# PERFORMANCE ANALYSIS OF MPLS OVER IP NETWORKS USING CISCO IP SLAs

By

Sathappan Kathiresan

PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ENGINEERING

In the
School of
Engineering Science



SIMON FRASER UNIVERSITY

Spring 2015

# APPROVAL

**Name:** **Sathappan Kathiresan**

**Degree:** **Master of Engineering**

**Title of Project:** **Performance Analysis of MPLS over IP networks using CISCO IP SLAs**

**Examining Committee:**

**Chair:** **Dr. Carlo Menon**
Associate Professor of the School of Engineering Science
Simon Fraser University

---

**Dr. Ljiljana Trajković**
Senior Supervisor
Professor of the School of Engineering Science
Simon Fraser University

---

**Dr. Parvaneh Saeedi**
Supervisor
Associate Professor of the School of Engineering Science
Simon Fraser University

**Date Approved:** _____

## Partial Copyright License

# ABSTRACT

Traffic Engineering (TE) is the method of optimizing performance of a communication network by vividly monitoring, envisaging, and regulating the behavior of data transmitted over the network. It involves methods and application of knowledge to gain performance objectives, which include movement of data through network, reliability, planning of network capacity, and efficient use of network resources. Deploying network services with Quality of Service enabled in an established IT infrastructure requires testing with current networking devices. This project addresses the problems of traffic engineering and evaluates the performance of Multi-Protocol Label Switching (MPLS) and Internet Protocol (IP) networks. In this project, I use CISCO IP Service Level Agreements (SLAs) for active traffic monitoring to analyze IP service levels for IP applications and services. The results compare performance of MPLS and IP networks.

**Keywords:** Traffic engineering, CISCO, IP SLAs, MPLS, IP networking, GNS3, network simulator.

## DEDICATION

*To my family for their love and support.*

# ACKNOWLEDGEMENTS

I would like to thank my senior supervisor, Prof. Ljiljana Trajković, for her valuable feedback and guidance. I would also like to thank Prof. Parvaneh Saeedi for her interest and support in my project.

# TABLE OF CONTENTS

ABSTRACT....iv
DEDICATION....v
ACKNOWLEDGEMENT....vi
TABLE OF CONTENTS....vii
LIST OF FIGURES....ix
LIST OF TABLES....x
LIST OF ACRONYMS....xi
1 INTRODUCTION....1
2 BACKGROUND....2
2.1 Traffic Engineering....2
2.2 IP Routing....5
2.3 Functionality of IP Routing....4
2.3.1 No Better Service....6
2.3.2 Class of Service (CoS)....7
2.3.3 Scalability....7
2.3.4 Recovery of IP Route....7
3 MULTI PROTOCL LABEL SWITCHING....8
3.1 Overview....8
3.2 MPLS Header....8
3.3 MPLS Label....9
3.4 MPLS Functionality....9
3.5 Components of the MPLS-TE Model....10
3.6 TE in MPLS network....11
3.6.1 MPLS Quick Rerouting....12
3.7 MPLS Signaling Protocols....12
3.7.1 Label Distribution Protocol (LDP)....12
3.7.2 Resorce Reservation Protocol (RSVP)....12
4 RELATED WORK....14
5 NETWORK ARCHITECTURE AND DESIGN....16
5.1 Implementation of IP and MPLS network....17
5.1.1 Introduction to Graphical Network Simulator....17
5.1.2 Router configuration for IP network....18
5.1.3 Router configuration for MPLS network....20
6 SIMULATION RESULTS....24
6.1 Simulation Model....24

6.2 Simulation Goal ..... 24
6.3 Simulation Configuration ..... 25
6.3.1 IP SLAs Configuration ..... 25
6.4 Simulation Scenarios ..... 26
6.4.1 First Scenario ..... 26
6.4.2 Second Scenario ..... 27
7 SIMULATION RESULTS AND DISCUSSION ..... 30
8 CONCLUSION ..... 34
REFERENCES ..... 35

# LIST OF FIGURES


Figure 1. Traffic engineering……... 4
Figure 2. IP routing functionality..……..... 5
Figure 3. MPLS header…….....8
Figure 4. MPLS label…….....9
Figure 5. MPLS forwarding..…….....10
Figure 6. MPLS TE…….....11
Figure 7. Proposed network architecture..... 16
Figure 8. IP forwarding table…….....19
Figure 9. MPLS forwarding table..... 22
Figure 10. MPLS TE tunnel status…..... 22
Figure 11. Screenshot from GNS3 software after configuring IP and MPLS..... 23
Figure 12. Simulation model…….....24
Figure 13. Simulation Scenario 1…….....27
Figure 14. Simulation Scenario 2…….....28
Figure 15. Latency for Tu {45,46,47} for IP and MPLS networks…….....30
Figure 16. RTT for Tu {45,46,47} for IP and MPLS networks…….....31
Figure 17. MOS for Tu {45,46,47} for IP and MPLS networks……..... 32

# LIST OF TABLES

Table 1. Topology details……..... 16
Table 2. Router interface details……..... 17
Table 3. IP network details..... 18
Table 4. MPLS network details……..... 20
Table 5. MPLD-TE tunnel details……..... 20
Table 6. VoIP schedule details..... 26
Table 7. MOS values…….. 32

# LIST OF ACRONYMS AND TECHNICAL TERMS

| | |
|---|---|
| AS | Autonomous System |
| TE | Traffic Engineering |
| MPLS | Multi-Protocol Label Switching |
| IP | Internet Protocol |
| VoIP | Voice over IP |
| P2P | Peer-to-Peer |
| RIP | Routing Information Protocol |
| OSPF | Open Shortest Path First |
| QoS | Quality of Service |
| RSVP | Resource Reservation Protocol |
| LDP | Label Distribution Protocol |
| CoS | Class of Service |
| FEC | Forward Equivalence Class |
| LER | Label Edge Router |
| LSR | Label Switching Router |
| LSP | Label Switching Path |
| LIB | Label Information Base |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |

# Chapter 1 INTRODUCTION

IP network is a collection of nodes that use the Internet protocol for communication. All nodes in an IP network are configured with the TCP/IP suite. Each node in an IP network is assigned a unique logical IP address that is used to differentiate between other nodes. IP network communication occurs when a host sends a data packet to another host by using its IP address [1]. Similarly, the receiving host identifies the sending host by its IP address. IP routing is a set of protocols that helps determine the most suitable path that the data packets may choose from source to destination. Data are routed from source to destination through a series of routers and across multiple networks. The IP routing protocols enable routers to build a routing table that associates final destinations with next hop addresses. When an IP packet is to be routed, a router uses its routing table to determine the next hop for the packet's destination (based on the destination IP address in the IP packet header) and routes the packet appropriately. The next router then repeats this process using its own routing table and on the process continues until the packet reaches its destination. At each stage, the IP address present in the packet header is sufficient to determine the next hop. A routing table is a set of rules that is used to determine the direction in which data packets have to travel. All IP-enabled devices, including routers and switches, use routing tables [2]. The routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network.

In this project, I have emulated a network architecture using Graphical Network Simulator (GNS3). The challenge of this project was to build a network architecture that can interact with external networks. CISCO IP Service Level Agreements are used to analyze the performance of MPLS over IP network.

The goal of this project is to emulate network architecture to compare the performance of IP and MPLS networks. We consider VoIP traffic (the most important service that requires TE) between source and destination and the statistics related to IP routing vs. MPLS are collected and analyzed. Following objectives are set to achieve the goal:

- Design a network architecture with routers configured for IP and MPLS networks.
- Emulate all routers in the network architecture.
- Configure routers to permit background traffic.
- Emulate two scenarios: Scenario 1 with background traffic and Scenario 2 without background traffic.
- Analyze simulation results.

# Chapter 2 BACKGROUND

In this Chapter, we discuss the fundamentals of key technologies involved in this project. In recent years, the Internet has undergone a significant change in its structure such as increased number of users and introduction of cloud computing. The increase in number of Internet users along with dynamic structural changes may cause Internet traffic congestion resulting in network failure, packet loss, and delay in delivering time-sensitive information [2]. The Internet Service Providers (ISPs) play a major role in connecting various geographical areas and have suggested a variety of solutions as:

- Capacity Expansion (CE)
- Network Architecture (NA)
- Traffic Engineering (TE).

TE overrides the other two methods because it ensures reliability and fast movement of data over network. It enables sending data to network nodes by overcoming the problems of congestion and network failures [3].

## 2.1 Traffic Engineering

TE is a technique to control the flow of data over the network by reserving bandwidth for specific services. TE may be also implemented to accommodate network maintenance [2]. The objective of the traffic engineering technique is to improve the performance of the operational network at the resource level as well as the traffic level. Parameters such as packet loss, delay, jitter, and throughput are used to measure the network performance. To choose between different routing paths, most IP networks use Interior Gateway Protocols (IGP) based on the Open Shortest Path First (OSPF) algorithm with static link weights. These weights provide the routers with a complete view of the network to populate routing tables. When links have distinct capacities, considering link utilization is more appropriate [2]. Network engineers employ a number of tools to automate

the process of monitoring network links and to send alerts when a link is heavily used. These network usage patterns collected over a certain period of time may help manage the flow of data at a particular time instance or for a particular service. The concept of traffic engineering in IP network is shown in Figure 1.

