

# **COMPARATIVE STUDY OF IP & MPLS** **TECHNOLOGY**

**A Project Report**

*Submitted by*

**Mr. HAJI MOHD SHARUKH HAROON**  
**Mr. SHAIKH SAMEER ALI**  
**Mr. GITE MOHAMMED MUKHTAR**  
**Mr. SHAIKH MOHD JAVED**

*in partial fulfilment for the award of the degree*

*of*

**B.E.**

**IN**

**ELECTRONICS & TELECOMMUNICATION**

**At**



**ANJUMAN-I-ISLAM'S**  
**KALSEKAR TECHNICAL CAMPUS**  
**PANVEL**

**OCT 2014-15**

## **DECLARATION**

We hereby declare that the project entitled “**COMPARATIVE STUDY OF IP & MPLS TECHNOLOGY**” submitted for the B.E. Degree is our original work and the project has not formed the basis for the award of any degree, associateship, fellowship or any other similar titles.

Signature of the Students:

Mr. HAJI MOHD SHARUKH HAROON  
Mr. SHAIKH SAMEER ALI  
Mr. GITE MOHAMMED MUKHTAR  
Mr. SHAIKH MOHD JAVED

Place: New Panvel

Date:

## **CERTIFICATE**

This is to certify that the project entitled “**Comparative Study Of IP & MPLS Technology**” is the bonafide work carried out by students of B.E., KALSEKAR Technical Campus, Panvel, during the year 2014-2015, in complete fulfillment of the requirements for the award of the Degree of B.E EXTC and that the project has not formed the basis for the award previously of any degree, diploma, associateship, fellowship or any other similar title.

---

(Prof. Mujib Tamboli)

H.O.D

---

(Prof. Mujib Tamboli)

Internal guide

---

(External)

## ACKNOWLEDGEMENT

We take this opportunity to offer our gratitude to our guide **Prof. Mujib Tamboli** for his support and guidance. He allowed us a great deal of freedom in choosing our topics for study and also provided us encouragement throughout this venture.

We also wish to thank **Mr. Manoj Chaudhari** and **Mr. Manoj Kumar** of CETTM (Centre for Excellence in Telecom Technology and Management) MTNL who took time off from their busy schedules to help us with the project. They allowed us full access to many facilities without which our project would have not been possible.

Last but not the least we are grateful to our parents for all their support and encouragement.

## ABSTRACT

MPLS is in discussion since last decade. It has been introduced to improve the performance and speed of the backbone network. There has been demand for transition from conventional network to the MPLS network in the service providers network. A comparative study and performance behaviour of the service providers network with MPLS network under different traffic conditions with various services is being proposed. An experimentation will be carried out on MPLS network with different traffic conditions to support the performance analysis on service provider routers.

There has been significant improvement in the demand for the bandwidth requirement in the near future. This requires the access network and the backbone network to be significantly improved with respect to various services. Specifically a high speed network with a improvement in performance in expected at the backbone network. One of the contenders for the above problem is MPLS protocols. A network with MPLS protocols will take care of all the future demands for large bandwidth access for the subscribers. The analysis of the MPLS protocols has been carried out which has been reported in literature. A performance analysis of MPLS network under different traffic conditions and under different services is required before it is deployed in the field. Wireshark ,VLC, Jperf are some open source tools used for traffic generation and network analysis .

This work proposes analysis of network performance parameter such as Latency, Throughput, Packet Loss, Jitter with traditional routing and MPLS. Testing scenario is created in with Service Provider MPLS enabled router and MPLS protocol features are analysed .

**Key Words :** *MPLS, LDP, Service Provider Network , Traffic Engineering ,VPN*

## Table of Contents

CHAPTER NO.	TITLE	PAGE NO.
	Title Page Declaration of the Students Certificate of the Guide Abstract Acknowledgement	
<b>1</b>	<b>Introduction to MPLS</b> 1.1 Definition of MPLS 1.2 Benefits of MPLS 1.2.1 The use of one unified network infrastructure 1.2.2 Better IP over ATM Integration 1.2.3 Traffic Engineering 1.3 Statement About the Problem 1.3.1 Why this particular topic is chosen 1.4 Objective and Scope of Project 1.5 Resources and Testing Technologies used 1.6 Organization of Report	1 1 2 2 2 4 4 4 5 5
<b>2</b>	<b>2. Literature Review</b>	<b>6</b>

<b>3</b>	<b>3. IP Paradigm</b> 3.1 Routing Basics 3.1.1 Configuring IP Routing in Our Network 3.2 Routing Protocol Basics 3.2.1 Routing Protocols 3.3 Open Shortest Path First (OSPF) Basics 3.3.1 OSPF Terminology 3.3.2 OSPF Metrics 3.3.3 OSPF and Loopback Interfaces 3.3.4 Verifying OSPF Configuration Commands	<b>8</b> 8 8 10 10 10 12 13 14 15
<b>4</b>	<b>MPLS Architecture</b> 4.1 Introducing MPLS Label 4.2 Label Stacking 4.3 Encoding of MPLS 4.4 MPLS and OSI reference model 4.5 Label Switched Router 4.6 Label Switched path 4.7 Forwarding Equivalence Class 4.8 Label Distribution 4.9 Label Distribution with LDP 4.10 Label Forwarding Instance Base	<b>16</b> 16 17 17 18 19 20 21 22 24 24
<b>5</b>	<b>5. Implementation</b> 5.1 Experimental Environment 5.2 3CX Software for Windows 5.2.1 Benefits of IP Phone System / IP PBX 5.2.2 SIP Phone 5.2.3 Software based SIP Phones 5.4 VLC Media Player 5.5 Wireshark for Packet Capture and Analysis 5.5.1 General Analysis Task	<b>25</b> 25 26 26 28 28 29 29 29

	5.5.2 Troubleshooting Task	30
	5.5.3 Security Analysis(Network Forensic) Task	30
	5.5.4 Application Analysis Task	31
<b>6</b>	<b>Evaluation</b>	<b>32</b>
	6.1 Experimental Setup	32
	6.2 Evaluation Metrics	33
	6.2.1 Latency in the Network	33
	6.2.2 Throughput of Network	33
	6.2.3 Packet Loss in Network	33
	6.2.4 Jitter in VoIP call	34
<b>7</b>	<b>Experimental Results and Discussion</b>	<b>35</b>
	7.1 Latency in Network	35
	7.1.1 Avg. Latency in IP and MPLS	35
	7.1.2 Max. Latency in IP and MPLS	36
	7.2 Throughput of Network	37
	7.2.2 Throughput obtain in Wireshark Capture	37
	7.3 Packet Loss	38
	7.3.1 TCP lost segment	38
	7.3.2 Retransmission of TCP packet	39
	7.4 Jitter in VoIP	41
	7.4.1 Analysis of VoIP call in IP and MPLS	41
<b>8</b>	<b>8. Summaries Conclusion and Future scope of MPLS</b>	<b>43</b>
	8.1 Conclusion	43
	8.2 Future Scope of MPLS	43
	<b>Appendix</b>	<b>45</b>
	<b>References</b>	<b>54</b>



## List of Figure

Figure 1.1	Traffic Engineering Example 1	3
Figure 3.1	OSPF Design Example	12
Figure 3.2	OSPF Router ID (RID)	16
Figure 4.1	Syntax of One MPLS Label	17
Figure 4.2	Label Stack	18
Figure 4.3	Encapsulation for Labeled Packet	18
Figure 4.4	OSI Reference Model	19
Figure 4.5	An LSP Through an MPLS Network	21
Figure 4.6	Nested LSP	22
Figure 4.7	An MPLS Network Running iBGP	23
Figure 4.8	An IPv4-over-MPLS Network Running LDP: Packet Switching	25
Figure 5.1	Router Topology	27
Figure 5.2	VoIP Phone System Overview	30
Figure 6.1	Experimental Lab Setup	34
Figure 7.1	Avg Latency in OSPF	37
Figure 7.2	Avg Latency in MPLS	37
Figure 7.3	Maximum Latency in OSPF	38
Figure 7.4	Maximum Latency in MPLS	38
Figure 7.5	Analysis of OSPF based on TCP destination port	39
Figure 7.6	Analysis of MPLS based on TCP destination port	39
Figure 7.7	Packet Loss Parameter 1 in OSPF	40
Figure 7.8	Analysis of TCP lost segment in IP	40
Figure 7.9	Packet Loss Parameter 1 in MPLS	41
Figure 7.10	Analysis of TCP lost segment in MPLS (L3 VPN)	41
Figure 7.11	Packet Loss Parameter 2 in OSPF	41
Figure 7.12	Analysis of TCP retransmission in IP (OSPF)	42
Figure 7.13	Packet Loss Parameter 2 in MPLS	42
Figure 7.14	Analysis of TCP retransmission in MPLS (L3 VPN)	42

## List of Abbreviations

AoTM	Any transport over MPLS
ATM	Asynchronous Transfer Mode
AS	Autonomous System
AD	Administrative Distance
BGP	Border gateway protocol
CE	Customer Edge
CIDR	Classless Inter-domain Routing
DHCP	Dynamic Host Configuration Protocol
EIGRP	Enhance interior gateway routing protocol
FTP	File Transfer Protocol
FEC	Forward Equivalence Class
FR	Frame Relay
GE	Gigabit Ethernet
GMPLS	Generalized MPLS
GRE	Generic Routing Encapsulation
GUI	Graphic User Interface
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IO	Input-Output
ISP	Internet Service Provider
ITU-T	International Telecommunication Union
LAN	Local Area Network
MAN	Metropolitan Area Network
MPLS	Multiprotocol Label Switching
MPLS-TP	Multiprotocol Label Switching Transport Profile
MP-BGP	Multiprotocol Border Gateway Protocol
MPLS TE	Multiprotocol Label Switching Traffic Engineering
NMS	Network Management Station
OAM	Operation Administration Maintenance
OTN	Optical Transport Network
OADM	Optical Add-Drop Multiplexer

OSPF	Open shortest path first
OS	Operating System
OSI	Open System Interconnection
PE	Provider Edge
QoS	Quality of Service
R	Router
RFC	Request For Comment
RIP	Routing Information Protocol
RT	Route Target
RR	Route Reflector
SDH	Synchronous Digital Hierarchy
SIP	Session Initiation Protocol
SONET	Synchronous Optical Network
SNMP	Simple Network Management Protocol
SMF	Single Mode Fiber
STM	Synchronous Transport Module
TDM	Time Division Multiplexing
TTL	Time To Leave
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VRF	Virtual Route Forwarding
VLSM	Variable Length Subnet Mask
VPN	Virtual Private network
VoIP	Voice over internet protocol
WDM	Wavelength Division Multiplexing
WAN	Wide Area Network



# **Chapter 1**

## **Introduction**

Multiprotocol Label Switching (MPLS) has been around for several years. It is a popular networking technology that uses labels attached to packets to forward them through the network. This chapter explains why MPLS became so popular in such a short time. This chapter starts with a definition of MPLS. It also provides a short overview of pre-MPLS network solutions. The benefits of MPLS are listed, and the end of the chapter explains briefly the history of MPLS.

### **1.1 Definition of MPLS**

The MPLS labels are advertised between routers so that they can build a label-to-label mapping. These labels are attached to the IP packets, enabling the routers to forward the traffic by looking at the label and not the destination IP address. The packets are forwarded by label switching instead of by IP switching. The label switching technique is not new. Frame Relay and ATM use it to move frames or cells throughout a network. In Frame Relay, the frame can be any length, whereas in ATM, a fixed-length cell consists of a header of 5 bytes and a payload of 48 bytes. The header of the ATM cell and the Frame Relay frame refer to the virtual circuit that the cell or frame resides on. The similarity between Frame Relay and ATM is that at each hop throughout the network, the “label” value in the header is changed. This is different from the forwarding of IP packets. When a router forwards an IP packet, it does not change a value that pertains to the destination of the packet; that is, it does not change the destination IP address of the packet. The fact that the MPLS labels are used to forward the packets and no longer the destination IP address have led to the popularity of MPLS.

### **1.2 Benefits of MPLS**

This section explains briefly the benefits of running MPLS in Service Provider network. These benefits include the following:

- The use of one unified network infrastructure
- Better IP over ATM integration
- Traffic engineering

### **1.2.1 The use of one unified network infrastructure**

With MPLS, the idea is to label ingress packets based on their destination address or other preconfigured criteria and switch all the traffic over a common infrastructure. This is the great advantage of MPLS. One of the reasons that IP became the only protocol to dominate the networking world is because many technologies can be transported over it. Not only is data transported over IP, but also telephony. By using MPLS with IP, we can extend the possibilities of what we can transport. Adding labels to the packet enables us to carry other protocols than just IP over an MPLS-enabled Layer 3 IP backbone, similarly to what was previously possible only with Frame Relay or ATM Layer 2 networks. MPLS can transport IPv4, IPv6, Ethernet, High-Level Data Link Control (HDLC), PPP, and other Layer 2 technologies. The feature whereby any Layer 2 frame is carried across the MPLS backbone is called Any Transport over MPLS (AToM). The routers that are switching the AToM traffic do not need to be aware of the MPLS payload; they just need to be able to switch the labeled traffic by looking at the label on top of it. In essence, MPLS label switching is a simple method of switching multiple protocols in one network. In short, AToM enables the service provider to provide the same Layer 2 service toward the customers as with any specific non-MPLS network. At the same time, the service provider needs only one unified network infrastructure to carry all kinds of customer traffic.

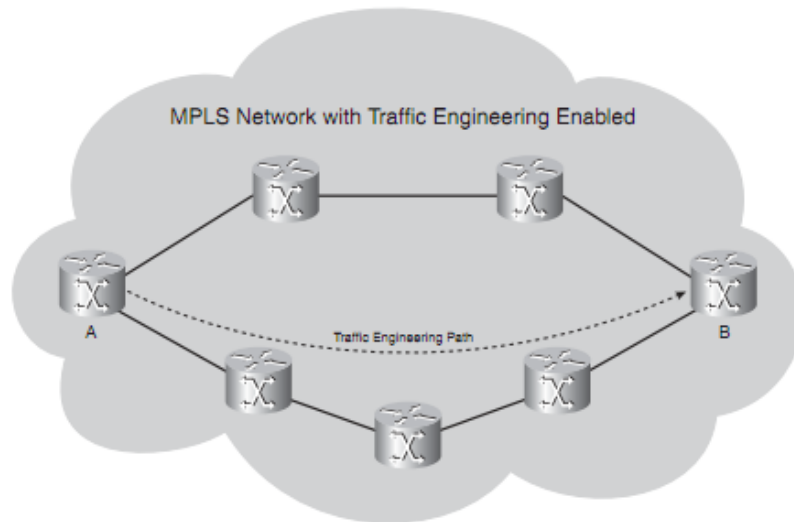
### **1.2.2 Better IP over ATM integration**

In the previous decade, IP won the battle over all other networking Layer 3 protocols, such as AppleTalk, Internetwork Packet Exchange (IPX), and DECnet. IP is relatively simple and omnipresent. A much-hyped Layer 2 protocol at the time was ATM. Although ATM as an end-to-end protocol or desktop-to-desktop protocol as some predicted, never happened, ATM did have plenty of success, but the success was limited to its use as a WAN protocol in the core of service provider network.

### **1.2.3 Traffic Engineering**

The basic idea behind traffic engineering is to optimally use the network infrastructure, including links that are underutilized, because they do not lie on the preferred path. This means that traffic engineering must provide the possibility to steer traffic through the network on paths different from the preferred path, which the least-cost path is provided by IP routing. The least-cost path is the shortest path as computed by the dynamic routing protocol. With traffic engineering implemented in the MPLS network, we could have the traffic that is destined for a particular prefix or with a particular quality of service flow from point A to

point B along a path that is different from the least-cost path. The result is that the traffic can be spread more evenly over the available links in the network and make more use of underutilized links in the network. Figure 1.9 shows an example of this



**Figure 1.1 Traffic Engineering Example 1 [2]**

As the operator of the MPLS-with-traffic-engineering-enabled network, we can steer the traffic from A to B over the bottom path, which is not the shortest path between A and B (four hops versus three hops on the top path). As such, we can send the traffic over links that might otherwise not be used much. We can guide the traffic in this network onto the bottom path by changing the routing protocols metrics. Examine Figure 1-10.

