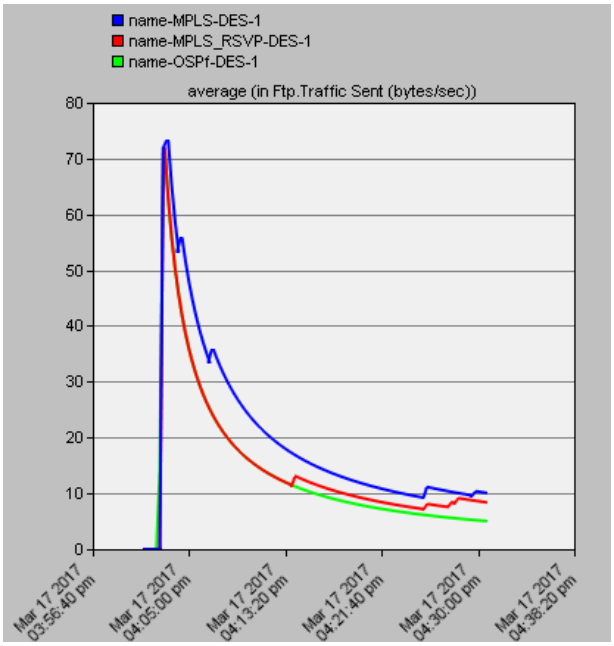

Figure 4-1: FTP Traffic Sent (Light Model)

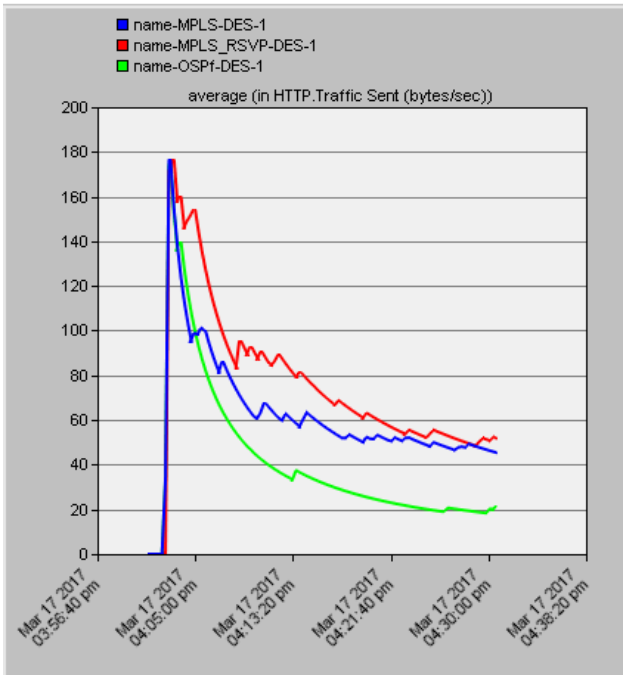

Figure 4-2: HTTP Traffic Sent (Light Model)

4.1.2 Light Video Conference Parameters

There are many parameters used to configure the video conference application and they are discussed in more details later.

4.1.2.1 Light Video Sent and Receive

In figure 4-3, the video conference traffic was sent in different scenarios .it was the same values and take the same shapes in graph with mean value equal 528,000 bps.

