



**T.C.
ERCIYES UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCE
DEPARTMENT OF COMPUTER ENGINEERING**

**NETWORK PROTOCOLS AND PERFORMANCE
ANALYSIS OF MPLS (MULTIPROTOCOL LABEL SWITCHING)
WITH TRAFFIC ENGINEERING**

**Prepared by
Mustafa Mahmood HAMZA**

**Supervisor
Asst. Prof. Dr. Mustafa DANACI**

M. Sc. Thesis

**July 2017
KAYSERI**

**T.C.
ERCIYES UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCE
DEPARTMENT OF COMPUTER ENGINEERING**

**NETWORK PROTOCOLS AND PERFORMANCE
ANALYSIS OF MPLS (MULTIPROTOCOL LABEL
SWITCHING) WITH TRAFFIC ENGINEERING**

(M. Sc. Thesis)

**Prepared by
Mustafa Mahmood HAMZA**

**Supervisor
Asst. Prof. Dr. Mustafa DANACI**

**July 2017
KAYSERI**

COMPLIANCE WITH SCIENTIFIC ETHICS

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

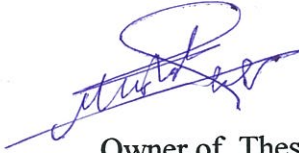


Owner of Thesis

MUSTAFA MAHMOOD HAMZA

COMPLIANCE WITH GUIDELINES

“NETWORK PROTOCOLS AND PERFORMANCE ANALYSIS OF MPLS (MULTIPROTOCOL LABEL SWITCHING) WITH TRAFFIC ENGINEERING” named Erciyes University Graduate Thesis has been prepared accordance with Erciyes University Graduate Thesis Proposal and Thesis Writing Guidelines.



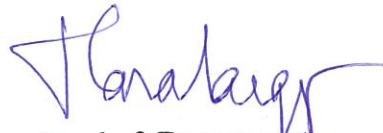
Owner of Thesis

MUSTAFA MAHMOOD HAMZA



Supervisor

Asst. Prof. Dr. Mustafa DANACI



Head of Department

Prof.Dr. Derviş KARABOĞA

ACCEPTANCE AND APPROVAL PAGE

The study called “**NETWORK PROTOCOLS AND PERFORMANCE ANALYSIS OF MPLS (MULTIPROTOCOL LABEL SWITCHING) WITH TRAFFIC ENGINEERING**” has been prepared by **MUSTAFA MAHMOOD HAMZA** supervised by **Asst. Prof. Dr. Mustafa DANACI**, is accepted as a M.Sc. thesis in Erciyes University Graduate School of Natural and Applied Science Department of Computer Engineering by the jury.

18 / 07 / 2017

JURY:

Supervisor : Asst. Prof. Dr. Mustafa DANACI



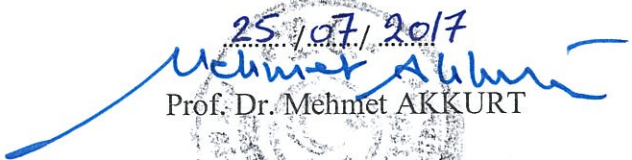
Member : Assoc. Prof. Dr. Bahriye AKAY



Member : Asst. Prof. Dr. Gülay YALÇIN



According to decision dated ...25/07/2017..... and numbered 2017./31-16 acceptance of this thesis is approved by Graduate School Administrative Board.

25/07/2017

Prof. Dr. Mehmet AKKURT
Director of the Institute

Director of the Institute

ACKNOWLEDGEMENT

All profound praise, glory and thanks to Allah Almighty, the most Compassionate and the most Merciful (Subhanahu Wa Taalaa) Who has given me courage and patience and inspired me to carry out this work. Allah's peace and blessings be upon His last Prophet MUHAMMAD.

I would like to thank my supervisor, Assist. Prof. Dr. Mustafa DANACI for his continuous support, encouragement and advice in the course of writing my thesis.

I dedicate this thesis to my father MAHMOOD HAMZA whose support makes my way of success.

I extend my acknowledgement and deep love to my mother for her support, kindness and her prayers which paved my way towards success in life.

I also wish to express my sincere gratitude to my dear wife for her continuous support and help in both good and hard times. Besides I would like to devote this effort for my children.

Finally, my thanks go to the friends who stood with me throughout the study period, and to everyone who helped in a way or another in bringing out this piece of work.

Kayseri, July 2017

AĞ PROTOKOLLERİ ve MPLS (ÇOK PROTOKOLLÜ ETİKET ANAHTARLAMASI) İLE TRAFİK MÜHENDİSLİĞİ PERFORMANS ANALİZİ

MUSTAFA MAHMOOD HAMZA

Erciyes Üniversitesi, Fen Bilimleri Enstitüsü

Yüksek Lisans Tezi, Temmuz 2017

Tez Danışmanı: Yrd. Doç. Dr. MUSTAFA DANACI

KISA ÖZET

Trafik Mühendisliği (TM), ağ performansının veri paketlerinin ağ üzerinden aktarıldığında oluşabilecek ağ sıkışıklığını azaltarak ağ mühendisliğini optimize etmeye çalışır. Çok Protokollü Etiket Anahtarlama (MPLS) veri paketlerinin iletilmesi için yöneticilere rotayı belirleme olanağı veren ve IP ağlarında Trafik Mühendisliği Yönetimi'ni sağlayan modern bir teknolojidir. Paket kaybı ve bekleme süresi gibi Hizmet Kalitesi (QoS) metrikleri, veri paketlerinin uzun mesafeler üzerinden iletilmesi gerekliliğinden beri ilgi alanları olmuşlardır. Trafik Mühendisliği bir çok internet uygulaması için Hizmet Kalitesi sağlamaktadır.

Bu tez; geleneksel IP, Çok Protokollü Etiket Anahtarlama (MPLS) ve Çok Protokollü Etiket Anahtarlama- Trafik Mühendisliği (MPLS-TE) ağları arasındaki elverişli bir karşılaştırma sunmaktadır. Bu tezde, simülasyon hedefi için ağ tasarlamak ve üzerinde uygulamak amacıyla Grafik Ağ Simülatörü (GNS3) kullanılmıştır. Simülasyon sonuçlarına göre; Çok Protokollü Etiket Anahtarlama- Trafik Mühendisliği (MPLS-TE), geleneksel IP ve MPLS'ye kıyasla daha iyi performans göstermiştir.

Anahtar Kelimeler: Geleneksel IP, MPLS, MPLS-TE, QoS, Bekleme Süresi, Paket Kaybı, Sıkışıklık.

NETWORK PROTOCOLS AND PERFORMANCE ANALYSIS OF MPLS (MULTIPROTOCOL LABEL SWITCHING) WITH TRAFFIC ENGINEERING

MUSTAFA MAHMOOD HAMZA

Erciyes University, Graduate School of Natural and Applied Sciences

M.SC. Thesis, June 2017

Supervisor: Asst. Prof. Dr. MUSTAFA DANACI

ABSTRACT

Traffic Engineering (TE) is the feature of network engineering of optimizing network performance by detracting the network congestion that may occurs when data packets being transmitted through the network. Multiprotocol label switching (MPLS) is a modern technology for data packet forwarding, which enables administrators to define routes and ensures the Traffic Engineering Management in IP networks. Quality of service (QoS) metrics such as packet loss and latency are issues of interest since data packets have to be forwarded to the destination over long distances. Traffic engineering (TE) provides Quality of service QoS for various internet application.

This thesis gives the practical comparison the performance between traditional IP, Multiprotocol label switching (MPLS), and multiprotocol label switching–Traffic Engineering (MPLS-TE) networks. In this thesis, Graphic Network Simulator (GNS3) has been used for simulation objective to design and implement the networks. According to simulation results, multiprotocol label switching–Traffic Engineering (MPLS-TE) showed better performance as compared to traditional IP and MPLS.

Keywords: Traditional IP, MPLS, MPLS-TE, QoS, Latency, Packet Loss, congestion.

CONTENTS

NETWORK PROTOCOLS AND PERFORMANCE ANALYSIS OF MPLS (MULTIPROTOCOL LABEL SWITCHING) WITH TRAFFIC ENGINEERING

COMPLIANCE WITH SCIENTIFIC ETHICS.....	i
COMPLIANCE WITH GUIDELINES	ii
ACKNOWLEDGEMENT	iv
KISA ÖZET	v
ABSTRACT	vi
CONTENTS.....	vii
LIST OF ABBREVIATIONS	x
LIST OF TABLES.....	xii
LIST OF FIGURES	xiii

CHAPTER 1

INTRODUCTION

1.1. Introduction	1
1.2. Thesis Goals.....	1
1.3. Thesis Organization	2
1.4. Literature Review	2

CHAPTER 2

MULTI-PROTOCOL LABEL SWITCHING (MPLS)

2.1. Overview.....	5
2.2. The Benefits of MPLS	6
2.3. MPLS Elements.....	7
2.4. MPLS with OpenFlow/SDN.....	11
2.5. Shared Risk Link Groups (SRLG).....	12

2.6. Protection and Restoration in MPLS Networks	12
2.7. Traffic Engineering with MPLS.....	15

CHAPTER 3

NETWORKING AND NETWORK ROUTING

3.1. IP subnetting and calculating	17
3.2. Classful address scheme.....	18
3.3. Network Mask.....	20
3.4. Variable Length Subnet Mask (VLSM).....	20
3.5. Classless Addressing	20
3.6. Classless Inter Domain Routing (CIDR):.....	21
3.7. Subnetting	21
3.8. Routing Techniques	23
3.9. Autonomous System (AS)	23
3.10. Interior Gateway Protocol (IGP).....	25
3.11. Distance Vector	25
3.12. Link state.....	26
3.13. Exterior Gateway Protocol (EGP).....	27
3.14. Comparison between Distance vector and Link state.....	28
3.15. Hybrid Routing Protocols (HRP)	30


CHAPTER 4

SIMULATION AND RESULTS

4.1. Design of network.....	31
4.2. Configuration of networks.....	33
4.3. Simulation results.....	39

CHAPTER 5**DISCUSSION, CONCLUSION AND FUTURE WORK**

5.1. Discussion	48
5.2. Conclusion	49
5.3. Validity Threat.....	49
5.4. Future Work.....	50
REFERENCES	51
CURRICULUM VITAE.....	54



LIST OF ABBREVIATIONS

AS	Autonomous System
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CEF	Cisco Express Forwarding
CIDR	Classless Inter Domain Routing
CR-LDP	Constraint Routed- Label Distribution Protocol
DiffServ	Differentiated services
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
FEC	Forwarding Equivalent Class
FIB	Forwarding Information Base
FR	Frame Relay
GNS3	Graphical Network Simulator
HDLC	high level data link control
HRP	Hybrid Routing Protocols
IGP	Internal Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version
IS-IS	Intermediate System to Intermediate System
ISP	Internet Server Provider
IT	Information Technology
LDP	Label Distribution Protocol
LER	Label Edge Router

LSP	Label Switching Path
LSR	Label Switching Router
MPLS	Multi-Protocol Label Switching
MPLS-TE	Multi-Protocol Label Switching-Traffic Engineering
NNHOP	next next-hop
OSPF	Open Shortest Path First
QoS	Quality of Service
QEMU	Quick Emulation
RIP	Routing Information Protocol
RIPv2	Routing Information Protocol version 2
PLR	Point of Local Repair
RSVP	Resource Reservation Setup Protocol
RSVP-TE	Resource Reservation Setup Protocol-Traffic Engineering
RTT	Round Trip Time
SDN	Software-Defined Networking
SLA	Service Level Agreements
SRLG	Shared Risk Link Groups
SONET	Synchronous Optical Network
TCP	Transmission Control Protocol
TE	Traffic Engineering
TTL	Time To Live
UDP	User Datagram Protocol
VLSM	Variable length subnet masks
VOIP	Voice Over IP
VPN	Virtual Private Network

LIST OF TABLES

Table 3.1. Classes and number of available network/host addresses	19
Table 3.2. Default network mask.....	19
Table 3.3. Comparison between Distance vector and Link state	28
Table 3.4. Comparison of routing protocols	29
Table 4.1. Network Topology Details.....	32
Table 4.2. Routers Interfaces.....	32
Table 4.3. Numerical representation of ping tests.....	43



LIST OF FIGURES

Figure 2.1. MPLS network with Traffic Engineering Enabled	6
Figure 2.2. MPLS header	7
Figure 2.3. Label edge routers.....	9
Figure 2.4. OpenFlow	11
Figure 2.5. Link Protection	13
Figure 2.6. Node Protection	14
Figure 2.7. Path Protection for MPLS TE.....	15
Figure 2.8. Traffic Engineering with MPLS	16
Figure 3.1. Blocks in classes A, B and C	18
Figure 3.2. Block in class D	19
Figure 3.3. Block in class E.....	19
Figure 3.4. Classless Interdomain Routing (CIDR).....	21
Figure 3.5. Dynamic Routing Protocols.....	24
Figure 4.1. Proposed network architecture.....	31
Figure 4.2. OSPF configuration.....	33
Figure 4.3. IP routing table.....	34
Figure 4.4. MPLS design	35
Figure 4.5. Configuration of MPLS and Frame Relay.....	36
Figure 4.6. MPLS IP routing table.....	36
Figure 4.7. MPLS-TE Tunnels	37
Figure 4.8. Tunnel configuration.....	38
Figure 4.9. Tunnel explicit path.....	38
Figure 4.10. Tunnel built up.....	38
Figure 4.11. Simulation Model.....	39
Figure 4.12. Performance analysis between Server 1 and Server 2 on IP network.....	40
Figure 4.13. Performance analysis between Server 1 and Server 2 on MPLS network .	40
Figure 4.14. Performance analysis between Server 1 and Server 2 on MPLS-TE	40
Figure 4.15. Performance analysis between Server 1 and Server 3 on IP network.....	41
Figure 4.16. Performance analysis between Server 1 and Server 3 on MPLS network .	41
Figure 4.17. Performance analysis between Server 1 and Server 3 on MPLS-TE.....	41
Figure 4.18. Performance analysis between Server 2 and Server 3 on IP network.....	42
Figure 4.19. Performance analysis between Server 2 and Server 3 on MPLS network .	42

Figure 4.20. Performance between Server 2 and Server 3 on MPLS-TE network	42
Figure 4.21. Graphical Representation of ping tests.....	43
Figure 4.22. MPLS network without traffic engineering tunnels	44
Figure 4.23. MPLS network without traffic engineering tunnels	44
Figure 4.24. Performance analysis between S1 and S2 on MPLS with TE.....	45
Figure 4.25. Performance analysis between S1 and S2 on MPLS without TE.....	45
Figure 4.26. Performance analysis between S1 and S3 on MPLS with TE.....	46
Figure 4.27. Performance analysis between S1 and S3 on MPLS without TE.....	46
Figure 4.28. Performance analysis between S2 and S3 on MPLS with TE.....	47
Figure 4.29. Performance analysis between S2 and S3 on MPLS without TE.....	47

CHAPTER 1

INTRODUCTION

1.1. Introduction

Considering enormous demand of internet services, traffic engineering is an issue concern at the design scale as well as handling of operations through Internet backbone networks [1]. For this reason, a lot of applications and equipment are being developed to provide better performance. Traffic engineering (TE) is a technique of optimizing network resources and performance by organizing traffic across the network backbone. Traffic engineering determines the routes for traffic flows to traverse the backbone [2]. Network performance indicates to measures of service quality of specific network.