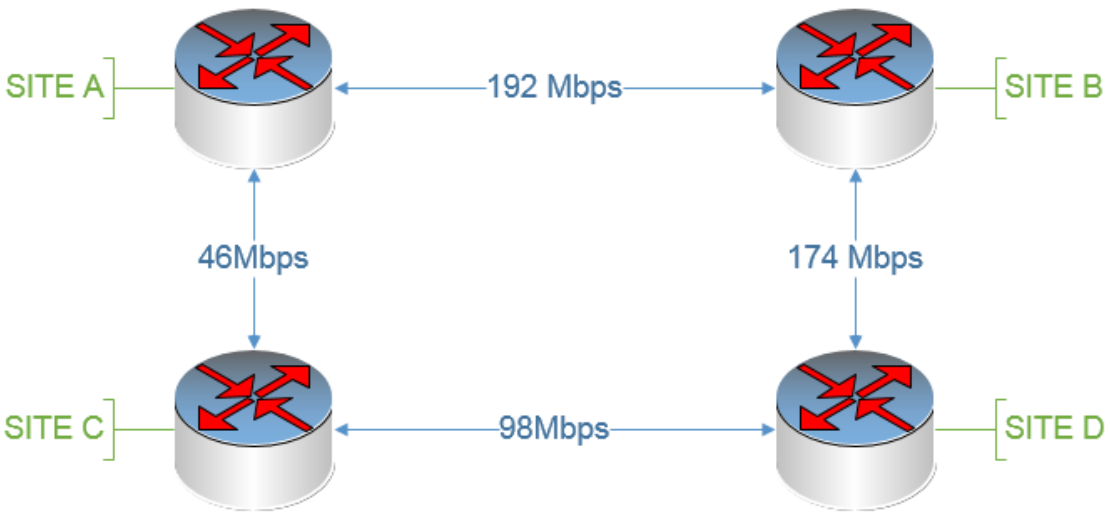


Figure 1: Traffic engineering in IP network.

All routers in sites {A, B, C, D} are configured with an Interior Gateway Protocol (IGP) and the networks are advertised between sites. The network shown in Figure 1 consists of four links with different link capacities. If site A wishes to communicate with site D, it can either communicate via site B or via site C. By default, a router dynamically selects the link with higher capacity to send the data unless a policy is defined through a static route.

## 2.2 IP Routing

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

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

## 2.3 Functionality of IP Routing

In an IP network, a router selects the next router for the destination of the packets based on its routing table. Every router in the path replicates the same process by using its routing table until the packet reaches its destination. IP routing is shown in Figure 2.

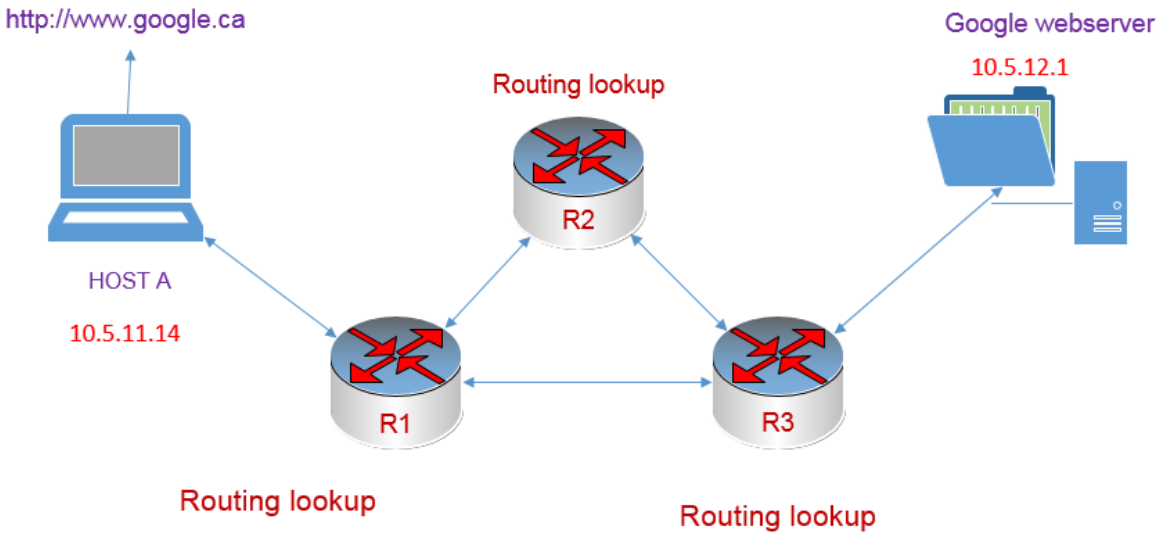


Figure 2: IP routing in a simple network.

The subnet associated with each router falls under the supernet (parent subnet) 10.5.0.0/16. If the host with IP address 10.5.11.4 wishes to access the webserver 10.5.12.1, it will send its packet on the path to the connected router via router R1 or via routers R1 and R2. Each router will check the destination address of the packet in its routing table. Routing table keeps information about the addresses of the interconnected network and the path that will be followed to send data towards the destination. Routing decision is based on the shortest path available to the destination. Protocols used for the IP routing are Border Gateway Protocol (BGP), Intermediate System-Intermediate System (IS-IS), OSPF (Open Shortest

Path First), and Routing Information Protocol (RIP) [2]. RIP keeps track of the closest router for each destination address and is suitable for smaller networks. OSPF keeps track of complete topological database of all connections in the local network and is suitable for larger networks. The Internet is divided into Autonomous Systems (AS). An AS is a group of routers that are under the control of a single administration. They exchange routing information by using a routing protocol [3].

AS is divided into the following three types:

- **Stub AS** has a single connection to the other autonomous system. Example of a stub network is a small campus network.
- **Transit AS** has multiple links with one or more autonomous systems. It allows data to be forwarded out of the autonomous system. Example of transit network is the Internet Service Provider (ISP) network.
- **Multi-homed AS** has multiple links with one or more autonomous systems but it does not allow data received on these links to be forwarded out of the autonomous systems. It is similar to a stub autonomous system. Example of multi-homed AS is a large enterprise network. Listed are some limitations of IP routing:

### 2.3.1 No Better Service

In IP routing for both residential and commercial networks, it is not possible to achieve better quality of service by paying a higher fee to the ISP provider. While smaller networks may not require better service, in case of larger networks a loss of data may result in a network outage.

### 2.3.2 Class of Service (CoS)

Class of Service (CoS) refers to the capability of a network to identify between different types of data. IP routing does not distinguish between different types of data traffic and all data are treated in a similar fashion. CoS support based on the source or service is impossible and, thus, it results in congestion. Multi-Protocol Label Switching (MPLS) solves this issue by using the Forward Equivalence Class (FEC) [4]. Destination-based routing does not provide a mechanism for load balancing across unequal paths.

### 2.3.3 Scalability

In IP routing, both route lookup and forwarding processes are combined. The route lookup process takes longer due to the growing size of routing table and is inversely proportional to the speed of the network link, which implies that it is not scalable. MPLS solves this problem by separating two planes: control plane is responsible for the route lookup process while the data plane performs forwarding of network traffic [4].

### 2.3.4 Recovery of an IP Route

The increasing size of the Internet makes it is vulnerable to network link failures. Hence, there is a need for devising a method for the fast recovery. When a link between two routers fails, the recovery of the IP route mainly depends on three factors: amount of time to detect the failure of the network, passing broken link information across the network, and calculating new routing tables. Each routing protocol is able to update the status of the links between its neighbors but is unable to find the locations of failed routes that create delay in building the IP routing tables [3].

# Chapter 3 MULTI PROTOCOL LABEL SWITCHING (MPLS)

## 3.1 Overview

MPLS was introduced by the Internet Engineering Task Force (IETF) to make the Internet scalable, fast, and adaptable to new routing mechanisms, and manageable [4]. MPLS uses TE to share the network load among unequal path links. In MPLS, packets are first encapsulated at the ingress router by assigning labels and then forwarded on label switched paths. At the egress router, the label is removed and the packet is delivered to the destination. MPLS is often called the Layer 2.5 technology. It enables easy construction of the explicit routes for a specific source or a service [4].

## 3.2 MPLS Header

A 32-bit MPLS header consists of a label field, experimental field, stack, and time to live field [5]. The fields present in the MPLS header are shown in Figure 3.