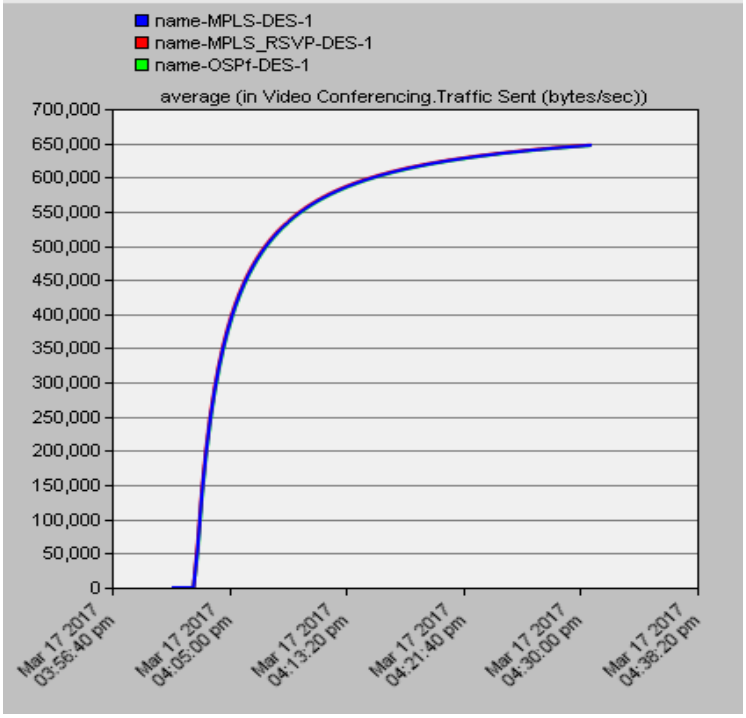

Figure 4-3: Video Conference Sent (Light Model)

The traffic received with different amount and it's clear by looking to figure 4-4.the mean values of video traffic received are 19.006, 243.566 and 264.265 bps for OSPF, MPLS and MPLS_RSVP respectively. MPLS_RSVP scenario gives the high amount of receiving traffic 8.64 % comparison to MPLS scenario. The reason for significantly reduce of received video in OSPF scenario is the high delay which represented in the next section.

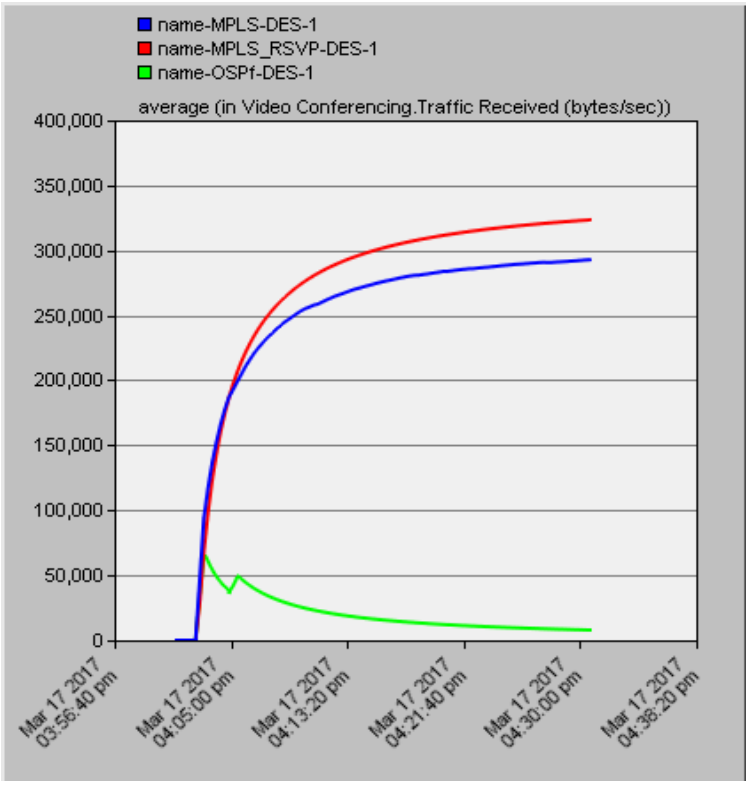

Figure 4-4: Video Conference Received (Light Model)

4.1.2.2 Light Video End-to-End Delay

In figure 4-5 (a), the mean values of End-to-End delay are 0.015, 5.14 and 5.97 seconds in MPLS_RSVP, MPLS and OSPF respectively. MPLS_RSVP gave the minimum delay. It reduced by 99.7% comparison to MPLS scenario. Figure 4-5 (b) represents End-to-End delay in MPLS_RSVP scenario which is closes to zero; because the sender granted the free path to the ultimate destination before start sending. So, MPLS scenario has acceptable delay comparison to OSPF scenario which is committed by shortest path regardless it congestion or not.