In this thesis, three network architectures have been emulated using Graphical Network Simulator (GNS3). The distributing of Cisco routers is done according to Iraq map. Open Shortest Path First (OSPF) as a routing protocol was used in IP network and as the MPLS core. Wireshark is used as a tool for analyzing the performance between three virtual machines as servers, which connected with each other for transmitting packets. MPLS is evolved through frame relay. In order to increase performance with reduce network complexity and internetworking costs, Frame Relay is exploited between the provider and provider edge routers.

1.2. Thesis Goals

The goal of this thesis is to emulate network architecture to compare the performance of IP, MPLS and MPLS-TE networks. To achieve this goal, following objectives are set:

- 1- Design the architecture for networks using Frame Relay and configure the routers for IP, MPLS and MPLS networks.
- 2- Setup the virtual machines and install Windows XP on all the systems, and connect each other.
- 3- Emulate all the routers and servers in networks architecture.
- 4- Investigate the performance of IP, MPLS, and MPLS-TE networks by conducting three scenarios using simulation.
- 5- Monitor and analyze the simulation results.

1.3. Thesis Organization

This thesis is included five chapters. Chapter two presents an introduction of MPLS architecture, the basic functionality of MPLS that could be utilized for traffic engineering. Additionally, includes common failures in MPLS networks, determination of failure detection and some recovery techniques for MPLS networks.

Chapter three, includes an overview of IP addressing, routing Techniques, routing protocols, and comparison between routing protocols.

The details of simulation architecture, configurations and results are contained in chapter four.

Chapter five presents the conclusion that is investigated and drawn from the analysis of the simulation results, discussion and Validity Threat. This is followed by a brief description of the opportunities for further research in the future.

1.4. Literature Review

This part provides a presentation of scientific references that specify the performance of MPLS. There are some parameters need to measure for network performance such as throughput, bandwidth, latency, and jitter. These parameters commonly estimated using network simulator like ns2, ns3, OPNET, and OMNEST. The following is a brief review of some related works in the literature of each study in terms of its goals, importance and the conclusions.

N. Aslam [3] presented implementation and comparison between IP and MPLS. Authors selected two scenarios and used MATLAB to develop a code to perform the comparison. The results of this simulation concluded that the MPLS is a good technique for traffic engineering, and performs better than IP networks.

The main objective of [4] the essential goal of this study is to implement comparison of MPLS and traditional IP in respect of VoIP. OPNET is used to assess the minimal number of VoIP calls maintained in both MPLS and IP networks. The simulations consisted of two scenarios considering the background traffic. The results of simulation explained that the MPLS with traffic engineering reduces the congestion in the network and takes less delay compared to traditional IP.

O. Akinsipe et al. [5] presented the modelling of IP, MPLS and MPLS RSVP-TE networks and the performance parameters of the networks are compared in this study. Authors used OPNET modeler for simulation and the comparison is done for parameters such as throughput, utilization and voice jitter. They concluded that the MPLS network performs better than other networks in terms of utilization while the MPLS RSVP-TE network provides best performance for voice traffic due to the reserved path and the MPLS networks provide better performance for voice traffic than traditional IP networks.

M. Bhandure et al. [6] presented an overview of MPLS technology and attached IETF standards. The authors compared the performance of MPLS and traditional IP routing networks without discuss to the traffic engineering, which is the fundamental portion of MPLS.

A. Sulaiman and O. Alhafidh [7] evaluated the performance measures for various types of traffic (VoIP, Video Conference, data) in their forward in the case of network congestion for both MPLS-TE and traditional IP network. Authors used OPNET modeler to create the topology to simulate both networks. The results of this simulation concluded that the MPLS-TE performed best solution as well as in the case of heavy load, and the networks wich used OSPF routing mechanism is not efficiently dealing the flowing traffic.

M. Kumar et al., [8] implements resources in the MPLS network and compared the analysis based on traffic engineering metric for both MPLS-TE and conventional IP networks. The authors used OPENT for simulation of comparison. The result of simulation observed that MPLS-TE performed better than traditional IP network model, as well as in the case of heavy load. S. Kathiresan, [9] emulated an architecture using GNS3. CISCO IP Service Level Agreements (SLAs) used to generate VoIP traffic and analyze the performance of MPLS over IP network such as latency, round-trip time (RTT), and mean opinion score (MOS). Author considered background traffic in the simulation. The simulation results showed that the MPLS is the better technique for traffic engineering than IP.

Akshay ad P. Ahlawat [10] presented the theoretical comparison between traditional IP Networks and MPLS. The comparison is made on focusing on Quality of Service (QoS), traffic Engineering (TE), scalability, overlapping IP addresses. Authors concluded that MPLS has significant advantages over traditional IP networks and provides the best solutions.

Charles N. et al. [11] compared the performance of each of IP, MPLS and MPLS-TE on the same congested WAN design. Authors used MPLS VPNs and BGP to the buildup of the control plane. Ping tests are used to measure the latency (RTT) and Wireshark to monitor packet loss. The results presnted that MPLS with traffic engineering had less latency and without any packet loss.

CHAPTER 2

MULTI-PROTOCOL LABEL SWITCHING (MPLS)

2.1. Overview

MPLS is a technology for forwarding packets through a network using information included in labels linked to IP packets. The main issue of MPLS is to make a resilient networking structure that provides enhanced performance and stability [12]. MPLS classify and identify IP packets at the ingress node with a label; routers use these labels to forward the packets. These forwarding decisions based on labels instead of analyses routing table and do not use the network layer addresses. Therefore, decrease usage of CPU on routers.

Packet forwarding in MPLS network enhances a service provider network, especially Virtual Private Networks (VPNs), guaranteed quality of service (QoS) across an MPLS network and for traffic engineering (TE). MPLS technique is interest more for providers to the massive users that have multiple levels of service and needed guaranteed QoS to share service traffic with other VPN users. An IP router performs both control and forwarding elements. The control element consists of routing protocols like OSPF, BGP, used to establish the routes and trade routing information between IP routers. The forwarding elements consist of procedures that routers use for making transmission decisions over an IP packet [13]. Therefore, the demands of IP routers are continuous from control and forwarding plane to optimize availability to construct modern routers. In MPLS network, the LSRs consider IP routers, which run the MPLS protocols.

2.2. The Benefits of MPLS

- MPLS provides traffic engineering.

The traffic engineering steers and managing the MPLS data flow through distributing it to the bandwidth. Traffic oriented objectives deal with decreasing traffic loss, delay and jitter, increasing throughput and realization of Service Level Agreements (SLA) [14]. With traffic engineering performed in the MPLS, the traffic can be spread more equally over the links in the network and make more use of underutilized links [15], as shown in Figure 2.1.

- MPLS supports Quality of Service (QoS) by setting up explicit paths or routers in the network. MPLS networks already included QoS. Thus, the marked packets transmitted with a high quality and low latency for voice and video.
- The Use of Standardized Network Infrastructure, the architecture of MPLS is flexible and could work in any combination of Layer 2 techniques. Supportive MPLS is available for all Layer 3 protocols. Typically, scaling is possible in today's networks . Using the MPLS with IP, the possibilities could extend as many as ISP (Internet Server Provider) want. The labeled packet supports carrying other protocols such as IPv4, IPv6, Point-to-Point, high-level data link control (HDLC), etc.

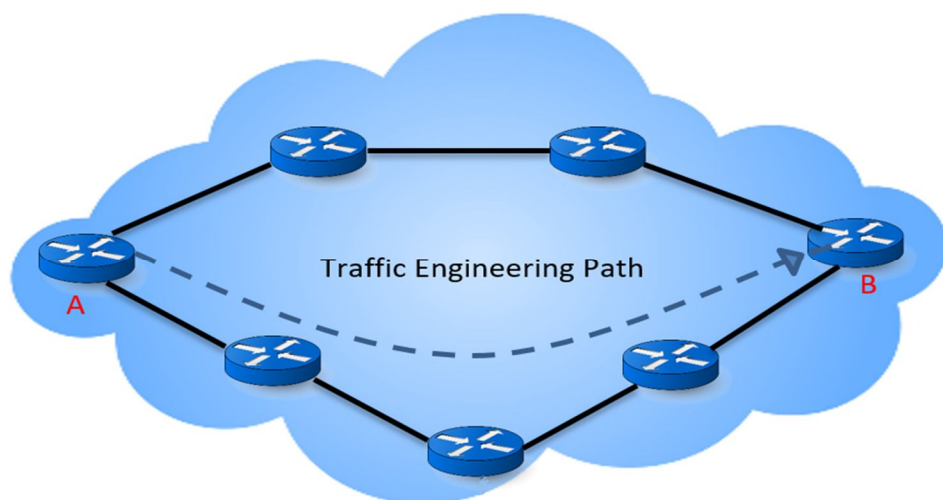


Figure 2.1. MPLS network with Traffic Engineering Enabled

- Virtual Private Network (VPN). Using the MPLS providers can create VPN networks at Layer 3 for multiple customers over the same network topology. Most Layer 3 VPNs based on the (MPLS). The publicity of Layer 3 VPN technique based on its ability to satisfy the requirements of customers and providers [16]. MPLS provides secure and powerful network due to its flexibility and simplicity for maintenance.

2.3. MPLS Elements

2.3.1. MPLS header

MPLS header located between the Layer 2 Header and IP packet of the packet as shown in Figure 2.2.

The MPLS header consists of 32 bits. The first 20 bits are dedicated as label bits; it forwards packets in MPLS, this value as an index used for look-up in MPLS table. The second 3 bits are specified as experimental used for DiffServ support on MPLS networks and bring the IP precedence value from IP packet. Cisco used this field to define a class of service (CoS). The Bottom of Stack (S-bit) is set on the bottom header used to indicate the bottom of the stack has been reached. The bit 1 means the last label in the packet. The time to live (TTL) used the last 8 bits. This field is used for loop prevention and possible path tracing in the MPLS cloud. This value decrements with each hop and packet discards occur at a zero value.

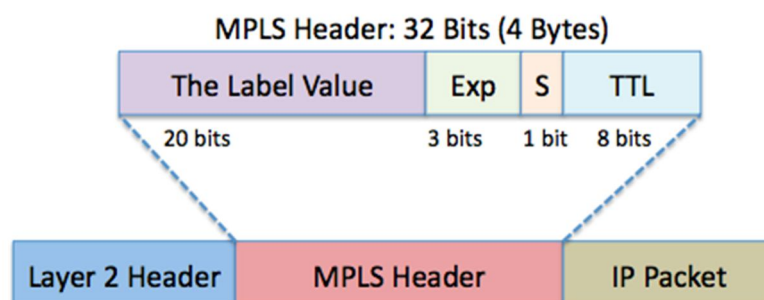


Figure 2.2. MPLS header

2.3.2. Label Stack

MPLS routers sometimes require more than one label of the packet to travel. MPLS allows carrying multiple labels on the packet, which regulated as a stack, through the MPLS network, that is done by packing the labels into the stack.

The MPLS label stack header is located between the Layer 2 header and the Layer 3 payload, the transmitter router indicate to the receiving router that the packet being transmitted is a labeled packet not the native IP packet.

2.3.3. Label Switch Routers (LSRs)

An MPLS network classified into label switching routers (LSR) and Label Edge Routers (LERs). The essential function of the Label Switch Router is to send packets between edge routers through MPLS domain in high speed. Label Switching Router (LSR) is an IP router that has the ability to run the protocol of MPLS. LSRs receive the labeled packets, exchange them with an outgoing one, and transit the new packets to the destination.

2.3.4 Label Edge Routers (LERs)

An MPLS network must have edge routers, which are the point where a native IP packet attached with an MPLS label; these routers known as label edge routers (LERs) [17]. They handle the input and output of information in the MPLS network. The main task of LERs is to assigns and attaches labels to the packets based on the information the packet carries and sends the packet to the network, then removes the attached labels on the packets to leave the MPLS network.

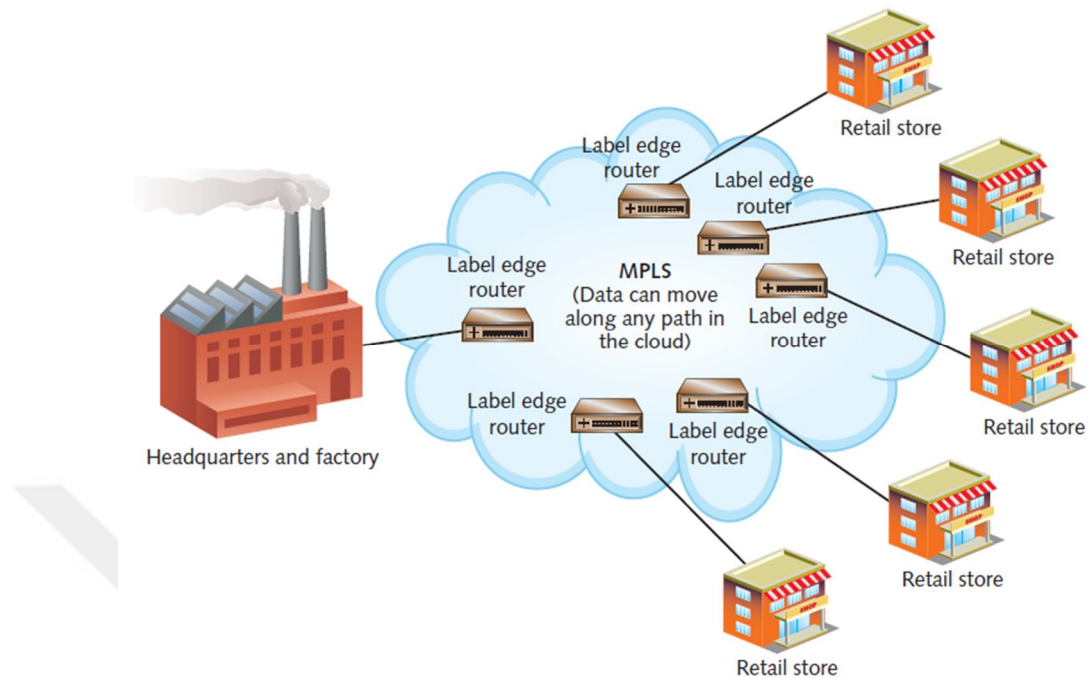


Figure 2.3. Label edge routers [18]

In the MPLS network, all LERs can automatically communicate with each other's, because connections are not dedicated along a specific circuit, but instead use label information to be able to move along any place in the cloud [18], as shown in figure 2.3.

2.3.5 Label Switch Path (LSP)

In MPLS networks, IP packets are forwarded along a Label Switched Path (LSP) established between ingress Label Switched Router (LSR) and egress Label Switched Router (LSR). The labeled packets are switched through LSPs. LSP is a path between Provider Edge routers (PEs) that the packets are forwarding cross the MPLS backbone. LSP can Replace the existing label with a new label, when an LSR performs an MPLS lookup.