If this network is an IP-only network, we cannot have router C send the traffic along the bottom path by configuring something on router A. The router C decision to send traffic on the top or bottom path is solely its own decision. If we enable MPLS traffic engineering in this network, we can have router A send the traffic toward router B along the bottom path. The MPLS traffic engineering forces router C to forward the traffic A-B onto the bottom path. This can be done in MPLS because of the label forwarding mechanism. The head end router of a traffic-engineered path here router A is the router that specifies the complete path that the traffic will take through the MPLS network. Because it is the head end router that specifies the path, traffic engineering is also referred to as a form of source-based routing. The label that is attached to the packet by the head end router makes the packet flow along the path as specified by the head end router. No intermediate router forwards the packet onto another path.

### **1.3 Statement about the Problem:**

MPLS is in discussion since last decade. It has been introduced to improve the performance and speed of the backbone network. There has been demand for transition from conventional network to the MPLS network in the service provider's network. A comparative study and performance behaviour of the service provider's network with MPLS network under different traffic conditions with various services is being proposed. An experimentation will be carried out on MPLS network with different traffic conditions to support the performance analysis.

#### **1.3.1 Why is the particular topic chosen**

There has been significant improvement in the demand for the bandwidth requirement in the near future [7]. This requires the access network and the backbone network to be significantly improved with respect to various services. Specifically a high speed network with a improvement in performance is expected at the backbone network. One of the contenders for the above problem is MPLS protocols. A network with MPLS protocols will take care of all the future demands for large bandwidth access for the subscribers. The analysis of the MPLS protocols has been carried out which has been reported in literature. A performance analysis of MPLS network under different traffic conditions and under different services is required before it is deployed in the field.

### **1.4 Objective & Scope of Project**

The scope of this project is to study a full Implementation of MPLS network in service providers Network (Mahanagar Telephone Nigam Limited., Mumbai) key MPLS advantages including Traffic Engineering and Quality of Service mechanisms. & how they are utilized to enable the delivery of the VPN & other services.

In addition full comprehensive simulation environment is created for a conventional network and MPLS applied over that traditional network to evaluate the comparative performance of network traffic behaviour and the functionalities of MPLS signalling protocols as well. Service availability, Latency, Throughput(Bandwidth), Packet Loss, Jitter in the network are the performance attributes measure and compare in traditional IP network and MPLS network.

### **1.5 Resources & Testing Technologies used:**

The MPLS Network of MTNL Mumbai has very big network of Huawei MPLS routers. The testing scenarios can be created in the Training centre of MTNL called CETTM (Centre of Excellence for Telecom Training & Management) at powai Mumbai where five Huawei NE



20 Routers are installed for training and also protocol monitoring tool which will be used to test the behaviour of MPLS protocol in Service Provider Environment

## **1.6 Organization of Report**

This report is organized as follows.

Chapter 1 states the basics of MPLS and need of MPLS in service provider environment. Objective and scope of project with which resource and testing technologies used are discussed.

Chapter 2 reviews the history of previous work in field of service provider network and literature survey related to the MPLS protocol in order to achieve information for better understanding the concepts.

Chapter 3 provides understating of traditional IP routing and routing protocols used in networking.

Chapter 4 provides the investigation of MPLS Architecture. Encapsulation of MPLS with iBGP and other terms used in MPLS are explained in this chapter.

Chapter 5 presents brief overview of MPLS VPN terminology and concepts used in real world environment of networking

Chapter 6 includes the implementation requirements and tool used in this experimental exercise with their important features and other applications.

Chapter 8 is investigation of capture files and this analysis is done with network monitoring tools . Results are extracted from capture file and it is discussed and compared with perspective of service provider environment.

Chapter 9 summarized the work and concludes the work carried out in this experiment with the future prospective of MPLS technology.

## Chapter 2

### Literature Review

In this chapter different author papers are discussed with their different approaches in MPLS topic. Some author perform simulation with different testing environment these methods are helpful for understanding concept.

Chuck Semeria in “MPLS enhancing routing in the new public network” explained about Multilayer switching describes the integration of Layer 2 switching and Layer 3 routing. Today, some ISP networks are built using an overlay model in which a logical IP IP routed topology runs over and is independent of an underlying Layer 2 switched topology (ATM or Frame Relay). Layer 2 switches provide high-speed connectivity, while the IP routers at the edge interconnected by a mesh of Layer 2 virtual circuits provide the intelligence to forward IP datagrams. The difficulty with this approach lies in the complexity of mapping between two distinct architectures that require the definition and maintenance of separate topologies, address spaces, routing protocols, signaling protocols, and resource allocation schemes. The emergence of the multilayer switching solutions and MPLS is part of the evolution of the Internet to decrease complexity by combining Layer 2 switching and Layer 3 routing into a fully integrated solution [10].

Wojtek, Bernard, Stephane, Morgane & Hisao in “Survivable MPLS over optical transport network: cost & resource usage analysis” investigated about different options for the survivability implementation in MPLS over Optical Transport Networks (OTN) in terms of network resource usage and configuration cost. We investigate two approaches to the survivability deployment: single layer and multilayer survivability and present various methods for spare capacity allocation (SCA) to reroute disrupted traffic. The comparative analysis shows the influence of the offered traffic granularity and the physical network structure on the survivability cost: for high bandwidth LSPs, close to the optical channel capacity, the multilayer survivability outperforms the single layer one, whereas for low bandwidth LSPs the single layer survivability is more cost-efficient. On the other hand, sparse networks of low connectivity parameter use more wavelengths for optical path routing and increase the configuration cost as compared with dense networks. We demonstrate that by mapping efficiently the spare capacity of the MPLS layer onto the resources of the optical layer one can achieve up to 22% savings in the total configuration cost and up to 37% in the optical layer cost. These results are based on a cost model with different cost variations, and were obtained for networks targeted to a nationwide coverage [9].

Karol Molnar & Martin Vlcek in “Evaluation of Bandwidth Constraint model for MPLS Network” proposed the two basic Bandwidth Constraint models for MPLS networks, called Maximum Allocation Model and Russian Dolls Model, from the point of view of Quality of Service guarantees and introduces the results of performance evaluation of these models in a simulation scenario. We evaluated the influence of the Bandwidth Constraint models on the most important transmission parameters such as throughput, packet loss, one-way delay and jitter [5].

Johnny Bass in “Cisco Service Provider Next Generation Network” reported about Cisco, “IP NGN is a platform for the Connected Life.” What does that really mean? It is an infrastructure for voice, video, mobile and cloud or managed services based on Cisco products, including the CRS Series, ASR Series, and Nexus Series. Service providers agree that the Carrier Ethernet and IP/Multiprotocol Label Switching (MPLS) technology is and will be the way to next-generation networks. Some of the challenges facing service providers are how to maintain growth and profitability, accommodate surging demand for broadband services, maintain competitive residential and business service offerings, avoid service commoditization by offering new and premium services, strengthen profitability by increasing revenue while reducing total cost of ownership, migrate existing legacy ATM/Frame Relay networks to more cost-effective Carrier Ethernet or MPLS services, and protect and grow business services in parallel with consumer services [11].

## Chapter 3

### IP Parameters

#### 3.1 Routing Basics

Once we create an internetwork by connecting service provider WANs and LANs to a router, we'll need to configure logical network addresses, like IP addresses, to all hosts on that internetwork for them to communicate successfully throughout it.

Routing is irrelevant if our network has no routers because their job is to route traffic to all the networks in service provider internetwork, but this is rarely the case! So here's an important list of the minimum factors a router must know to be able to affectively route packets:

- Destination address
- Neighbours routers from which it can learn about remote networks
- Possible routes to all remote networks
- The best route to each remote network
- How to maintain and verify routing information

The router learns about remote networks from neighbouring routers or from an administrator. The router then builds a routing table, which is basically a map of the internetwork, and it describes how to find remote networks. If a network is directly connected, then the router already knows how to get to it. But if a network isn't directly connected to the router, the router must use one of two ways to learn how to get to the remote network

##### 3.1.1 Configuring IP Routing in Our Network

Different types of routing will be really helpful when choosing the best solution for our specific environment and business requirements. These are the three routing methods I'm going to cover here

- Static routing
- Default routing
- Dynamic routing

### **3.1.1.1 Static Routing**

Static routing is the process that ensues when we manually add routes in each router's routing table. Predictably, there are pros and cons to static routing, but that's true for all routing approaches.

#### **Here are the pros:**

There is no overhead on the router CPU, which means we could probably make do with a cheaper router than we would need for dynamic routing.

There is no bandwidth usage between routers, saving our money on WAN links as well as minimizing overhead on the router since we are not using a routing protocol.

It adds security because, the administrator, can be very exclusive and choose to allow routing access to certain networks only.

#### **And here are the cons:**

Whoever the administrator is must have a vault-tight knowledge of the internetwork and how each router is connected in order to configure routes correctly. If we have a good, accurate map of our internetwork, things will get very messy quickly.

If we add a network to the internetwork, we have to tediously add a route to it on all routers by hand, which only gets increasingly insane as the network grows.

Due to the last point, it's just not feasible to use it in most large networks because maintaining it would be a full-time job in itself.

### **3.1.1.2 Default Routing**

We use default routing to send packets with remote destination network not in the routing table to the next-hop router. We should only use default routing on stub networks those with only one exit path out of the network, although there are exceptions to this statement, and default routing is configured on a case by case basis when a network is designed. If we tried to put a default route on a router that isn't a stub, it is possible that packets wouldn't be forwarded to the correct network because they have more than one interface routing to other router. We can easily create loops with default routing, which is avoided in any network. To configure default route, we use wildcards in the network address and mask location of static route.

### **3.1.1.3 Dynamic Routing**

Dynamic routing is when protocols are used to find networks and update routing tables on routers. This is whole lot easier than using static or default routing, but it will cost us in terms of router CPU processing and bandwidth on network links. A routing protocol defines the set of rules used by a router when it communicates routing information between neighbouring routers. The routing protocol I'm going to talk about in this chapter is Open Shortest Path First (OSPF).

Two types of routing protocols are used in internetworks: interior gateway protocols (IGPs) and exterior gateway protocols (EGPs). IGPs are used to exchange routing information with routers in the same autonomous system (AS). An AS is either a single network or a collection of networks under a common administrative domain, which basically means that all routers sharing the same routing-table information are in the same AS. EGPs are used to communicate between ASs.

## **3.2 Routing Protocol Basics**

There are some important things we should know about routing protocols before we get deeper into them. Being familiar with administrative distances, the three different kinds of routing protocols, and routing.

### **3.2.1 Routing Protocols**

There are three classes of routing protocols:

1. Distance vector: The distance-vector protocols in use today find the best path to a remote network by judging distance. In RIP routing, each instance where a packet goes through a router is called a hop, and the route with the least number of hops to the network will be chosen as the best one.
2. Link state: In link-state protocols, also called shortest-path-first protocols, the routers each create three separate tables. One of these tables keeps track of directly attached neighbours, one determines the topology of the entire internetwork, and one is used as the routing table.
3. Hybrid: Hybrid protocols use aspects of both distance-vector and link-state protocols, and EIGRP is a great example. There's no set of rules to follow that dictate exactly how to broadly configure routing protocols for every situation. It's a task that really

must be undertaken on a case-by-case basis, with an eye on specific requirements of each one.

If we understand how the different routing protocols work, we can make good, solid decisions that will solidly meet the individual needs of any business.

### **3.3 Open Shortest Path First (OSPF) Basics**

Open Shortest Path First is an open standard routing protocol that's been implemented by a wide variety of network vendors, and it's that open standard characteristic that's the key to OSPF's flexibility and popularity.

Most people opt for OSPF, which works by using the Dijkstra algorithm to initially construct a shortest path tree and follows that by populating the routing table with the resulting best paths. OSPF has quick convergence therefore it's a favourite. Another two great advantages OSPF offers are that it supports multiple, equal-cost routes to the same destination, and it also supports both IP and IPv6 routed protocols.

Here's a list that summarizes some of OSPF's best features:

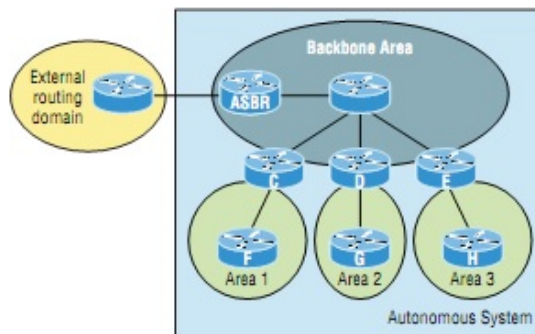
- Allows for the creation of areas and autonomous systems
- Minimizes routing update traffic
- Is highly flexible, versatile, and scalable
- Supports VLSM/CIDR
- Offers an unlimited hop count
- Is open standard and supports multi-vendor deployment

OSPF has many features and all of them combine to produce a fast, scalable, robust protocol that's also flexible enough to be actively deployed in a vast array of production networks. One of OSPF's most useful traits is that its design is intended to be hierarchical in use, meaning that it allows us to subdivide the larger internetwork into smaller internetworks called areas. It's a really powerful feature

Here are three of the biggest reasons to implement OSPF in a way that makes full use of its intentional, hierarchical design:

1. To decrease routing overhead
2. To speed up convergence
3. To confine network instability to single areas of the network

Let's start by checking out Figure 3.1, which shows a very typical, yet simple OSPF design. I want to point out the fact that some routers connect to the backbone called area 0 the backbone area. OSPF absolutely must have an area 0, and all other areas should connect to it except for those connected via virtual links, which are beyond the scope of this book. A router that connects other areas to the backbone area within an AS is called an area border router (ABR), and even these must have at least one of their interfaces connected to area 0.



**Figure 3.1 OSPF Design Example**

OSPF runs great inside an autonomous system, but it can also connect multiple autonomous systems together. The router that connects this ASs is called an autonomous system boundary router (ASBR). Ideally, our aim is to create other areas of networks to help keep route updates to a minimum, especially in larger networks. Doing this also keeps problems from propagating throughout the network, affectively isolating them to a single area.

### 3.3.1 OSPF Terminology

**Link:** A link is a network or router interface assigned to any given network. When an interface is added to the OSPF process, it's considered to be a link. This link, or interface, will have up or down state information associated with it as well as one or more IP addresses.

**Router ID:** The router ID (RID) is an IP address used to identify the router. Router chooses the router ID by using the highest IP address of all configured loopback interfaces. If no loopback interfaces are configured with addresses, OSPF will choose the highest IP address out of all active physical interfaces. To OSPF, this is basically the “name” of each router.

**Neighbour:** Neighbours are two or more routers that have an interface on a common network, such as two routers connected on a point-to-point serial link.

**Adjacency:** An adjacency is a relationship between two OSPF routers that permits the direct exchange of route updates. OSPF is really picky about sharing routing information and will directly share routes only with neighbors that have also established adjacencies.



**Designated router:** A designated router (DR) is elected whenever OSPF routers are connected to the same broadcast network to minimize the number of adjacencies formed and to publicize received routing information to and from the remaining routers on the broadcast network or link. Elections are won based upon a router's priority level, with the one having the highest priority becoming the winner synchronized.

**Backup designated router:** A backup designated router (BDR) is a hot standby for the DR on broadcast, or multi-access, links. The BDR receives all routing updates from OSPF adjacent routers but does not disperse LSA updates.

**Hello protocol:** The OSPF Hello protocol provides dynamic neighbour discovery and maintains neighbour relationships. Hello packets and Link State Advertisements (LSAs) build and maintain the topological database. Hello packets are addressed to multicast address 224.0.0.5.

**Neighborship database:** The neighborship database is a list of all OSPF routers for which Hello packets have been seen. A variety of details, including the router ID and state, are maintained on each router in the neighborship database.

**Topological database:** The topological database contains information from all of the Link State Advertisement packets that have been received for an area. The router uses the information from the topology database as input into the Dijkstra algorithm that computes the shortest path to every network.