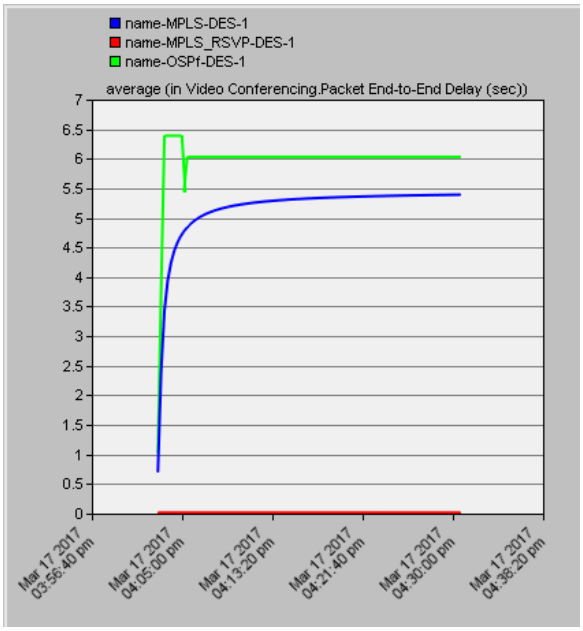

Figure 4-5 (a): Video Conference End-to-End Delay (Light Model)

Figure 4-5(b) shows the actual value for Video Conference End-to-End delay in scenario which applied MPLS_RSVP.

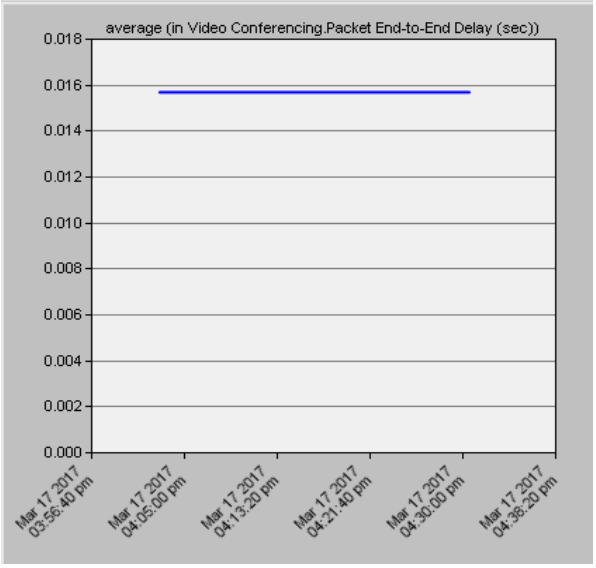

Figure 4-5 (b): Video End-to-End Delay in MPLS_RSVP (Light Model)

4.1.2.3 Light Video Delay Variation

The delay variation gives mean values for MPLS_RSVP is very small (approximately zero), the mean value in MPLS equal 0.913 and 11.19

seconds in OSPF. The reason for this result back to routing process used in MPLS and reserved resources in RSVP.

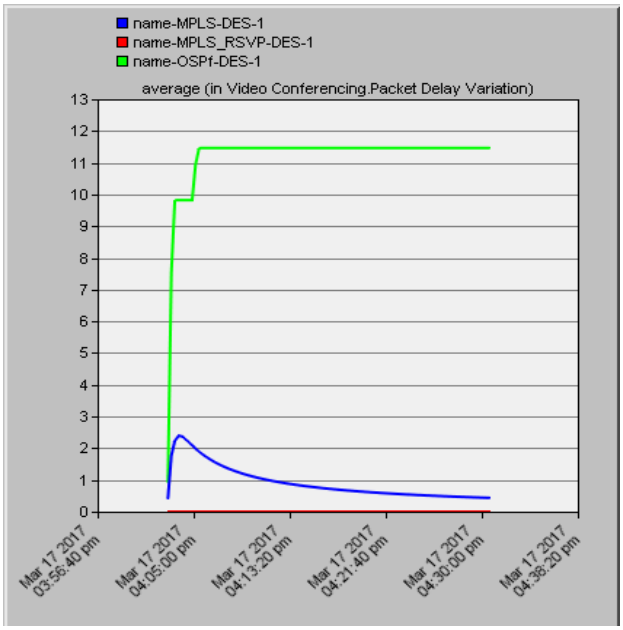

Figure 4-6 (a): Video Conference Delay Variation (Light Model)

Figure 4-6 (b) shows actual value of packet delay variation for MPLS_RSVP scenario.

