A STUDY ON THE USE OF MPLS- TE IN IP CORE NETWORKS

A thesis presented by,
ANANDAMURUGA GAJENDRAN
Admission Number: 05/8369

Supervised by
ENG. A.T.L.K. SAMARASINGHE

In partial fulfillment of the requirement for the degree of
MASTER OF SCIENCE IN TELECOMMUNICATIONS

At the
DEPARTMENT OF ELECTRONICS AND TELECOMMUNICATION ENGINEERING
UNIVERSITY OF MORATUW A
SRI LANKA

2009

Abstract

Keywords: Core network, NGN, MPLS, MPLS-TE, QoS, DSCP, differentiated services, SLA, SNMP, ICT

Today's demand for various applications like voice, data and real time video etc., are increasing in the consumer market and stakeholders mostly expect all services from a service provider. The tremendous growth in ICT adds more users and also traffic adds another dimension. NGN is expected to be the emerging IP network to transport converged services and MPLS and MPLS- TE plays an important role in this context. These new applications have increased demand for guaranteed bandwidth in the limited backbone capacity in the provider's network and the challenge is to provide differentiated class of services with required QoS and also to produce SLA performance reports to the end users when requested. Due to numerous benefits such as guaranteed end to end QoS, link protection and efficient use of core bandwidth MPLS- TE is being recognized and becoming popular among service providers. TE enables service providers to route network traffic in such a way that they can offer the best service to their users in terms of throughput and delay.

In this research MPLS- TE approach is used to implement end to end QoS for prioritized services and a SLA program is developed using SNMP to produce end to end reports on critical performance metrics like delay, round trip time, jitter and application aware services to customers. The study also investigates the process of steering traffic across the MPLS/IP core backbone to facilitate efficient use of available bandwidth between a pair of backbone routers to ensure the required service levels. Hence in a multilink environment where many links are available for routing we can avoid the shortest paths being congested. Since network can have different types of packets; packets were generated and marked based on DSCP for QoS which were routed in different TE tunnels in a lab environment. The lab results showed that, using, TE tunriels constrained routing can provide explicit paths to required destinations regardless of the paths calculated by the routing protocols thus

bandwidth efficiency can be achieved in the core while ensuring end to end QoS for critical applications for a given IP SLA. Also, results obtained by the SLA program from a live operational network were acceptable in providing SLA performance reports.

DECLARATION

I do hereby declare that the work reported in this research project was exclusively carried out by me under the supervision of Eng. A.T.L.K. Samarasinghe. The work included in the thesis has not been submitted for any other academic qualification at any institution.

Signature: UOM Verified Signature Date: [illegible]

Certified by:

Supervisor Eng. A.T.L.K. Samarasinghe

Signature: UOM Verified Signature Date: [illegible]