**Link State Advertisement:** A Link State Advertisement (LSA) is an OSPF data packet containing link-state and routing information that's shared among OSPF routers. There are different types of LSA packets. An OSPF router will exchange LSA packets only with routers to which it has established adjacencies.

**OSPF areas:** An OSPF area is a grouping of contiguous networks and routers. All routers in the same area share a common area ID. Because a router can be a member of more than one area at a time, the area ID is associated with specific interfaces on the router. This would allow some interfaces to belong to area 1 while the remaining interfaces can belong to area 0.

**Broadcast (multi-access):** Broadcast (multi-access) networks such as Ethernet allow multiple devices to connect to or access the same network, enabling a broadcast ability in which a single packet is delivered to all nodes on the network. In OSPF, a DR and BDR must be elected for each broadcast multi-access network.

**Non broadcast multi-access:** Non broadcast multi-access (NBMA) networks are networks such as Frame Relay, X.25, and Asynchronous Transfer Mode (ATM). These types of networks allow for multi-access without broadcast ability like Ethernet. NBMA networks require special OSPF configuration to function properly.

**Point-to-point:** Point-to-point refers to a type of network topology made up of a direct connection between two routers that provides a single communication path. The point-to-point connection can be physical for example, a serial cable that directly connects two routers or logical, where two routers thousands of miles apart are connected by a circuit in a Frame Relay network.

**Point-to-multipoint:** Point-to-multipoint refers to a type of network topology made up of a series of connections between a single interface on one router and multiple destination routers. All interfaces on all routers share the point-to-multipoint connection and belong to the same network. Point-to-multipoint networks can be further classified according to whether they support broadcasts or not. This is important because it defines the kind of OSPF configurations we can deploy.

### **3.3.2 OSPF Metrics**

OSPF uses a metric referred to as cost. A cost is associated with every outgoing interface included in an SPF tree. The cost of the entire path is the sum of the costs of the outgoing interfaces along the path. Because cost is an arbitrary value as defined in RFC 2338. Default OSPF cost of 1 and a 1,000 Mbps Ethernet interface would have a cost of 1. Important to note is that this value can be overridden with the `ip ospf cost` command. The cost is manipulated by changing the value to a number within the range of 1 to 65,535. Because the cost is assigned to each link, the value must be changed on the specific interface we want to change the cost on.

#### **3.3.3.1 Configuring OSPF**

Configuring basic OSPF isn't as simple as configuring other routing protocol, and it can get really complex once the many options that are allowed within OSPF are factored in. But that's okay because we really only need to focus on basic, single-area OSPF configuration at this point. The two factors that are foundational to OSPF configuration are enabling OSPF and configuring OSPF Areas

## **Enabling OSPF**

The easiest and also least scalable way to configure OSPF is to just use a single area. Doing this requires a minimum of two commands.

The first command used to activate the OSPF routing process is as follows:

```
Router (config)#router ospf ?
```

```
<1-65535> Process ID
```

A value in the range from 1 to 65,535 identifies the OSPF process ID. It's a unique number on this router that groups a series of OSPF configuration commands under a specific running process. Different OSPF routers don't have to use the same process ID to communicate. It's a purely local value that doesn't mean a lot, but we still need to remember that it cannot start at 0; it has to start at a minimum of 1. We can have more than one OSPF process running simultaneously on the same router if we want, but this isn't the same as running multi-area OSPF. The second process will maintain an entirely separate copy of its topology table and manage its communications independently of the first one and we use it when we want OSPF to connect multiple ASs together.

## **Configuring OSPF Areas**

After identifying the OSPF process, we need to identify the interfaces that we want to activate OSPF communications on as well as the area in which each resides. This will also configure the networks we're going to advertise to others.

### **3.3.3 OSPF and Loopback Interfaces`**

It's really vital to configure loopback interfaces when using OSPF. Loopback interfaces are logical interfaces, which means they're virtual, software only interfaces, not actual, physical router interfaces. A big reason we use loopback interfaces with OSPF configurations is because they ensure that an interface is always active and available for OSPF processes. Loopback interfaces also come in very handy for diagnostic purposes as well as for OSPF configuration. Understand that if we don't configure a loopback interface on a router, the highest active IP address on a router will become that router's RID during bootup.

Figure 9.6 illustrates how routers know each other by their router ID.



**Figure 3.2 OSPF Router ID (RID)**

### **3.3.4 Verifying OSPF Configuration commands**

There are several ways to verify proper OSPF configuration and operation,

OSPF uses wildcards in the configuration.

#### **The display ospf brief Command:**

The display brief ospf command is what we'll need to display OSPF information for one or all OSPF processes running on the router. Information contained therein includes the router ID, area information, SPF statistics, and LSA timer information.

#### **The display ospf interface Command:**

The display ospf interface command reveals all interface-related OSPF information. Data is displayed about OSPF information for all OSPF-enabled interfaces or for specified interfaces.

#### **The display ospf peer Command:**

The display ospf peer command is super-useful because it summarizes the pertinent OSPF information regarding neighbors and the adjacency state. If a DR or BDR exists, that information will also be displayed.

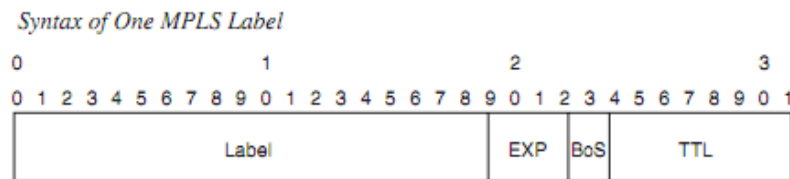
## Chapter 4

### MPLS Architecture

MPLS stands for Multiprotocol Label Switching. The multiprotocol aspect of MPLS was fulfilled after the initial implementation of MPLS. Although at first only IPv4 was being label switched, later on more protocols followed. Label switching indicates that the packets switched are no longer IPv4 packets, IPv6 packets, or even Layer 2 frames when switched, but they are labeled. The most important item to MPLS is the label. This chapter explains what the label is used for, how. The most important item to MPLS is the label. This chapter explains what the label is used for, how it is used, and how it is distributed in a network.

#### 4.1 Introducing MPLS Labels

One MPLS label is a field of 32 bits with a certain structure. Figure 4.1 shows the syntax of one MPLS label.



**Figure 4.1 Syntax of One MPLS Label [10]**

The first 20 bits are the label value. This value can be between 0 and 220–1, or 1,048,575. However, the first 16 values are exempted from normal use; that is, they have a special meaning. The bits 20 to 22 are the three experimental (EXP) bits. These bits are used solely for quality of service (QoS).

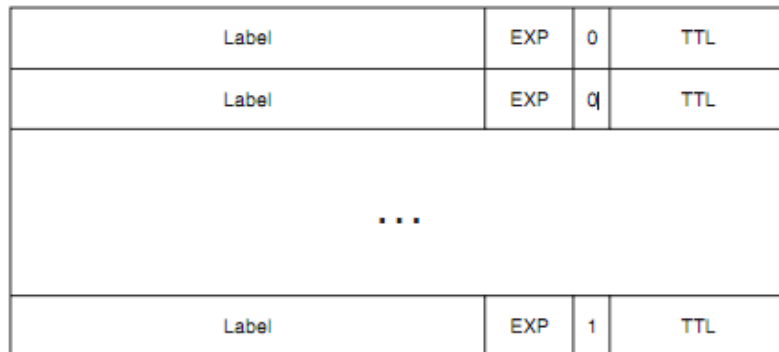
Bit 23 is the Bottom of Stack (BoS) bit. It is 0, unless this is the bottom label in the stack. If so, the BoS bit is set to 1. The stack is the collection of labels that are found on top of the packet. The stack can consist of just one label, or it might have more. The number of labels (that is, the 32-bit field) that we can find in the stack is limitless, although we should seldom see a stack that consists of four or more labels. Bits 24 to 31 are the eight bits used for Time To Live (TTL). This TTL has the same function as the TTL found in the IP header. It is simply decreased by 1 at each hop, and its main function is to avoid a packet being stuck in a routing loop. If a routing loop occurs and no TTL is present, the packet loops forever. If the TTL of the label reaches 0, the packet is discarded.

#### 4.2 Label Stacking

MPLS-capable routers might need more than one label on top of the packet to route that

packet through the MPLS network. This is done by packing the labels into a stack. The first label in the stack is called the top label, and the last label is called the bottom label. In between, we can have any number of labels. Figure 4.2 shows us the structure of the label stack.

*Label Stack*



**Figure 4.2 Label Stack**

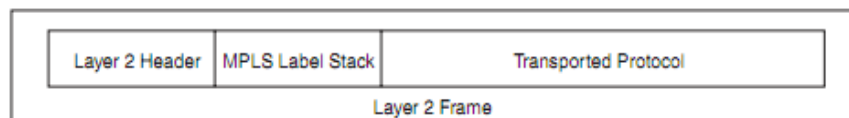
Notice that the label stack in Figure 4.3 shows that the BoS bit is 0 for all the labels, except the bottom label. For the bottom label, the BoS bit is set to 1. Some MPLS applications actually need more than one label in the label stack to forward the labeled packets.

### 4.3 Encoding of MPLS

Where does this label stack reside? The label stack sits in front of the Layer 3 packet that is, before the header of the transported protocol, but after the Layer 2 header. Often, the MPLS label stack is called the shim header because of its placement.

Figure 4.3 shows us the placement of the label stack for labeled packets.

*Encapsulation for Labeled Packet*



**Figure 4.3 Encapsulation for Labeled Packet**

The Layer 2 encapsulation of the link can be almost any encapsulation that router OS supports: PPP, High-Level Data Link Control (HDLC), Ethernet, and so on. Assuming that the transported protocol is IPv4, and the encapsulation of a link is PPP, the label stack is present after the PPP header but before the IPv4 header. Because the label stack in the Layer 2 frame is placed before the Layer 3 header or other transported protocol, we must have new values for the Data Link Layer Protocol field, indicating that what follows

the Layer 2 header is an MPLS labeled packet. The Data Link Layer Protocol field is a value indicating what payload type the Layer 2 frame is carrying. Table 4.1 shows us what the names and values are for the Protocol Identifier field in the Layer 2 header for the different Layer 2 encapsulation types.

**Table 4.1 MPLS Protocol Identifier Values for Layer 2 Encapsulation Types**

*MPLS Protocol Identifier Values for Layer 2 Encapsulation Types*

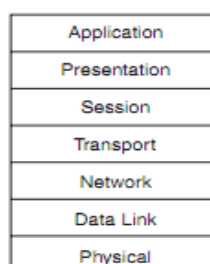
Layer 2 Encapsulation Type	Layer 2 Protocol Identifier Name	Value (hex)
PPP	PPP Protocol field	0281
Ethernet/802.3 LLC/SNAP encapsulation	Ethertype value	8847
HDLC	Protocol	8847
Frame Relay	NLPID (Network Level Protocol ID)	80

ATM is absent from Table 4.1 because it uses a unique way of encapsulating the label for the encapsulation of a labeled packet in ATM. For Frame Relay, the NLPID is 0x80, indicating that an IEEE Sub-network Access Protocol (SNAP) header is used. The SNAP header is used here in Frame Relay to tell the receiver what protocol Frame Relay carries. The SNAP header contains an Organizationally Unique Identifier (OUI) of 0x000000 and an Ether type of 0x8847, indicating that the transported protocol is MPLS. The transported protocol can theoretically be anything; router OS supports IPv4 and IPv6. In the case of AToM, we will see that the transported protocol can be any of the most MPLS label stack is called the shim header because of its placement. popular Layer 2 protocols, such as Frame Relay, PPP, HDLC, ATM, and Ethernet.

#### 4.4 MPLS and the OSI Reference Model

The OSI reference model consists of seven layers. Refer to Fig 4.4 for the OSI reference model.

*OSI Reference Model*



**Figure 4.4 OSI Reference Model**

The bottom layer is Layer 1, or the physical layer, and the top layer is Layer 7, or the application layer. Whereas the physical layer concerns the cabling, mechanical, and electrical characteristics, Layer 2, the data link layer, is concerned with the formatting of the frames. Examples of the data link layer are Ethernet, PPP, HDLC, and Frame Relay. The significance of the data link layer is only on one link between two machines, but not beyond. This means that the data link layer header is always replaced by the machine at the other end of the link. Layer 3, the network layer, is concerned with the formatting of packets end to end. It has significance beyond the data link. The most well-known example of a protocol operating at Layer 3 is IP. Where does MPLS fit in? MPLS is not a Layer 2 protocol because the Layer 2 encapsulation is still present with labeled packets. MPLS also is not really a Layer 3 protocol because the Layer 3 protocol is still present, too. Therefore, MPLS does not fit in the OSI layering too well. Perhaps the easiest thing to do is to view MPLS as the 2.5 layer and be done with it.

#### **4.5 Label Switch Router**

A label switch router (LSR) is a router that supports MPLS. It is capable of understanding MPLS labels and of receiving and transmitting a labeled packet on a data link. Three kinds of LSRs exist in an MPLS network:

- Ingress LSRs—Ingress LSRs receive a packet that is not labeled yet, insert a label (stack) in front of the packet, and send it on a data link.
- Egress LSRs—Egress LSRs receive labeled packets, remove the label(s), and send them on a data link. Ingress and egress LSRs are edge LSRs.
- Intermediate LSRs—Intermediate LSRs receive an incoming labeled packet, perform an operation on it, switch the packet, and send the packet on the correct data link.

An LSR can do the three operations: pop, push, or swap.

It must be able to pop one or more labels (remove one or more labels from the top of the label stack) before switching the packet out. An LSR must also be able to push one or more labels onto the received packet. If the received packet is already labeled, the LSR pushes one or more labels onto the label stack and switches out the packet. If the packet is not labeled yet, the LSR creates a label stack and pushes it onto the packet. An LSR must also be able to swap a label. This simply means that when a labeled packet is received, the top label of the label stack is swapped with a new label and the packet is switched on the outgoing data link. An LSR that pushes labels onto a packet that was not labeled yet is called an imposing LSR because it is the first LSR to impose labels onto the packet. One that is doing imposition is

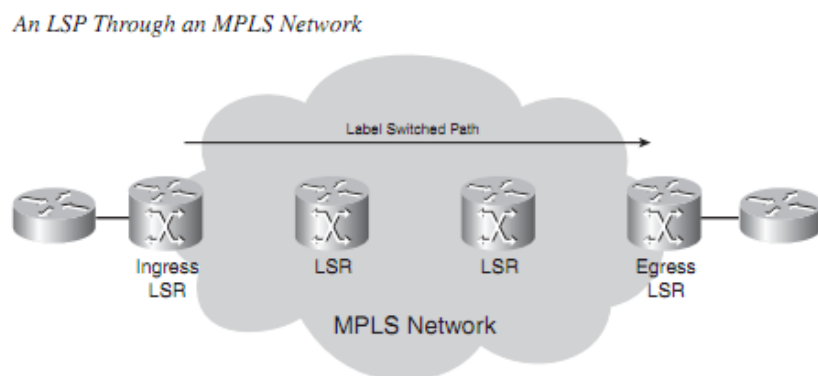


ingress LSR. An LSR that removes all labels from the labeled packet before switching out the packet is a disposing LSR. One that does disposition is an egress LSR.

In the case of MPLS VPN, the ingress and egress LSRs are referred to as provider edge (PE) routers. Intermediate LSRs are referred to as provider (P) routers. The terms PE and P routers have become so popular that they are also used when the MPLS network does not run MPLS VPN.