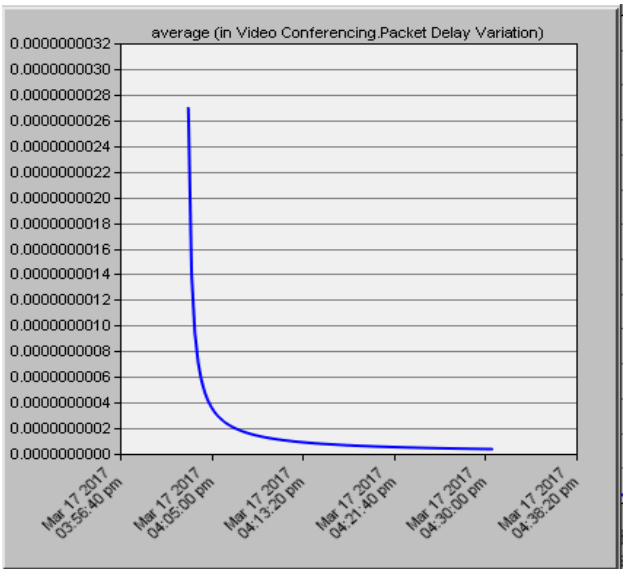

Figure 4-6 (b): Video Delay Variation in MPLS_RSVP (Light Model)

4.1.2.4 Light Video Throughput

MPLS network give us best throughput with mean value equal 1,590,962, 469,347 in MPLS_RSVP and 247,708 bps in OSPF. In MPLS scenario the links are used to transfer traffics does not suffering from updating messages or discovery messages which are the main reason for congesting the link .however, throughput is better in MPLS by three times more than MPLS_RSVP.

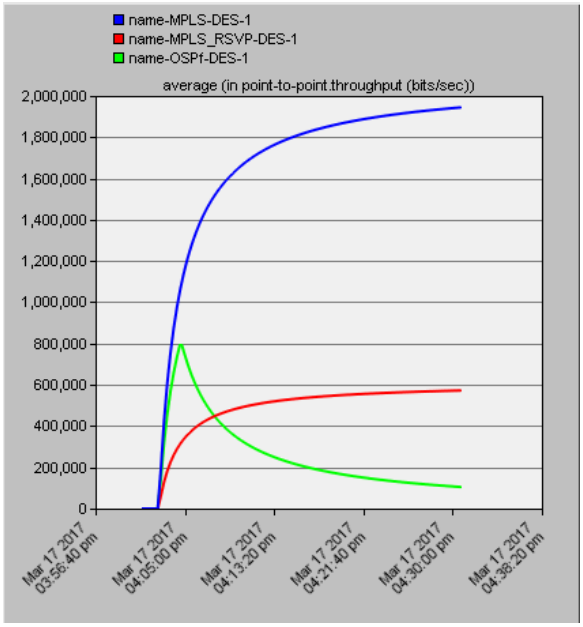

Figure 4-7: Video Conference Throughput (Light Model)

4.2 Heavy Network Model

In this design the high traffic is created considering all types of application are used (video, HTTP and FTP). The traffic sent is huge compare to light traffic. This traffic make network congested and it influence performance parameters.

4.2.1 Heavy Background Traffic

By looking to the previous model, the mean value of FTP is raised from 19.49 to 648,378 bytes/sec as illustrate in figure 4-8.

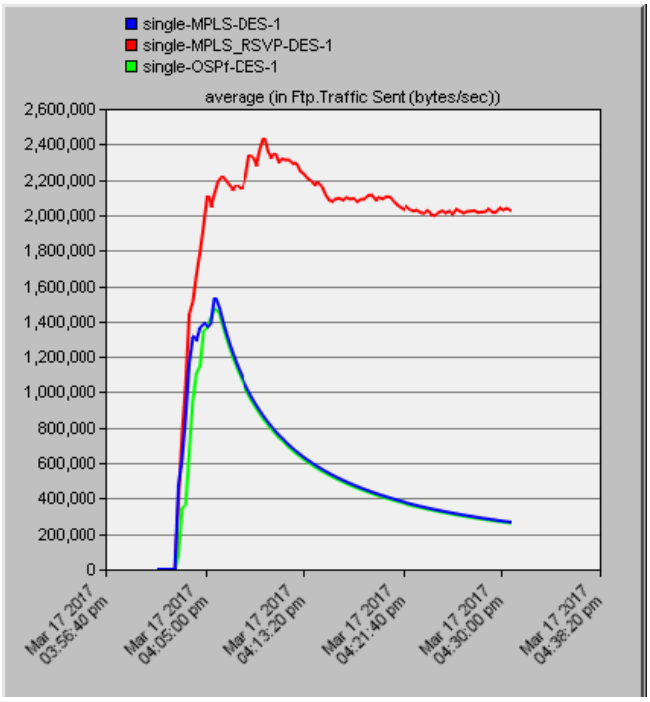

Figure 4-8: FTP Traffic Sent (Heavy Model)

The mean value of HTTP traffic is raised from 60.96 to 597,140 bytes/sec as explain in figure 4-9.