A. T. L. K. Samarasinghe
Head
Department of Electronic &
Telecommunication Engineering
University of Moratuwa, Sri Lanka

TABLE OF CONTENTS

LIST OF FIGURES vii

LIST OF TABLES x

ACRONYMS xi

ACKNOWLEDGEMENT xiii

ABSTRACT xiv

1.0 Introduction

1.1 Background and motivation for the thesis 1

1.2 Goal of the thesis 2

1.3 Structure of the thesis 3

2.0 MPLS

2.1 Introduction 4

2.2 Brief History of MPLS communications 5

2.3 Benefits of using MPLS communication 9

2.4 Architecture of MPLS Protocol stack 10

2.5 MPLS Network over view 11

2.6 Traditional Routing and Packet Switching 13

2.7 MPLS Operation 13

2.7.1 Label Switch Routers (LSRs) or Label Edge Routers (LERs) 16

2.7.2 Forward Equivalent Class (FEC) 16

2.7.3 Labels and Label Bindings 16

2.7.4 Label creation and Distribution 18

2.7.5 Label Switched Paths (LSPs) 19

3.0 MPLS Traffic Engineering (TE) and Techniques

3.1 Overview 21

3.2 How TE Operates Operation 23

3.2.1 MPLS TE Signaling Protocols 25

3.2.2 Resource Reservation protocol (RSVP) Extensions 25

3.2.3 Traffic Selection 26

4.0 MPLS and Quality of Service

4.1 Overview 27

4.2 Differentiated Services 27

4.3 Per-Hop Behaviors (PHBs) and Codepoints 30

4.4 IP Service Level Agreements (SLA) 31

5.0 Simulation and Results

5.1 Introduction 37

5.2 Setting up MPLS topology and assigning traffic via TE tunnels 38

5.3 QoS Marking using Differentiated Services Code Point (DSCP) 51

5.4 IP Service Level Agreements (SLAs) customer reports 55

6.0 Conclusion & Discussion of Results 60

6.1 Future works 61

APPENDIX A 62

APPENDIX B 73

REFERENCES 90

BIBLIOGRAPHY 92

LIST OF FIGURES

Figure 2.1	:	Label Switching Timeline	5
Figure 2.2	:	IETF Standards	6
Figure 2.3	:	Typical MPLS block diagram	7
Figure 2.4	:	Typical MPLS Protocol Stack	10
Figure 2.5	:	LDP Header	10
Figure 2.6	:	MPLS Network Overview	11
Figure 2.7	:	MPLS Operation	12
Figure 2.8	:	Packet Flow in MPLS	13
Figure 2.9	:	MPLS Header	16
Figure 2.10	:	Label Request and Label Mapping	31
Figure 3.1	:	IP forwarding network	30
Figure 3.2	:	MPLS TE Tunnels	23
Figure 4.1	:	IP version 4 Type of Service (TOS) field	27
Figure 4.5	:	End to End IPSLA	31
Figure 4.6	:	MIB tree for vendor CISCO (1.3.6.1.4.1.9.X.X.X.X.X) where "X" represents values specific to a product.	34
Figure 4.7	:	SLA program logic to generate performance reports	35
Figure 5.1	:	Initial Topology creations in GNS3, all routers are CISCO 3640 with IOS version 12.3(26)	38
Figure 5.2	:	MPLS network Topology implemented in Lab, all routers are CISCO 2800 and core serial links are connected via a Frame Relay Switch	39
Figure 5.3a	:	Topology Information in Router PE1	39
Figure 5.3b	:	Topology Information in Router PE2	40
Figure 5.3c	:	Topology Information in Router PE3	40
Figure 5.3d	:	Topology Information in Router C1	40

Figure 5.3e	:	Topology Information in Router C2	40
Figure 5.3f	:	Topology Information in Router C3	41
Figure 5.4	:	IP routing table showing customer subnets and next hop addresses	41
Figure 5.5a	:	Trace through PE1 to PE3 takes the shortest path always for 192.168.3.52 and 192.168.7.1 destination network.	42
Figure 5.5b	:	Trace through PE1 to PE3 for 192.168.7.1 takes the alternative path	42
Figure 5.6	:	Total bandwidth reservation by both tunnels at fast Ethernet 0/0 is 80Kbps at PE1	42
Figure 5.7a		T0 reserved with 48Kbbps and priority 7	43
Figure 5.7b		T1 reserved with 32Kbps and priority 2 and explicit route shows the longest path hops via C2 C1 C3	44
Figure 5.8a		Bandwidth allocation in PE1 at Fast Ethernet 0/0 interface of router PE1. BW (2) and BW (7) are the priorities of the tunnels	45
Figure 5.8b		Bandwidth allocation by both tunnels T0 and T1 at Fast Ethernet 0/0 interface of router PE1	45
Figure 5.9		IP routing table after tunnels are been setup and PE3 (10.12.0.8) has two paths Tunnel T0 and T1	46
Figure 5.10a		"Iperf" tool is sending 12Kbps UDP traffic to destination 182.168.7.1	46
Figure 5.10b		"Iperf" tool is sending 30Kbps UDP traffic to destination 192.168.3.52 for 120 seconds	46
Figure 5.11a		Tunnel 0 interface bandwidth 29Kbps.	47
Figure 5.11b		Tunnel 1 interface bandwidth 11Kbps.	48
Figure 5.12		Triggered flooding at C2 during T1 shutdown at PE1. The highlighted portion shows T1 bandwidth 32Kbps been released during tunnel shutdown and this information is flooded to all TE enabled three links at router C2.	49
Figure 5.14		Packet drops at C2 serial interface 0/0/0, Queue type is FIFO	52
Figure 5.15		Packet drops are avoided at C2 serial interface 0/0/0 after QoS at PE1 router	53
Figure 5.16		UDP packet generation using "iperf" tool	53
Figure 5.17		marked packets are queued into their appropriate queues and excess	54

low priority are dropped at class-default

Figure 5.18 Class based queue at PE1 output interface 54

Figure 5.19 Packets are matched at the input interface PE1 and marked accordingly to DSCP markings 55

Figure 5.20a Round trip time (RTT) response using "icmpecho" protocol. 50

Figure 5.20b Availability of link from source to destination. Average availability 51

Figure 5.20c HTTP transaction time to a web-server 52

Figure 5.20d Source to Destination positive source to destination Jitter. 53

LIST OF TABLES

Table 4.2	:	DSCP and IP Precedence mappings	28
Table 4.3		DSCP AF and EF values	29
Table 4.4		General drop order based on classes	30
Table 5.13		Classifying of packets based on DSCP marking	52