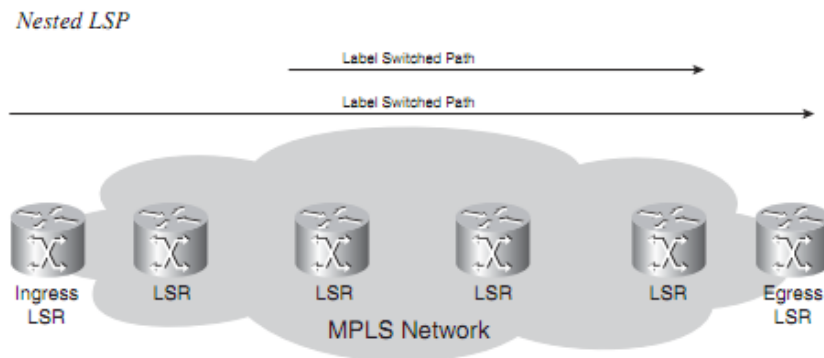
#### 4.6 Label Switch path

A label switched path (LSP) is a sequence of LSRs that switch a labeled packet through an MPLS network or part of an MPLS network. Basically, the LSP is the path through the MPLS network or a part of it that packets take. The first LSR of an LSP is the ingress LSR for that LSP, whereas the last LSR of the LSP is the egress LSR. All the LSRs in between the ingress and egress LSRs are the intermediate LSRs. In Figure 4.5, the arrow at the top indicates the direction, because an LSP is unidirectional. The flow of labeled packets in the other direction right to left between the same edge LSRs would be another LSP.



**Figure 4.5 An LSP Through an MPLS Network**

A label switched path (LSP) is a sequence of LSRs that switch a labeled packet through an MPLS network or part of an MPLS network. Basically, the LSP is the path through the MPLS network or a part of it that packets take. The first LSR of an LSP is the ingress LSR for that LSP, whereas the last LSR of the LSP is the egress LSR. All the LSRs in between the ingress and egress LSRs are the intermediate LSRs. In Figure4.-5, the arrow at the top indicates the direction, because an LSP is unidirectional. The flow of labeled packets in the other direction right to left between the same edge LSRs would be another LSP.



**Figure 4.6 Nested LSP [2]**

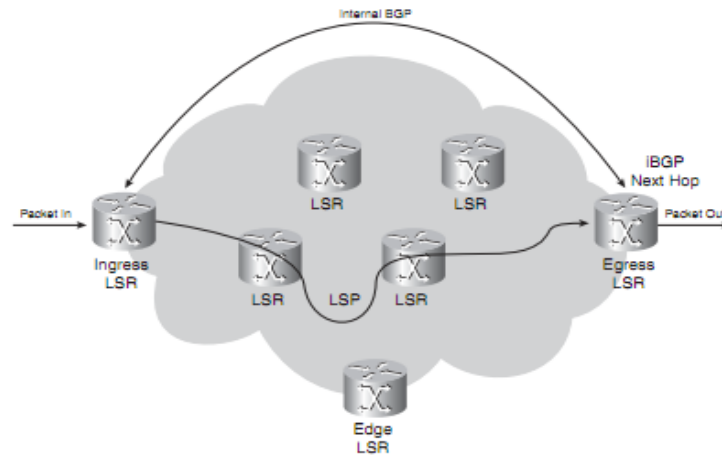
### 4.7 Forwarding Equivalence class

A Forwarding Equivalence Class (FEC) is a group or flow of packets that are forwarded along the same path and are treated the same with regard to the forwarding treatment. All packets belonging to the same FEC have the same label. However, not all packets that have the same label belong to the same FEC, because their EXP values might differ; the forwarding treatment could be different, and they could belong to a different FEC. The router that decides which packets belong to which FEC is the ingress LSR. This is logical because the ingress LSR classifies and labels the packets. Following are some examples of FECs:

- Packets with Layer 3 destination IP addresses matching a certain prefix
- Multicast packets belonging to a certain group
- Packets with the same forwarding treatment, based on the precedence or IP DiffServ Code Point (DSCP) field
- Layer 2 frames carried across an MPLS network received on one VC or (sub)interface on the ingress LSR and transmitted on one VC or (sub)interface on the egress LSR
- Packets with Layer 3 destination IP addresses that belong to a set of Border Gateway Protocol
- (BGP) prefixes, all with the same BGP next hop

This last example of a FEC is a particularly interesting one. All packets on the ingress LSR for which the destination IP address points to a set of BGP routes in the routing table all with the same BGP next-hop address belong to one FEC. It means that all packets that enter the MPLS network get a label depending on what the BGP next hop is. Figure 4.7 shows an MPLS network in which all the edge LSRs run internal BGP (iBGP).

*An MPLS Network Running iBGP*



**Figure 4.7 An MPLS Network iBGP [2]**

The destination IP address of all IP packets entering the ingress LSR will be looked up in the IP forwarding table. All these addresses belong to a set of prefixes that are known in the routing table as BGP prefixes. Many BGP prefixes in the routing table have the same BGP next-hop address, namely one egress LSR. All packets with a destination IP address for which the IP lookup in the routing table reuses to the same BGP next-hop address will be mapped to the same FEC. As already mentioned, all packets that belong to the same FEC get the same label imposed by the ingress LSR.

#### **4.8 Label Distribution**

The first label is imposed on the ingress LSR and the label belongs to one LSP. The path of the packet through the MPLS network is bound to that one LSP. All that changes is that the top label in the label stack is swapped at each hop. The ingress LSR imposes one or more labels on the packet. The intermediate LSRs swap the top label (the incoming label) of the received labelled packet with another label (the outgoing label) and transmit the packet on the outgoing link. The egress LSR of the LSP strips off the labels of this LSP and forwards the packet.

Consider the example of plain IPv4-over-MPLS, which is the simplest example of an MPLS network. Plain IPv4-over-MPLS is a network that consists of LSRs that run an IPv4 Interior Gateway Protocol (IGP) (for example, Open Shortest Path First [OSPF], Intermediate System-to-Intermediate System [IS-IS], and Enhanced Interior Gateway Routing Protocol [EIGRP]). The ingress LSR looks up the destination IPv4 address of the packet, imposes a label, and forwards the packet. The next LSR (and any other intermediate LSR) receives the labelled packet, swaps the incoming label with an outgoing label, and forwards the packet.

The egress LSR pops the label and forwards the IPv4 packet without labels on the outgoing link. For this to work, adjacent LSRs must agree on which label to use for each IGP prefix. Therefore, each intermediate LSR must be able to figure out with which outgoing label the incoming label should be swapped. This means that we need a mechanism to tell the routers which labels to use when forwarding a packet. Labels are local to each pair of adjacent routers. Labels have no global meaning across the network. For adjacent routers to agree which label to use for which prefix, they need some form of communication between them; otherwise, the routers do not know which outgoing label needs to match which incoming label. A label distribution protocol is needed.

We can distribute labels in two ways:

- Piggyback the labels on an existing IP routing protocol
- Have a separate protocol distribute labels

#### Piggyback the Labels on an Existing IP Routing Protocol

The first method has the advantage that a new protocol is not needed to run on the LSRs, but every existing IP routing protocol needs to be extended to carry the labels. This is not always an easy thing to do. The big advantage of having the routing protocol carry the labels is that the routing and label distribution are always in sync, which means that we cannot have a label if the prefix is missing or vice versa. It also eliminates the need of another protocol running on the LSR to do the label distribution. The implementation for distance vector routing protocols (such as EIGRP) is straightforward, because each router originates a prefix from its routing table. The router then just binds a label to that prefix.

Link state routing protocols (such as IS-IS and OSPF) do not function in this way. Each link state update is then forwarded unchanged by all routers inside one area. The problem is that for MPLS to work, each router needs to distribute a label for each IGP prefix even the routers that are not originators of that prefix. Link state routing protocols need to be enhanced in an intrusive way to be able to do this. The fact that a router needs to advertise a label for a prefix it does not originate is counterintuitive to the way link state routing protocols work anyway. Therefore, for link state routing protocols, a separate protocol is preferred to distribute the labels. None of the IGPs has been changed to deploy the first method. However, BGP is a routing protocol that can carry prefixes and distribute labels at the same time. However, BGP is not an IGP; it is used to carry external prefixes. BGP is used primarily for label distribution in MPLS VPN networks.

Several varieties of protocols distribute labels

- Label Distribution Protocol (LDP)
- Resource Reservation Protocol (RSVP)

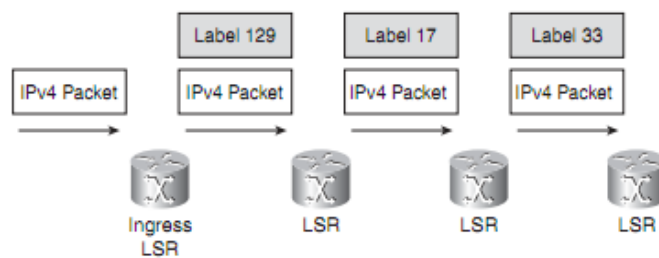
Label distribution by RSVP is used for MPLS TE only.

#### 4.9 Label Distribution with LDP

Label Distribution with LDP For every IGP IP prefix in its IP routing table, each LSR creates a local binding that is, it binds a label to the IPv4 prefix. The LSR then distributes this binding to all its LDP neighbours. These received bindings become remote bindings. The neighbours then store these remote and local bindings in a special table, the label information base (LIB). Therefore, we can have one label per prefix or one label per prefix per interface, but the LSR gets more than one remote binding because it usually has more than one adjacent LSR. Out of all the remote bindings for one prefix, the LSR needs to pick only one and use that one to determine the outgoing label for that IP prefix. The routing table (sometimes called the routing instance base, or RIB) determines what the next hop of the IPv4 prefix is. The LSR chooses the remote binding received from the downstream LSR, which is the next hop in the routing table for that prefix.

Figure 4.8 shows the IPv4 packet destined for 10.0.0.0/8 entering the MPLS network on the ingress LSR, where it is imposed with the label 129 and switched toward the next LSR. The second LSR swaps the incoming label 129 with the outgoing label 17 and forwards the packet toward the third LSR. The third LSR swaps the incoming label 17 with the outgoing label 33 and forwards the packet to the next LSR and so on.

*An IPv4-over-MPLS Network Running LDP: Packet Switching*



**Figure 4.8 an IPv4-over-MPLS Network Running LDP: Packet Switching [2]**

#### 4.10 Label Forwarding Instance Base

The LFIB is the table used to forward labelled packets. It is populated with the incoming and outgoing labels for the LSPs. The incoming label is the label from the local binding on the particular LSR. The outgoing label is the label from the remote binding chosen by the LSR

from all possible remote bindings. All these remote bindings are found in the LIB. The LFIB chooses only one of the possible outgoing labels from all the possible remote bindings in the LIB and installs it in the LFIB.

## Chapter 5

### Implementation

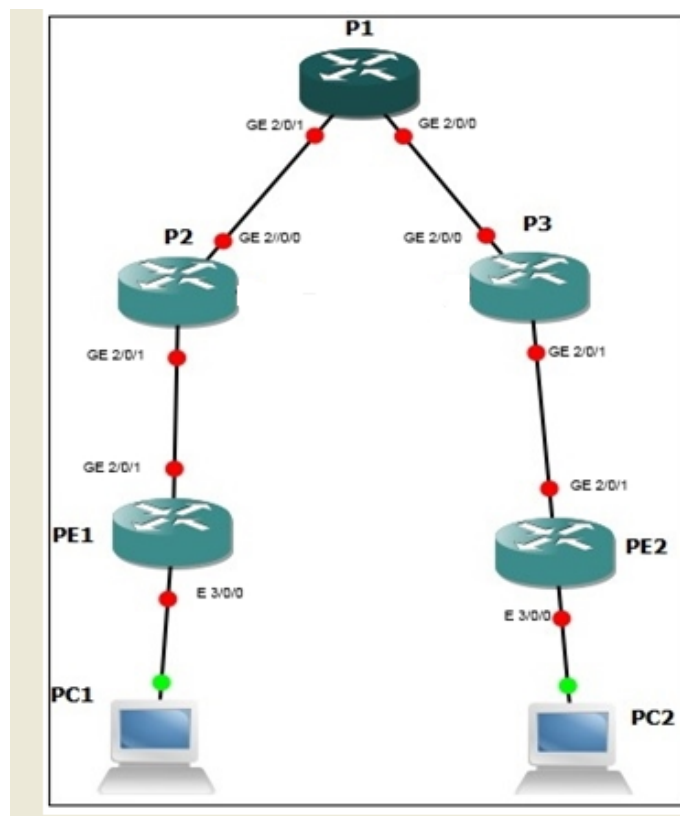
In this chapter experiment environment lab and tools used in the experiment are discussed.

Most of software based tools are open source.

#### 5.1 Experimental Environment

The experiment is carried out in MPLS lab at MTNL training centre (CETTM Powai) where five Huawei NE20 Series MPLS enable routers are used for testing and troubleshooting purpose. Two windows based PCs are used in this Experiment, one for traffic generation and other for traffic capture.

They are connected as shown in figure 5.1



**Figure 5.1 Router Topology**

GE links are connected by fibre optic cable and Ethernet links are connected by CAT-6 cable. For analyse the network performance three different flows of traffic is created .For generation of TCP flow we used Wireshark tool is used for TCP flow. For RTP (VoIP) flowed 3CX software is used and for Video (UDP) VLC media player is used. Wireshark Network Protocol Analyser is used at PC1 for capturing all traffic send from PC2.

## **5.2 3CX Software for windows**

3CX Phone System is a software-based IP PBX that replaces a traditional PBX and delivers employees the ability to make, receive and transfer calls. The IP PBX supports all traditional PBX features. An IP PBX is also referred to as a VOIP Phone System, IP PABX or SIP server. Calls are sent as data packets over the computer data network instead of via the traditional phone network. Phones share the network with computers and separate phone wiring can therefore be eliminated. With the use of a VOIP gateway, we can connect existing phone lines to the IP PBX and make and receive phone calls via a regular PSTN line. The 3CX phone system uses standard SIP software or hardware phones, and provides internal call switching, as well as outbound or inbound calling via the standard phone network or via a VOIP service.

### **5.2.1 Benefits of an IP Phone System / IP PBX**

- Much easier to install & configure than a proprietary phone system:

A software program running on a computer can take advantage of the advanced processing power of the computer and user interface of Windows. Anyone with an understanding of computer networks and windows can install and configure the PBX. A proprietary phone system often requires an installer trained on that particular proprietary phone system.

- Easier to manage because of web based configuration interface:

A VOIP phone system has a web based configuration interface, allowing us to easily maintain and fine tune our phone system. Proprietary phone systems often have difficult to use interfaces which are designed so that only the phone system installers can use it effectively.

- Call cost reduction:

We can save substantially by using a VOIP service provider for long distance or international calls. Easily connect phone systems between offices/branches via the Internet or WAN and make free phone calls.

- No need for separate phone wiring use computer network:

A VOIP phone system allows We to connect hardware phones directly to a standard computer network port (which it can share with the adjacent computer). Software phones can be installed directly onto the PC. This means that we do not need to install & maintain a separate wiring network for the phone system, giving us much greater flexibility to add users/extensions. If we are moving into an office and have not yet installed phone wiring, we can save significantly by just installing a computer network.



- No vendor lock-in:

VOIP phone systems are open standard all modern IP PBX systems use SIP as a protocol. This means that we can use almost any SIP VOIP phone or VOIP gateway hardware. In contrast, a proprietary phone system often requires proprietary phones, designed specifically for that phone system and proprietary expansion modules to add features and lines.

- Scalable:

Proprietary systems are easy to outgrow: Adding more phone lines or extensions often requires expensive hardware upgrades. In some cases we need an entirely new phone system. Not so with a VOIP phone system: a standard computer can easily handle a large number of phone lines and extensions – just add more phones to our network to expand!

- Better customer service & productivity:

Because calls are computer based, it is much easier for developers to integrate with business applications. For example: an incoming call can automatically bring up the customer record of the caller, dramatically improving customer service and cutting cost. Outbound calls can be placed directly from Outlook, removing the need for the user to type in the phone number.

- Software based Phones are easier to use:

It is often difficult to use advanced phone system features such as conferencing on proprietary phones. Not so with software based SIP phones all features are easily performed from a user friendly windows GUI.

- More features included as standard:

Because a VOIP phone system is software based, it is easier for developers to improve feature sets and performance. Therefore most VOIP phone systems come with a rich feature set, including auto attendant, voice mail, call queuing and more. These options are often very expensive in proprietary systems.