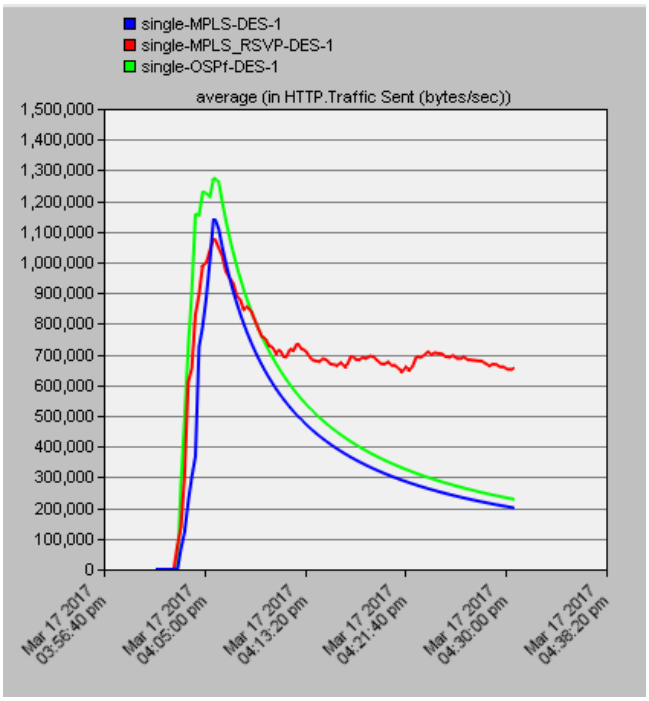

Figure 4-9: HTTP Traffic Sent (Heavy Model)

4.2.2 Heavy Video Conference Parameters

As the description is mentioned for heavy model and it's affect on video parameters. , that effect is presented in following sections.

4.2.2.1 Heavy Video Sent and Receive

Figure 4-10 represents the sending traffic of video traffic which is equal 2,390,457 bytes/sec. It's greater than light traffic by three hundred times which was 528,425 bytes/sec.

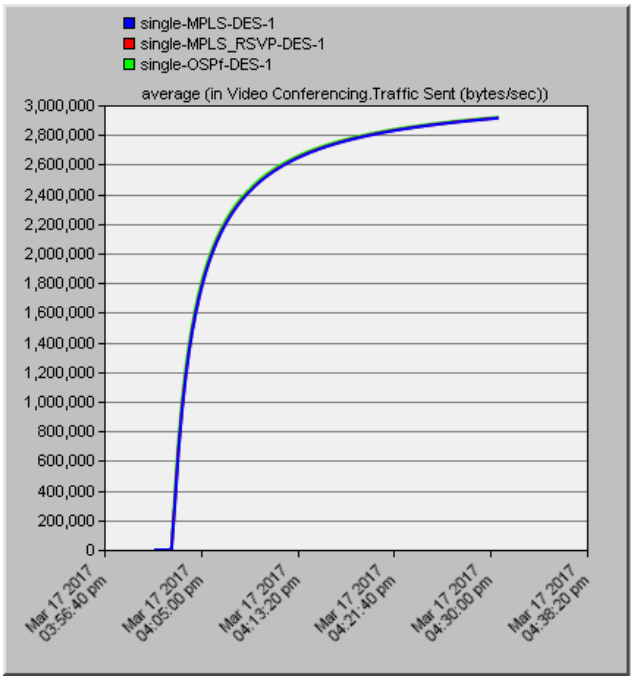

Figure 4-10: Video Conference Sent (Heavy Model)

Figure 4-11 represents the received video traffic which is measure using mean values for every scenario. OSPF scenario has received 1,235,005 bytes/sec (51.66% of sending traffic). MPLS scenario has received 1,217,556 bytes/sec (50.9% of sending traffic).MPLS_RSVP scenario has received 1,497,765 bytes/sec (62.65 % of sending traffic). MPLS_RSVP scenario has enhanced by 21.2% as compared to OSPF or pure MPLS scenario.