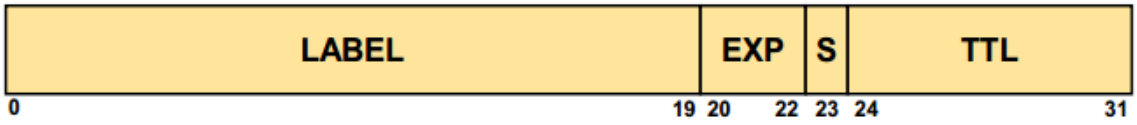


Figure 3: 32 BIT MPLS header [5].

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

## 3.3 MPLS Label

MPLS label is inserted between L2 and L3 headers. The location of the MPLS label is shown in Figure 4.

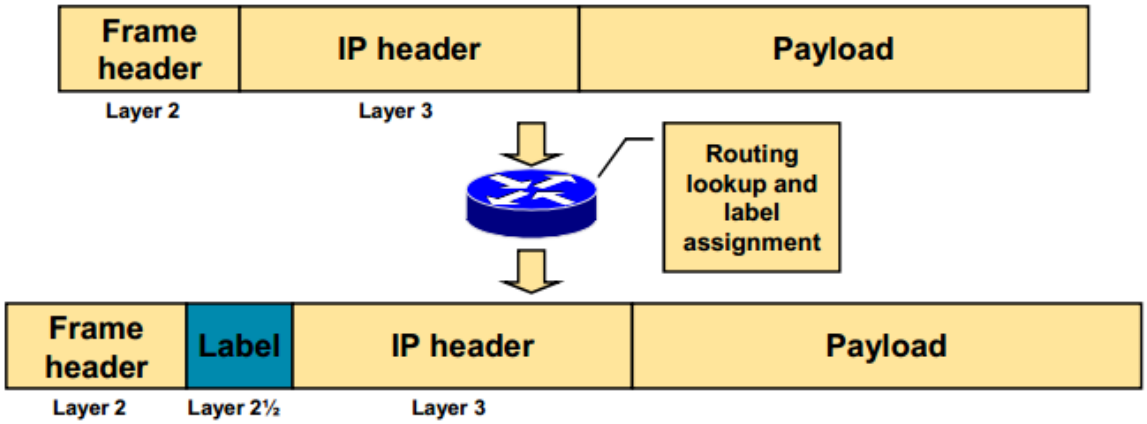


Figure 4: MPLS label [5].

## 3.4 MPLS Functionality

MPLS process is performed on two types of routers: Label Edge Router (LER) and Label Switch Router (LSR). LER R1 (ingress router) shown in Figure 5 works at the edge of the MPLS network. Its interfaces are connected to other networks. It routes traffic and works as an interface between the MPLS network and the IP network. 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 path called Label Switched Path (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 [5]. 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 [5]. MPLS forwarding mechanism is shown in Figure 5.

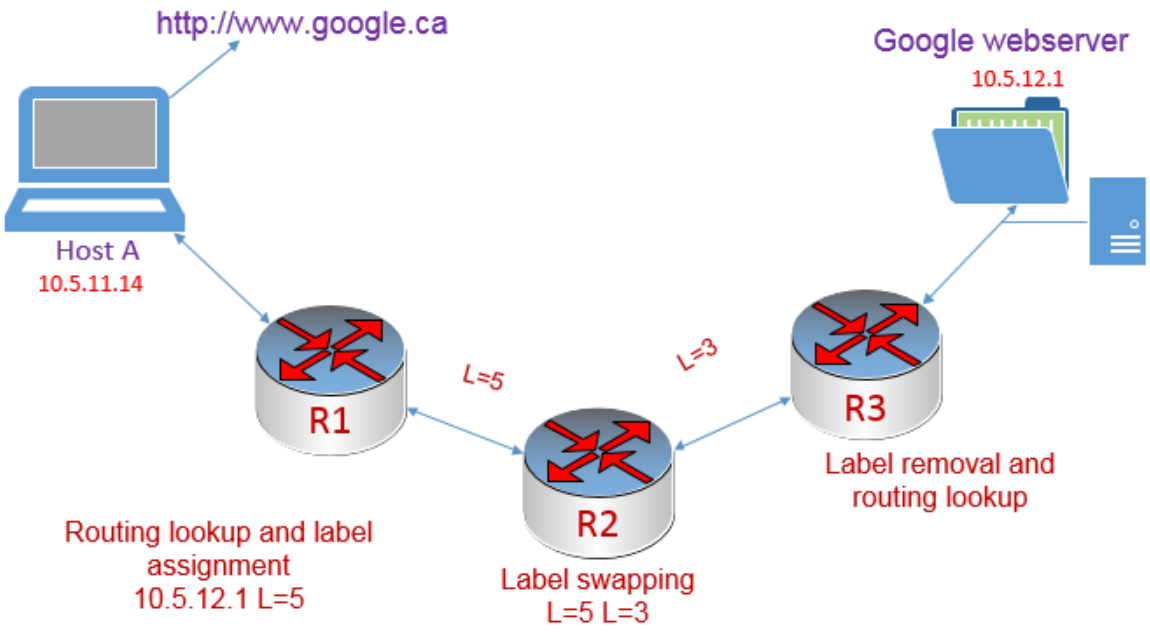


Figure 5: MPLS forwarding mechanism.

All routers in Figure 5 are configured for MPLS. Only the LER routers perform a routing lookup and assign a label. LSR routers switch packets based on simple label lookups and swap labels. In Figure 5, R1 and R3 are the edge routers while R2 is the core router. To reach webserver 10.5.12.1 from R1, R1 performs route lookup and assigns a label L=5 and forwards the packets while core router R2 performs label lookup and swaps the label to L=3 and forwards the packet. Finally, at the egress end, router R3 removes the label and performs route lookup and delivers data to the destination.

## 3.5 Components of the MPLS-TE Model

MPLS consists of the following basic components [4], [5]:

- Packet Forwarding

- MPLS label switching
- Information Distribution Component
  - IGP (OSPF/IS-IS) extension
- Path Selection
  - Calculates Label Switching Path (LSP)
- Signaling Component
  - MPLS signaling protocols.

## 3.6 TE in MPLS network

In MPLS-TE, traffic may be forwarded based on other parameters such as QoS, source, or policy and is show in Figure 6.

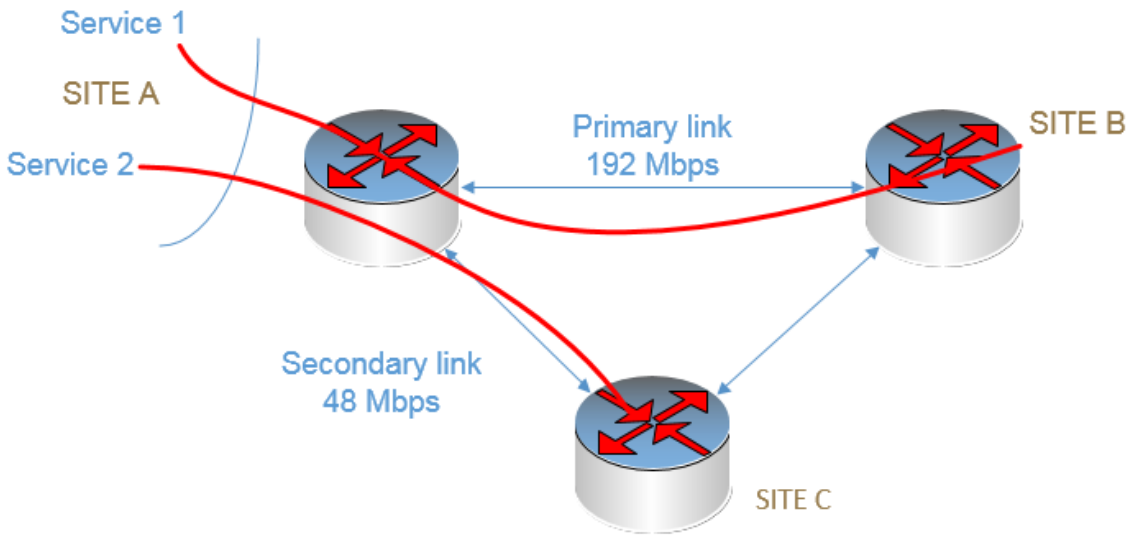


Figure 6: MPLS traffic engineering.

All routers are configured with MPLS enabled and the Resource Reservation Protocol (RSVP). MPLS-TE tunnels are configured between Service 1 and Site B, and Service 2 and Site C. Thus, load sharing across unequal paths can be achieved [6] – [10].

### 3.6.1 MPLS Quick Rerouting

There are two types of MPLS quick reroute methods: One-to-one backup method is used to create alternative route LSPs for every protected LSP on every point of failure and Facility backup method that generates a bypass tunnel to guard a failure point.

## 3.7 MPLS Signaling Protocols

The two primary signaling protocols of MPLS are Label Distribution Protocol (LDP) and Resource Reservation Protocol (RSVP) [7], [11], [12].

### 3.7.1 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 [6], [7].

### 3.7.2 Resource Reservation Protocol (RSVP)

RSVP offers TE features that are not available with LDP-signaled 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. 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.