Additionally, LSPs can be manually established in networks to maintain QoS guarantee and to provide other services.

2.3.6 Forwarding Equivalence Class (FEC)

The routers forward an IP packets according to its prefix. In a given router, the group of all address source and destination that have the same way indicates to as the Forwarding Equivalent Class (FEC) and packets that belong to the same FEC, have the same output interface. In MPLS technology, each FEC is associated with a different label. This label is a short fixed length identifier and has local importance. The FEC built from the information taken from IGP.MPLS label is useful for the identification of the output interface of an IP packet without having to look up its IP address every time in the forwarding table [13].

2.3.7 Label Distributions

Labels can be static or distributed by label distribution protocols (LDP). LDP is the most widespread label distribution protocol. The labels are distributed and used to encapsulate ingress traffic through an MPLS networks. This encapsulation mechanism indicates to as pushing labels [19]. In MPLS networks, Constraint-based routing label distribution protocol (CR-LDP) used to set up a clear way and to create tunnels.

MPLS routers must have a method to distribute labels between LSRs. MPLS does not determine by single label distribution protocol. Label distribution protocol (LDP) and resource reservation protocol – traffic engineering (RSVP–TE) are the widespread protocols for the distribution of labels. LDP used to create and exchange label bindings between two LSPs correlated with a particular FEC.

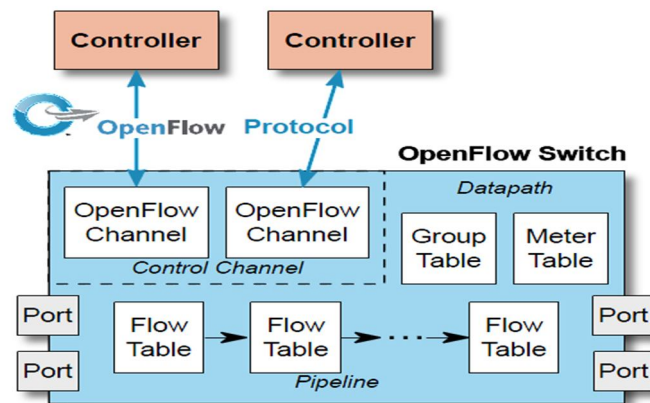


Figure 2.4. OpenFlow

2.4. MPLS with OpenFlow/SDN.

2.4.1. OpenFlow (OF)

An OF Switches consist of flow tables and a group tables, which implement packet look-ups and forwarding, and OF channels to an exterior controller. The switch connects with the controller; the controller manages the switch by the OF switch protocol as well as it can manage flow entries in flow table. As shown in figure 2.4 [20]. (OF) is a choice for a control protocol in Software-Defined Networking (SDN) and the most prevalent. As (OF) presently evolves, the modern releases are more robust, as their features support IPv6, MPLS, etc. [21].

2.4.2. Software-Defined Networking (SDN):

A packet-flow is a rational combination between packets that are portions of the same connection and are given the same processing in the network.

To recognize the various elements of SDN, the essential terminology can be described bottom-up as: Forwarding Devices, Data Plane, Southbound Interface, Control Plane, Northbound Interface, and Management Plane [22]. SDN is the architecture separates the network control from forwarding functions, and the network control dominance the application and network services. This architecture is dynamic, flexible, manageable, and cost effective. OpenFlow protocol is an essential element for constructing SDN solutions [23].

2.5. Shared Risk Link Groups (SRLG)

In MPLS-TE, SRLG is a collection of links share the same risk of failure, which belongs to same SRLG. A link might be a member of multiple SRLGs; the SRLG of path in LSP is the group of SRLGs for all links in the path. SRLG is a feature which able the user to build the backup secondary LSP which is disjoint from the primary path. Therefore, when calculating the secondary path for an LSP, it is best to find a path both secondary and the primary path do not have sharing links. This guarantees that a failure on a specific link does not effect the primary and secondary paths in LSP [24]. SRLG mechanism is same the MPLS admin sets, to announce SRLG. SRLG one of the most important criteria related with the route calculation, by using these criteria, user could choose a route taking into account logical structure and physical resources.

2.6. Protection and Restoration in MPLS Networks

MPLS rapid reroute equips protection for the traffic following links or node failures, in times are practically non-discoverable. This is the main demand for transporting sensitive traffic like video or voice and is an important structure block for associating all services on to the MPLS domain.

Applied jointly with traffic engineering, fast reroute is able ensure obligation to accurate QoS guarantees. There are many kinds of errors can happen in networks, the most common error in the networks is a link failures as a result of link disconnect or unplugged. Usually a human is the main culprit in many of the failures that occur in a network. Human failures are not just limited to the implementation; they can happen at all steps of a process in a specific network and directly or indirectly can participate to a main accident. Failures may cause by senility of tools, its components, or other software/hardware failures in router.

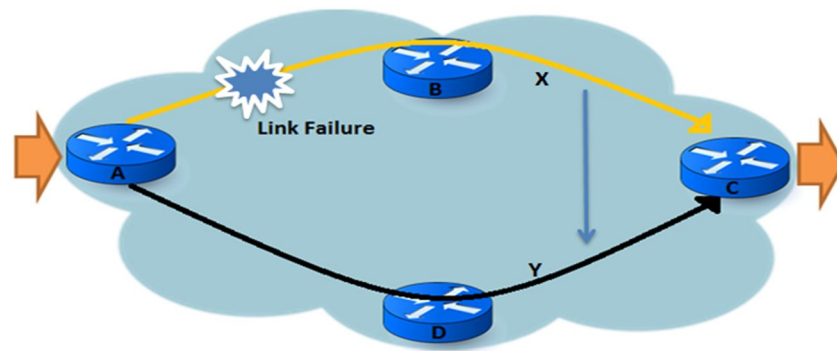


Figure 2.5. Link Protection

2.6.1. Link Protection

Link protection indicates to the capability for protecting in case of link failure. To make the protection of link failure, the backup tunnel is installing around the link. Figure 2.5 shows LSP(X) from A to C through B, this link is protected by backup LSP(Y) that tacking the path from A to C through D. When the LSP(X) fails, traffic from LSP(X) forwarded on backup LSP(Y) from A and delivered to node C. The protection of link failure is necessary in any network, wherefore; the backup should always be ready for forwarding traffic in case of failure occurs.

2.6.2. Node Protection for MPLS TE Tunnels

Failures could occur to link itself or node failure. The node protection (also called next next-hop (NNHOP) or Fast Reroute (FRR)) mechanism is similar to the link protection except that the backup channel which always is ready for the node that is after the next hop. When failure is discovered by losing the transporter or alarms of Synchronous Optical Network (SONET), the Point of Local Repair (PLR) reroutes traffic inside the backup tunnel, then to the NNHOP.

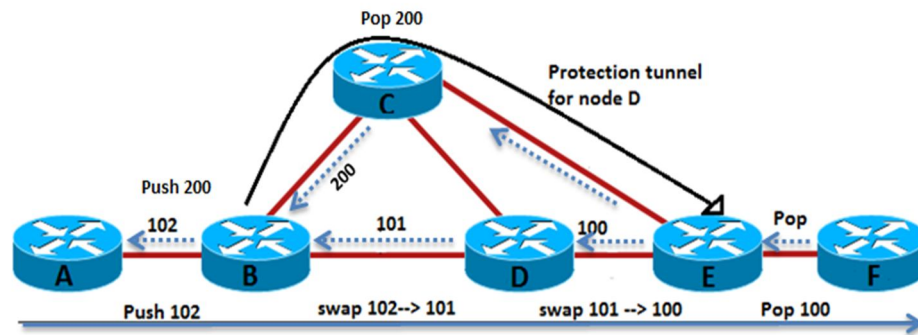


Figure 2.6. Node Protection

In Figure 2.6 a DiffServ TE is installed from A to F routers along the path A-B-D-E-F. This TE is protected avoiding failure of D router by a backup tunnel taking the path B-C-E that merges back into the main TE path at E router. When D router fails, traffic is forwarded onto the backup path at B router, PLR and merges back to the main path at E router where it continues on its normal path to F router. As a result, the node protection for MPLS TE tunnels which protects avoiding of link failure as well as node failure. Additionally, the PLR should define a label that will refer to the MP that packets arrived with that label must be transformed along the protected LSP to avoid traffic rejection.

2.6.3. Path Protection for MPLS TE

The Path protection (also called End-to-End protection) is performed using two LSPs, the primary LSP runs with normal status, and Secondary LSP run when a failure on Primary LSP occurs. When a failure occurs along the path such as link/node failure, the end of the header reroutes the traffic inside backup tunnel. Therefore, the backup (secondary) path protects immediately the main (primary) path as an alternative from kinds of failures along the path except the failures that may occur at the ingress LER and at the egress of LER or the failures that may occur on both the primary and secondary at a time. To avoid this case, both of the primary and secondary must have different paths over the network.

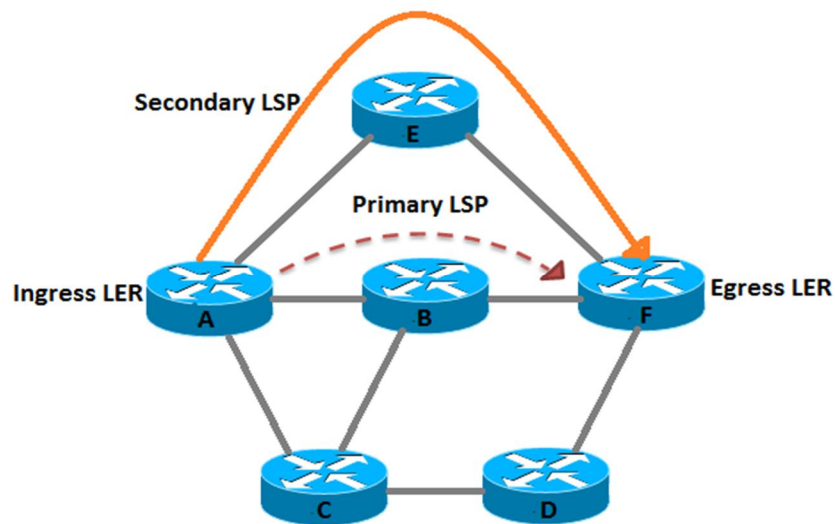


Figure 2.7. Path Protection for MPLS TE

Figure 2.7 shows secondary LSP along the path A-E-F provides path protection for Primary LSP A-B-F. For the fastest recovery times, the secondary is prepared and ready to take over the traffic. When a failure is detected on the primary LSP, Resource Reservation Protocol (RSVP) error is propagated to the LSP head end. Based on the failure message, the head-end forwards the traffic to the secondary LSP.

2.7. Traffic Engineering with MPLS

MPLS traffic engineering means that routers use the MPLS label switching mechanism for the purpose of optimize the network resource utilization. The ingress router transmits labels to packets using label distribution protocol (LDP). These packets then transmitted using label switching. In MPLS domain, routers can communicate with each other after the label information is shared. MPLS allows the LSP source to compute the path, build MPLS transmitting state and maps packets on to that specific LSP. The notion of traffic trunk is used to perform traffic engineering in the MPLS network [25]. The main exceptional feature of MPLS is that makes it beneficial for traffic engineering is the ability to setup label switched paths to conserve bandwidth. Furthermore, the possibility to calculate the path from ingress to egress, which is yield to constraints, is another property. Traffic engineering handled with performance optimization of the network, which designed to control the traffic flow over the network. Traffic engineering enables the operator to move away from the shortest path selected by the

IGP and onto a probable lower congested physical path over the network, as shown in Figure 2.8 A and G are the ingress routers establish LSPs separately according to demands. Routers B, C, and D are transit routers that linked to the egress routers E and F. All traffic passing through router B with destination routers E and F. If Router G receives an order with 5 capacity from G to destination F, then G forwards it through the shortest path LSP1 along the path G-B-D-F based on the capacity. If the shortest path algorithm is used, when Router A receives the second order of capacity 10 from routers A to destination E, then it forwards through LSP2, along the path A-B-C-E as a shortest path. However, when the order from router A to destination E increases from 10 to 15, Router A cannot forward LSP2 using the same path along A-B-C-E because the B-C link has lower capacity. Router A should forward the increased order on LSP2 using the alternative path A-B-D-C-E to distribute traffic evenly in the network. Traffic engineering helps solve congestion trouble that might occur by sources overlapping in some links in the networks that used the shortest path algorithm. Furthermore, the overriding of capacity of the shortest path from ingress to egress while a non-shortest path underused.

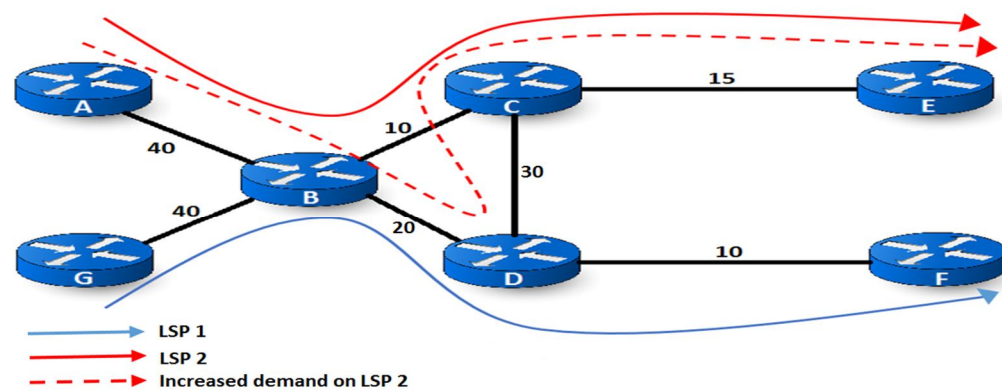


Figure 2.8. Traffic Engineering with MPLS

CHAPTER 3

NETWORKING AND NETWORK ROUTING

3.1. IP subnetting and calculating

Before diving into subnetting, we need to review some basics. The first clause is the IP address. An IP addressing is the most assignment of TCP/IP. Every device must have a unique address to be in contact on a network. An IPv4 address is a 32-bit symbolized in four portions called “octets”.

Designing, realization and managing an IP addressing plan ensures that network can operate conveniently and successfully. This is specifically actual because the number of host connections to a network increases. Working out the hierarchical structure of the IP address and the right way to modify that hierarchy with a purpose to meet more efficaciously routing specifications is an important portion of planning an IP addressing scheme.

In the IP address, hierarchy is divided into two fields of: a network and a host. These two phases of addressing enable for general network groupings that facilitate routing packets to a destination network. A router forwards packet founded on the network component of an IP address; as soon as the network is placed, the host component of the address allows for identification of the destination system. Subdividing a network adds phase to the network hierarchy, creating, in essence, three phases: a network, subnetwork, and a host. Introducing further phase to the hierarchy creates additional sub-sets inside an IP network that facilities faster packet delivery and brought filtration, by helping to shrink "local traffic".

3.2. Classful address scheme

3.2.1. Classes

IPv4 has 5 address classes (A, B, C, D and E); although, A, B, and C use a fixed length subnet mask and assign addresses to clients. Class D is reserved for multicast addressing, and class E is reserved for experimental purposes just for research and development or study and not organized with any subnet mask. The IP address in classes A, B, and C is divided into netid and hostid, but in classes D and E, are not.