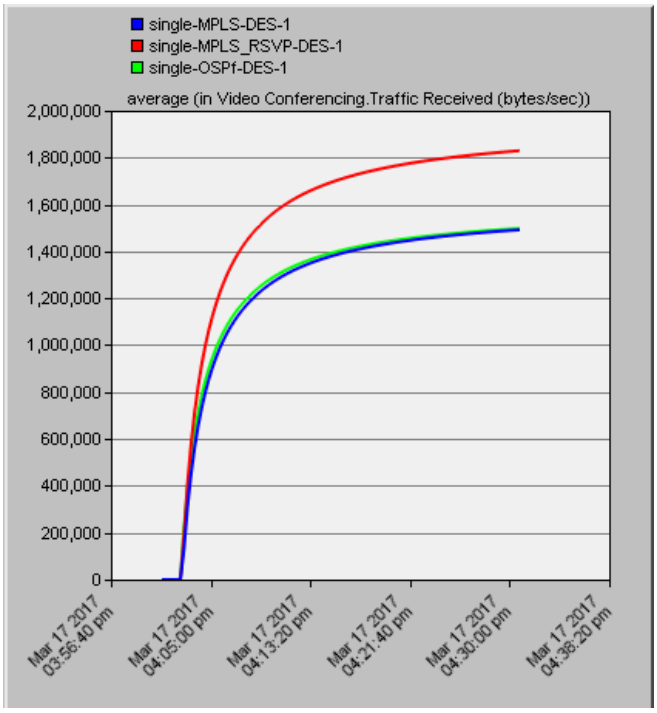

Figure 4-11: Video Conference Received (Heavy Model)

4.2.2.2 Heavy Video End-to-End Delay

End-to-End delay also increase through running time. Its value measured based on mean value. OSPF scenario has 94.84 sec delay. MPLS scenario has 97.02 sec delay .MPLS_RSVP scenario has 19.93 sec delay .MPLS_RSVP reduced End-to-End delay by four times comparison to MPLS scenario. The causes for this result, the mechanism of routing that used on MPLS and the reservation resource which done before start sending.

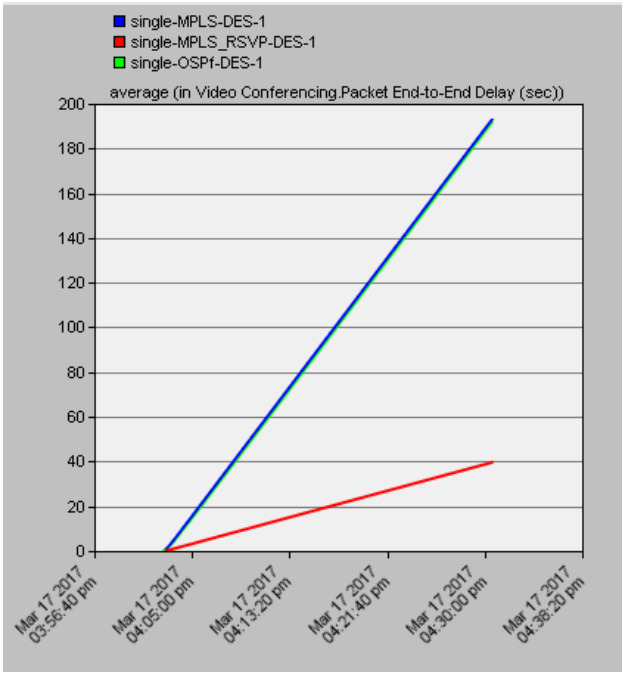

Figure 4-12: Video Conference End-to-End Delay (Heavy Model)

4.2.2.3 Heavy Video Delay Variation

Figure 4-13 represents the delay variation which increases through time of run .All scenarios give the same mean value which equal 1,440.