ACRONYMS

MPLS	:	Multiprotocol Label Switching
GMPLS	:	Generalized MPLS
TE	:	Traffic Engineering
ICT	:	Information and Communication Technology
NGN	:	Next Generation Network
SLA	:	Service Level Agreement
ISP	:	Internet Service Provider
IP	:	Internet Protocol
UDP	:	User Datagram Protocol
TCP	:	Transmission Control Protocol
PDU	:	Protocol Data Unit
LIB	:	Label information base
LSP	:	Label Switched Path
LSR	:	Label Switch Router
LER	:	Label Edge Router
LSP	:	Label Switched Path
LDP	:	Label Distribution Protocol
CR-LDP	:	Constraint-based LDP
FEC	:	Forward Equivalent Class
PoP	:	Point of Presence
CoS	:	Class of Service
QoS	:	Quality of Service
PIM	:	Protocol Independent Multicast
DSCP	:	Differentiated Services Code Point
OSPF	:	Open Shortest Path First
ISIS	:	Intermediate System-to-Intermediate System
BGP	:	Border Gateway protocol
RIP	:	Routing Information Protocol
IGP	:	Interior Gateway Protocol
LSA	:	Link State Advertisement
TOS	:	Type of Service
PHB	:	Per Hop Behavior
ECN	:	Explicit Congestion Notification
CSCP	:	Class Sector Code Points
AF	:	Assured Forwarding
EF	:	Expedited Forwarding
WRED	:	Weighted Random Early Detection
WRR	:	Weighted Round Robin
CBR	:	Constraint Based Routing

CSPF	:	Constrained Shortest Path Calculation
ATM	:	Asynchronous Transfer Mode
VPN	:	Virtual Private Network
VLSI	:	Very Large Scale Integration
ASIC	:	Application Specific Integrated Circuits
PE	:	Provider Edge
C	:	Core
RSVP	:	Resource Reservation Protocol
CIR	:	Committed Information Rate
OPEX	:	Operational Expenditure
CAPEX	:	Capital Expenditure
CSR	:	Cell Switch Router
SONET	:	Synchronous Optical Network
SDH	:	Synchronous Digital Hierarchy
DWDM	:	Dense Wavelength Division Multiplexing
LAN	:	Local Area Network
WAN	:	Wide Area Network
TTL	:	Time to Live
CPE	:	Customer Premises Equipment
ERP	:	Enterprise Resource Management
CRM	:	Customer Relationship Management
MRP	:	Material Requirements Planning
SNMP	:	Simple Network Management Protocol
MIB	:	Management Information Base
OID	:	Object Identifiers
VoIP	:	Voice over IP
MTTR	:	Mean-Time-To-Repair
FIFO	:	First In First Out

ACKNOWLEDGEMENTS

I would like to make this a great opportunity to thank everyone who helped me in numerous ways to complete this research project successfully.

First of all, I wish to express my sincere gratitude to my supervisor Eng. A.T.L.K. Samarasinghe Head of the Department, of the Electronic and Telecommunication Engineering, University of Moratuwa, Sri Lanka for his kind, untiring supervision and guidance during the project work. Secondly, I would like to thank Dr. Priyantha Thilakumara and Dr.Ajith Pasqual, course coordinators of M. Sc. in Telecommunications 2005/2006, for the guidance given during the course and Dr. Sankassa Senevirathna for his encouragement.

Also I would like to thank Eng. Subhash Edirisinghe, Eng, Sudeera Mudugamuwa, Eng. Himidiri Wedande and Eng. Nethadum Harshana of Millennium Information Technologies (MIT) for providing me with the lab environment and equipments.

Finally also thankful to all of my friends, for their support and encouragement extended towards the successful completion of this research project and to my family and my wife for their constant love and unending support.

Chapter 1

Introduction

1.1 Background and Motivation of the Thesis

Today's market trend severely push Telecom Operators to undergo a transformation of their existing network infrastructure to an "all-Internet Protocol (IP)" transport service environment to meet the demand for Next Generation Networking (NGN) for the next 5 to 10 years. The general idea behind NGN is that one network transports all information such as services like voice, data, and all sorts of media such as video by encapsulating these into packets. NGN is a packet based network which able to provide services including telecommunication services and able to make use of multiple Quality of Service (QoS) enabled broadband transport technologies and in which service-related functions are independent from underlying transport-related technologies. NGN is based on Internet technologies including IP and Multiprotocol Label Switching (MPLS).