# Chapter 4 RELATED WORK

Various simulations and experiments were performed to analyze the performance of MPLS over IP networks. Network performance measures are bandwidth, throughput, latency, jitter, and error rate. They are usually evaluated using network simulators such as ns-2, ns-3, Riverbed Modeler, OMNEST, and OMNET++. D. Adami et al., [13] discussed the design and development of the control and data planes that are required to provide Label Switching Path (LSP) support in an MPLS node. In particular, they have developed a simulator and implemented new software modules for the Peer-to-Peer (P2P) LSPs path computation, the RSVP-TE signaling protocol, and the forwarding mechanism.

D. Adami et al., [14] proposed a new ns-2 module to speed-up the design, development, and deployment of DiffServe-aware MPLS network. MPLS DiffServ-aware allows network operators to provide services that require strict QoS performance guarantees. The new software module is used to simulate the RSVP-TE protocol using the ns-2 simulator.

N. Aslam [10] compared performance of MPLS networks and IP networks. A network topology is designed and a MATLAB based simulation tool is used to send bulk data within a network. Network performance is measured with MPLS enabled or disabled. The author illustrates that MPLS network may perform better than the traditional IP networks. Sending data file from a source to destination does not require traffic engineering.

Deshmukh et al., [15] presented an overview of MPLS networks and compared performance of IP routing and the MPLS forwarding mechanism. The authors did not discuss TE, which is an essential part of MPLS.

None of these contributions require implementation of MPLS-TE and were evaluated in a simulated environment without taking the real-time traffic into consideration. Especially when deploying a new network service such as VoIP in

an enterprise infrastructure, it is essential to consider network traffic. Thus, failing to consider the existing network traffic and measuring network performance in a simulated environment may not give the same performance result compared to deployed network service.

# Chapter 5 NETWORK ARCHITECTURE AND DESIGN

Functionalities, components, and characteristics of IP and MPLS networks have been discussed in Chapter 2 and Chapter 3. The network proposed for the performance study is shown in Figure 7. Details of network topology and configuration of routers' interfaces are explained in Table 1 and Table 2, respectively.

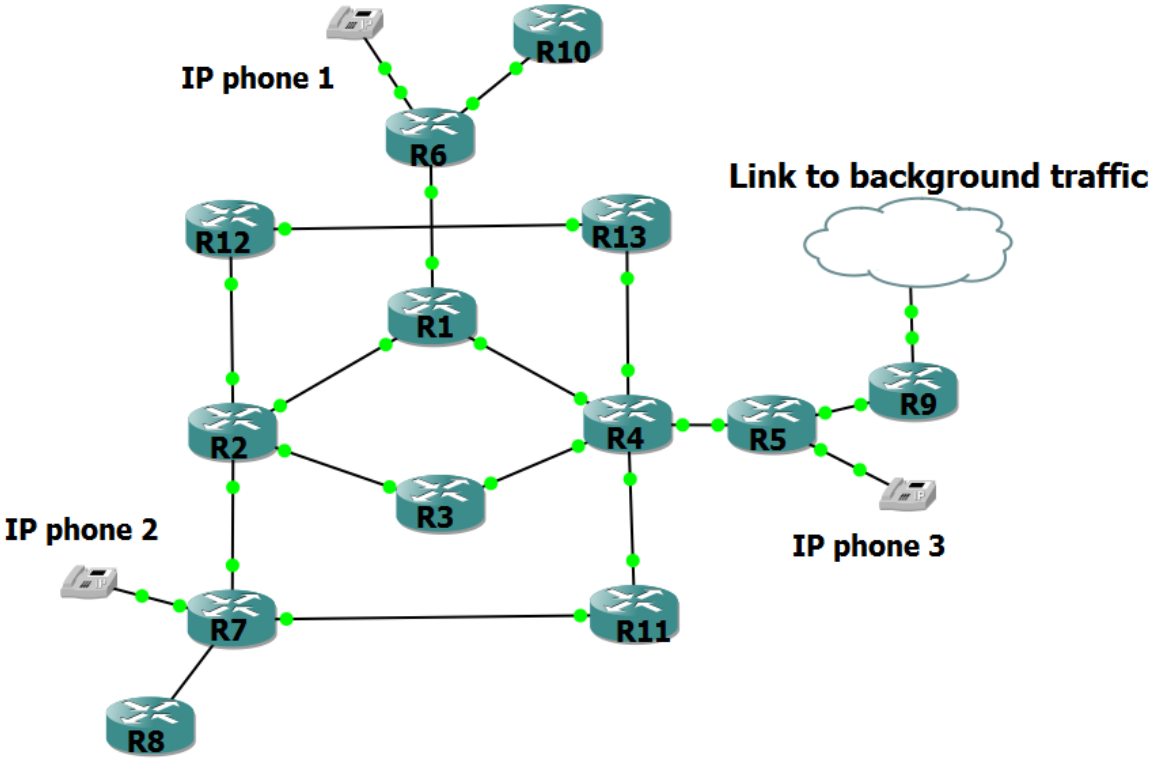


Figure 7: Proposed network architecture.

Network topology details:

| | |
|---|---|
| Number of routers | 13 |
| Number of IP phones | 3 |
| Number of links | 19 |
| Router model | 7400 series |
| Router operating system | CISCO 7400 15.4.M2/12.4(4)T1 |
| Cloud interface | Internet gateway |

Table 1: Topology details.

Router Interface Configuration:

| Routers | Networks |
|---|---|
| R1 | 10.0.12.0/24,10.0.13.0/24,10.0.14.0/24 |
| R2 | 10.0.17.0/24,10.0.11.0/24,10.0.12.0/24 |
| R3 | 10.0.16.0/24,10.0.15.0/24 |
| R4 | 10.0.15.0/24,10.0.21.0/24, 10.0.22.0/24,10.0.23.0/24,10.0.14.0/24 |
| R5 | 10.0.22.0/24,10.0.24.0/24, 10.0.115.0/24 |
| R6 | 10.0.13.0/24,10.0.25.0/24, 10.0.110.0/24 |
| R7 | 10.0.18.0/24,10.0.20.0/24, 10.0.105.0/24 |
| R8 | 10.0.19.0/24,10.0.18.0/24 |
| R9 | 10.0.24.0/24,10.0.19.0/24 |
| R10 | 10.0.25.0/24,10.0.26.0/24 |
| R11 | 10.0.20.0/24, 10.0.21.0/24 |
| R12 | 10.0.11.0/24,10.0.10.0/24 |
| R13 | 10.0.10.0/24,10.0.23.0/24 |
| Cloud | 0.0.0.0/0.0.0.0,10.0.19.0/24 |

Table 2: Router interface details.

## 5.1 Configuration of IP and MPLS networks

### 5.1.1 Introduction to Graphical Network Simulator (GNS3)

GNS3 provides a virtual environment to design and optimize networks of any size without the need to build physical hardware infrastructure. GNS3 uses real Cisco

IOS images that emulate routers using a program called Dynamips. GNS3 is similar to the Graphical User Interface (GUI) part of any other installed software. Using GUI, it is easy to build complex labs consisting of a variety of supported Cisco routers. Dynampis is often referred to as the back-end while Dynagen is the front-end system mainly because Dynagen communicates with Dynamips using a hypervisor. The entire system simplifies the configuration process. Graphical Network Simulator is installed on a computer system and the network architecture is designed and configured for IP and MPLS networks.

## 5.1.2 Router configuration for IP network

IP network requires configuration of routing protocols in each router to advertise its network and also to identify the path to the destination address. IP network details are shown in the Table 3.

**IP network configuration:**

| | |
|---|---|
| Routing protocols | OSPF |
| Routers | R {1-13} |

Table 3: IP network details.

### 5.1.2.1 Open Shortest Path First (OSPF) configuration:

```
interface FastEthernet1/0
 ip address 10.0.14.2 255.255.255.0
 !
interface FastEthernet2/0
 ip address 10.0.22.1 255.255.255.0
 !
interface FastEthernet3/0
 ip address 10.0.21.2 255.255.255.0
 !
router ospf 1
 log-adjacency-changes
 network 10.0.14.0 0.0.0.255 area 0
 network 10.0.15.0 0.0.0.255 area 0
 network 10.0.21.0 0.0.0.255 area 0
 network 10.0.22.0 0.0.0.255 area 0
 network 10.0.23.0 0.0.0.255 area 0
```

!