A Class A address uses the first “octet” to represent the network portion, the left bit should be (0), the next 7 bits can be changed to find the number of blocks. Class A is divided into 126 blocks; each block in this class contains 16,777,214 addresses. Wherefore, the network addresses in this class use a large number of nodes.

The first two octets to present the network portion in class B define the class, and the two left bit begin with (10). However, Class B divided into 16,384 blocks; each block contains 65,534 addresses. Wherefore, not so many network addresses can use so many nodes. A Class C address uses the first three bits set as (110), divided into 2,097,152 blocks; each block contains 254 nodes. However, a larger number of networks use a smaller number of nodes. Figure 3.1 shows blocks in classes A, B, and C.

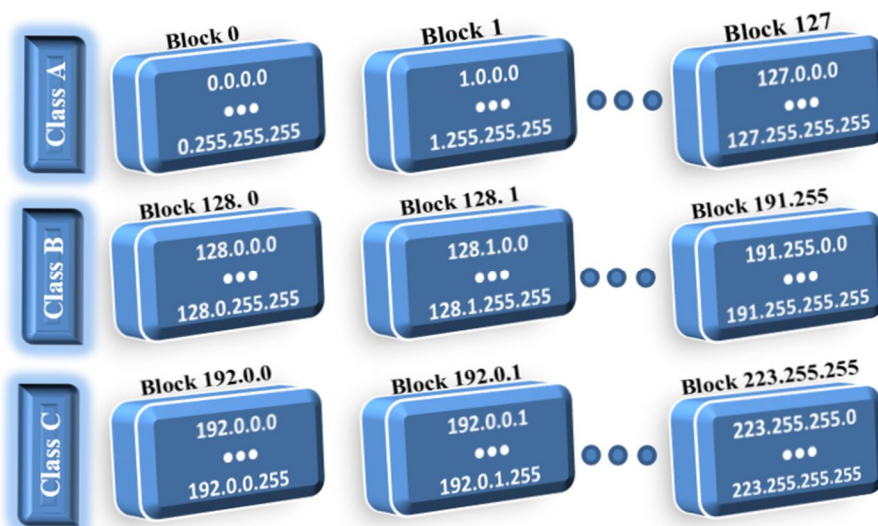


Figure 3.1. Blocks in classes A, B and C

Class D has one block; each address in class D used to define a group of hosts on the Internet. Class D uses the first four bits to indicate that it is a multicast address and are set to (1110). There is just one block in Class E. The first five bits set as (11110). Figures 3.2 and 3.3 show blocks in classes D and E.

To determine classes in a particular network, table 2.1 presents the Range and bits of first octets for each class.

224.0.0.0 ... 239.255.255.255

Figure 3.2. Block in class D

240.0.0.0 ... 255.255.255.255

Figure 3.3. Block in class E

Table 3.1. Classes and number of available network/host addresses

Address Class	Range	No. of networks	No. of Hosts Per Network	First Octet (Binary)
A	1 - 126	126	16,777,214	0xxxxxxx
B	128 - 191	16,384	65,534	10xxxxxx
C	192 - 223	2,097,152	254	110xxxxx
D	224 - 239	-	-	1110xxxx
E	240 - 255	-	-	1111xxxx

Table 3.2. Default network mask

Class	Default network mask	Format
A	255.0.0.0	11111111 00000000 00000000 00000000
B	255.255.0.0	11111111 11111111 00000000 00000000
C	255.255.255.0	11111111 11111111 11111111 00000000

3.3. Network Mask

The network mask is a 32-bit value represents the length of the network. It used to identify the range of IP. The network mask allows recognizing the netid part from the hostid part. Classes A, B, and C have default network masks as shown in table 3.2.

3.4. Variable Length Subnet Mask (VLSM)

When the subnetting performed, the number of hosts are equal for each subnet. This leads to waste the number of IP addresses. VLSM allows dividing different subnet sizes in the network. This method lead to more efficiencies, because it reduces the number of wasted IP addresses. VLSM allows dividing the large subnet into smaller sets of sub-subnets to use it in smaller host groups. An example of VLSM, consider the IP address of a company 192.168.1.0, this company consists of four departments with a different number of hosts: the accounting department with 70 hosts, marketing department with 50 hosts, human resource department with 20 hosts, and IT department with 25 hosts. If fixed subnetting performed, the 255 host addresses divided into four sets, each set contains 62 hosts. It does not meet the demand of accounting department and vastly wasting addresses for human resource and IT departments. Using VLSM, first, the space divide in two, each subnet has 126 hosts. Accounting department covered by one subnet.

The second part will divide in two sub-subnet, each part supply 62 hosts. Marketing department covered by one, and the other will divide in two sub-sub-subnets, each part supply 30 hosts to cover human resource and IT departments. It is worth pointing out here, routing protocols must utilize in order to perform VLSM such as Routing Information Protocol v2 (RIPv2) and Open Shortest Path First (OSPF).

3.5. Classless Addressing

The number of networks grew and the classful addresses became restricted. Therefore, the Internet moved away from a classful address area to a classless address area. In other words, the number of bits used for the network part of an IP address became variable instead of fixed [26].

Classless Addressing used to change the distribution of addresses in the same of IPv4 addresses for each network by dividing into blocks called “variable length blocks”. In classful addressing, each class has a number of bits related with the value of the first byte. Like class C addresses use 24 bits and the value is (192-223), but in classless do not use this relation.

3.6. Classless Inter Domain Routing (CIDR):

CIDR is a group of standards Internet protocol (IP), used to identify unique networks and individual devices. Internet Service Provider (ISP) uses this method to allocate the number of address to customers.

In IPv4, the IP address consists of 32 bits, CIDR indicates the mask to extraction the network where the ones are the most important bits. For example, in class C, the available prefix 192.168.99.0/24. “/24” means there are 24 bits are ones and the other 8 bits are zeros as shown in figure 3.4. CIDR used to manage and provide better utilization the IP address space of IPv4 and to minimize the entries of the routing table. It is worth mentioning here that CIDR used for IPv4 and IPv6 addresses.

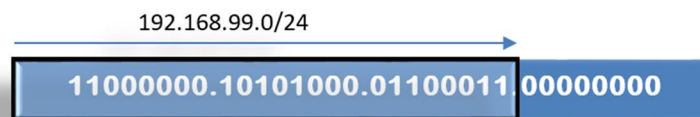


Figure 3.4. Classless Interdomain Routing (CIDR)

3.7. Subnetting

IP address partitioned into two parts: a network and a host. Subnetting is a process of to break it in to the network into smaller portions. Briefly, this process done by picking bits from the host part of the IP. There are many advantages of subnetting such as it minimizes traffic congestion in the network, optimizes network performance, simplifies resource organization, and provides more security.

Subnetting is varies for each class according to its default subnet mask. In other words, each class equipped with its default subnet mask. The host part is required to apply subnetting, like the host part of class C is last eight bits.

To get the first IP, the “AND” operation should apply to the given IP and subnet mask. The result of this operation represents the first IP .An example of Subnetting a Class C, consider the address of a network is 192.168.40.0/26 or 192.168.40.0 and the subnet mask is 255.255.255.192. After applied “AND” operation the result is:

192.168.40.0	11000000.10101000.00101000.00000000	
255.255.255.192	11111111.11111111.11111111.11000000	available bits =
		8
192.168.40.0	11000000.10101000.00101000.00000000	Taken bits = 2

The first IP address will be 192.168.40.0. The following equation used to determine the number of subnets:

$$\text{Number of subnets} = 2^{(\text{taken bits})} \quad 3.1$$

“Taken bits” represents the number of bits that have been taken in the result of “AND” operation. The following equation used to determine the number of hosts per subnet:

$$\text{Number of hosts per subnet} = 2^{(\text{taken bits}-\text{available bits})}-2 \quad 3.2$$

- The taken bits of the example above is 2. So, $2^2=4$ subnets.
- The number of hosts per subnet= $2^{(2-8)}-2= 62$ hosts.

Here, this network divided into four subnets, each subnet has 62 hosts. Each subnet take the first IP called “IP subnet”, and last IP called “broadcast IP”. Therefore, the ranges of valid IP will be:

1st subnet		2nd subnet	
192.168.40.0	IP subnet	192.168.40.64	IP subnet
192.168.40.1	First valid IP	192.168.40.65	First valid IP
192.168.40.62	Last valid IP	192.168.40.126	Last valid IP
192.168.40.63	IP broadcast	192.168.40.127	IP broadcast
3rd subnet		4th subnet	
192.168.40.128	IP subnet	192.168.40.192	IP subnet
192.168.40.129	First valid IP	192.168.40.193	First valid IP
192.168.40.190	Last valid IP	192.168.40.254	Last valid IP
192.168.40.191	IP broadcast	192.168.40.255	IP broadcast

3.8. Routing Techniques

Routing is a process of choosing a path to send data from the source node (ingress) to a destination node (egress) in a network, each node in the network represents as a router [27]. Routing protocols are sets of rules and procedures that allow routers to exchange information with each other's. There are many protocols may differ from one to another depending on their characteristics and which can be used. Routing protocols share a feature with another routing protocol to create routing algorithm. The main function of routing protocol is to provide the information required by the routing algorithm to calculate its decision. The routing protocol collects some information about network and routers from the network environment and stores in a table called "routing table". The routing algorithms operate based on the information that stored in the table to compute the preferable path to convey the data from the source to the destination. It is not possible to choose the algorithm to run on a particular router directly. Rather, the selected routing protocol defines which routing algorithm will be use.

3.9. Autonomous System (AS)

The internet became so huge. Therefore, one routing algorithm cannot manage the missions of all routers. So, an internet is splitted into autonomous systems (AS's). The AS is a collection of networks and routers controlled by a single administrator. Routing inside an AS is called intra-domain routing also referred Interior Gateway Protocols (IGP). Routing between AS's is called inter-domain routing and referred Exterior

Gateway Protocols (EGP). Each AS can use single or multiple intradomain routing protocols to deal with routing inside the AS. However, only single interdomain routing protocol deal with routing between AS's [28]. Protocols can be static or dynamic routing. Static routing is frugally the procedure of manually entering routes into the routing table by a configuration file that works when the router starts up. In static routing, all the variations in the logical network layout should be done manually by the administrator. However, dynamic routing enables routers to select paths according to real time logical network layout change [29].

Figure 3.5 shows; there are two main concepts of intradomain or Interior Gateway Protocol (IGP) routing algorithms that utilize by routing protocols: distance vector and link state. For interdomain, BGP protocol classified as a path vector routing protocol based on Exterior Gateway Protocol (EGP).

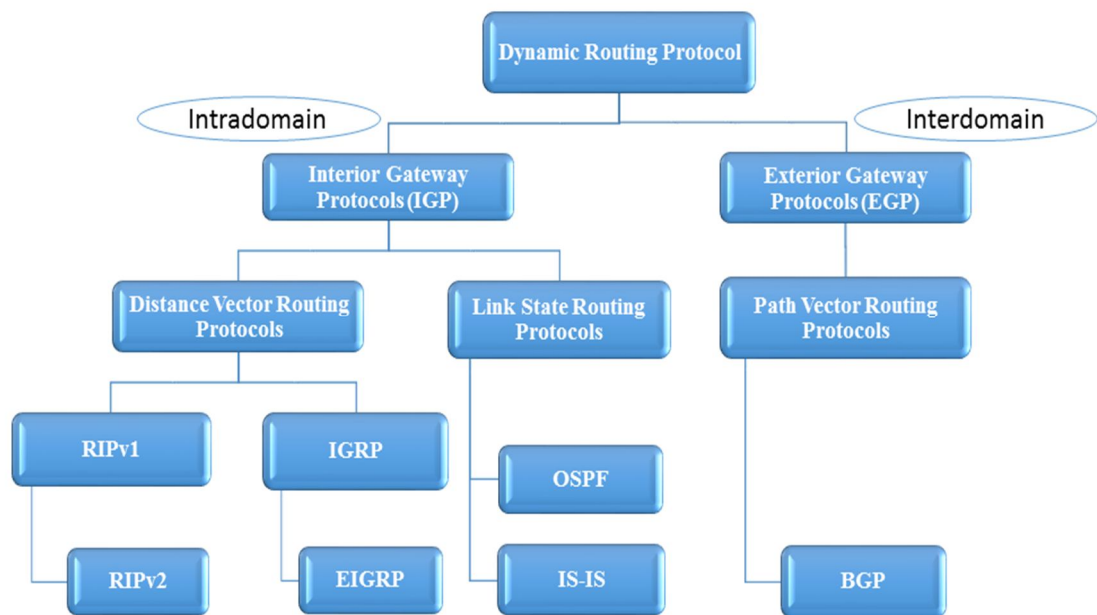


Figure 3.5. Dynamic Routing Protocols

3.10. Interior Gateway Protocol (IGP)

Interior Gateway Protocol (IGP) routing protocols used to determine the path information in AS such as Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS) and Interior Gateway Routing Protocol (IGRP) as well as MPLS signaling protocols like Resource Reservation Protocol - Traffic Engineering (RSVP-TE), Border Gateway Protocol (BGP) and Constraint-based Routing Label Distribution Protocol (CR-LDP). MPLS protocols extended as specified in ISIS-TE, OSPF-TE, RSVP-TE and CR-LDP in order to create a tunnel for traffic to allow better Traffic Engineering (TE) functionality as defined in TE-REQ [RFC 3785].

3.11. Distance Vector

In this routing scheme, periodically, routers sharing information about the network with their neighbors. Distance vector protocol is the simplest dynamic routing protocol because it is easy to setup and troubleshooting. The routers update their tables by sharing the information with their closest neighbors. In distance vector protocol, the distance cost information about the neighbors for all destinations is required to let the routers determine the shortest path to all directions like Routing Information Protocol (RIP) and IGRP. Distance Vector protocols use the Bellman-Ford algorithm to find the best paths to destinations.

3.11.1. Routing Information Protocol version 1 (RIPv1)

RIP (v1 and v2) is an Interior Gateway Protocol (IGP) based on distance vector routing protocol. The metric value of RIP is Hop count that uses and the hop limit limits the size of network that this protocol can support. The maximum hop count of RIP is limited to 15, so any network with more than 15 hops cannot be reached by RIP, and it sends full updates every 30 seconds. For these reasons, RIP is only suitable for small networks. There are two different versions of RIP: RIPv1 and RIPv2. RIPv1 is a simple protocol based on Distance Vector routing protocols, used for small networks. RIPv1 uses classful addressing and it does not support Variable length subnet masks (VLSM) or discontinuous subnets.

3.11.2. Routing Information Protocol version 2 (RIPv2)

RIPv2 defined in RFC 2473. RIPv2 uses classless addressing sense that it has the ability for distinguishing among different subnets. In RIPv2, Variable length subnet masks (VLSM) is supported and subnet masks in the routing update is included.

3.11.3. Interior Gateway Routing Protocol (IGRP)

(IGRP) uses a developed metric based on delay and bandwidth to find the metric value. IGRP does not support variable length subnet masking (VLSM). It forwards updates every 90 sec on average. It is one of distance vector routing protocols family, means that each router forwards whole or part of its table in routing message to each neighbor routers. IGRP uses delay and bandwidth as criteria to locate the best path.