- Better control via better reporting:

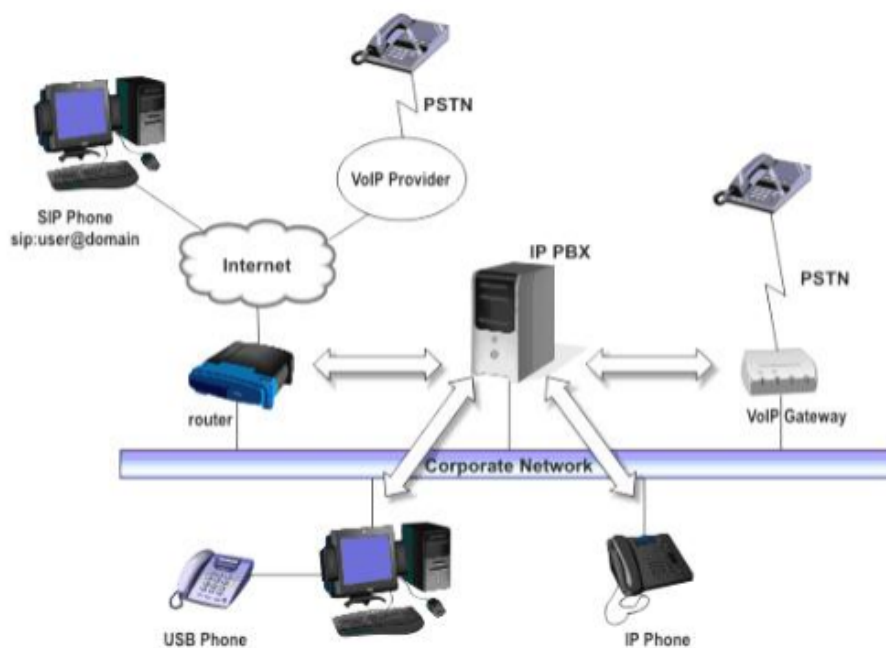
VOIP settings store inbound and outbound call information in a database on our server, allowing for much more powerful reporting of call costs and call traffic.

- Better overview of current system status and calls:

Proprietary systems often require expensive „system“ phones to get an idea what is going on in our phone system. Even then, status information is cryptic at best. With VOIP systems we can define which users can see phone system status graphically via a web browser.

- Allows easy roaming of users:

Calls can be diverted anywhere in the world because of the SIP protocol characteristics. How an IP Phone system works. A VOIP Phone System, also referred to as an IP PBX, consists of one or more SIP standard based phones, an IP PBX server and optionally a VOIP Gateway. The IP PBX server is similar to a proxy server: SIP clients, being either soft phones or hardware based phones, register with the IP PBX server, and when they wish to make a call they ask the IP PBX to establish the connection. The IP PBX has a directory of all phones/users and their corresponding sip address and thus is able to connect an internal call or route an external call via either a VOIP gateway or a VOIP service provider.



**Figure 5.2 VoIP Phone System Overview**

The image illustrates how an IP PBX integrates on the network and how it uses the PSTN or Internet to connect calls.

### **5.3.2 SIP phones**

A VOIP phone system requires the use of SIP phones. These phones are based on the Session Initiation Protocol (SIP), an industry standard to which all modern IP PBXs adhere. The SIP protocol defines how calls should be established and is specified in RFC 3261. Because of SIP, it is possible to mix and match IP PBX software, phones and gateways. This protects our investment in the phone hardware. SIP phones are available in several versions.

### **5.3.3 Software based SIP phones**

A software based SIP phone is a program which makes use of our computers microphone and speakers, or an attached headset to allow us to make or receive calls. Examples of SIP phones are the included 3CXPhone or X-Lite from Counterpath.

## **5.4 VLC Media Player**

VLC is a free and open source cross-platform multimedia player and framework that plays most multimedia files as well as DVD, Audio CD, VCD, and various streaming protocols.

Features

- Simple, fast and powerful media player.
- Plays everything: Files, Discs, Webcams, Devices and Streams.
- Plays most codecs with no codec packs needed:
  - MPEG-2, DivX, H.264, MKV, WebM, WMV, MP3 etc.
- Runs on all platforms: Windows, Linux, Mac OS X, Unix.
- Completely Free, 0 spyware, 0 ads and no user tracking.
- Can do media conversion and streaming.
- 

## **5.5 Wireshark for Packet Capture and Analysis**

Wireshark is the world's most popular network analysis tool with an average of over 500,000 downloads per month. Wireshark is also ranked 1 in the world as a security tool . Named one of the "Most Important Open-Source Apps of All Time", Wireshark runs on Windows, Mac OS X, and \*NIX. Wireshark can even be run as a Portable App. Wireshark is a free open source software program available at [wireshark.org](http://wireshark.org). When run on a host that can see a wired or wireless network, Wireshark captures and decodes the network frames, offering an ideal tool for network troubleshooting, optimization, security (network forensics), and application analysis. Captured traffic can be saved in numerous trace file formats (defaulting to the new .pcapng format).

Wireshark's decoding process uses dissectors that can identify and display the various fields and values in network frames. In many instances, Wireshark's dissectors offer an interpretation of frame contents as well a feature that significantly reduces the time required to locate the cause of poor network performance or to validate security concerns.

### **5.5.1 General Analysis Tasks**

- Find the top talkers on the network
- See network communications in "clear text"

- See which hosts use which applications
- Baseline normal network communications
- Verify proper network operations
- Learn who's trying to connect to our wireless network
- Capture on multiple networks simultaneously
- Perform unattended traffic capture
- Capture and analyse traffic to/from a specific host or subnet
- View and reassemble files transferred via FTP or HTTP
- Import trace files from other capture tools
- Capture traffic using minimal resources

### **5.5.2 Troubleshooting Tasks**

- Create a custom analysis environment for troubleshooting
- Identify path, client, and server delays
- Identify TCP problems
- Detect HTTP proxy problems
- Detect application error responses
- Graph IO rates and correlate drops to network problems
- Identify overloaded buffers
- Compare slow communications to a baseline of normal communications
- Find duplicate IP addresses
- Identify DHCP server or relay agent problems on a network
- Identify WLAN signal strength problems
- Detect WLAN retries
- Capture traffic leading up to (and possibly the cause of) problems
- Detect various network misconfigurations
- Identify applications that are overloading a network segment
- Identify the most common causes of poorly performing applications

### **5.5.3 Security Analysis (Network Forensics) Tasks**

- Create a custom analysis environment for network forensics
- Detect applications that are using non-standard ports

- Identify traffic to/from suspicious hosts
- See which hosts are trying to obtain an IP address
- Identify "phone home" traffic
- Identify network reconnaissance processes
- Locate and globally map remote target addresses
- Detect questionable traffic redirections
- Examine a single TCP or UDP conversation between a client and server
- Detect maliciously malformed frames
- Locate known keyword attack signatures in our network traffic

#### **5.5.4 Application Analysis Tasks**

- Learn how applications and protocols work
- Graph bandwidth usage of an application
- Determine if a link will support an application
- Examine application performance after update/upgrade
- Detect error responses from a newly installed application
- Identify which users are running a particular application
- Examine how an application uses transport protocols such as TCP or UDP

## Chapter 6

### Evaluation

In this chapter actual experiment setup along configuration steps on Router is given .Brief overview of network performance analysis attributes are also discussed.

#### 6.1 Experimental Setup

Figure 6.1 shows actual experimental setup .Configuration of router with other commands are given in Appendix I.

##### Steps for Configuring Router in both Cases IP (OSPF) and MPLS

- a. Connecting Routers as shown in above topology
- b. Assign IP addresses to router interfaces including loopback interfaces
- c. Enable OSPF protocol on each router
- d. Verify Configuration of OSPF
- e. Generate Traffic for three flows (Data, Voice, Video) and take capture file for IP(OSPF) at PC1
- f. Enable MPLS on each router
- g. Configure MPLS L3 VPN
- h. Verify configuration of MPLS L3 VPN

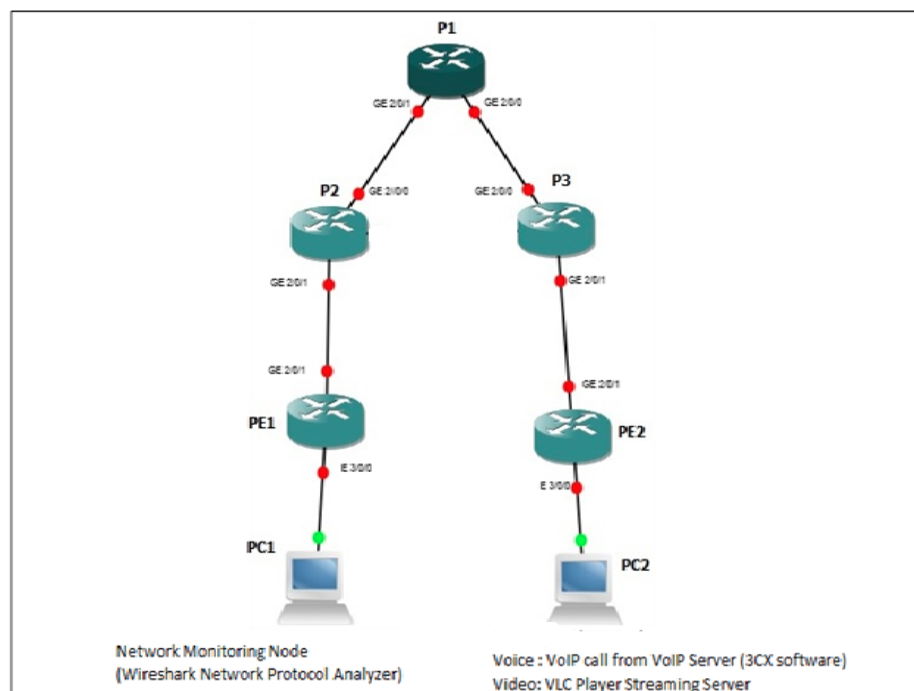


Figure 6.1 Experimental Lab Setup

## **6.2 Evaluation Metrics**

Latency, throughput, Packet loss, Jitter are four network performance parameter used in this experiment. Brief introduction is given in this section.

### **6.2.1 Latency in the network**

Bandwidth is just one element of what a person perceives as the speed of a network. Latency is another element that contributes to network speed. The term latency refers to any of several kinds of delays typically incurred in processing of network data. A so-called low latency network connection is one that generally experiences small delay times, while a high latency connection generally suffers from long delays.

Although the theoretical peak bandwidth of a network connection is fixed according to the technology used, the actual bandwidth we will obtain varies over time and is affected by high latencies. Excessive latency creates bottlenecks that prevent data from filling the network pipe, thus decreasing effective bandwidth. The impact of latency on network bandwidth can be temporary (lasting a few seconds) or persistent (constant) depending on the source of the delays [12].

### **6.2.2 Throughput of network**

Throughput is a measure of how much actual data can be sent per unit of time across a network, channel or interface. While throughput can be a theoretical term like bandwidth, it is more often used in a practical sense, for example, to measure the amount of data actually sent across a network in the “real world”[11]. Throughput is limited by bandwidth, or by rated speed: if an Ethernet network is rated at 100 megabits per second, that's the absolute upper limit on throughput, even though we will normally get quite a bit less. So, we may see someone say that they are using 100 Mbps Ethernet but getting throughput of say, 71.9 Mbps on their network.

### **6.2.3 Packet Loss in Network**

Packet loss is the failure of one or more transmitted packets to arrive at their destination. This event can cause noticeable effects in all types of digital communications.

The effects of packet loss:

- In data, packet loss produces errors.
- In videoconference environments it can create jitter.

- In pure audio communications, such as VoIP, it can cause jitter and frequent gaps in received speech.

In the worst cases, packet loss can cause severe mutilation of received data, broken-up images, unintelligible speech or even the complete absence of a received signal.

The causes of packet loss include inadequate signal strength at the destination, natural or human-made interference, excessive system noise, hardware failure, software corruption or overburdened network nodes. Often more than one of these factors is involved.

#### **6.2.4 Jitter in VoIP call for the network**

Another network quality issue to examine is jitter[1]. Each packet of voice information takes a different amount of time to go from one end of the network to the other. This variation is called “jitter”. The VOIP equipment on the receiving end is responsible for putting the packets into a buffer so that they can be played out as an unbroken stream of audio.



## Chapter 7

### Experimental Results And Discussion

In this chapter results of experiment after configuration and verification of system are shown with graphical and statistical format. Latency, Throughput, Packet loss, Jitter results are obtain in case of traditional IP and MPLS L3 VPN. These results are compared and analysis in with real world scenario of service provider network. Graphical and statistical results are obtain by using wireshark capture file during test and by applying appropriate filter.

#### 7.1 Latency in Network

In this section latency result is shown. This Latency is based on TCP connection of network it is round trip time for each packet. Network Latency is measured in terms of milliseconds.

##### 7.1.1 Average Latency in IP and MPLS

Graphical representation of latency is obtain by using capture file during test. By applying appropriate filters in Wireshark we can obtain different graphical and statistical

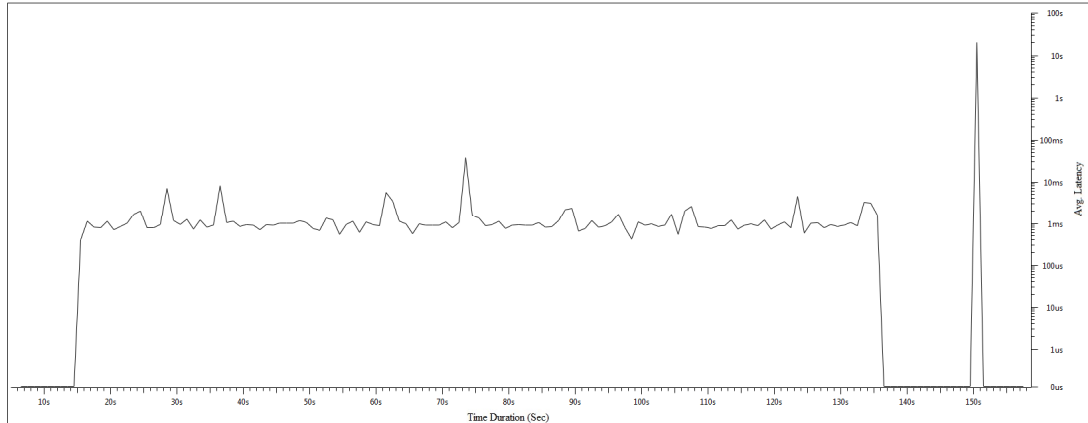


Figure 7.1 Avg Latency in OSPF

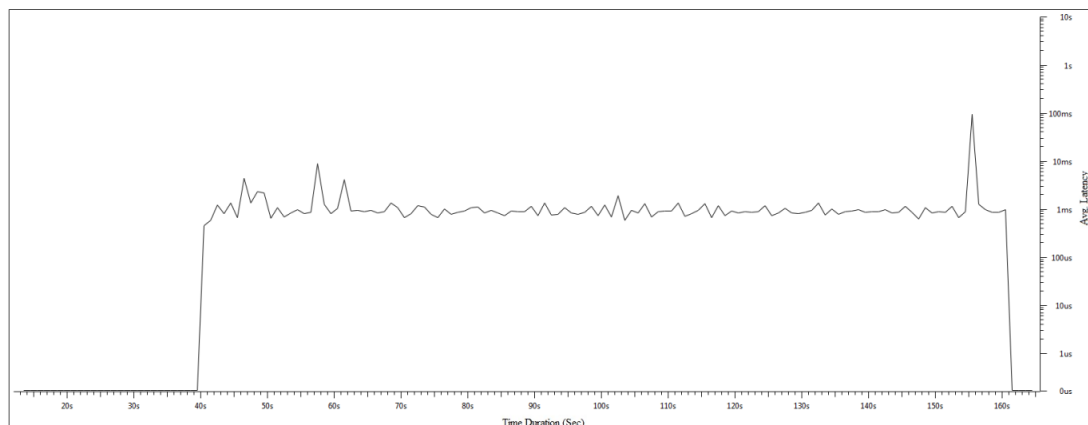
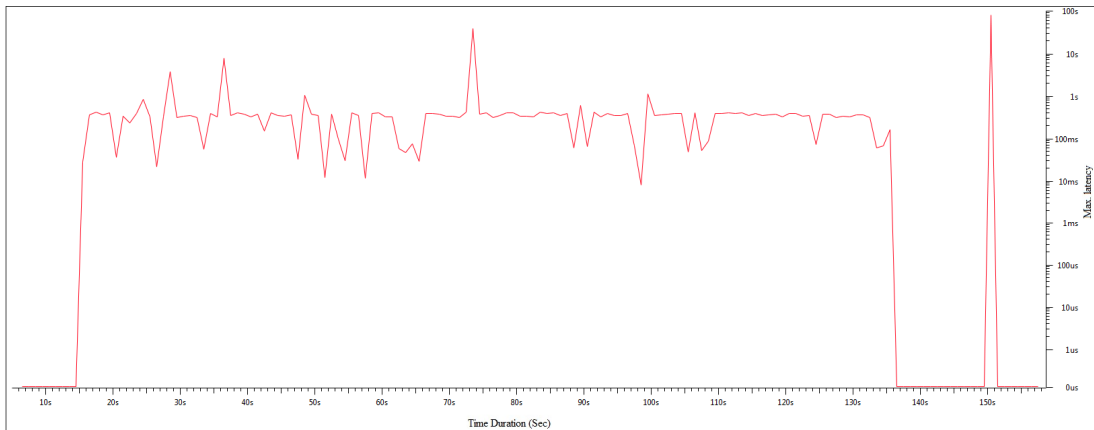