"All-IP" network transition and evolution to new services and its widespread use of IP pose new challenges for network operations like network dimensioning, planning, and engineering. Operators have to rapidly deploy new services on a converged network, making ensure for the QoS for given Service Level Agreement (SLA). These data-oriented new services generate a wide variety of traffic profiles, characterized by dynamics on a broad time-scale. These different classes of traffic have to be classified based on available QoS architectures to ensure service delivery at the same time maximizing network resources. One of the promising ways to achieve this is to use MPLS-TE with differentiated services (DiffServ) [1] and these services can be specified with multiple parameters based on per hop behavior (PHB) specified at each router. The main reason to provide differentiated services is to safe guard higher premium or platinum service customer traffic even under network congestion. Two major categories proposed by IETF for DiffServ [19] are assured forwarding (AF) and expedited forwarding (EF).

The standardization of DiffServ over MPLS-TE has been carried out by IETF [1-5] and several similar researches have been done in this area. Some of these are described below.

1. MPLS and TE in IP Networks – Rapid growth and increasing requirement for service equality, reliability and efficiency have made traffic engineering as essential consideration in the design and operation of a large Internet backbone networks. Internet TE addresses the issue of performance optimization of operational networks and discusses the applications of MPLS to TE in IP networks [6].

2. Internet QoS: A big picture – Presents a framework for the emerging QoS. The important components of the framework are RSVP, differentiated services, MPLS and constrained routing. Described how differentiated services are implemented and two architectures are presented for end to end service deliveries [7].

In this work we propose a flexible customizable IP SLA program to provide SLA performance reports to customers and an implementation of MPLS-TE tunnels for effective backbone links utilization is simulated in a lab environment. To ensure QoS packets were classified according to differentiated service code point values and mapped to a proper traffic engineered tunnel so that important traffic reaches the destination during congestion. MPLS-TE is a growing implementation in today's service provider networks. MPLS adoption in service provider networks has increased heavily due to its inherent TE capabilities. Very high data transfer rates have been achieved in the backbone and the significance of all MPLS switched networks are increasing. Therefore for the long run this technology and its capabilities are an attractive alternative to growing operators.

1.2 Goal of the Thesis

This thesis is a demonstration of how to effectively use under-utilized core network backbone links and controlling that bandwidth for different service types while ensuring a guaranteed SLA to the end customers. An open source based network simulator is used for initial study purpose and to build a network topology with MPLS-TE tunnels and actual results are derived from a real lab network environment. TE shows ways of utilizing the

backbone constantly rather than routing protocols to decide upon desired paths always, and also a software program being developed using JAVA to provide SLA performance reports to end users. Together with MPLS-TE coupled with Differentiated services QoS architecture for packet treatment service provider can ensure the required SLAs to their customers and provide customizable SLA reports on those services economically using the IP SLA program.

1.3 Structure of the Thesis

The second chapter of this thesis starts with a review of historical development of MPLS communication systems, describes the generations and advantages of using MPLS network. Section 2.4 introduces architecture of MPLS protocol stack and in section 2.5 MPLS network over view is explained. Sections 2.6 and 2.7 describe the traditional routing and packet switching and MPLS operation. The Chapter 3 introduces MPLS-TE and techniques and operation.

Chapter 4 describes the MPLS and QoS when using differentiated services for packet treatment, and use of IP Service Level Agreements (SLAs) to ensure quality of service to end users. Chapter 5 discusses setting up a MPLS network topology and assigning traffic via TE tunnels in a real lab environment. Furthermore it also describes a method to obtain IP SLA performance reports. These reports are obtained from a real operational live network. Chapter 6 gives the, conclusion and discussion of results and future works.

Chapter 2

Multi Protocol Label Switching (MPLS)

2.1 Introduction

The deployment of a flexible, efficient Internet Protocol/Multiprotocol Label Switching (IP/MPLS) packet infrastructure has become the key driver for service providers in building next-generation networks (NGNs). There are compelling financial, technological and competitive advantages in deploying a converged network. Capital expenditures (CAPEX) are focused on efficient and extensible packet infrastructures. Convergence allows service providers flexibility and economies of scale that are not possible with multiple single-purpose networks.

When moving from circuit-switched to packet-switched technology operators have to implement packet-based connectivity for both voice and data services in the IP core network. This means that local area connectivity is needed between core network elements on the sites and wide area connectivity is needed between the core network sites. MPLS is an Internet Engineering Task Force (IETF) specified framework which provides for efficient routing, forwarding and switching of traffic packets through the network. MPLS depends independent to layer 2 and 3 protocols. This technology maps IP addresses to fixed length labels used by different packet-forwarding and packet-switching technologies. MPLS data transmission occurs on label switch paths (LSPs). LSPs are sequence of labels at each and every node along the path from source to destination and are established prior to data transmission or upon detection of certain flow of traffic.