3.11.4. Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is from the distance vector protocols family, EIGRP defined as hybrid routing protocol because it is a Distance Vector protocol and has some characteristics of Link State routing protocols. It provides significant improvements on IGRP. EIGRP is commonly used in large networks, and it updates only when changes in topology occur. The Diffusing Update Algorithm (DUAL) is the default convergence algorithm, which is used in EIGRP to avoid routing loops from re-computing routes.

3.12. Link state

In this routing technique, each router share information with all routers in the network about the neighbors to determine the best path. Each router computes its best paths separately. The router updates itself gradually whenever alterations occur. Link state protocols are based on Shortest Path First (SPF) algorithm. SPF algorithm also called Dijkstra algorithm, which used to get the shortest path between two nodes. Examples of Link State protocols are Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS).

3.12.1 Open Shortest Path First (OSPF)

OSPF is defined in RFC 2328. OSPF protocol is widely used in huge company networks, it is Interior Gateway Protocol (IGP) based on link state routing technique using Shortest Path First (SPF) algorithm to find the shortest path to destination. OSPF uses cost to find the metric value. OSPF has no limitation due to hops and can handle Variable Length Subnet Masks (VLSM) because it uses classless address.

3.12.2 Intermediate System to Intermediate System (IS-IS)

It is an Interior Gateway Protocols (IGPs). IS-IS is one of the most widespread protocols, using shortest path first (SPF) Algorithm for its routing table. In MPLS traffic engineering, IS-IS protocol is expanded to include edge specifications due to its flexibility.

3.13. Exterior Gateway Protocol (EGP)

Used to exchange routers between clearly splitted networks that have no administrator. On the Internet, routers use an Exterior Gateway Protocol (EGP) to get redundancy and load balance. Therefore, the companies that deal with more than one ISP use EGP.

3.13.1. Path Vector Routing Protocol

Distance vector and link state routing are interior routing protocols, used inside an AS's as intradomain. Path vector routing is an exterior routing protocol prepared to be advantageous for interdomain. In this kind of routing, a router has a list of networks, witch connected with each one with its path. The distance vector routing determines the distance to each network while the path vector routing locates the path.

3.13.2. Border Gateway Protocol (BGP)

Based on RFC 4271. BGP is an exterior gateway protocol (EGP) used for exchanging routing and reachability information through autonomous systems (AS) on the Internet. BGP categorized as a path vector protocol. This protocol used to connect one (AS) to another (ASs), which means used to conversion to another ISP link when the primary connection fails. For this reason, most common enterprises run BGP on internet edge. BGP computes routing paths based on some information, like as an AS path, IGP metric, multi-exit discriminator, community, preferences, next hop, weight. It updates the routing table when changes occur. BGP supports classless interdomain routing and VLSM.

3.14. Comparison between Distance vector and Link state

Distance Vector and Link State are terms, used to describe Routing Protocols, which are used by routers to forward packets between networks. Table 3.3 presents the differences between Distance vector and Link state protocols. The comparison of the protocols which illustrated above is presented in table 3.4.

Table 3.3. Comparison between Distance vector and Link state

Distance vector	Link state
Each router receives the routing update, increment the metric, compare the result to the routes in the routing table, and update the routing table if necessary.	Each router receives the state of all the network's links through periodically flooded link-state updates and makes routing decisions based on the link states.
simple protocols and easy to setup, configuring and troubleshooting.	more complex and expensive to implement and support.
consume less memory and less router resources.	more CPU power and memory are required.
Convergence time is very slow.	convergence more quickly and they are less prone to Routing Loops.
use the distance and direction to find paths to destinations.	use a hierarchical structure.
using limited broadcasts to share the routing Information.	Use multicasts to share the routing information.
based on Bellman Ford algorithms.	based on Dijkstra algorithms.

Table 3.4. Comparison of routing protocols

Protocols criteria	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS	BGP
Class	Classful	Classless	Classful	Classless	Classless	Classless	Classless
Domain	Intradomain	Intradomain	Intradomain	Intradomain	Intradomain	Intradomain	Interdomain
Protocol Type	Distance Vector	Distance Vector	Distance Vector	Advanced distance vector	Link state	Link State	Path Vector
Support VLSM	No	Yes	No	Yes	Yes	Yes	Yes
Metric value	Hop count	Hop count	Bandwidth/Delay	Bandwidth/Delay	Cost	Cost	MED, Preferences, Next Hop, Weight...
Update Time	30 sec	30 sec	90 sec	When modifications occur	When modifications occur	When modifications occur	When modifications occur
Convergence	Slow	Slow	Slow	Very fast	Fast	Fast	Slow
Network size	Small	Small	Large	Large	Large	Large	Very Large
Hop count	15	15	Unlimited	Unlimited	None	None	1
Algorithm	Bellman-Ford	Bellman-Ford	Bellman-Ford	DUAL	Dijkstra	Dijkstra	Best Path

3.15. Hybrid Routing Protocols (HRP)

A Hybrid Routing protocol is the third category of routing protocols has the features of both Distance vector and Link State Routing protocols and combines them into a new protocol. HRP is based on a Distance Vector protocol and contains some features and advantages of Link State Routing protocols. Hybrid Routing Protocol is a very robust protocol, it can handle with many various criteria such as bandwidth, load, delay, reliability, and hop count. It can make a decision to determine the best route to destination, HRPs require less processing power and memory than Link State routing protocol.



CHAPTER 4

SIMULATION AND RESULTS

4.1. Design of network

In chapters 2 and 3, the characteristics and properties of traditional IP, MPLS and MPLS-TE, and the features of various routing protocols have been illustrated. Figure 4.1 shows the proposed network architecture and design for this study. The routers and servers are geographically distributed according to Iraq map.

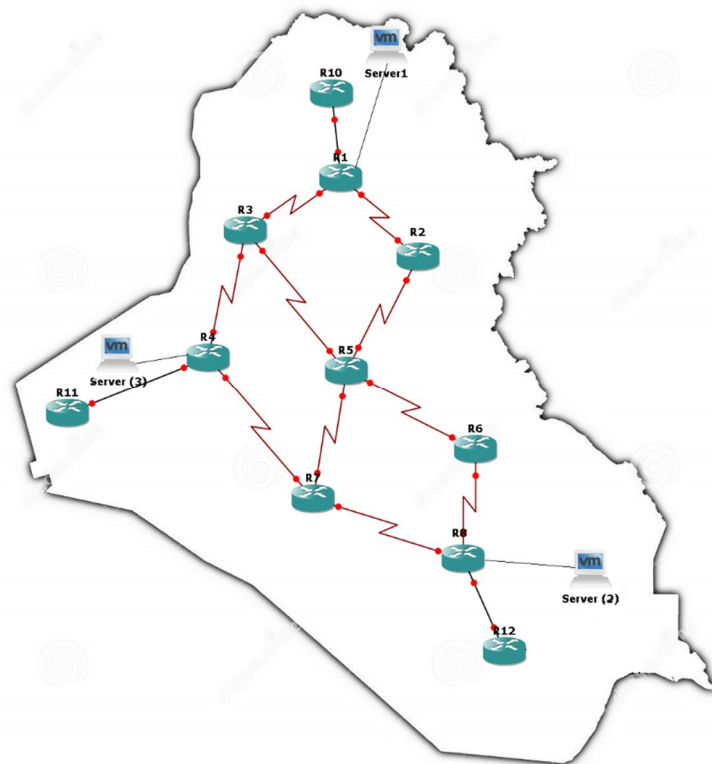


Figure 4.1. Proposed network architecture

The details of routers and servers for the network topology shown in table 4.1. The arrangements of routers illustrated in table 4.2.

Table 4.1. Network Topology Details

No. of routers	11
No. of servers	3
No. of links	16
Routers Model and OS	Cisco7200 15.2.4S5(MD)
Servers OS	Microsoft Windows XP Professional x64 Edition

Table 4.2. Routers Interfaces

Routers	Links
R1	10.1.1.0/30, 10.1.2.0/30, 140.140.0.0/30, 192.168.16.0/24
R2	10.1.1.0/30, 10.1.3.0/30
R3	10.1.2.0/30, 10.1.4.0/30, 10.1.5.0/30
R4	10.1.5.0/30, 10.1.6.0/30, 100.100.0.0/30, 192.168.15.0/24
R5	10.1.3.0/30, 10.1.4.0/30, 10.1.7.0/30, 10.1.8.0/30
R6	10.1.8.0/30, 10.1.9.0/30
R7	10.1.6.0/30, 10.1.7.0/30, 10.1.10.0/30
R8	10.1.9.0/30, 10.1.10.0/30, 11.3.3.0/30, 192.168.17.0/24
R10	140.140.0.0/30
R11	100.100.0.0/30
R12	11.3.3.0/30
Server1	192.168.16.0/24
Server2	192.168.17.0/24
Server3	192.168.15.0/24

4.2. Configuration of networks

The network designed, configured and simulated using Graphical Network Simulator (GNS3). GNS3 is an Open Source simulator used on multiple operating systems, based on Dynamips and Dynagen to create a virtual Cisco network. Additionally, GNS3 can integrate Quick Emulation (QEMU) and Virtual machines to run an operating system such as Windows or Linux. Virtual machine is used to install and run Windows XP in current networks as servers. The purpose of this network is to compare the performance of traditional IP, MPLS, and MPLS-TE. The network consists of 11 routers and 3 servers applied on virtual map of Iraq to achieve the desired goal.

4.2.1. Implementation of traditional IP

In traditional IP, each router independently makes routing decisions to forward the packet out to reach the destination. The routing table determines the destinations of packets by storing the information of IP network. To create the routing table, each router must run routing protocol such as BGP, IS-IS, RIP, or OSPF.

In the current network, OSPF for all routers are implemented as an open standard routing protocol. Figure 4.2 shows the OSPF configuration.

```
interface Serial1/0
 ip address 10.1.1.2 255.255.255.252
 serial restart-delay 0
!
interface Serial1/1
 ip address 10.1.3.1 255.255.255.252
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 1
 network 10.1.1.0 0.0.0.255 area 1
 network 10.1.3.0 0.0.0.255 area 1
```

Figure 4.2. OSPF configuration

After configuring OSPF in all routers in the network, it determined routers dynamically by gaining information from other routers and advertised routes to other routers. The routing tables in each router are populated. IP routing table shown in Figure 4.3.

```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 15 subnets, 2 masks
  C    10.1.1.0/30 is directly connected, Serial1/0
  L    10.1.1.1/32 is directly connected, Serial1/0
  C    10.1.2.0/30 is directly connected, Serial1/1
  L    10.1.2.1/32 is directly connected, Serial1/1
  O    10.1.3.0/30 [110/128] via 10.1.1.2, 00:01:18, Serial1/0
  O    10.1.4.0/30 [110/128] via 10.1.2.2, 00:01:18, Serial1/1
  O    10.1.5.0/30 [110/128] via 10.1.2.2, 00:01:18, Serial1/1
  O    10.1.6.0/30 [110/192] via 10.1.2.2, 00:01:18, Serial1/1
  O    10.1.7.0/30 [110/192] via 10.1.2.2, 00:01:18, Serial1/1
       [110/192] via 10.1.1.2, 00:01:18, Serial1/0
  O    10.1.8.0/30 [110/192] via 10.1.2.2, 00:01:18, Serial1/1
       [110/192] via 10.1.1.2, 00:01:18, Serial1/0
  O    10.1.9.0/30 [110/256] via 10.1.2.2, 00:01:18, Serial1/1
       [110/256] via 10.1.1.2, 00:01:18, Serial1/0
  O    10.1.10.0/30 [110/256] via 10.1.2.2, 00:01:18, Serial1/1
       [110/256] via 10.1.1.2, 00:01:18, Serial1/0
  O    10.10.10.10/32 [110/2] via 140.140.0.2, 00:00:11, FastEthernet0/0
  O    10.10.10.11/32 [110/130] via 10.1.2.2, 00:00:00, Serial1/1
  O    10.10.10.12/32 [110/258] via 10.1.2.2, 00:00:27, Serial1/1
       [110/258] via 10.1.1.2, 00:00:27, Serial1/0
  11.0.0.0/30 is subnetted, 1 subnets
  O    11.3.3.0 [110/257] via 10.1.2.2, 00:01:18, Serial1/1
       [110/257] via 10.1.1.2, 00:01:18, Serial1/0
  100.0.0.0/24 is subnetted, 1 subnets
  O    100.100.0.0 [110/129] via 10.1.2.2, 00:01:18, Serial1/1
  140.140.0.0/16 is variably subnetted, 2 subnets, 2 masks
  C    140.140.0.0/24 is directly connected, FastEthernet0/0
  L    140.140.0.1/32 is directly connected, FastEthernet0/0
  O    192.168.15.0/24 [110/130] via 10.1.2.2, 00:00:00, Serial1/1
  O    192.168.16.0/24 [110/2] via 140.140.0.2, 00:00:11, FastEthernet0/0
  O    192.168.17.0/24 [110/258] via 10.1.2.2, 00:00:27, Serial1/1
       [110/258] via 10.1.1.2, 00:00:27, Serial1/0

R1#
```

Figure 4.3. IP routing table

4.2.2. Implementation of MPLS

MPLS was enabled on router that located inside the MPLS domain. In the MPLS domain, packet transmitting decision is based on labels. OSPF as an open standard routing protocol was used as a routing protocol for this design. Router redistribution was enabled to propagate routers informed with the use of OSPF, into RIP and EIGRP.

To obtain the advantages of traffic prioritization and management, Frame Relay was run over MPLS network. Moreover, loopbacks are configured to simulate the network. Figure 4.4 shows the setup of MPLS network.

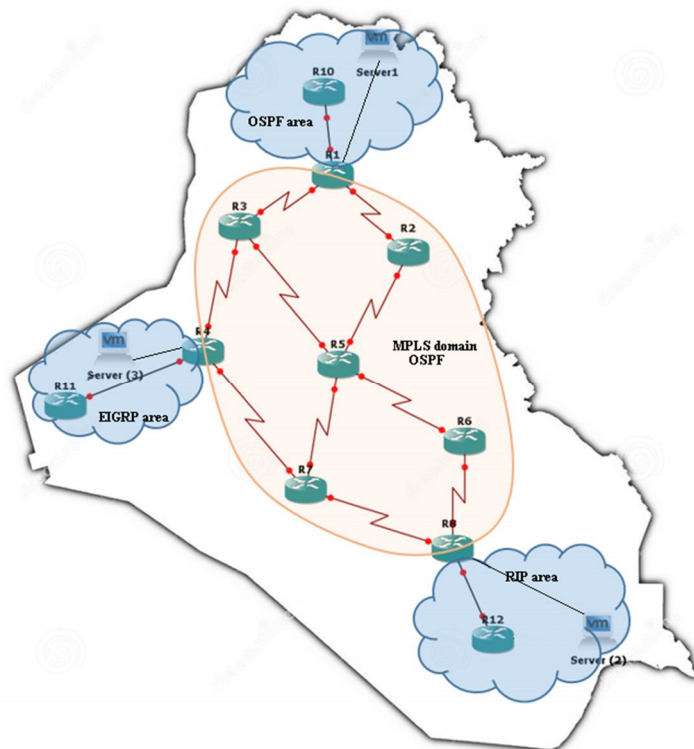


Figure 4.4. MPLS design

The configurations are done on MPLS domain routers, which include LSR and LER, and on the Frame Relay as shown in Figure 4.5.

```
interface Serial1/0
  no ip address
  encapsulation frame-relay
  mpls ip
  serial restart-delay 0
!
interface Serial1/0.1 point-to-point
  bandwidth 512
  ip address 10.1.1.2 255.255.255.252
  mpls ip
  frame-relay interface-dlci 201
!
interface Serial1/0.2 point-to-point
  bandwidth 512
  ip address 10.1.3.1 255.255.255.252
  mpls ip
  frame-relay interface-dlci 205
```

Figure 4.5. Configuration of MPLS and Frame Relay

After configuring all protocols, the routers advertised their networks to other routers.