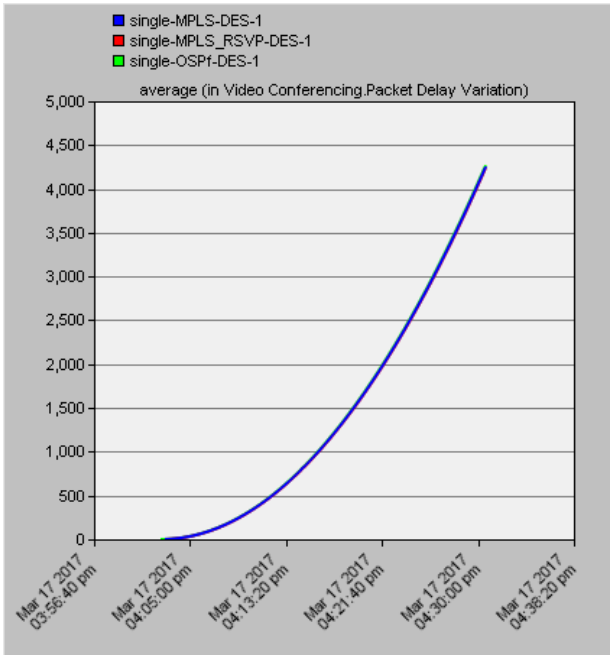

Figure 4-13: Video Conference Delay Variation (Heavy Model)

4.2.2.4 Heavy Video Throughput

Eventually, Figure 4-14 displays small different represents the priority of MPLS_RSVP in throughput measuring with mean equal 7,111 bits/sec and the OSPF give the bad throughput with mean equal 6,378 bits/sec. MPLS scenario give throughput equal 6,955 bits/sec. MPLS_RSVP scenario give enhancement equal 2.24% comparison to MPLS scenario. The values of throughput were close together because the heavy traffic which forced network to use all available paths.

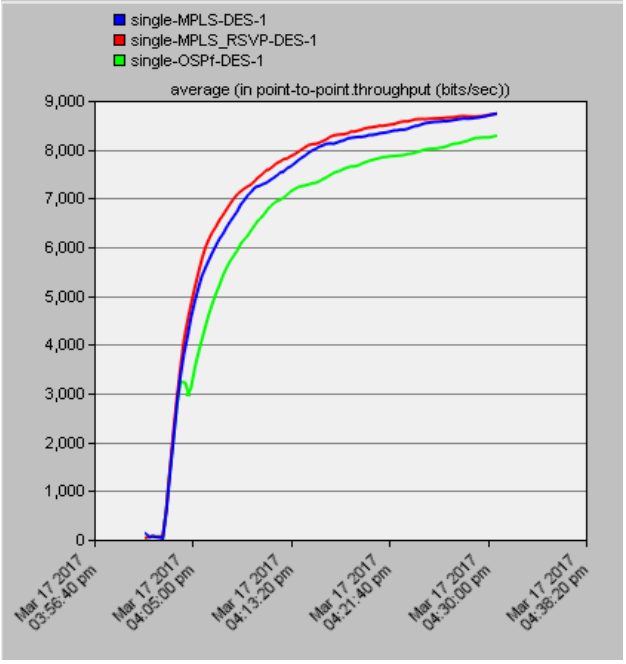

Figure 4-14: Video Conference Throughput (Heavy Model)

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

In this research, OPNET modular is used to investigate and evaluate the performance of OSPF, MPLS and MPLS_RSVP routing protocols considering video traffic metrics for instance delays, throughput and video traffic received. The results are taken after simulate light and heavy traffic models.

After results analysis, it can be said the video conference gives high received traffic in MPLS _RSVP scenario in both models. It is increased by 8.64% in light model and 21.2% heavy model compare to OSPF or MPLS scenarios. Moreover, MPLS _RSVP enhanced the End-to-End delay by 99.7% in light model and reduced four times in heavy model rival to OSPF or MPLS scenarios.

The delay variation measurements in MPLS_RSVP give results very close to others scenarios in heavy model, while it gives optimum result in light model. Pure MPLS gives best throughput in light model while MPLS RSVP gives best throughput in heavy model.

5.2 Recommendations

After finish this thesis, there are many issues for new research areas can be considered.

In this work QoS applied using RSVP which considered as integrated services. Differentiated services can be applied as QoS. Moreover, the analysis could be done for VoIP application instead of Video Conference.

IPv6 consist many features, it can be used with MPLS to improve packet transmission and increase flexibility of payload.

REFERENCES

[1] A. Al Mamun, T. R. Sheltami, H. Ali, and S. Anwar, "Performance Evaluation of Routing Protocols for Video Conference over MPLS VPN Network," *Journal of Ubiquitous Systems & Pervasive Networks,* vol. 7, pp. 01-06, 2016.