After configuring OSPF in each router, the routers can advertise their networks to other routers and, thus, populate a routing table in each router. IP routing table is shown in Figure 8.

```
R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.22.3 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 18 subnets, 2 masks
O       10.0.10.0/24 [110/2] via 10.0.23.2, 00:12:28, FastEthernet4/0
O       10.0.11.0/24 [110/3] via 10.0.23.2, 00:12:28, FastEthernet4/0
                     [110/3] via 10.0.15.1, 00:12:28, FastEthernet0/0
                     [110/3] via 10.0.14.1, 00:12:28, FastEthernet1/0
C       10.0.14.0/24 is directly connected, FastEthernet1/0
C       10.0.15.0/24 is directly connected, FastEthernet0/0
O       10.0.12.0/24 [110/2] via 10.0.14.1, 00:12:28, FastEthernet1/0
O       10.0.13.0/24 [110/2] via 10.0.14.1, 00:12:28, FastEthernet1/0
O IA    10.0.24.0/24 [110/2] via 10.0.22.3, 00:12:28, FastEthernet2/0
O IA    10.0.25.0/24 [110/3] via 10.0.14.1, 00:12:28, FastEthernet1/0
O IA    10.0.18.0/24 [110/3] via 10.0.21.1, 00:12:28, FastEthernet3/0
O       10.0.16.0/24 [110/2] via 10.0.15.1, 00:12:28, FastEthernet0/0
O       10.0.17.0/24 [110/3] via 10.0.21.1, 00:12:29, FastEthernet3/0
                     [110/3] via 10.0.15.1, 00:12:29, FastEthernet0/0
                     [110/3] via 10.0.14.1, 00:12:29, FastEthernet1/0
C       10.0.22.0/24 is directly connected, FastEthernet2/0
C       10.0.23.0/24 is directly connected, FastEthernet4/0
O       10.0.20.0/24 [110/2] via 10.0.21.1, 00:12:29, FastEthernet3/0
C       10.0.21.0/24 is directly connected, FastEthernet3/0
O       10.0.105.1/32 [110/3] via 10.0.21.1, 00:12:29, FastEthernet3/0
O       10.0.110.1/32 [110/3] via 10.0.14.1, 00:12:29, FastEthernet1/0
O       10.0.115.1/32 [110/2] via 10.0.22.3, 00:12:29, FastEthernet2/0
S*   0.0.0.0/0 [1/0] via 10.0.22.3
R4#
```

Figure 8: IP forwarding table.

### 5.1.3 Router configuration for MPLS network

MPLS network requires tag switching to be enabled on all interfaces of a router that belongs to the MPLS domain. The protocol, which advertises label number across the network (similar to advertising subnets in IP network), should also be enabled. LDP uses the MPLS forwarding mechanism while RSVP takes

advantage of the TE options. MPLS network configuration details are shown in Table 4 and Table 5.

MPLS network configuration:

| | |
|---|---|
| Routing protocols | RIP, IS-IS, OSPF |
| Forwarding mechanism | MPLS, MPLS-TE |
| No. of TE tunnels | 3 |

Table 4: MPLS network details.

| Tunnel number | Source | Destination |
|---|---|---|
| 45 | R7 | R6 |
| 46 | R6 | R5 |
| 47 | R5 | R7 |

Table 5: MPLS-TE tunnel details.

### 5.1.3.1 Multi-Protocol Label Switching (MPLS) configuration:

```
mpls ip
mpls traffic-eng tunnels
!
ip cef
!
ip rsvp bandwidth 1000 sub-pool 10
!
tag-switching ip
!
interface FastEthernet1/0
 ip address 10.0.14.2 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
!
interface FastEthernet2/0
 ip address 10.0.22.1 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
!
interface FastEthernet3/0
 ip address 10.0.21.2 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
!
interface FastEthernet4/0
 ip address 10.0.23.1 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
```

```
!
router ospf 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 log-adjacency-changes
 network 10.0.14.0 0.0.0.255 area 0
 network 10.0.15.0 0.0.0.255 area 0
 network 10.0.21.0 0.0.0.255 area 0
 network 10.0.22.0 0.0.0.255 area 0
 network 10.0.23.0 0.0.0.255 area 0
!
```

#### 5.1.3.2 MPLS-TE tunnels configuration:

It is a best practice to create a loopback interface in the router to enable MPLS-TE tunnel and assign the IP address of loopback to the tunnel.

```
!
interface Loopback0
 ip address 10.0.105.1 255.255.255.0
!
interface Tunnel45
 ip unnumbered Loopback0
 tunnel destination 10.0.110.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 5 5
 tunnel mpls traffic-eng bandwidth  250
 tunnel mpls traffic-eng path-option 1 explicit name path1
 tunnel mpls traffic-eng path-option 2 dynamic
 no routing dynamic
!
```

An explicit path for each tunnel to reach the destination should be specified. The source and destination for each tunnel are shown in Table 5.

Listed is the explicit path configuration for tunnel 45 (R7 to R6):

```
tunnel mpls traffic-eng path-option 1 explicit name path1

!
ip explicit-path name path1 enable
 next-address 10.0.17.1
 next-address 10.0.12.2
 next-address 10.0.110.1
!
```

If the selected link is broken, the dynamic path is set:

```
tunnel mpls traffic-eng path-option 2 dynamic
```

After configuring MPLS and MPLS-TE, the router advertises its MPLS forwarding table to its neighbors as shown in Figure 9. The MPLS forwarding table for various subnets and at the local tags 28 and 29 are shown in Figure 9. Shown is the point2point tunnel 45.

```
Local  Outgoing    Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     22          10.0.21.0/24     0          Fa1/0      10.0.17.1
17     Pop tag     10.0.12.0/24     0          Fa1/0      10.0.17.1
18     Pop tag     10.0.16.0/24     0          Fa1/0      10.0.17.1
19     20          10.0.15.0/24     0          Fa1/0      10.0.17.1
20     17          10.0.13.0/24     0          Fa1/0      10.0.17.1
21     16          10.0.14.0/24     0          Fa1/0      10.0.17.1
22     19          10.0.22.0/24     0          Fa1/0      10.0.17.1
23     Untagged[T] 10.0.25.0/24     0          Tu45       point2point
24     21          10.0.24.0/24     0          Fa1/0      10.0.17.1
25     Pop tag     10.0.11.0/24     0          Fa1/0      10.0.17.1
26     23          10.0.23.0/24     636        Fa1/0      10.0.17.1
27     Pop tag [T] 10.0.110.1/32    0          Tu45       point2point
28     25          10.0.115.1/32    0          Fa1/0      10.0.17.1
29     26          192.168.137.0/24 0          Fa1/0      10.0.17.1
30     32          10.0.10.0/24     0          Fa1/0      10.0.17.1

[T]     Forwarding through a TSP tunnel.
        View additional tagging info with the 'detail' option
R7#
```

Figure 9: MPLS forwarding table.

The tunnel status is shown in Figure 10.

```
R7#
R7#
R7#sh ip int br | inc Tunn
Tunnel45                  10.0.105.1      YES TFTP   up                    up
R7#
R7#
```

Figure 10: MPLS-TE tunnel status.

The proposed network architecture with the implementation of IP and MPLS networks ready for simulation is shown in Figure 11.

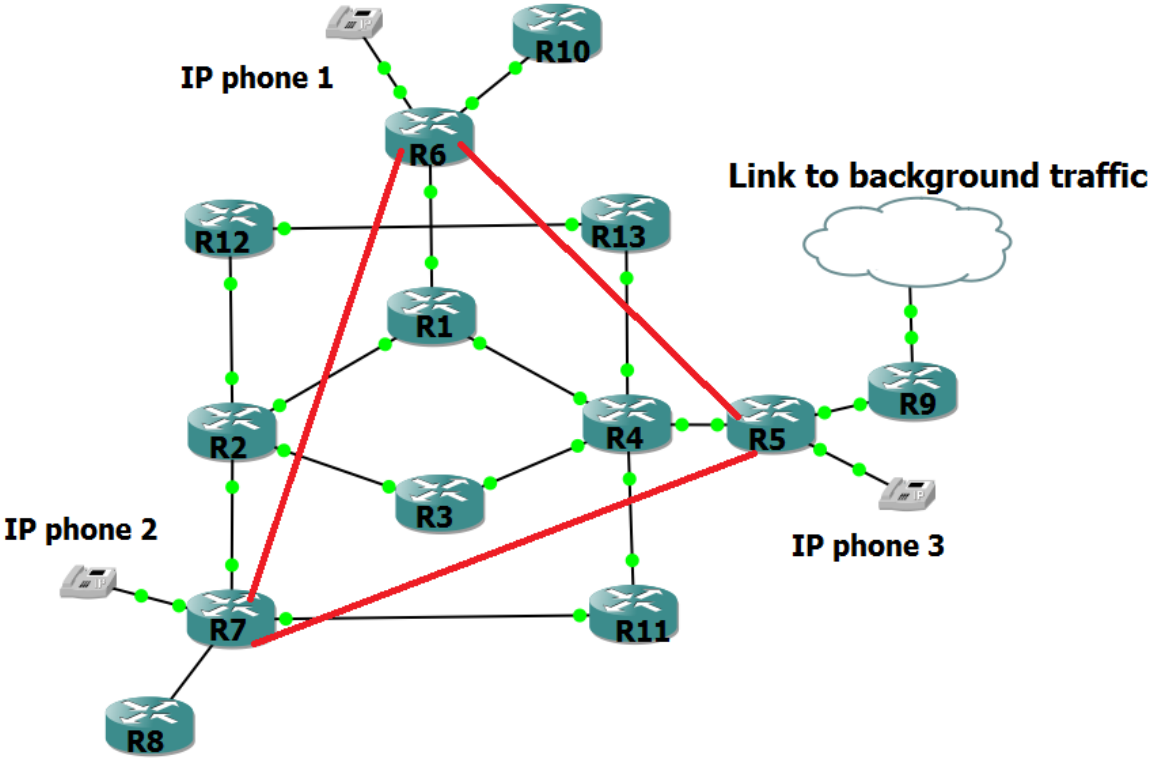


Figure 11: Screenshot from the GNS3 software after configuring IP and MPLS networks.