For cost efficiency and in order to ensure compatibility with the emerging new services IP/MPLS and Ethernet Local Area Network (LAN) are the baseline technologies for the IP NGN network connectivity. In addition to being future proof these technologies offer the best price performance ratio and best service availability on the market. Additionally the IP/MPLS backbone can be used for consolidating dedicated networks such as charging network management and Intranet traffic to one unified infrastructure.

2.2 Brief History of MPLS Communications

MPLS enables enterprises and service providers to build next-generation intelligent networks that can deliver a wide variety of advanced, value-added services over a single infrastructure.

MPLS was originally presented as a way of improving the forwarding speed of routers but is now emerging as a significant standard technology that offers new capabilities for large scale IP enterprise networks. Traffic engineering, the ability of network operators to specify the path that traffic takes through their network, and Virtual Private Network (VPN) support are examples of two key applications where MPLS is superior to any currently available IP technology.

MPLS was originally proposed by a group of engineers from Ipsilon Networks but their "IP Switching" technology, which was defined only to work over asynchronous transfer mode (ATM), did not achieve market dominance. Cisco Systems, Inc. introduced a related proposal, not restricted to ATM transmission, called "Tag Switching". It was a Cisco proprietary proposal, and was renamed "Label Switching". It was handed over to the IETF for open standardization. The IETF work involved proposals from other vendors, and development of a consensus protocol that combined features from several vendors' work. The label switching timelines are shown in figure 2.1 and RFC specifications in figure 2.2.

One original motivation was to allow the creation of simple high-speed switches; however for a significant length of time it was not possible to switch IP packets entirely in hardware. However, advances in very large scale integration (VLSI) have made such devices possible. Therefore the advantages of MPLS primarily revolve around the ability to support multiple service models and perform traffic management.

MPLS has become a leading vehicle for connecting an organization's decentralized locations. It offers advantages to both service providers and enterprises. For the service provider, MPLS reduces cost, simplifies provisioning, provides wider service coverage, and enables differentiated services. In addition to the promise of multiple levels of QoS,

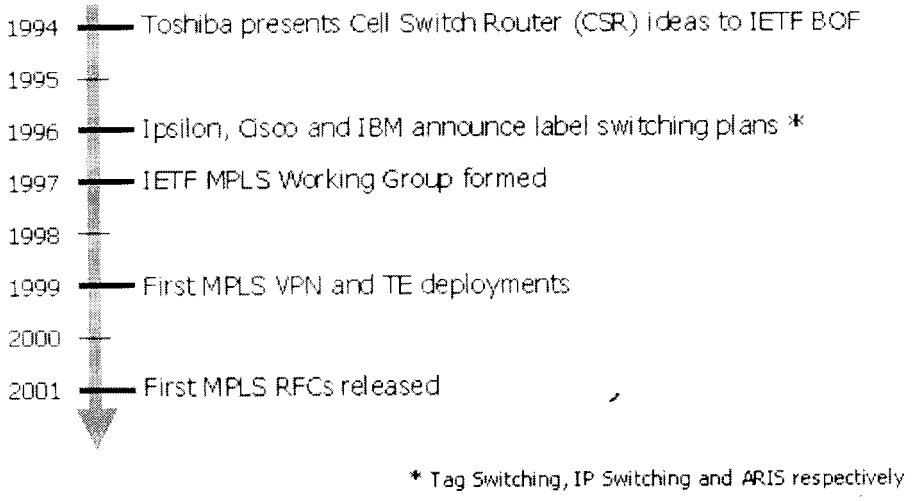


Figure 2.1: Label Switching Timeline [8]

MPLS offers the enterprise a meshed architecture, scalability, and network convergence, eliminating the need for multiple networks.

If we consider a normally routed environment, frames pass from a source to a destination in a hop-by-hop basis. Transit routers evaluate each frame's layer 3 headers and perform a route table lookup to determine the next hop toward the destination. This tends to reduce throughput in a network because of the intensive processor requirements to process each frame. Although some routers implement hardware and software switching techniques to accelerate the evaluation process by creating high-speed cache entries, these methods rely upon the layer 3 routing protocol to determine the path to the destination.