Figure 4.6 shows the IP routing table.

```
10.0.0.0/8 is variably subnetted, 25 subnets, 2 masks
O   10.1.1.0/30 [110/390] via 10.1.3.1, 03:20:57, Serial1/0.1
O   10.1.2.0/30 [110/390] via 10.1.4.1, 03:20:57, Serial1/0.2
C   10.1.3.0/30 is directly connected, Serial1/0.1
L   10.1.3.2/32 is directly connected, Serial1/0.1
C   10.1.4.0/30 is directly connected, Serial1/0.2
L   10.1.4.2/32 is directly connected, Serial1/0.2
O   10.1.5.0/30 [110/390] via 10.1.4.1, 03:20:57, Serial1/0.2
O   10.1.6.0/30 [110/390] via 10.1.7.2, 03:20:57, Serial1/0.3
C   10.1.7.0/30 is directly connected, Serial1/0.3
L   10.1.7.1/32 is directly connected, Serial1/0.3
C   10.1.8.0/30 is directly connected, Serial1/0.4
L   10.1.8.1/32 is directly connected, Serial1/0.4
O   10.1.9.0/30 [110/390] via 10.1.8.2, 03:20:57, Serial1/0.4
O   10.1.10.0/30 [110/390] via 10.1.7.2, 03:20:57, Serial1/0.3
O   10.10.10.1/32 [110/391] via 10.1.4.1, 03:20:57, Serial1/0.2
    [110/391] via 10.1.3.1, 03:20:57, Serial1/0.1
O   10.10.10.2/32 [110/196] via 10.1.3.1, 03:20:57, Serial1/0.1
O   10.10.10.3/32 [110/196] via 10.1.4.1, 03:20:57, Serial1/0.2
O   10.10.10.4/32 [110/391] via 10.1.7.2, 03:20:32, Serial1/0.3
    [110/391] via 10.1.4.1, 03:20:32, Serial1/0.2
C   10.10.10.5/32 is directly connected, Loopback0
O   10.10.10.6/32 [110/196] via 10.1.8.2, 03:20:57, Serial1/0.4
O   10.10.10.7/32 [110/196] via 10.1.7.2, 03:20:57, Serial1/0.3
O   10.10.10.8/32 [110/391] via 10.1.8.2, 03:20:57, Serial1/0.4
    [110/391] via 10.1.7.2, 03:20:57, Serial1/0.3
O E2 10.10.10.10/32 [110/10] via 10.1.4.1, 01:35:04, Serial1/0.2
    [110/10] via 10.1.3.1, 01:35:04, Serial1/0.1
O E2 10.10.10.11/32 [110/10] via 10.1.7.2, 03:20:32, Serial1/0.3
    [110/10] via 10.1.4.1, 03:20:32, Serial1/0.2
O E2 10.10.10.12/32 [110/1] via 10.1.8.2, 03:20:57, Serial1/0.4
    [110/1] via 10.1.7.2, 03:20:57, Serial1/0.3
11.0.0.0/30 is subnetted, 1 subnets
O E2 11.3.3.0 [110/1] via 10.1.8.2, 03:20:57, Serial1/0.4
    [110/1] via 10.1.7.2, 03:20:57, Serial1/0.3
100.0.0.0/30 is subnetted, 1 subnets
O E2 100.100.0.0 [110/10] via 10.1.7.2, 03:20:32, Serial1/0.3
    [110/10] via 10.1.4.1, 03:20:32, Serial1/0.2
140.140.0.0/30 is subnetted, 1 subnets
O E2 140.140.0.0 [110/10] via 10.1.4.1, 03:20:57, Serial1/0.2
    [110/10] via 10.1.3.1, 03:20:57, Serial1/0.1
O E2 192.168.15.0/24 [110/10] via 10.1.7.2, 03:20:32, Serial1/0.3
    [110/10] via 10.1.4.1, 03:20:32, Serial1/0.2
O E2 192.168.16.0/24 [110/10] via 10.1.4.1, 01:35:04, Serial1/0.2
    [110/10] via 10.1.3.1, 01:35:04, Serial1/0.1
O E2 192.168.17.0/24 [110/1] via 10.1.8.2, 03:20:57, Serial1/0.4
    [110/1] via 10.1.7.2, 03:20:57, Serial1/0.3
```

Figure 4.6. MPLS IP routing table

4.2.3. Implementation of MPLS-TE

The MPLS Traffic Engineering (TE) based Tunnel Selection feature enables the routing and forwarding traffic dynamically. MPLS tunnels allow traffic to transmit through devices that have no information of traffic's destination. RSVP is necessary for traffic engineering. Using RSVP-TE to reserve bandwidth over the network. LSP is a tunnel between two nodes in the network. Under RSVP, each LSP has a bandwidth value correlated with it. It is compulsory to create a loopback interface for each router to setup traffic engineering.

Three tunnels are configured between LERs to implement MPLS over traffic engineering (TE) tunnels in MPLS network, which shown in Figure 4.7.

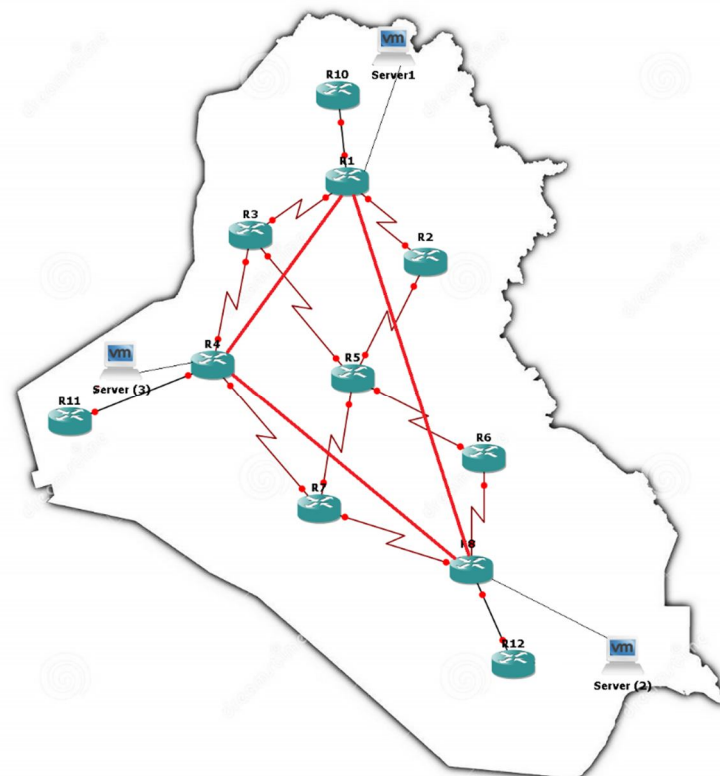


Figure 4.7. MPLS-TE Tunnels

The configuration of tunnels is shown in Figure 4.8.

```
interface Tunnell
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 10.10.10.8
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth 512
 tunnel mpls traffic-eng path-option 1 explicit name path1
 tunnel mpls traffic-eng path-option 2 dynamic
```

Figure 4.8. Tunnel configuration

The configuration includes two path options to reach the destination, explicit and dynamic. Explicit paths are specified in each LER as shown in Figure 4.9.

```
ip explicit-path name path1 enable
 next-address 10.1.1.2
 next-address 10.1.3.2
 next-address 10.1.8.2
 next-address 10.1.9.2
 !
```

Figure 4.9. Tunnel explicit path

Figure 4.10 shows the status of tunnels are built up successfully

```
Signalling Summary:
  LSP Tunnels Process:          running
  Passive LSP Listener:        running
  RSVP Process:                 running
  Forwarding:                   enabled
  Periodic reoptimization:      every 3600 seconds, next in 1394 seconds
  Periodic FRR Promotion:       Not Running
  Periodic auto-bw collection:  every 300 seconds, next in 194 seconds

P2P TUNNELS/LSPs:
TUNNEL NAME          DESTINATION    UP IF    DOWN IF    STATE/PROT
PE1_t1                10.10.10.8    -        Se1/0.1    up/up
PE3_t3                10.10.10.1    Se1/0.2  -          up/up
Displayed 1 (of 1) heads, 0 (of 0) midpoints, 1 (of 1) tails
```

Figure 4.10. Tunnel built up

The proposed IP, MPLS, and MPLS-TE network architectures are implemented and ready for simulation.

4.3. Simulation results

4.3.1. Simulation model

The concept of computer network simulation is based on Real World Networks Modelling on a computer machine using dedicated software programs. The real computer networks are the networks already executed or the networks that will implement in the future. Network simulation used to assist the network engineers by embodying a network model to execute the configuration and analyse the output to optimize the performance, as shown in Figure 4.11.

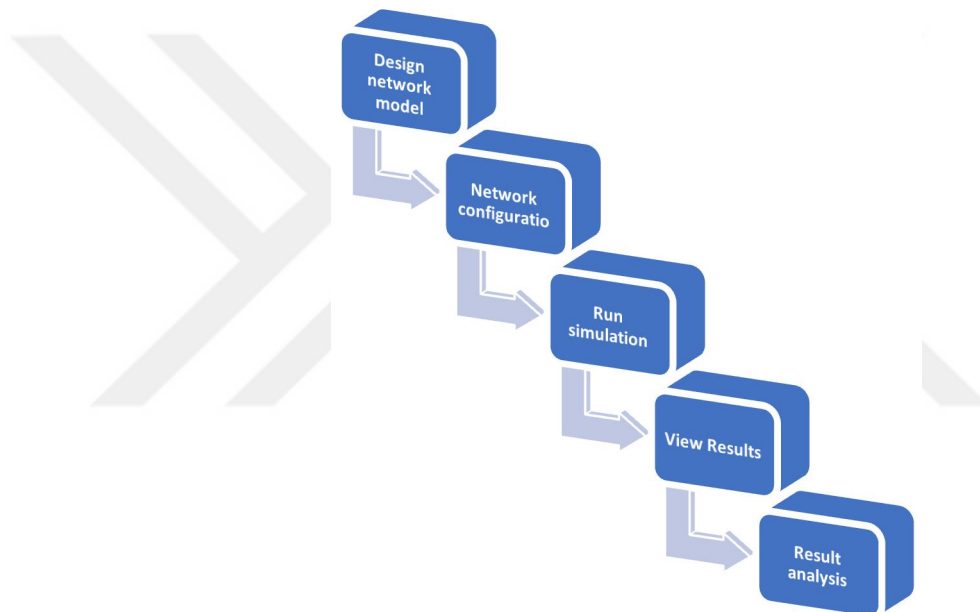


Figure 4.11. Simulation Model

4.3.2. Simulation goals

The objective of this simulation is to compare and evaluate the performance of traditional IP, MPLS, and MPLS-TE. Wherefore, three scenarios have been considered for simulations having the same topology.

Scenario □

To analyse the traffic flow on network, Wireshark was used to monitor throughput, packet loss and RTT. Wireshark is perhaps one of the best packet analysers used for network analysis and troubleshooting. Networks are congested with a bulk of data sent between the servers. The results are presented in the Figures 4.12-4.20, respectively.



Figure 4.12. Performance analysis between Server 1 and Server 2 on IP network

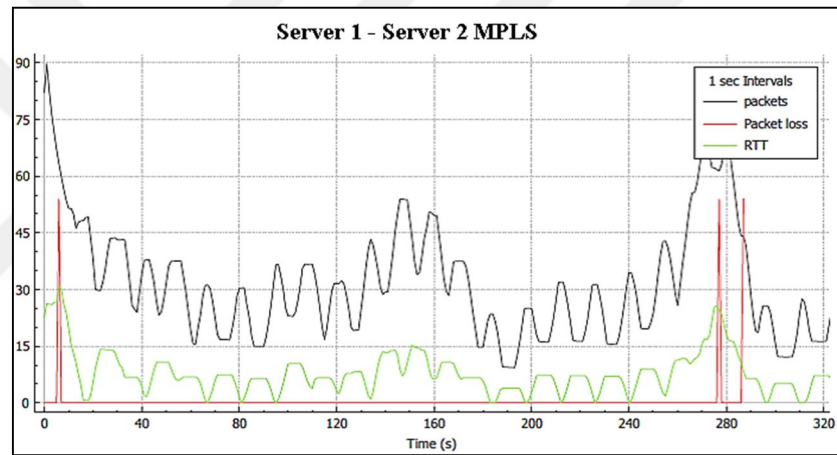


Figure 4.13. Performance analysis between Server 1 and Server 2 on MPLS network

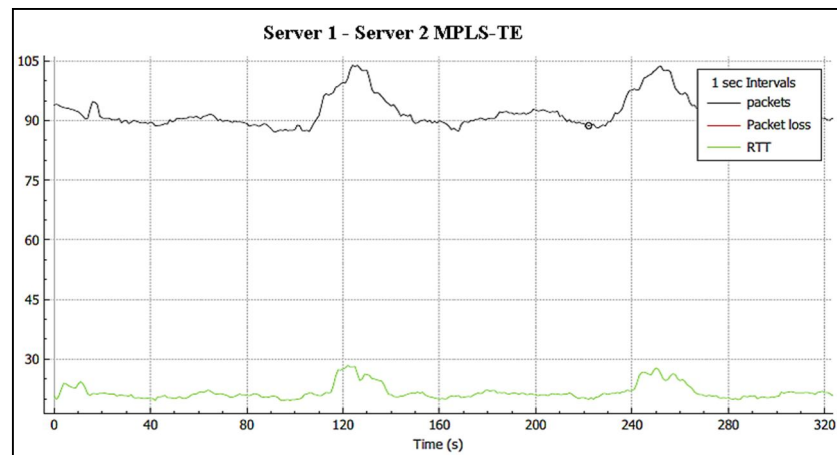


Figure 4.14. Performance analysis between Server 1 and Server 2 on MPLS-TE network