# Chapter 6 SIMULATION RESULTS

## 6.1 Simulation Model

Computer network simulations help network engineers identify the techniques and technologies that may be used to improve network performance. Simulation model is shown in Figure 12.

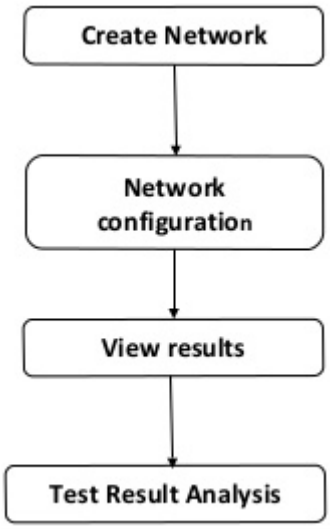


Figure 12: Simulation model.

## 6.2 Simulation Goals

The purpose of this simulation project is to evaluate performance of MPLS and IP networks. Performance analysis is usually performed in a simulated environment. We consider two simulation scenarios: without and with background traffic.

## 6.3 Simulation Configuration

We use Cisco IP SLAs (Service Level Agreements) to generate VoIP traffic between source and destination. CISCO IP SLA is a part of Cisco Operating System (IOS) software that enables Cisco customers to analyze IP service levels for IP applications and services using active traffic monitoring and generation of traffic in a continuous, reliable, and predictable manner for measuring network performance. With Cisco IOS IP SLAs, service provider's customers may measure and provide service level agreements while enterprise customers may verify service levels, verify outsourced service level agreements, and understand network performance. Cisco IOS IP SLAs may perform network assessments, verify quality of service (QoS), ease the deployment of new services, and assist with network troubleshooting [16].

### 6.3.1 IP SLAs Configuration

To test the network performance using Cisco IP SLAs, IP SLAs should be configured at the source and destination. In this project, we generate VoIP traffic between routers R7 and R6, R6 and R5, R5 and R7. We compare the performance of IP and MPLS networks under two scenarios [17]–[20]. Types of traffic that may be generated using Cisco IP SLAs are:

```
dhcp          DHCP Operation
dns           DNS Query Operation
exit          Exit Operation Configuration
frame-relay   Frame-relay Operation
ftp           FTP Operation
http          HTTP Operation
icmp-echo     ICMP Echo Operation
path-echo     Path Discovered ICMP Echo Operation
path-jitter   Path Discovered ICMP Jitter Operation
slm           SLM Operation
tcp-connect   TCP Connect Operation
udp-echo      UDP Echo Operation
udp-jitter    UDP Jitter Operation
voip          Voice Over IP Operation
```

## 6.4 Simulation Scenarios

In this phase, we validate simulation results using graphs and statistics. Two scenarios are chosen that shows the time taken to perform VoIP IP SLAs operations by analyzing the following three parameters:

1. Round Trip Time (RTT): The time required for a packet to travel from a specific source to a destination and back again. The RTT can range from a few milliseconds to several seconds.

2. Mean Opinion Score (MOS): A voice quality metric.

3. Latency: It is an expression of how much time it takes for a packet of data to travel from a source to a destination.

### 6.4.1 First Scenario

The IP SLA configuration to generate VoIP traffic between source and destination is shown in Table 6. IP SLAs VoIP operation uses UDP traffic to generate VoIP scores and use UDP jitter operation to proactively monitor VoIP quality inside the network. First Scenario has no background traffic and evaluates the RTT, MOS value, and latency for IP and MPLS networks and is shown in Figure 13.

| | |
|---|---|
| Codec | G.711 A-LAW |
| Packet Payload | 180 bytes |
| No of packets | 1000 |
| Packet interval | 20ms |
| Frequency | 60000ms |
| Graph results are plotted for every | 300 seconds |

Table 6: VoIP schedule details.

**Source:**

```
Configure terminal
ip sla 10
source-ipaddress 10.0.17.2
udp-jitter 10.0.25.1 16548 codec g711alaw codec-interval 20
codec-numpackets 1000 codec-size 25 control enable advantage-
factor 0
frequency 1000ms
request-data-size 180
history distributions-of-statistics-kept 3
history distributions-of-statistics-kept 3
sh ip sla configuration
sh ip sla statistics
```

**Destination:**

```
ip sla responder
sh ip sla responder
```

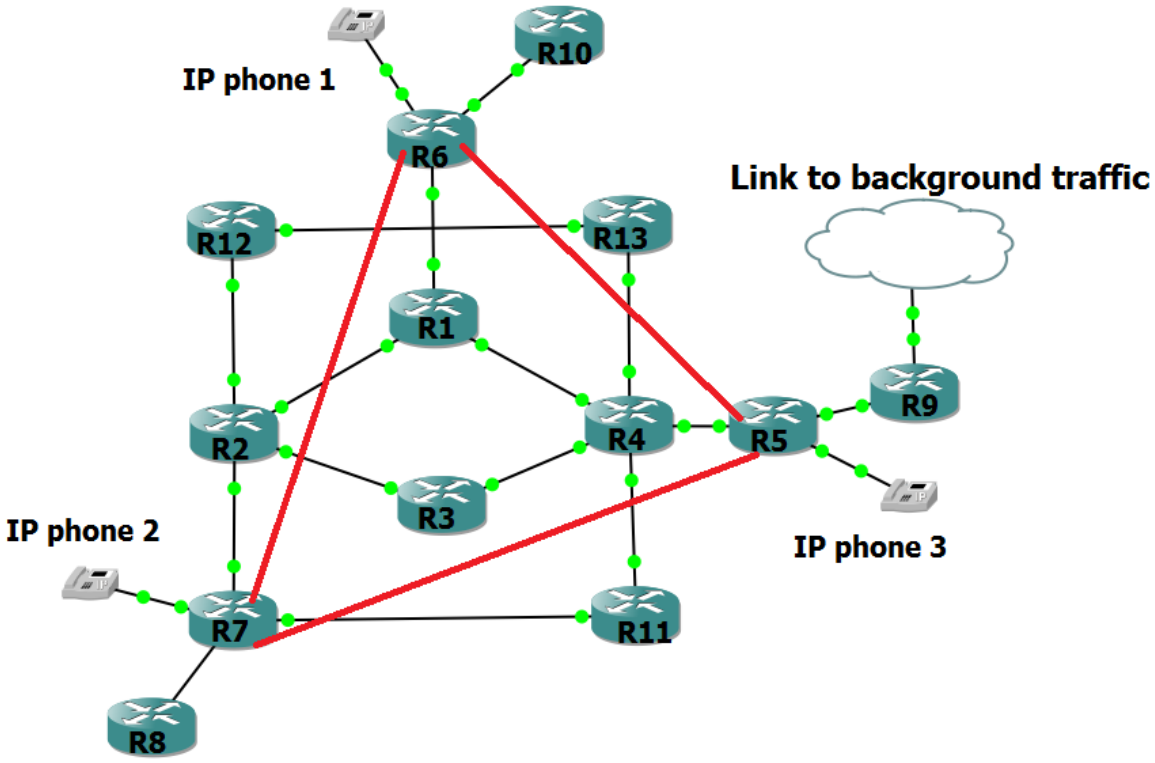


Figure 13: Simulation Scenario 1.

### 6.4.2 Second Scenario

Scenario 2 is similar to Scenario 1 except that it introduces background traffic. RTT, MOS value, and latency are measured for IP and MPLS networks shown in Figure 14. Background traffic is initiated by the neighboring networks.