Unfortunately, routing protocols have little visibility into the layer 2 characteristics of the network, particularly in regard to QoS and loading. Rapid changes in the type and quantity of traffic handled by the Internet and the explosion in the number of Internet users are putting an unprecedented strain on the Internet's infrastructure. This pressure mandates new traffic-management solutions. MPLS and its predecessor, tag switching, are aimed at resolving many of the challenges facing an evolving Internet and high-speed data communications demands in general. [20]

Standard	Description
RFC 3031	MPLS Architecture
RFC 3032	MPLS Label Stack Encoding
RFC 3035	MPLS using LDP and ATM VC Switching
RFC 3036	LDP Specification

Figure 2.2: IETF Standards

To meet these new demands, MPLS changes the hop-by-hop paradigm by enabling devices to specify paths in the network based upon QoS and bandwidth needs of the applications. In other words, path selection can now take into account layer 2 attributes. Before MPLS, vendors implemented proprietary methods for switching frames with values other than the layer 3 headers.

As a brief reminder of how MPLS operates, recall that in the typical network without MPLS, packet paths are determined in real time as routers decide each packet's appropriate next hop. Conventional IP routing requires time and eliminates opportunity to influence packet's paths. With MPLS, explicit and pre-defined network paths transport specific types of traffic. MPLS solved the problem that router manufacturers faced when incorporating QoS into very large IP-VPN networks ensuring that each and every router can identify and process each and every traffic flow appropriately otherwise requires so much processing power as to be ineffective and non-scaleable.

A better approach, and the one that MPLS adopts, is to label traffic flows at the edge of the network and let core routers identify the required class of service with a simple and quick label check. MPLS reduces the burden of differentiating types of traffic and assigning appropriate class-of-service labels by focusing the task on the edge of the MPLS network on a router, called the Label Edge Router (LER) and optimally, the MPLS labels indicates the best and fastest service classes go into the most urgent applications packets queues. Figure 2.3 shows a typical MPLS network.

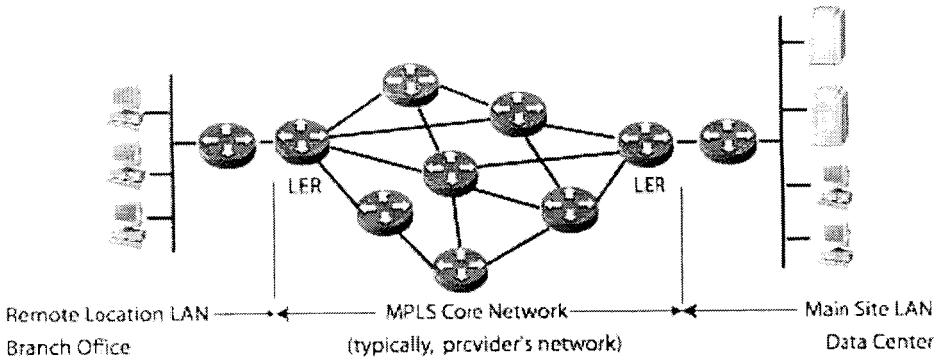


Figure 2.3: Typical MPLS block diagram [9]

Traditional IP networks are connectionless; when a packet is received, the router determines the next hop using the destination IP address on the packet alongside information from its own forwarding table. The router's forwarding tables contain information on the network topology. They use an IP routing protocol, such as open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), Border Gateway Protocol (BGP), Routing Information Protocol (RIP) or static configuration, to keep their information synchronized with changes in the network.

MPLS also uses IP addresses, either version 4 or 6, to identify end points and intermediate switches and routers. This makes MPLS networks IP-compatible and easily integrated with traditional IP networks. However, unlike traditional IP, MPLS flows are connection-oriented and packets are routed along pre-configured Label Switched Paths (LSPs).

Moreover services such as broadband available to a mass market open up a wide variety of interactive communications for both consumers and businesses, bringing to reality interactive video networks, interactive banking and shopping from the home, and interactive distance learning. Therefore despite some initial challenges MPLS will play an important role in the routing, switching, and forwarding packets through the next generation networks in order to meet the service demand of the network end users.

2.3 Benefits of using MPLS Communication

Communication systems using MPLS have a number of extremely attractive features. It addresses today's network backbone requirements effectively by providing a standard based solution. Therefore it is useful to consider the merits and special features offered by IP/MPLS infrastructure over conventional layer 3 IP routing. Some of the advantages are described below.

1. Profitability increases as capital and operational expenditures decrease with a converged network and services revenues increase. MPLS-TE also provides higher return on network backbone infrastructure investment because the best route between a pair of point of presence (PoPs) is determined taking into account the constraints of the backbone network and the total traffic load on the backbone.

2. Improves packet performance in the network by simplifying forwarding through layer 2 switching and routing via switching at wired line speeds. Since MPLS is simple it caters for easy deployment.

3. QoS and class of service (COS) are easily supported for differentiating services by using traffic engineering path setups and helps to ensure service guarantees. MPLS also provisions for constrained-based and explicit path setup.

4. MPLS integrates IP and ATM by bridging between access IP and core ATM while reusing existing router or ATM hardware effectively.