Figure 4.15. Performance analysis between Server 1 and Server 3 on IP network

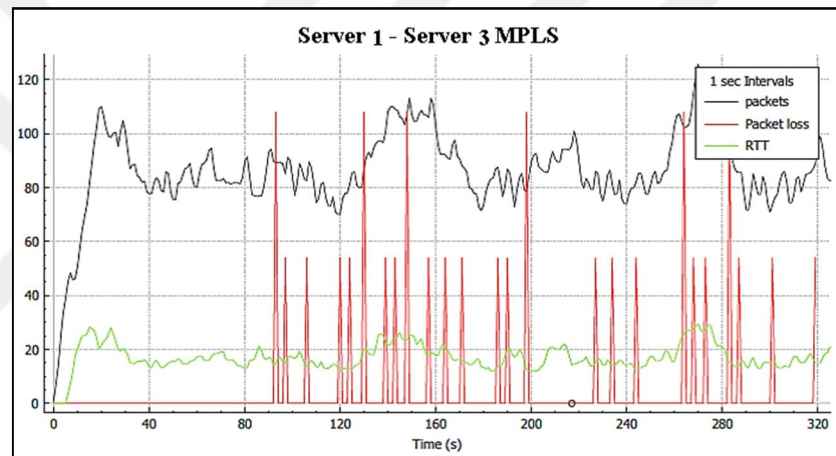


Figure 4.16. Performance analysis between Server 1 and Server 3 on MPLS network

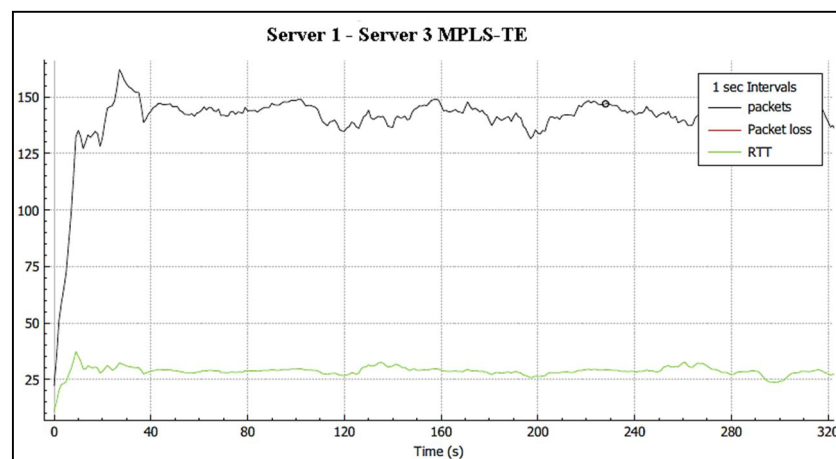


Figure 4.17. Performance analysis between Server 1 and Server 3 on MPLS-TE network



Figure 4.18. Performance analysis between Server 2 and Server 3 on IP network

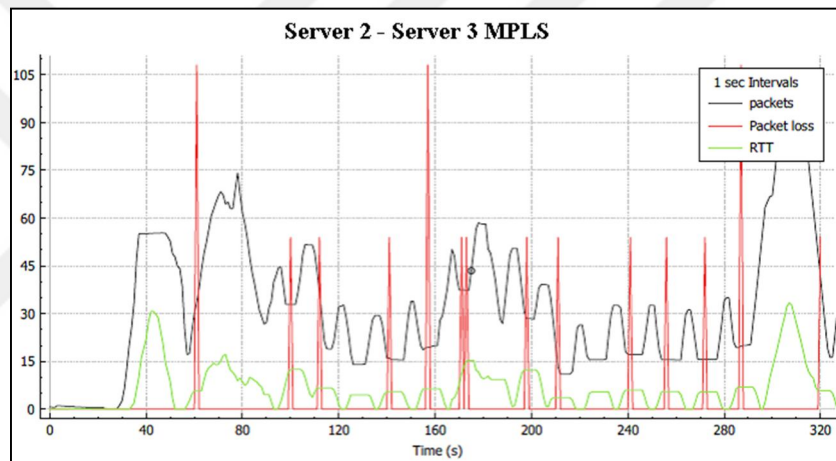


Figure 4.19. Performance analysis between Server 2 and Server 3 on MPLS network

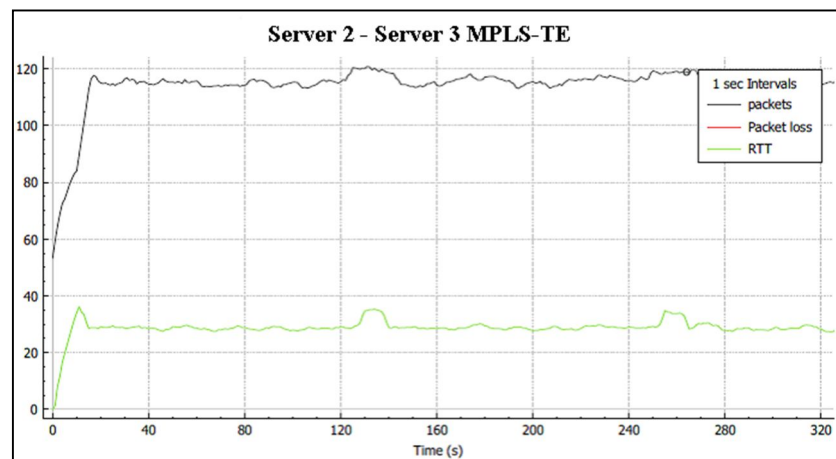


Figure 4.20. Performance analysis between Server 2 and Server 3 on MPLS-TE network

Scenario □

Second scenario presents the Round Trip Time (RTT) between customer edges (CEs) in each of the IP, MPLS, and MPLS-TE networks. 18000-byte data packets are sent between (CEs) using ping test to measure the RTT. The results are presented in Figure 4.21 and table 4.3.

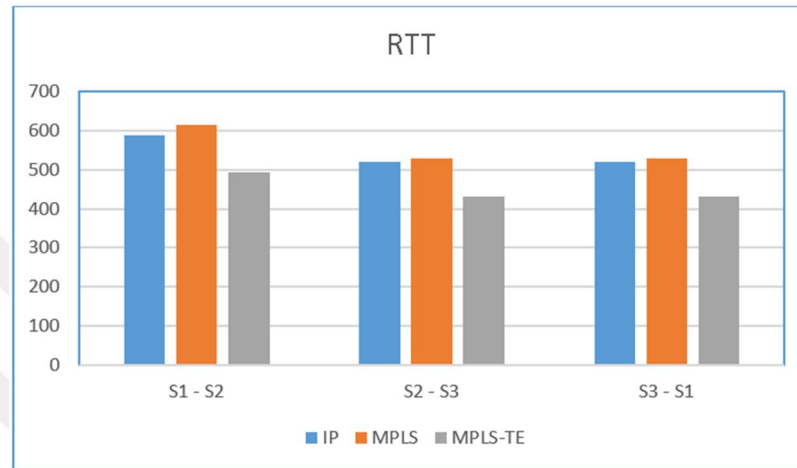


Figure 4.21. Graphical representation of ping tests

Table 4.3. Numerical representation of ping tests

Router	IP	MPLS	MPLS-TE
CE1-CE2	590	615	495
CE2-CE3	520	530	432
CE3-CE1	520	530	432

Scenario □

Third scenario is similar to the first scenario except that another topology are prepared. The network in this scenario is a full mesh network consists of (9) routers and (3) servers distributed in three VPNs (Virtual Private Networks). This network was subjected to the same experiment in the first scenario network by sending data between the servers twice. First time without traffic engineering tunnels, the second with traffic

engineering tunnels are configured between Provider Edge Routers (PEs) over MPLS domain, as shown in Figures 4.22 and 4.23.

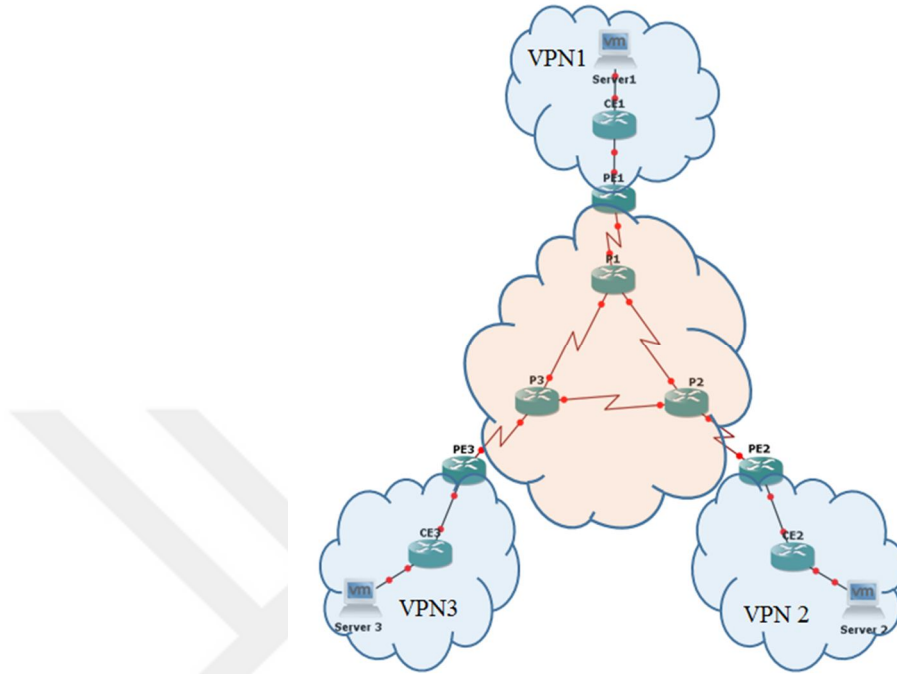


Figure 4.22. MPLS network without traffic engineering tunnels

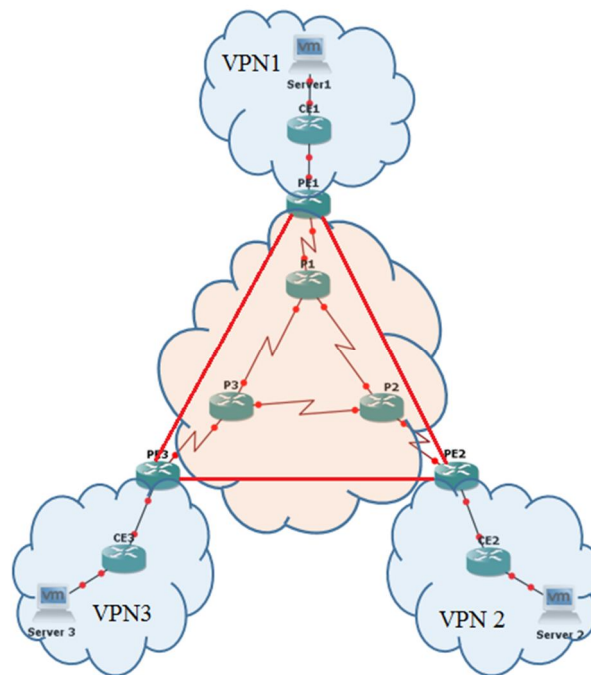


Figure 4.23. MPLS network with traffic engineering tunnels

Wireshark was used to monitor throughput, packet loss and RTT. The results are presented in the Figures 4.24 - 4.29, respectively.

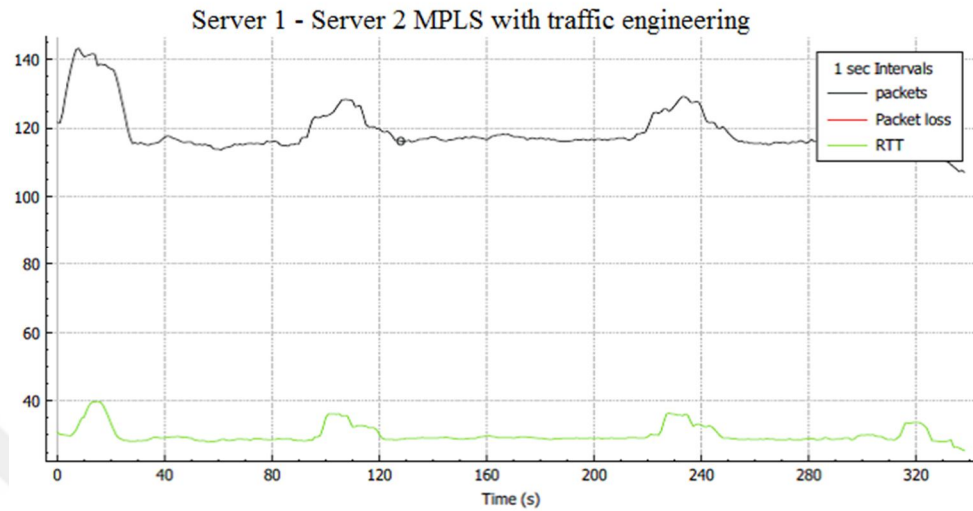


Figure 4.24. Performance analysis between Server 1 and Server 2 on MPLS with TE

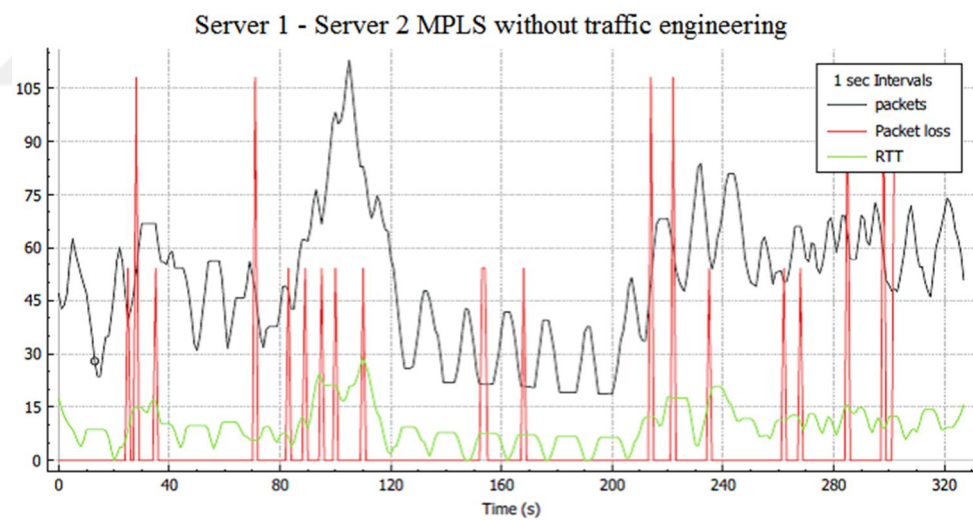


Figure 4.25. Performance analysis between Server 1 and Server 2 on MPLS without TE