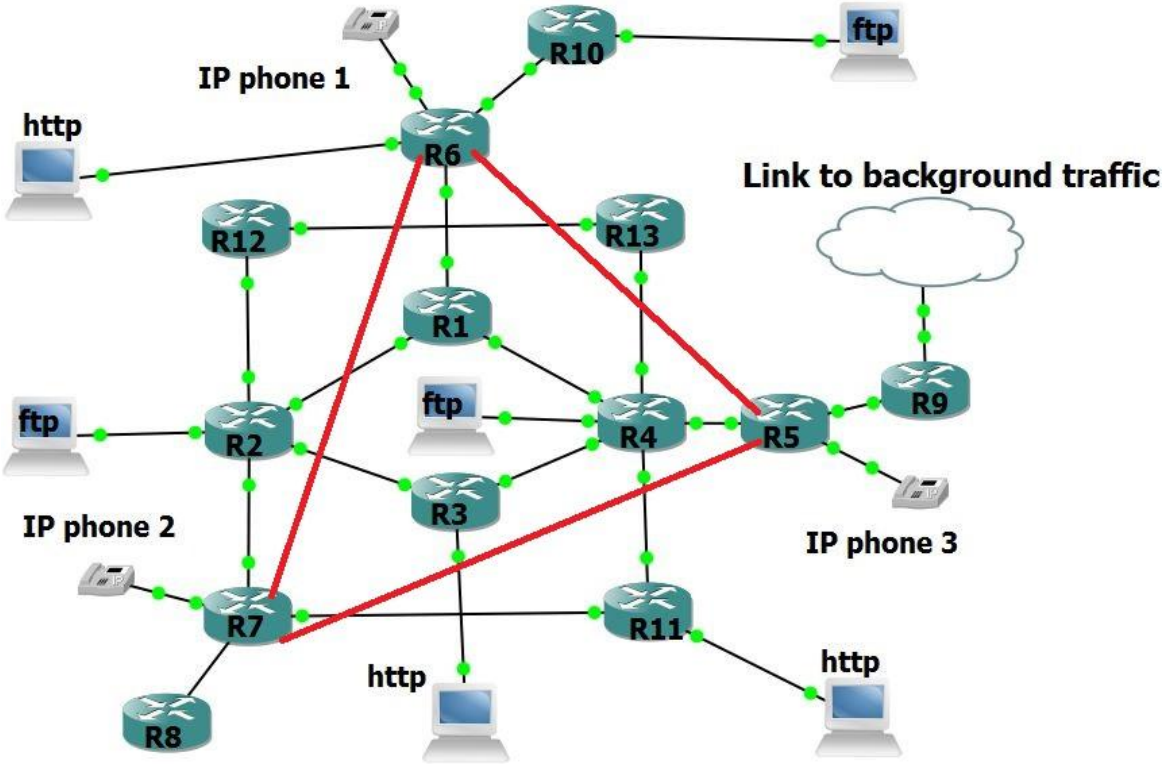


Figure 14: Simulation Scenario 2.

#### 6.4.2.1 Background traffic configuration:

Global configuration

```
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.137.1
ip nat inside source list 1 interface FastEthernet 1/0 overload
```

## HTTP traffic

```
ip sla 20
http get http://www.sfu.ca
frequency 60
http get http://www.facebook.com
frequency 60
sh ip sla configuration
sh ip sla statistics
```

## FTP traffic

```
ip sla 25
ftp get ftp://test:P@$$w0rd@50.0.0.0:777/test.png
frequenct 60
sh ip sla configuration
sh ip sla statistics
```

# Chapter 7 SIMULATION RESULTS AND DISCUSSION

The main theme of the project is to compare the performance of MPLS and IP networks using two simulation scenarios. In simulations, we have initiated VoIP IP SLAs operation from a source to a specific destination and analyzed the RTT, MOS, and Latency for both networks. Latency and RTT are shown in Figure 15 and Figure 16, respectively.

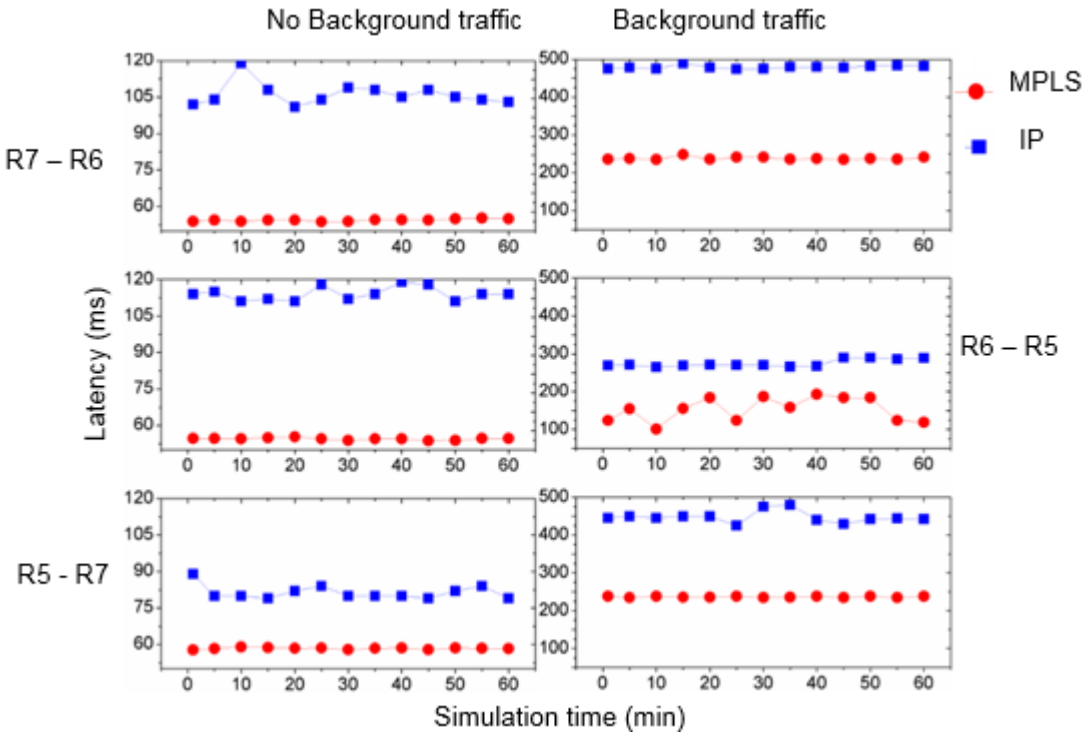


Figure 15: Latency for links R7–R6 (Tu45), R6–R5 (Tu46), and R5–R7 (Tu47) with and without background traffic for MPLS and IP networks.

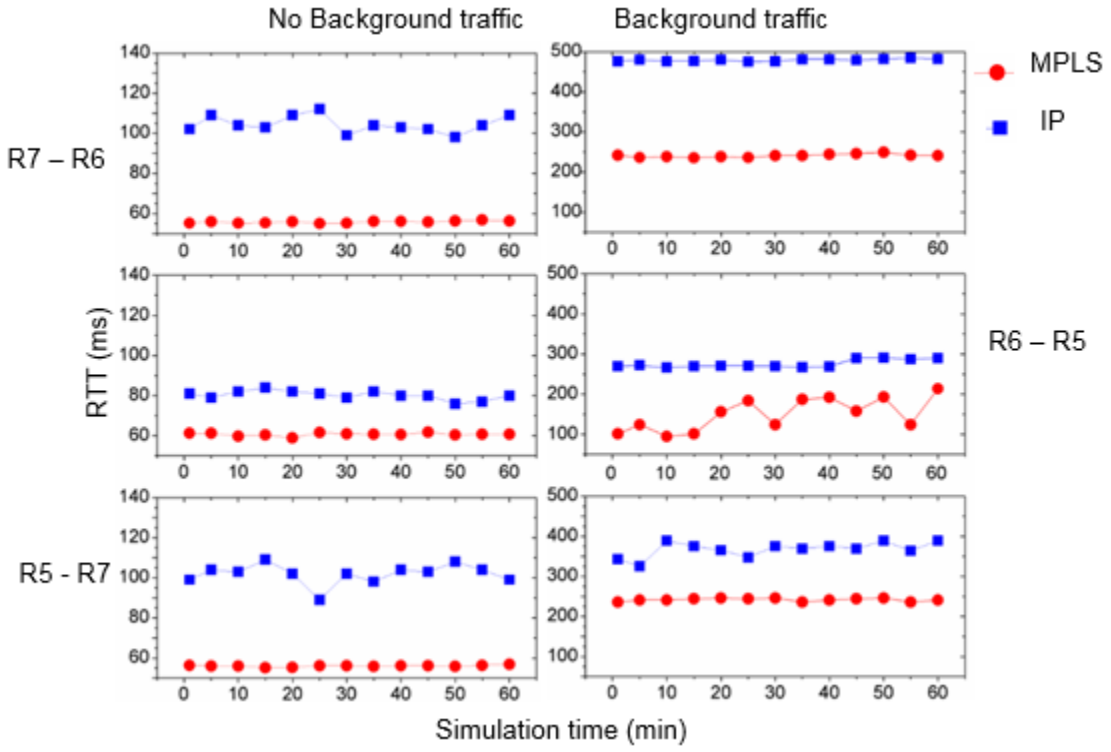


Figure 16: RTT for link R7–R6 (Tu45), R6–R5 (Tu46), and R5–R7 (Tu47) with and without background traffic for MPLS and IP networks.