5. MPLS builds interoperable networks due its standard based solution that achieves synergy between IP and ATM networks and also facilitates IP over Synchronous Optical Network (SONET) integration in optical switching. MPLS supports to build scalable VPNs with TE capability.

Along with the above features the concept of a label has been extended in Generalized MPLS (GMPLS) where the label no longer needs to be carried as an identifier on the data

flow, but may be implicit. For example, time-slots in Synchronous Optical Network / Synchronous Digital Hierarchy (SONET/SDH) and wavelengths in Dense Wavelength Division Multiplexing (DWDM) can be labels. In these cases, the label switching operations translate to operations such as "switching incoming wavelength onto this outgoing wavelength". GMPLS is therefore ideal for optical networking, and many extensions to the protocols have been defined, including user-to-network interfaces and network-to-network interfaces.

Therefore in overall, network complexity is reduced as overlay network infrastructures are reduced and eliminated thus lowering operational expenditures and costs are also reduced because a number of important processes are automated, including set up, configuration, mapping, and selection of MPLS-TE tunnels. Service revenues increase as it becomes easier to offer innovative new services, with faster time to market, to all customers.

2.4 Architecture of MPLS Protocol Stack

Figure 2.4 shows MPLS protocol stack. The two main sections are control plane and data plane. First one could be an embedded processor for fast efficient operation and data plane could be implemented in programmable logic. The "IP Fwd" is the usual forwarding module at layer 3 to do routing based on next hop information in fact MPLS "Fwd" forwarding module matches a label to an outgoing port for a given packet.

From the diagram LDP module uses TCP for reliable transmission of control data from one LSR to another during a session. Label distribution protocol (LDP) is a new protocol that defines a set of procedures and messages by which one LSR informs another of the label bindings it has made. The LDP maintains the Label information base (LIB) and uses user datagram protocol (UDP) during discovery phase. During this phase LSR tries to identify neighboring elements and signals itself to inform about its presence in the network using hello messages.

LDP protocol structure is illustrated in figure 2.4 and protocol stack fields are described below. More on LDP messages are explained in section 2.7.4 and LDP header is shown in figure 2.5 with header fields described below.

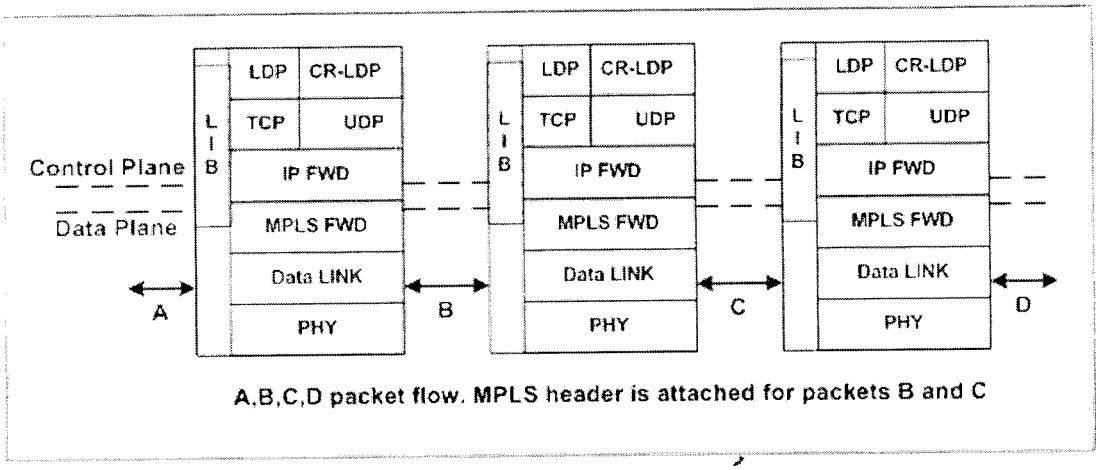


Figure 2.4: Typical MPLS Protocol Stack [10]

a. Version - The protocol version number. The present number is 1.

b. PDU Length - The total length of the Protocol Data Unit (PDU) excluding the version and the PDU length field.

c. LDP identifier - This field uniquely identifies the label space of the sending LSR for which this PDU applies. The first 4 bytes encode the IP address assigned to the LSR. The last 2 indicate a label space within the LSR.