Figure 7.2 Avg Latency in MPLS

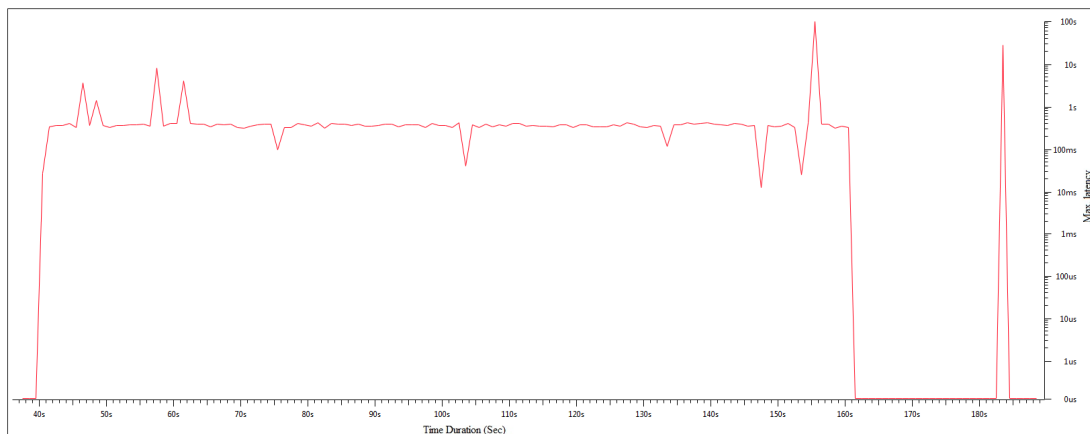
Figure 7.1,7.2 Shows Average latency in OSPF and MPLS L3 VPN . Latency is round trip time of any packet. By applying tcp.time\_delta filter in wireshark (Network Protocol Analyser) I get latency of network. In Figure 8.1 at interval around 25<sup>th</sup>,30<sup>th</sup>,38<sup>th</sup>,62<sup>nd</sup>,75<sup>th</sup>,123<sup>rd</sup> Sec time duration Avg. Latency is 10ms and above and other interval its around 1ms . In Figure 7.2 at interval around 47<sup>th</sup>,58<sup>th</sup>,62<sup>nd</sup> Sec time duration of testing Latency is around 10ms and overall latency is less than 1 ms .

Average latency in MPLS is less than traditional IP network . Latency is critical parameter in Data communication network. Performance of network in terms of Latency is improved.

### 7.1.2 Maximum Latency in IP and MPLS



**Figure 7.3 Maximum Latency in ospf**



**Figure 7.4 Maximum Latency in MPLS**

Figure 7.3,7.4 shows maximum latency in particular experiment with OSPF and MPLS L3 VPN respectively . It is clearly seen in above graph average .

Avg. latency is better in MPLS than IP, Maximum latency in this experiment is linear and stable in MPLS than IP. In figure 7.3 throughout test time more spikes are seen than less spikes are seen in figure 7.4.

## 7.2 Throughput of Network

As earlier discussed in earlier chapter about measuring throughput. Throughput is observed in the experiment with Wireshark Tool for TCP connection. Jperf itself generate throughput graph and it is been verified by wireshark capture file fetch at PC1.

### 7.2.1 Throughput obtain In Wireshark Capture

Statistics	Count	Bytes	Filter	Count	Bytes
Packets:	120000	1000000	tcp.dstport==5016	0	000000
Direction: first and last packet:	120000	1000000			
Avg. packet size:	8333.33	8333.33			
Avg. packet size:	10000000 bytes	10000000 bytes			
Bytes:	10000000	10000000	tcp.dstport==5016	0	000000
Avg. bytes:	10000000	10000000			
Avg. filter:	0.000	0.000			

Figure 7.5 Analysis of OSPF based on TCP destination port

Statistics	Count	Bytes	Filter	Count	Bytes
Packets:	120000	1000000	tcp.dstport==5016	0	000000
Direction: first and last packet:	120000	1000000			
Avg. packet size:	8333.33	8333.33			
Avg. packet size:	10000000 bytes	10000000 bytes			
Bytes:	10000000	10000000	tcp.dstport==5016	0	000000
Avg. bytes:	10000000	10000000			
Avg. filter:	0.000	0.000			

Figure 7.6 Analysis of MPLS based on TCP destination port

Figure 7.5, 7.6 gives us analysis of capture file when I apply wireshark filter tcp.dstport==5016, It indicate total number of packets send at TCP port no: 5016 for particular capture file.

In both cases (IP and MPLS) time between first and last packet is 120sec. Here Avg.Mbit/sec is throughput of the network for TCP connection.

By seeing the results of MPLS and traditional IP capture file throughput difference is 0.587 Mbits/sec, which is approximately same which I get in Jperf test . MPLS definitely added advantage in terms of network throughput.

### 7.3 Packet Loss

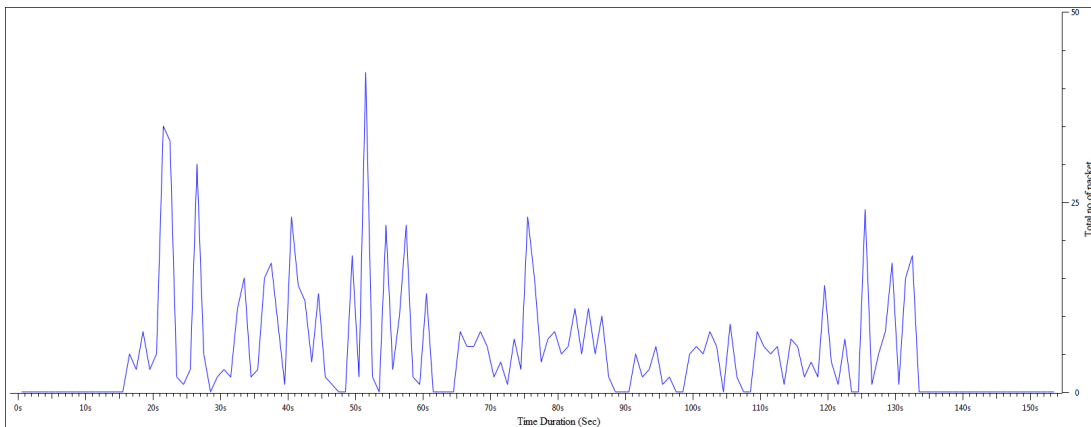
Packet loss is caused due to congestion in the network, connectivity issue, delay in network etc. Wireshark Capture file at PC1 gives details about packet loss.

#### 7.3.1 TCP Lost Segment

TCP lost Segment (tcp.analysis.lost\_segment) is filter in Wireshark which gives Packet loss analysis in IP and MPLS with graph and statistics.

In Figure 7.7 and 7.8 , x axis represents total time duration with interval and y axis represent total number of packet count at particular time interval .

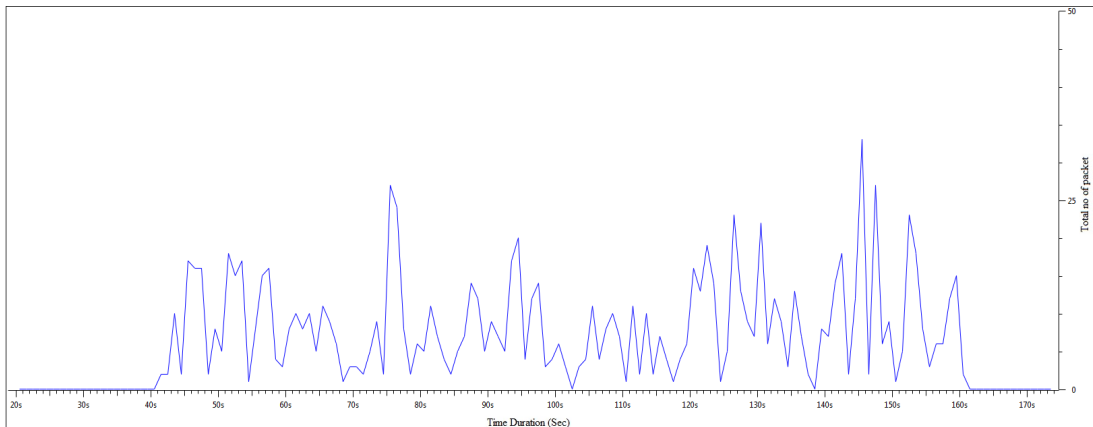
In figure 7.7, 12<sup>th</sup> to 62<sup>nd</sup> sec interval packet loss is more where as in figure 8.13 packet loss is more in between 120<sup>th</sup> to 160<sup>th</sup> sec interval.



**Figure 7.7 Packet Loss Parameter 1 in OSPF**

Statistic	0:24:56.000	0:25:00.000	0:25:04.000	0:25:08.000	0:25:12.000
Packets:	1262601	6000	600000	00	6000000
High speed time and high loss packets:	1:02:10:000	1:16:10:000			
Avg. packet/frame:	6000000	60000			
Avg. packet/frame:	1000000000 bytes	1:02:10:000 bytes			
Bytes:	1600000000	10000000	600000	00	6000000
Avg. bytes/frame:	1000000000	60000000			
Avg. diff/frame:	80000	60000			

**Figure 7.8 Analysis of TCP lost segment in IP**



**Figure 7.9 Packet Loss Parameter 1 in MPLS**

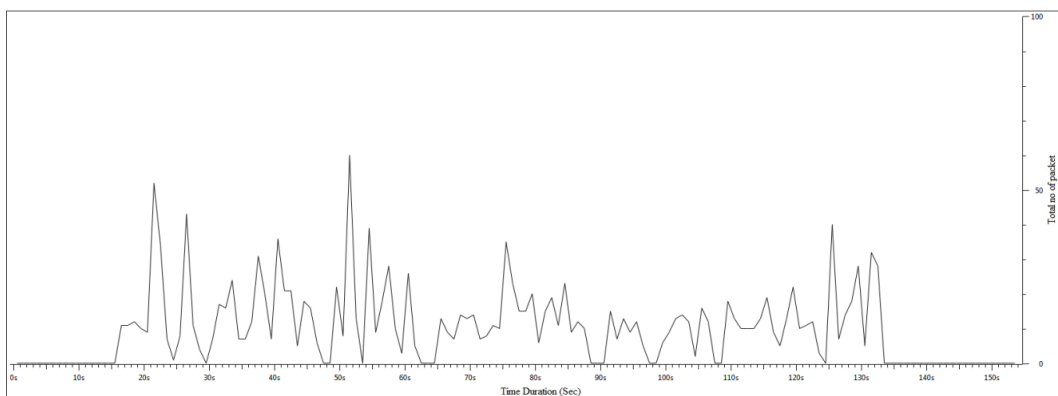
Interface	IP Configuration	IP Configuration	IP Configuration	IP Configuration	IP Configuration
Packet loss:	1000/1000	1000/1000	00.0000%	00	00.0000%
Maximum number of lost packets:	1000/1000	1000/1000			
Avg. packet loss:	00.0000	00.0000			
Avg. packet loss rate:	1000.0000 bytes	1000.0000 bytes			
Bytes:	1000.000000	1000.0000	00.0000%	00	00.0000%
Avg. bytes:	00.000000	1000.0000			
Avg. rate:	00.0000	00.0000			

**Figure 7.10 Analysis of TCP lost segment in MPLS (L3 VPN)**

Figure 7.9 & 7.10 gives packet count and other values in packet loss parameter, IP has packet loss 804 whereas 1038 in MPLS.

### 7.3.2 Retransmission of TCP packet

In TCP connection retransmission of packet is another factor for calculating Packet loss in the network. As we can say it is another way of representing packet loss in the network.

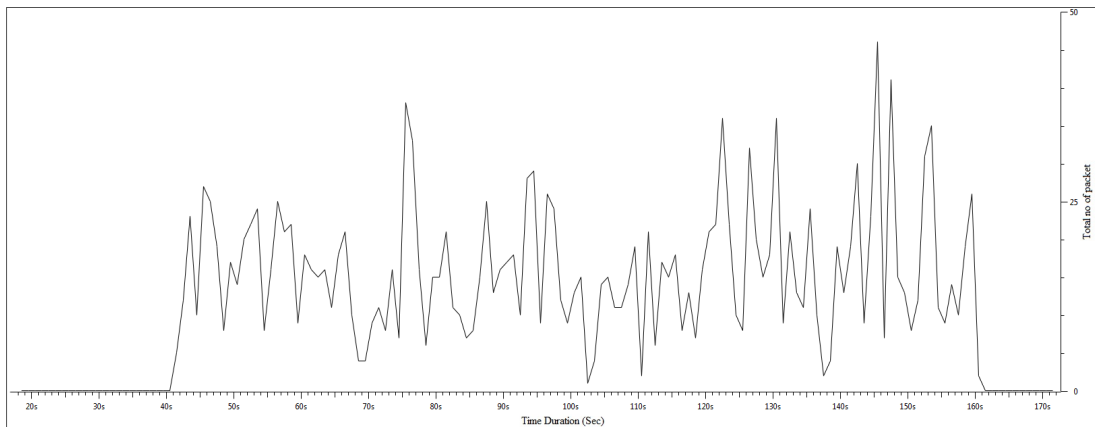


**Figure 7.11 Packet Loss Parameter 2 in OSPF**

Statistic	OSPF case	MPLS case	MPLS case %	OSPF case	OSPF case %
Packets:	1533	1533	100%	0	0%
Bytes:	106080	106080			
Avg. packet size:	69.204	69.204			
Avg. packet size:	106080 bytes	106080 bytes			
Bytes:	106080	106080	100%	0	0%
Avg. bytes:	106080	106080			
Avg. bits:	850	850			

**Figure 7.12 Analysis of TCP retransmission in IP (OSPF)**

Applying (tcp.analysis.retransmission) TCP retransmission filter is used for generating graph and statistical result in case of packet retransmission analysis.



**Figure 7.13 Packet Loss Parameter 2 in MPLS**

Statistic	OSPF case	MPLS case	MPLS case %	OSPF case	OSPF case %
Packets:	1928	1928	100%	0	0%
Bytes:	136000	136000			
Avg. packet size:	70.544	70.544			
Avg. packet size:	136000 bytes	136000 bytes			
Bytes:	136000	136000	100%	0	0%
Avg. bytes:	136000	136000			
Avg. bits:	6300	6300			

**Figure 7.14 Analysis of TCP retransmission in MPLS (L3 VPN)**

Figure 7.13 & 7.14 gives statistics of retransmission of packets occur in both cases.