In both scenarios, all three links in the IP network have higher latency and higher RTT compared to MPLS network, as shown in Figure 15 and Figure 16. There is a difference in latency and RTT between Scenario 1 and Scenario 2 for both IP and MPLS networks. This difference is due to the presence of background traffic. When there is additional traffic, IP network cannot load balance the data traffic and, thus, has a greater one-way delay. However, MPLS network experiences a slight delay due to background traffic but manages to send data through TE tunnels and retains the Quality of Service. Higher one-way delay implies higher RTT. Thus, MPLS network exhibits better performance than IP network.

The Mean Opinion Score (MOS) is a test that has been widely used to obtain the user's view of the quality of the network, as shown in Table 8.

| Score | Quality | Description of Quality Impairment |
|---|---|---|
| 5 | Excellent | Imperceptible |
| 4 | Good | Just perceptible, but not annoying |
| 3 | Fair | Perceptible and slightly annoying |
| 2 | Poor | Annoying but not objectionable |
| 1 | Bad | Very annoying and objectionable |

Table 7: MOS ratings (Cisco IP SLAs).

All three links in the MPLS network have higher MOS values compared to the IP network, as shown in Figure 17.

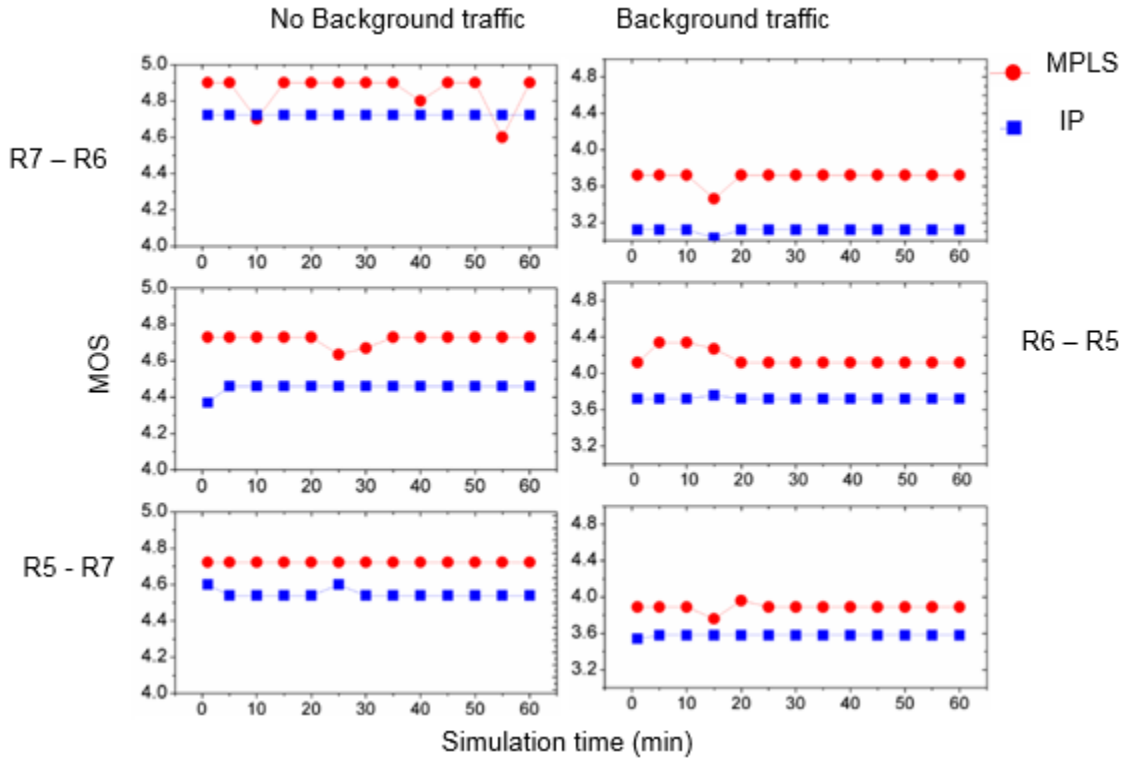


Figure 17: MOS for link R7–R6 (Tu45), R6–R5 (Tu46), R5–R7 (Tu47) with and without background traffic for MPLS and IP networks.

MPLS network forwards traffic based on parameters (QoS, source IP) and provides higher call quality. Simulation results show that the MPLS network has advantages when compared with the traditional IP network.

# Chapter 8 Summary and Conclusion

This project presented the design, implementation, and comparison of the MPLS and IP networks. We considered background traffic in the simulation and used Cisco IP SLA technology to generate and analyze network performance. The IP SLAs are unique to each vendor and provide better performance statistics when compared to model libraries accompanying simulation tools, such as OPNET. Since IP SLA technology is designed to bind and respond well with real time traffic, a network engineer may seamlessly design network architecture. IP SLA technology helps analyze the network traffic performance in real time without the need for simulation tools that may not produce realistic network performance-related results.

Our results show that:

- ✓ IP network is affected by high latency, round-trip time (RTT), and the mean opinion score (MOS).
- ✓ MPLS forwarding technique is faster than IP forwarding.
- ✓ MPLS network labels the traffic at the source.
- ✓ MPLS network is able to assign priorities to different data packets based on their labels.
- ✓ MPLS network is more efficient in terms of routing updates than IP network.
- ✓ MPLS network is able to produce higher call quality compared to IP network.

Simulation results show that MPLS is a better technique for traffic engineering than traditional IP.

# REFERENCES


[1] F. Baker, “Requirements for IP version 4 routers,” *IETF RFC 1812*, June 1995.

[2] B. Fortz, J. Rexford, and M. Thorup, “Traffic engineering with traditional IP routing protocols,” *IEEE Communications Magazine*, vol. 40, no. 10, pp. 18–124, October 2002.

[3] A. Viswanathan, N. Feldman, Z. Wang, and R. Callon, “Evolution of multiprotocol label switching,” *IEEE Communications Magazine*, vol. 36, no. 5, pp. 165–173, March 1998.

[4] E. Rosen, A. Viswanathan, and R. Callon, “Multiprotocol Label Switching architecture,” *IETF RFC 3031*, January 2001.

[5] A Feldmann, A. Greenberg, C. Lund, N. Reingold, and J. Rexford “Traffic engineering for IP networks,” *IEEE ACM Transactions on Networking* vol. 9, no. 12, pp. 142–147, June 2001.

[6] D. O. Awduche, “MPLS and traffic engineering in IP networks,” IEEE *Communication Magazine*, vol. 37, no. 12, pp. 42–48 December 1999.

[7] A. Ghanwani, "Traffic engineering standards in IP networks using MPLS," *IEEE Communications Magazine*, vol. 37, no. 12, pp. 49–53, December 1999.

[8] I. Hussain “Overview of MPLS technology and traffic engineering applications,” Internet Technologies Divisions, Cisco Systems, USA.

[9] N. Aslam, “Traffic engineering with MPLS,” Master Thesis, School of Engineering Science, Blekine Institute of Technology, Ronneby, Sweden.

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

[11] O. Gure, B. K. Boyaci, and N. O. Unverdi, “Analysis of the service quality on MPLS networks,” *5th European Conference on Circuits and Systems for Communication (ECCSC’10)*, Belgrade, Serbia, November 2010, pp. 43–46.

[12] J. L. Marzo, E. Calle, C. Scoglio, and T. Anjali, “QoS online outing and MPLS multilevel protection: a survey,” *IEEE Communication Magazine*, vol. 41, no. 10, pp. 126–132, October 2003.

[13] D. Adami, "A new ns2 module for the simulation of MPLS networks with point-to-multipoint LSPs support,” *IEEE International Conference on Communications (ICC 2009)*, Dresden, Germany, June 2009, pp. 1–5.

[14] D. Adami, "Signaling protocols in DiffServ-aware MPLS networks: Design and Implementation of RSVP-TE network simulator,” *IEEE Global Telecommunications Conference (GLOBECOM 2005)*, St. Louis, MO, USA, November 2008, pp. 792–796.

[15] M. Bhandure, G. Deshmukh, and J. N. Varshapriya, “Comparative analysis of MPLS and non–MPLS networks,” *International Journal of Engineering Research and Application*, vol. 3, no. 4, pp.71–76, July 2013.

[16] L. Andersson and G. Swallow, “The Multiprotocol Label Switching (MPLS) Working Group decision on MPLS signaling protocols,” *IETF RFC 3468*, February 2003.

[17] D. Awduche, L. Berger, D. Gan, T. Li, V. Srivasan, and G. Swallow, “RSVP-TE: Extensions to RSVP for LSP tunnels,” *IETF RFC 3209*, December 2001.

[18] J. M. Chung, “Analysis of MPLS traffic engineering,” *Proceedings of the IEEE Midwest Symposium on Circuits and Systems*, San Francisco, CA, USA, August 2000, pp. 550–553.

[19] D. Wang and G. Li, “Efficient distributed bandwidth management for MPLS fast reroute,” AT&T Labs-Research, Florham Park, NJ, USA.

[20] (2015) GNS3. [Online]. Available: http://www.gns3.com.