[2] O. Akinsipe, F. Goodarzi, and M. Li, "Comparison of IP, MPLS and MPLS RSVP-TE Networks using OPNET," *International Journal of Computer Applications,* vol. 58, pp. 01-03, 2012.

[3] I. Cisco, "Quality of Service Solutions Configuration Guide," *Congestion Avoidance Overview. Cisco, Accessed,* vol. 18, 2014.

[4] A. B. Forouzan, *Data communications & networking (sie)*: Tata McGraw-Hill Education, 2006.

[5] B. A. Forouzan, *TCP/IP protocol suite*: McGraw-Hill, Inc., 2002.

[6] S. Kathiresan, "Performance Analysis of MPLS over IP networks using CISCO IP SLAs," SIMON FRASER UNIVERSITY, 2015.

[7] D. E. Comer, *Computer networks and internets*: Prentice Hall Press, 2008.

[8] J. Deng, S. Wu, and K. Sun, "Comparison of RIP, OSPF and EIGRP Routing Protocols based on OPNET," 2014.

[9] A. M. S.Ahmed, A. Osman, "Comparative Study between OSPF and MPLS network using OPNET Simulation," *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE),* vol. 10, p. 40, 2015.

[10] F. Gonzales, C.-H. Chang, L.-W. Chen, and C.-K. Lin, "Using MultiProtocol Label Switching (MPLS) to Improve IP Network Traffic Engineering," *Proc. Interdisciplinary Telecommunications Program, Spring,* p. 03, 2000.

[11] G. K. A.Albdoor, "Analysis of MPLS and IP Networks Performance to Improve the Qos using Opnet Simulator," *Journal of Emerging Trends in Computing and Information Sciences,* vol. 8, pp. 01-03, 2017.

[12] S. K. Ibrahim and M. M. Al-quzwini, "Performance Evaluation of MPLS TE Signal Protocols with Different Audio Codecs for Voice Application," *International Journal of Computer Applications,* vol. 57, p. 57, 2012.

[13] R. Peterkin and D. Ionescu, "A hardware/software co-design for rsvp-te mpls," in *Electrical and Computer Engineering, 2006. CCECE'06. Canadian Conference on*, 2006, pp. 1409-1412.
[14] P. Oppenheimer, *Top-down network design*, Third ed.: Cisco Press, 2004.
[15] A. A. O. Yousif, S. M. Sharif, and H. A. Ali, "Comparison Between Ngn Core Networks Protocol (Mpls) And Traditional Networks Core Protocols (Rip & Ospf) Using Opnet," pp. 01-12, 2015.
[16] E. N. H. E. A. Algasim, D. Mohamed, A. Amin Babiker, and N. Mustafa, "MPLS Vs IP Routing and its Impact on QoS Parameters," *International Journal of Engineering and Technical Research (IJETR)* vol. 2, pp. 01-02, 2014.
[17] M. Tamboli, M. S. H. Haji, S. Shaikh, M. M. Gite, and M. J. Shaikh, "Comparative study of IP & MPLS technology," p. 05, 2015.
[18] S. Blair, C. Booth, B. De Valck, D. Verhulst, C. Kirasack, K. Wong, *et al.*, "Validating secure and reliable IP/MPLS communications for current differential protection," *DPSP-Developments in Power Systems Protection*, p. 02, 2016.
[19] M. Bhandure, G. Deshmukh, and J. Varshapriya, "Comparative Analysis of Mpls and Non-Mpls Network," *Jurnal. Mumbai: IJERA*, vol. 3, pp. 71-76, 2013.
[20] M. Aziz, M. S. Islam, and A. Popescu, "Effect of Packet Delay Variation on Video-Voice over DiffServ-MPLS in IPv4-IPv6 Networks," *arXiv preprint arXiv:1202.1877*, vol. 3, pp. 01-03, 2012.
[21] C. Kocak, I. Erturk, and H. Ekiz, "Comparative performance analysis of MPLS over ATM and IP over ATM methods for multimedia transfer applications," in *International Conference on Electrical and Electronics Engineering, ELECO*, 2003, pp. 316-320.
[22] M. N. Islam, "Simulation based EIGRP over OSPF performance analysis," Blekinge Institute of Technology,p. 30, 2010.