In retransmission of TCP packet in MPLS case is 1928 packets and in OSPF case its 1539 packets . Time duration between first and last packet of TCP retransmission is approximately 116 sec and 119 sec for MPLS and OSPF case respectively.

Packet loss is always present in any congested network it depend of various factor i.e. TCP window size, TCP buffer, Router MTU, Delay in network etc . I have keep default setting on router and PC for both cases i.e. IP and MPLS. Packet loss is analyse for TCP connection number of packets lost and retransmitted in TCP are more in the MPLS than traditional IP . Packet loss rate is also more in MPLS.

#### 7.4 Jitter in VoIP

Jitter is also known as delay in time. Jitter is important aspect in VoIP communication.

VoIP analysis is needed while doing analysis of MPLS protocol in service provider environment.

##### 7.4.1 Analysis of VoIP call in IP and MPLS

Table 7.1 and Table 7.2 gives us analysis of VoIP call made during experiment and with their Maximum latency ,maximum jitter ,Mean jitter and lost RTP packets in Forward and reverse direction .H263 is video codec and g711U is audio codec having 95.2 Kb/sec bandwidth including overhead. Mean jitter in IP (OSPF) is Avg. 3.35ms and in MPLS L3 VPN it is Avg. 2.875ms.

**Table 7.1 IP (OSPF) Network VoIP call analysis**

Traditional IP VOIP call Analysis					
Parameter	Forward Direction	Reverse Direction	Forward Direction	Reverse Direction	Analysis
	h263		g711U		
<b>Max.Delta</b>	46.07ms	69.03ms	58.10ms	2080.42ms	Avg 563.405 ms
<b>Max.Jitter</b>	34.19ms	77.21ms	5.52ms	135.23ms	Avg 63.037ms
<b>Mean.Jitter</b>	1.89ms	2.12ms	0.86ms	8.53ms	Avg 3.35 ms
<b>Total RTP Packets</b>	4145	3731	6089	6157	Total 20122
<b>Lost RTP Packets</b>	0	11	0	8	Total Lost RTP Pckts 19
<b>Duration</b>	121.74sec	125.50sec	121.76sec	123.11sec	Avg Call Duration 123.02 sec

**Table 7.2 MPLS Network VoIP call Analysis**

MPLS L3 VPN Analysis					
Parameter	Forward Direction	Reverse Direction	Forward Direction	Reverse Direction	Analysis
	h263		g711U		
<b>Max.Delta</b>	135.95ms	66.75ms	2615.38ms	62.58ms	Avg 720.165ms
<b>Max.Jitter</b>	152.90ms	35.35ms	165.13ms	4.93ms	Avg 89.57ms
<b>Mean.Jitter</b>	2.20ms	1.85ms	6.84ms	0.61ms	Avg 2.875ms
<b>Total RTP Packets</b>	3029	4158	6070	6094	Total RTP Pckts 19351
<b>Lost RTP Packets</b>	6	0	10	0	Total Lost Pckts 16
<b>Duration</b>	123.52sec	121.84sec	121.35sec	121.86sec	Avg Call Duration 122.142 sec

Loss RTP packet in ospf is 19 and in MPLS it is 16, call duration are approximately 123 sec and 122 sec respectively.

This analysis is obtain with help of wireshark, which has separate exclusive tool for VoIP call. RTP streams are analyse in both IP and MPLS. Jitter value should be as small as possible, Mean jitter difference between traditional IP and MPLS is 3.35ms- 2.875ms = 0.475ms . Jitter performance is VoIP call is improved in MPLS than IP.



## Chapter 8

### Summary, Conclusion And Future Scope

Conclusion and future scope of MPLS discussed in this chapter. Conclusion is based on result obtain in this testing condition created for Service Provider Network Environment.

#### 8.1 Conclusion

In this work, experimentation is carried out in Lab environment with the MPLS network under various traffic conditions. The traffic condition is similar to the present traffic conditions of the service providers. The enhanced condition of the traffic is generated considering the future demand in the growth of the traffic. This is achieved by limiting the link bandwidth and traffic was generated by various tools to check Performance parameter. This traffic causes congestion in the network and behaviour of MPLS protocol is observed. Latency is improved MPLS enabled network than traditional IP network. There is significant visible difference in throughput of MPLS network which can generate high revenue for Service provider . As throughput was increased packet loss also increased in MPLS. This indicate performance is not as good as traditional IP but this can be improved with TCP packet loss avoidance mechanism. Average one way jitter in VoIP call is less than 30ms and we observed MPLS has edge in jitter value which is less than IP (OSPF), only one VoIP call is made between 3CX phone system clients, when traffic is more congested and severe then we may get different values of jitter but both mean jitter values are accepted for making VoIP call successful. MPLS definitely has edge in Service provider network where internet traffic is increasing day by day / The effect of various performance parameters of and MPLS network under different conditions will helpful in finally deploying and designing the MPLS network for a service providers (Such as MTNL).

#### 8.2 Future Scope of MPLS

MPLS has become popular and has seen many implementations and deployments by service providers. The original idea for inventing MPLS was a better integration of IP in ATM networks. A big part of the sensation is the result of the huge success of MPLS VPN in the industry. Service providers quickly recognized the great benefits of MPLS VPN and deployed it quickly while features for it were still being developed. These days even enterprise customers are looking at MPLS VPN with interest. They might have already deployed MPLS VPN for the benefit of a greater scalability. Other benefits to them is the separation of departments, or the easier deployment of PE and CE routers. Today, Any Transport over

MPLS (AToM), MPLS traffic engineering (TE), and VPLS are experiencing a growing interest from the industry, and service providers are deploying these MPLS applications [18]. Because most service provider networks are already running MPLS for the MPLS VPN service, the operators and technical support people have the experience in deploying and troubleshooting MPLS. It then becomes a smaller step to deploy one of the other MPLS applications

The Internet Engineering Task Force (IETF) and the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T) have undertaken a joint effort to standardize a new transport profile for the multi-protocol label switching (MPLS) technology that is intended to provide the basis for the next generation packet transport network. The fundamental idea of this activity is to extend MPLS where necessary with Operations, Administration and Maintenance (OAM) tools that are widely applied in existing transport network technologies such as SONET/SDH or OTN. These functions are targeted at making MPLS comparable to SONET/SDH and OTN in terms of reliability and monitoring capabilities, i.e., MPLS-TP will become a true carrier grade packet transport technology. An MPLS-TP network can be operated in an SDH-like fashion and a network management system (NMS) can be used to configure connections. Connection management and restoration functions, however, can alternatively be provided utilizing the Generalized MPLS (GMPLS) control plane protocols which are also applicable to the MPLS-TP data plane. In addition to the simplification of the network operation leading to reduced operational expenditures (OPEX), the GMPLS control plane provides network restoration capabilities in addition to the network protection features that the MPLS-TP data plane already provides; this results in a further improved network resiliency.

## Appendix

### JPERF Throughput Test in OSPF and MPLS Statistics

#### JPERF Generated file in OSPF throughput test

```
Bin/iperf.exe -s -P 0 -i 1 -m -p 5016 -C -f m
```

```
-----  
Server listening on TCP port 5016
```

```
TCP window size: 0.01 MByte (default)  
-----
```

```
OpenSCManager failed - Access is denied. (0x5)
```

```
[264] local 10.200.10.2 port 5016 connected with 100.100.100.2 port 49268
```

```
[ ID] Interval    Transfer    Bandwidth
```

```
[264] 0.0- 1.0 sec  1.88 MBytes 15.7 Mb/s
```

```
[264] 1.0- 2.0 sec  1.29 MBytes 10.8 Mb/s
```

```
[264] 2.0- 3.0 sec  1.03 MBytes  8.65 Mb/s
```

```
[264] 3.0- 4.0 sec  1.52 MBytes 12.7 Mb/s
```

```
[264] 4.0- 5.0 sec  1.05 MBytes  8.78 Mb/s
```

```
[264] 5.0- 6.0 sec  1.41 MBytes 11.9 Mb/s
```

```
[264] 6.0- 7.0 sec  1.23 MBytes 10.3 Mb/s
```

```
[264] 7.0- 8.0 sec  1.08 MBytes  9.04 Mb/s
```

```
[264] 8.0- 9.0 sec  0.93 MBytes  7.80 Mb/s
```

```
[264] 9.0-10.0 sec  1.43 MBytes 12.0 Mb/s
```

```
[264] 10.0-11.0 sec  1.45 MBytes 12.1 Mb/s
```

```
[264] 11.0-12.0 sec  1.05 MBytes  8.82 Mb/s
```

```
[264] 12.0-13.0 sec  0.80 MBytes  6.75 Mb/s
```

```
[264] 13.0-14.0 sec  1.74 MBytes 14.6 Mb/s
```

```
[264] 14.0-15.0 sec  0.74 MBytes  6.23 Mb/s
```

```
[264] 15.0-16.0 sec  1.60 MBytes 13.4 Mb/s
```

```
[264] 16.0-17.0 sec  1.13 MBytes  9.46 Mb/s
```

```
[264] 17.0-18.0 sec  1.25 MBytes 10.5 Mb/s
```

```
[264] 18.0-19.0 sec  1.10 MBytes  9.24 Mb/s
```

[264]	19.0-20.0 sec	1.12 MBytes	9.37 Mb/s
[ ID]	Interval	Transfer	Bandwidth
[264]	20.0-21.0 sec	1.20 MBytes	10.1 Mb/s
[264]	21.0-22.0 sec	1.57 MBytes	13.2 Mb/s
[264]	22.0-23.0 sec	1.22 MBytes	10.2 Mb/s
[264]	23.0-24.0 sec	1.03 MBytes	8.65 Mb/s
[264]	24.0-25.0 sec	1.38 MBytes	11.5 Mb/s
[264]	25.0-26.0 sec	1.14 MBytes	9.58 Mb/s
[264]	26.0-27.0 sec	1.18 MBytes	9.88 Mb/s
[264]	27.0-28.0 sec	0.92 MBytes	7.73 Mb/s
[264]	28.0-29.0 sec	1.58 MBytes	13.3 Mb/s
[264]	29.0-30.0 sec	0.99 MBytes	8.29 Mb/s
[264]	30.0-31.0 sec	1.07 MBytes	8.98 Mb/s
[264]	31.0-32.0 sec	0.83 MBytes	6.95 Mb/s
[264]	32.0-33.0 sec	0.84 MBytes	7.08 Mb/s
[264]	33.0-34.0 sec	1.85 MBytes	15.5 Mb/s
[264]	34.0-35.0 sec	1.00 MBytes	8.38 Mb/s
[264]	35.0-36.0 sec	1.46 MBytes	12.2 Mb/s
[264]	36.0-37.0 sec	1.04 MBytes	8.77 Mb/s
[264]	37.0-38.0 sec	0.55 MBytes	4.65 Mb/s
[264]	38.0-39.0 sec	1.96 MBytes	16.4 Mb/s
[264]	39.0-40.0 sec	1.07 MBytes	8.98 Mb/s
[ ID]	Interval	Transfer	Bandwidth
[264]	40.0-41.0 sec	1.39 MBytes	11.7 Mb/s
[264]	41.0-42.0 sec	1.22 MBytes	10.2 Mb/s
[264]	42.0-43.0 sec	0.77 MBytes	6.46 Mb/s
[264]	43.0-44.0 sec	1.02 MBytes	8.52 Mb/s
[264]	44.0-45.0 sec	1.47 MBytes	12.3 Mb/s
[264]	45.0-46.0 sec	0.76 MBytes	6.36 Mb/s
[264]	46.0-47.0 sec	0.29 MBytes	2.42 Mb/s
[264]	47.0-48.0 sec	0.48 MBytes	4.06 Mb/s
[264]	48.0-49.0 sec	1.66 MBytes	14.0 Mb/s

[264]	49.0-50.0 sec	1.37 MBytes	11.5 Mbbits/sec
[264]	50.0-51.0 sec	1.31 MBytes	11.0 Mbbits/sec
[264]	51.0-52.0 sec	1.09 MBytes	9.18 Mbbits/sec
[264]	52.0-53.0 sec	0.96 MBytes	8.06 Mbbits/sec
[264]	53.0-54.0 sec	1.41 MBytes	11.8 Mbbits/sec
[264]	54.0-55.0 sec	1.44 MBytes	12.1 Mbbits/sec
[264]	55.0-56.0 sec	0.96 MBytes	8.03 Mbbits/sec
[264]	56.0-57.0 sec	1.45 MBytes	12.2 Mbbits/sec
[264]	57.0-58.0 sec	0.87 MBytes	7.27 Mbbits/sec
[264]	58.0-59.0 sec	1.46 MBytes	12.3 Mbbits/sec
[264]	59.0-60.0 sec	1.10 MBytes	9.24 Mbbits/sec
[ ID]	Interval	Transfer	Bandwidth
[264]	60.0-61.0 sec	1.20 MBytes	10.1 Mbbits/sec
[264]	61.0-62.0 sec	1.23 MBytes	10.4 Mbbits/sec
[264]	62.0-63.0 sec	1.43 MBytes	12.0 Mbbits/sec
[264]	63.0-64.0 sec	0.89 MBytes	7.42 Mbbits/sec
[264]	64.0-65.0 sec	1.39 MBytes	11.7 Mbbits/sec
[264]	65.0-66.0 sec	1.21 MBytes	10.2 Mbbits/sec
[264]	66.0-67.0 sec	1.00 MBytes	8.39 Mbbits/sec
[264]	67.0-68.0 sec	1.53 MBytes	12.8 Mbbits/sec
[264]	68.0-69.0 sec	1.17 MBytes	9.83 Mbbits/sec
[264]	69.0-70.0 sec	0.88 MBytes	7.34 Mbbits/sec
[264]	70.0-71.0 sec	1.24 MBytes	10.4 Mbbits/sec
[264]	71.0-72.0 sec	1.42 MBytes	11.9 Mbbits/sec
[264]	72.0-73.0 sec	0.76 MBytes	6.36 Mbbits/sec
[264]	73.0-74.0 sec	0.21 MBytes	1.77 Mbbits/sec
[264]	74.0-75.0 sec	1.35 MBytes	11.3 Mbbits/sec
[264]	75.0-76.0 sec	1.49 MBytes	12.5 Mbbits/sec
[264]	76.0-77.0 sec	1.39 MBytes	11.7 Mbbits/sec
[264]	77.0-78.0 sec	1.03 MBytes	8.63 Mbbits/sec
[264]	78.0-79.0 sec	1.16 MBytes	9.76 Mbbits/sec
[264]	79.0-80.0 sec	1.52 MBytes	12.7 Mbbits/sec

[ ID]	Interval	Transfer	Bandwidth
[264]	80.0-81.0 sec	0.91 MBytes	7.60 Mbites/sec
[264]	81.0-82.0 sec	0.35 MBytes	2.95 Mbites/sec
[264]	82.0-83.0 sec	1.52 MBytes	12.8 Mbites/sec
[264]	83.0-84.0 sec	0.91 MBytes	7.67 Mbites/sec
[264]	84.0-85.0 sec	1.53 MBytes	12.8 Mbites/sec
[264]	85.0-86.0 sec	1.24 MBytes	10.4 Mbites/sec
[264]	86.0-87.0 sec	1.00 MBytes	8.38 Mbites/sec
[264]	87.0-88.0 sec	1.47 MBytes	12.3 Mbites/sec
[264]	88.0-89.0 sec	1.11 MBytes	9.31 Mbites/sec
[264]	89.0-90.0 sec	1.11 MBytes	9.31 Mbites/sec
[264]	90.0-91.0 sec	1.28 MBytes	10.7 Mbites/sec
[264]	91.0-92.0 sec	0.25 MBytes	2.10 Mbites/sec
[264]	92.0-93.0 sec	0.70 MBytes	5.83 Mbites/sec
[264]	93.0-94.0 sec	2.09 MBytes	17.5 Mbites/sec
[264]	94.0-95.0 sec	1.03 MBytes	8.67 Mbites/sec
[264]	95.0-96.0 sec	0.93 MBytes	7.84 Mbites/sec
[264]	96.0-97.0 sec	1.34 MBytes	11.2 Mbites/sec
[264]	97.0-98.0 sec	1.38 MBytes	11.6 Mbites/sec
[264]	98.0-99.0 sec	1.10 MBytes	9.24 Mbites/sec
[264]	99.0-100.0 sec	1.23 MBytes	10.3 Mbites/sec

[ ID]	Interval	Transfer	Bandwidth
[264]	100.0-101.0 sec	1.32 MBytes	11.1 Mbites/sec
[264]	101.0-102.0 sec	0.95 MBytes	8.00 Mbites/sec
[264]	102.0-103.0 sec	1.53 MBytes	12.8 Mbites/sec
[264]	103.0-104.0 sec	1.16 MBytes	9.76 Mbites/sec
[264]	104.0-105.0 sec	0.94 MBytes	7.86 Mbites/sec
[264]	105.0-106.0 sec	1.52 MBytes	12.7 Mbites/sec
[264]	106.0-107.0 sec	0.90 MBytes	7.55 Mbites/sec
[264]	107.0-108.0 sec	0.94 MBytes	7.92 Mbites/sec
[264]	108.0-109.0 sec	0.88 MBytes	7.41 Mbites/sec
[264]	109.0-110.0 sec	1.67 MBytes	14.0 Mbites/sec

```

[264] 110.0-111.0 sec 1.17 MBytes 9.80 Mb/s
[264] 111.0-112.0 sec 0.99 MBytes 8.29 Mb/s
[264] 112.0-113.0 sec 1.30 MBytes 10.9 Mb/s
[264] 113.0-114.0 sec 1.05 MBytes 8.85 Mb/s
[264] 114.0-115.0 sec 1.28 MBytes 10.7 Mb/s
[264] 115.0-116.0 sec 1.42 MBytes 12.0 Mb/s
[264] 116.0-117.0 sec 1.15 MBytes 9.68 Mb/s
[264] 117.0-118.0 sec 0.56 MBytes 4.72 Mb/s
[264] 118.0-119.0 sec 0.36 MBytes 3.01 Mb/s
[264] 119.0-120.0 sec 0.55 MBytes 4.59 Mb/s
[ ID] Interval    Transfer  Bandwidth
[264] 0.0-120.0 sec 139 MBytes 9.70 Mb/s
[264] MSS and MTU size unknown (TCP_MAXSEG not supported by OS?)