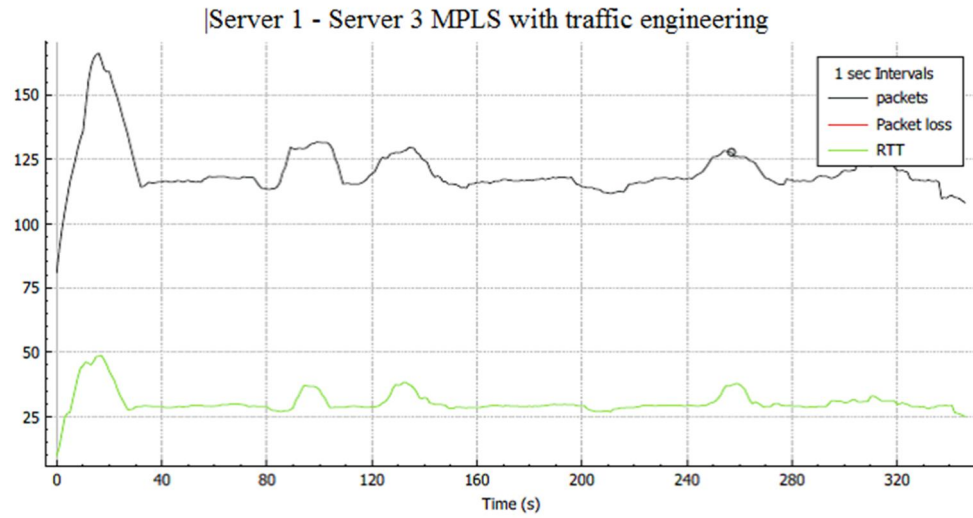


Figure 4.26. Performance analysis between Server 1 and Server 3 on MPLS with TE

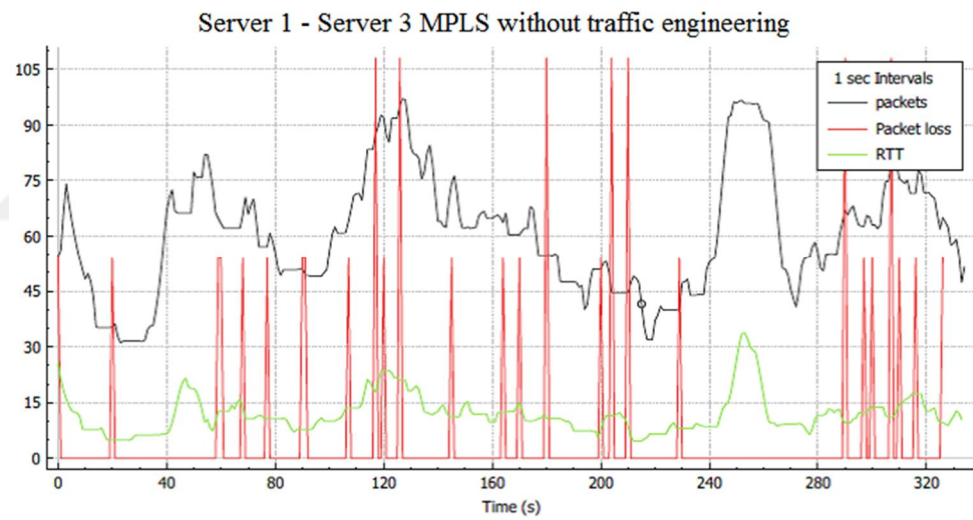


Figure 4.27. Performance analysis between Server 1 and Server 3 on MPLS without TE

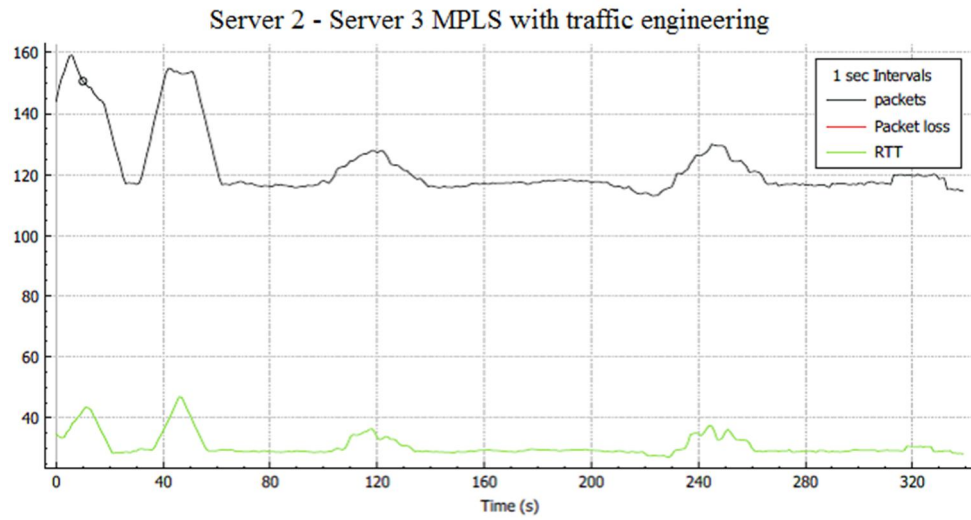


Figure 4.28. Performance analysis between Server 2 and Server 3 on MPLS with TE

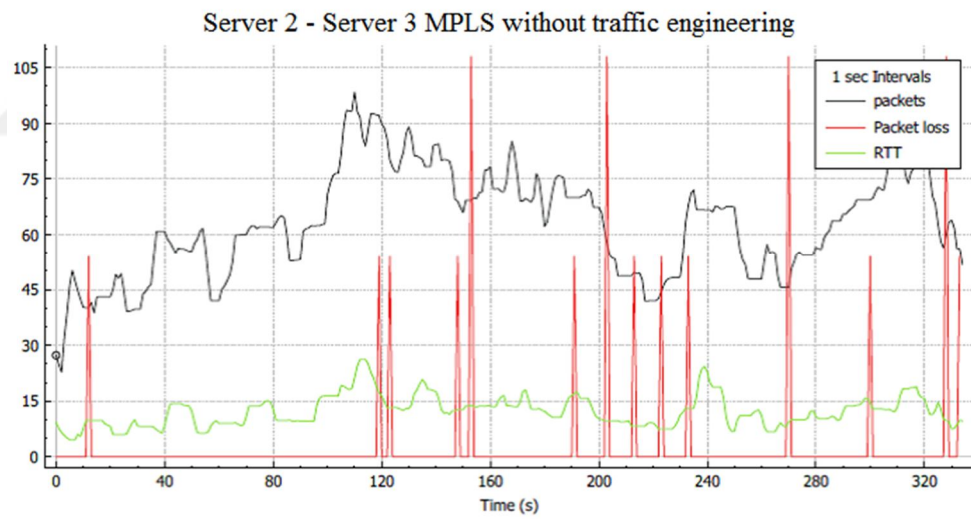


Figure 4.29. Performance analysis between Server 2 and Server 3 on MPLS without

CHAPTER 5

DISCUSSION, CONCLUSION AND FUTURE WORK

5.1. Discussion

The main objective of this thesis is to compare performance of traditional IP, MPLS and MPLS-TE. For this purpose, three scenarios for simulation are done. In the first scenario, data packets are sent between servers (1, 2 and 3) as virtual machines in each network. The results of this scenario indicate that MPLS with traffic engineering took less time than IP and MPLS networks. The line graphs for IP and MPLS networks showed that there are increase in the number of packet loss and latency when packets are sent between their servers, while there was no packet loss noticed on the MPLS-TE network. MPLS-TE proved higher throughput than other networks. There is no drastic difference between the results of IP and MPLS but simulation noticed that MPLS has higher latency and RTT than traditional IP network. The variance of results for each network due to the number of routers are involved on the path to the destination.

The second scenario, the ping test is used to measure the RTT by sending the amount of data between the different areas. The results showed reduction in RTT for MPLS-TE.

The third scenario is similar to the first scenario except that different network are used. The data packet are sent twice between three servers. In the first experiment, the network was configured without MPLS traffic engineering tunnels. The second experiment, the network was configured with MPLS traffic engineering tennels are enabled between the provider edge routers (PEs). The line graphs for MPLS network without traffic engineering indicated a rise in packet loss and latency rates, while there are no packet loss in the second experiment. Moreover, the MPLS with traffic engineering network indicates reduction of RTT and latency.

After critically analysing the results, the simulation proved that, the MPLS with traffic engineering consumed less delay and provides high throughput compared to traditional IP and MPLS networks. It can greatly improve performance in the network. Therefore, MPLS-TE will be good option to reduce network congestion.

5.2. Conclusion

This thesis presents design, implementation and evaluation in order to compare the performance of traditional IP, MPLS with MPLS-TE networks. Data packet transmission between servers was considered as a base to perform the objective of the simulation. The simulation results showed that the MPLS-TE obtains minimum latency and provides high throughput compared to IP and MPLS networks due to the tunnels. As well as the performance of MPLS-TE, parameters such as packet loss and latency are very stable and much better as compared to traditional IP and MPLS networks. Therefore, implementation MPLS with traffic engineering overcoming the problems of congestion and provides the better utilization of network links. The performance analysis are presented as line graphs for each network.

5.3. Validity Threat

In order to validate the simulation of this thesis results, there were three different scenarios performed to achieve the desired goal. In all scenarios, data packets are sent between virtual machines as servers. There are some threats in the simulation results as the simulation for results validation was done. The comparison of all networks has been performed in the simulation environment, which may obtain different results in another environment as well as in the real environment or real computers. The data packets sent between servers are validated for Zip file. Therefore, results may have different if another type of data are sent. Author has tried to do this simulation close to a practical environment.

5.4. Future Work

To enhance the performance of the proposed system, some future studies are recommended:

- Use MPLS family methods such as MPLS-VPN or a variant of the MPLS like MPLS-TP.
- Use another environment such as NS3 or applying in a real environment.
- Use IS-IS protocol instead of OSPF as IGP inside the MPLS network and making comparison between them.
- Use more than three servers and measuring the performance between each other.
- Apply different scenarios and analysing the performance of the networks.

REFERENCES

1. Faiz Ahmed, Dr. Irfan Zafar, 2011. Analysis of traffic engineering parameters while using multi-protocol label switching (MPLS) and traditional IP networks, **Asian Transactions on Engineering**, 1(3): 2221-4267.
2. Tim Fiola, Jamie Panagos, 2011. Junos Networking Technologies, This Week: Deploying MPLS, **Juniper Networks Books**. ISBN 9367792468.
3. M. Aslam, 2008. Traffic engineering with Multi-Protocol Label Switching, Master Thesis, School of Engineering Science, Blekinge Institute of Technology, Ronneby, Sweden.
4. ES Jain, 2012. Performance Analysis of Voice over Multiprotocol Label Switching Communication Networks with Traffic Engineering, **International Journal of Advanced Research in Computer Science and Software Engineering**, 2(7): 195-199.
5. O. Akinsipe et al., 2012. Comparison of IP, MPLS and MPLS RSVP-TE Networks Using OPNET, **International Journal of Computer Applications (IJCA)**, 58(2).
6. M. Bhandure, G. Deshmukh, and J. N. Varshapriya, 2013. Comparative analysis of MPLS and non-MPLS networks, **International Journal of Engineering Research and Application**, 3(4): 71-76.
7. A. Sulaiman and O. Alhafidh, 2014. Performance Analysis of Multimedia Traffic over MPLS Communication Networks with Traffic Engineering, **International Journal of Computer Networks and Communications Security**, 2(3): 93-101.
8. M. Kumar, S. Sangal, 2015. Improving the usage of Network Resources using MPLS Traffic Engineering (TE), **International Journal of Current Engineering and Technology**, 5 (1): 261-265.
9. S. Kathiresan, 2015. Performance Analysis of MPLS over IP networks using CISCO IP SLAs. Simon Fraser University, M.Sc. thesis.

10. Akshay and P. Ahlawat, 2015. Comparison between Traditional IP Networks/Routing and MPLS, **International Journal of Scientific Engineering and Research (IJSER)**, 3(3).
11. Charles N. et al., 2016. A Comparative Simulation Study of IP, MPLS, MPLS-TE for Latency and Packet Loss Reduction over a WAN, **International Journal of Networks and Communications**, 6(1):1-7.
12. ALWAYN V., 2002. Advanced MPLS Design and Implementation, **Cisco Press**, 496-498, USA.
13. Harry G. Perros, 2005. Connection-oriented Networks SONET/SDH, ATM, MPLS and Optical Networks, John Wiley & Sons Ltd, (ISBN 0-470-02163-2).
14. Mümin GÜNGÖR, 2006. MULTI-PROTOCOL LABEL SWITCHING AND MPLS VPN SOLUTIONS, Dokuz Eylül University, Master Thesis, Izmir, Turkey.
15. GHEIN D. L., 2007. MPLS Fundamentals, **Cisco Press**.
16. L. Cittadini, G. Di Battista, M. Patrignani, 2013. MPLS Virtual Private Networks, in H. Haddadi, O. Bonaventure (Eds.), Recent Advances in Networking, 275-304.
17. Deepankar Medhi, & Karthikeyan Ramasamy, 2007. Network Routing: Algorithms, Protocols, and Architectures, Morgan Kaufmann. ISBN **0-12-088588-3**.
18. Michael Palmer, 2013. Hands-On Networking Fundamentals, Second Edition. Course Technology, Cengage Learning, ISBN-13: 978-1-111-30674-8, ISBN-10: 1-111-30674-5.
19. Jeffrey Cole; Walter E. Thain, 2016. A Small Network for Modeling MPLS, IEEE SoutheastCon.
20. OpenFlow Switch Specification, 2014. version 1.5.0, Open Networking Foundation.

21. Wolfgang Braun, Michael Menth, 2014. Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices, **future internet**, ISSN 1999-5903.
22. D. Kreutz, F. M. Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolkly, and S. Uhlig, 2015. Software-defined networking: A comprehensive survey, **proceedings of the IEEE**, **103(1)**.,14-76.
23. Antonio Sanchez-Monge, Krzysztof Grzegorz Szarkowicz, 2015. MPLS in the SDN Era, O'Reilly Media, Inc.
24. Junos OS, 2013. MPLS Configuration Guide, **Juniper Networks**, Inc.
25. Manoj Kumar and Shishir Sangal, 2015. Improving the usage of Network Resources using MPLS Traffic Engineering (TE), **International Journal of Current Engineering and Technology**, **5(1)**.
26. Bill Parkhurst, 2005. Routing first-step, **Cisco press**. ISBN: 1587201224,.
27. Adyasha Behera, Amrutanshu Panigrahi, 2015. Determining the network throughput and flow rate using GRS and AAL2R, **International Journal of UbiComp (IJU)**, **6(3)**.
28. Behrouz A. Forouzan, 2010. TCP/IP Protocol Suite-fourth Edition, McGraw-Hill Forouzan Networking. ISBN 978-0-07-337604-2.
29. Archana C., 2015. Analysis of RIPv2, OSPF, EIGRP Configuration on router Using CISCO Packet tracer, **International Journal of Engineering Science and Innovative Technology (IJESIT)**, **4(2)**.

CURRICULUM VITAE

Name and surname: MUSTAFA MAHMOOD HAMZA

Nationality: Iraq

Birth date and place: Baghdad 03/ 02/ 1980

Marital status: Married

Cell phone: +905315019100
+9647901583479

E-mail: mustafaalrawi80@yahoo.com, eng.alrawi80@gmail.com.

Correspondence Address: Bahçelievler Mah. Bahçelievler Cad. SUDE Apt. Blok
No: 52 İç kapı No: 11 TALAS, KAYSERİ, TURKEY.

EDUCATION

Degree	Institution	Date of graduation
M.Sc	Eeciyes University	2017
B.Sc	AL- Rafidain University Collage	2004
High school	Al-A'amiriya	1998

FOREIGN LANGUAGE

Arabic

English