```

**JPERF Generated file in MPLS VPN throughput test**

```
Bin/iperf.exe -s -P 0 -i 1 -m -p 5016 -C -f m
```

```

-----
Server listening on TCP port 5016
TCP window size: 0.01 MByte (default)
-----

```

```

OpenSCManager failed - Access is denied. (0x5)
[264] local 50.50.50.2 port 5016 connected with 40.40.40.40 port 49272
[ ID] Interval    Transfer  Bandwidth
[264] 0.0- 1.0 sec 1.91 MBytes 16.0 Mb/s
[264] 1.0- 2.0 sec 1.22 MBytes 10.2 Mb/s
[264] 2.0- 3.0 sec 1.24 MBytes 10.4 Mb/s
[264] 3.0- 4.0 sec 1.29 MBytes 10.8 Mb/s
[264] 4.0- 5.0 sec 1.32 MBytes 11.1 Mb/s
[264] 5.0- 6.0 sec 1.30 MBytes 10.9 Mb/s
[264] 6.0- 7.0 sec 1.24 MBytes 10.4 Mb/s
[264] 7.0- 8.0 sec 0.85 MBytes 7.14 Mb/s

```

[264]	8.0- 9.0 sec	1.45 MBytes	12.2 Mbbits/sec
[264]	9.0-10.0 sec	1.36 MBytes	11.4 Mbbits/sec
[264]	10.0-11.0 sec	0.93 MBytes	7.79 Mbbits/sec
[264]	11.0-12.0 sec	1.30 MBytes	10.9 Mbbits/sec
[264]	12.0-13.0 sec	1.40 MBytes	11.8 Mbbits/sec
[264]	13.0-14.0 sec	0.90 MBytes	7.51 Mbbits/sec
[264]	14.0-15.0 sec	1.58 MBytes	13.2 Mbbits/sec
[264]	15.0-16.0 sec	1.29 MBytes	10.8 Mbbits/sec
[264]	16.0-17.0 sec	1.09 MBytes	9.18 Mbbits/sec
[264]	17.0-18.0 sec	1.20 MBytes	10.1 Mbbits/sec
[264]	18.0-19.0 sec	0.85 MBytes	7.14 Mbbits/sec
[264]	19.0-20.0 sec	1.53 MBytes	12.9 Mbbits/sec
[ ID]	Interval	Transfer	Bandwidth
[264]	20.0-21.0 sec	1.35 MBytes	11.3 Mbbits/sec
[264]	21.0-22.0 sec	1.19 MBytes	10.0 Mbbits/sec
[264]	22.0-23.0 sec	0.97 MBytes	8.13 Mbbits/sec
[264]	23.0-24.0 sec	1.44 MBytes	12.1 Mbbits/sec
[264]	24.0-25.0 sec	1.35 MBytes	11.3 Mbbits/sec
[264]	25.0-26.0 sec	1.11 MBytes	9.27 Mbbits/sec
[264]	26.0-27.0 sec	1.23 MBytes	10.3 Mbbits/sec
[264]	27.0-28.0 sec	1.17 MBytes	9.83 Mbbits/sec
[264]	28.0-29.0 sec	1.01 MBytes	8.45 Mbbits/sec
[264]	29.0-30.0 sec	1.22 MBytes	10.2 Mbbits/sec
[264]	30.0-31.0 sec	1.53 MBytes	12.8 Mbbits/sec
[264]	31.0-32.0 sec	0.96 MBytes	8.06 Mbbits/sec
[264]	32.0-33.0 sec	1.09 MBytes	9.18 Mbbits/sec
[264]	33.0-34.0 sec	1.34 MBytes	11.2 Mbbits/sec
[264]	34.0-35.0 sec	1.44 MBytes	12.1 Mbbits/sec
[264]	35.0-36.0 sec	1.05 MBytes	8.85 Mbbits/sec
[264]	36.0-37.0 sec	1.19 MBytes	9.96 Mbbits/sec
[264]	37.0-38.0 sec	1.22 MBytes	10.3 Mbbits/sec
[264]	38.0-39.0 sec	1.46 MBytes	12.2 Mbbits/sec



[264]	39.0-40.0 sec	0.99 MBytes	8.32 Mbites/sec
[ ID]	Interval	Transfer	Bandwidth
[264]	40.0-41.0 sec	1.25 MBytes	10.5 Mbites/sec
[264]	41.0-42.0 sec	1.20 MBytes	10.1 Mbites/sec
[264]	42.0-43.0 sec	1.25 MBytes	10.5 Mbites/sec
[264]	43.0-44.0 sec	1.11 MBytes	9.31 Mbites/sec
[264]	44.0-45.0 sec	1.29 MBytes	10.8 Mbites/sec
[264]	45.0-46.0 sec	1.42 MBytes	11.9 Mbites/sec
[264]	46.0-47.0 sec	1.21 MBytes	10.2 Mbites/sec
[264]	47.0-48.0 sec	1.20 MBytes	10.0 Mbites/sec
[264]	48.0-49.0 sec	1.00 MBytes	8.39 Mbites/sec
[264]	49.0-50.0 sec	1.29 MBytes	10.8 Mbites/sec
[264]	50.0-51.0 sec	1.21 MBytes	10.2 Mbites/sec
[264]	51.0-52.0 sec	0.98 MBytes	8.18 Mbites/sec
[264]	52.0-53.0 sec	1.58 MBytes	13.2 Mbites/sec
[264]	53.0-54.0 sec	0.85 MBytes	7.14 Mbites/sec
[264]	54.0-55.0 sec	1.27 MBytes	10.7 Mbites/sec
[264]	55.0-56.0 sec	1.32 MBytes	11.1 Mbites/sec
[264]	56.0-57.0 sec	1.49 MBytes	12.5 Mbites/sec
[264]	57.0-58.0 sec	0.89 MBytes	7.44 Mbites/sec
[264]	58.0-59.0 sec	1.38 MBytes	11.6 Mbites/sec
[264]	59.0-60.0 sec	1.24 MBytes	10.4 Mbites/sec
[ ID]	Interval	Transfer	Bandwidth
[264]	60.0-61.0 sec	1.17 MBytes	9.83 Mbites/sec
[264]	61.0-62.0 sec	0.96 MBytes	8.06 Mbites/sec
[264]	62.0-63.0 sec	1.59 MBytes	13.4 Mbites/sec
[264]	63.0-64.0 sec	1.09 MBytes	9.12 Mbites/sec
[264]	64.0-65.0 sec	1.36 MBytes	11.4 Mbites/sec
[264]	65.0-66.0 sec	1.09 MBytes	9.18 Mbites/sec
[264]	66.0-67.0 sec	1.09 MBytes	9.18 Mbites/sec
[264]	67.0-68.0 sec	1.49 MBytes	12.5 Mbites/sec
[264]	68.0-69.0 sec	0.98 MBytes	8.19 Mbites/sec

[264]	69.0-70.0 sec	1.39 MBytes	11.7 Mbbits/sec
[264]	70.0-71.0 sec	0.93 MBytes	7.81 Mbbits/sec
[264]	71.0-72.0 sec	1.19 MBytes	10.0 Mbbits/sec
[264]	72.0-73.0 sec	1.62 MBytes	13.6 Mbbits/sec
[264]	73.0-74.0 sec	0.84 MBytes	7.03 Mbbits/sec
[264]	74.0-75.0 sec	1.43 MBytes	12.0 Mbbits/sec
[264]	75.0-76.0 sec	1.11 MBytes	9.29 Mbbits/sec
[264]	76.0-77.0 sec	1.19 MBytes	9.96 Mbbits/sec
[264]	77.0-78.0 sec	1.36 MBytes	11.4 Mbbits/sec
[264]	78.0-79.0 sec	1.02 MBytes	8.53 Mbbits/sec
[264]	79.0-80.0 sec	1.52 MBytes	12.8 Mbbits/sec
[ ID]	Interval	Transfer	Bandwidth
[264]	80.0-81.0 sec	1.27 MBytes	10.7 Mbbits/sec
[264]	81.0-82.0 sec	1.24 MBytes	10.4 Mbbits/sec
[264]	82.0-83.0 sec	1.22 MBytes	10.2 Mbbits/sec
[264]	83.0-84.0 sec	0.84 MBytes	7.01 Mbbits/sec
[264]	84.0-85.0 sec	1.30 MBytes	10.9 Mbbits/sec
[264]	85.0-86.0 sec	1.31 MBytes	11.0 Mbbits/sec
[264]	86.0-87.0 sec	1.05 MBytes	8.85 Mbbits/sec
[264]	87.0-88.0 sec	1.25 MBytes	10.5 Mbbits/sec
[264]	88.0-89.0 sec	1.32 MBytes	11.1 Mbbits/sec
[264]	89.0-90.0 sec	1.45 MBytes	12.1 Mbbits/sec
[264]	90.0-91.0 sec	1.14 MBytes	9.56 Mbbits/sec
[264]	91.0-92.0 sec	1.01 MBytes	8.45 Mbbits/sec
[264]	92.0-93.0 sec	1.21 MBytes	10.1 Mbbits/sec
[264]	93.0-94.0 sec	0.88 MBytes	7.38 Mbbits/sec
[264]	94.0-95.0 sec	1.61 MBytes	13.5 Mbbits/sec
[264]	95.0-96.0 sec	1.09 MBytes	9.11 Mbbits/sec
[264]	96.0-97.0 sec	1.26 MBytes	10.6 Mbbits/sec
[264]	97.0-98.0 sec	1.12 MBytes	9.37 Mbbits/sec
[264]	98.0-99.0 sec	1.33 MBytes	11.1 Mbbits/sec
[264]	99.0-100.0 sec	1.30 MBytes	10.9 Mbbits/sec

[ ID]	Interval	Transfer	Bandwidth
[264]	100.0-101.0 sec	1.09 MBytes	9.11 Mbites/sec
[264]	101.0-102.0 sec	0.95 MBytes	7.93 Mbites/sec
[264]	102.0-103.0 sec	1.38 MBytes	11.6 Mbites/sec
[264]	103.0-104.0 sec	1.33 MBytes	11.1 Mbites/sec
[264]	104.0-105.0 sec	1.21 MBytes	10.2 Mbites/sec
[264]	105.0-106.0 sec	1.08 MBytes	9.04 Mbites/sec
[264]	106.0-107.0 sec	1.51 MBytes	12.7 Mbites/sec
[264]	107.0-108.0 sec	0.94 MBytes	7.89 Mbites/sec
[264]	108.0-109.0 sec	1.17 MBytes	9.83 Mbites/sec
[264]	109.0-110.0 sec	1.19 MBytes	9.96 Mbites/sec
[264]	110.0-111.0 sec	1.37 MBytes	11.5 Mbites/sec
[264]	111.0-112.0 sec	1.29 MBytes	10.8 Mbites/sec
[264]	112.0-113.0 sec	1.31 MBytes	11.0 Mbites/sec
[264]	113.0-114.0 sec	1.08 MBytes	9.04 Mbites/sec
[264]	114.0-115.0 sec	1.05 MBytes	8.85 Mbites/sec
[264]	115.0-116.0 sec	1.43 MBytes	12.0 Mbites/sec
[264]	116.0-117.0 sec	1.10 MBytes	9.24 Mbites/sec
[264]	117.0-118.0 sec	1.36 MBytes	11.4 Mbites/sec
[264]	118.0-119.0 sec	1.15 MBytes	9.63 Mbites/sec
[264]	119.0-120.0 sec	1.30 MBytes	10.9 Mbites/sec

[ ID] Interval Transfer Bandwidth

[264] 0.0-120.0 sec 147 MBytes 10.3 Mbites/sec

[264] MSS and MTU size unknown (TCP\_MAXSEG not supported by OS?)

Done.

## References

### Books,

- [1] Sam Halabi & Danny McPherson, Internet Routing Architecture , Second Edition ,CISCO Press,ISBN:1-57870-223-X,Aug 23 2000
- [2] Luc De Ghein , MPLS Fundamentals , CISCO Press, ISBN: 1-58705-197-4, 2007
- [3] Todd Lammle ,Cisco Certified Network Associate Routing and Switching Study Guide , John Wiley & Sons SYBEX , 2013

### Journal papers,

- [4] Dilmohan Narula, Mauricio Rojasmartinez, Venkatachalapati Rayipati, “Evaluating Performance on an ISP MPLS Network” ,University of Colorado,6 Dec 2010
- [5] Karol Molnar & Martin Vleck, “Evaluation of Bandwidth Constrain model for MPLS networks”,Annual Journal of Electronics, ISSN 1313-1842,2009
- [6] Daniel Backman ,roy Herrera , “The Essential guide to Deploying MPLS for Enterprise Network” , Juniper Networks,Part no:200183-001, May 2009
- [7] Md. Arifur Rahman, Ahmedul Kabir, K.A.M. lutfullah, M.Zahedul Hassan. M.R. Amin ,“Performance Analysis and the Study of Behavior of MPLS Protocols,”in Proc. International Conference on Computer and Communication Engineering,Kaula Lumpur. Malashiya,IEEE, May 2008
- [8] Wojtek nigos, Bernard Cousin, Stephaane Gosselin, Morgane le Foll, Hisao Nakajima, “Survivable MPLS Over Optical Transport Networks: Cost & Resource Usage Analysis” ,IEEE Journal on selected areas in communcation,Vol.25,No.5,June 2007
- [9] Chuck Semeria ,“MPLS Enhancing routing in the new public network”,White paper, Juniper Network INC, Part no :200001-002 Sept 2000
- [10] Johnny Bass, “Cisco Service Provider Next Generation Networks”, Global Knowledge Training LLC, White Paper,2012

### Institutes,

CETTM, Centre for Excellence in Telecom Technology and Management,  
MTNL,(Mahanagar Telecom Nigam Ltd.), Powai