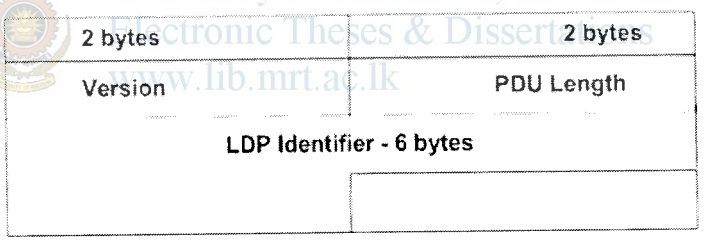


Figure 2.5: LDP Header [18]

a. LDP = Label distribution protocol

b. LIB = Label information base; table of labels mapping input port/label to output port/label

c. CR-LDP = Constraint-based (CR) LDP, used for traffic engineering; resource reservation protocol traffic engineering (RSVP-TE) is another signaling mechanism used for traffic engineering

d. Internet protocol (IP) FWD = Next hop forwarding based on IP address; longest match forwarding used

e. TCP = Transmission control protocol

f. MPLS FWD = Label switching based on MPLS label and LIB lookup

g. UDP = User datagram protocol

2.5 MPLS Network Overview

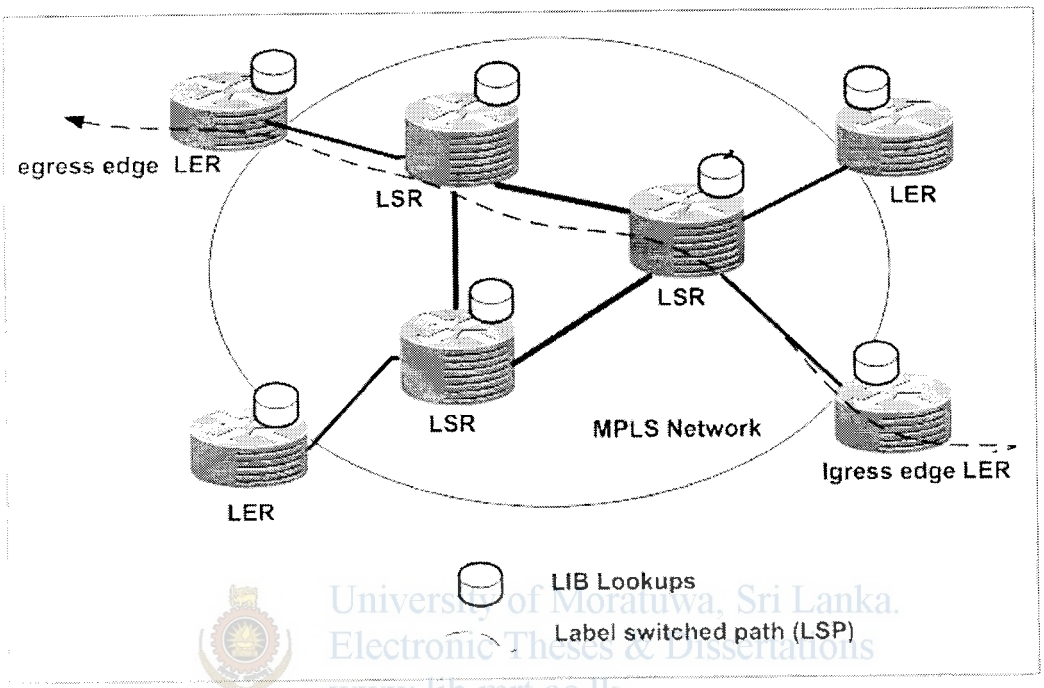


Figure 2.6: MPLS Network Overview

Routers at the edge of the network are known as Label Edge Routers (LERs) and routers at the MPLS core is known as Label Switch Routers (LSRs). An edge router converts IP packets to MPLS labels and vise versa. An ingress LER is the one by which a packet enters the MPLS network, an egress LER is one by which a packet leaves the MPLS network as shown in figure 2.6. Labels are small identifiers placed in the traffic. They are inserted by the ingress LER, and subsequently removed by the egress LER, so nothing will remain to perplex the non-MPLS devices outside the MPLS network.

As traffic transits the MPLS network, label tables are consulted in each MPLS device. These are known as the Label Information Base (LIB). By looking up the inbound interface and label in the LIB, the outbound interface and label are determined. The LSR can then substitute the outbound label for the incoming, and forward the frame.

2.6 Traditional Routing and Packet Switching

As the demand for higher data rates emerged devices with capabilities to switch at the data-link and network layers in hardware are needed. Layer 2 switching devices addresses the bottlenecks within the subnets of LAN and layer 3 switching devices reduced the bottleneck in layer-3 routing by moving route lookup forwarding to high speed switching hardware. Initial solutions address the need for wire speed transfer of packets but they did not consider the service requirements of the information contained in the packets. Most of the routing protocols are based on shortest path and does not take other factors such as jitter, delay and congestion which could further degrade the network performance.

2.7 MPLS Operation

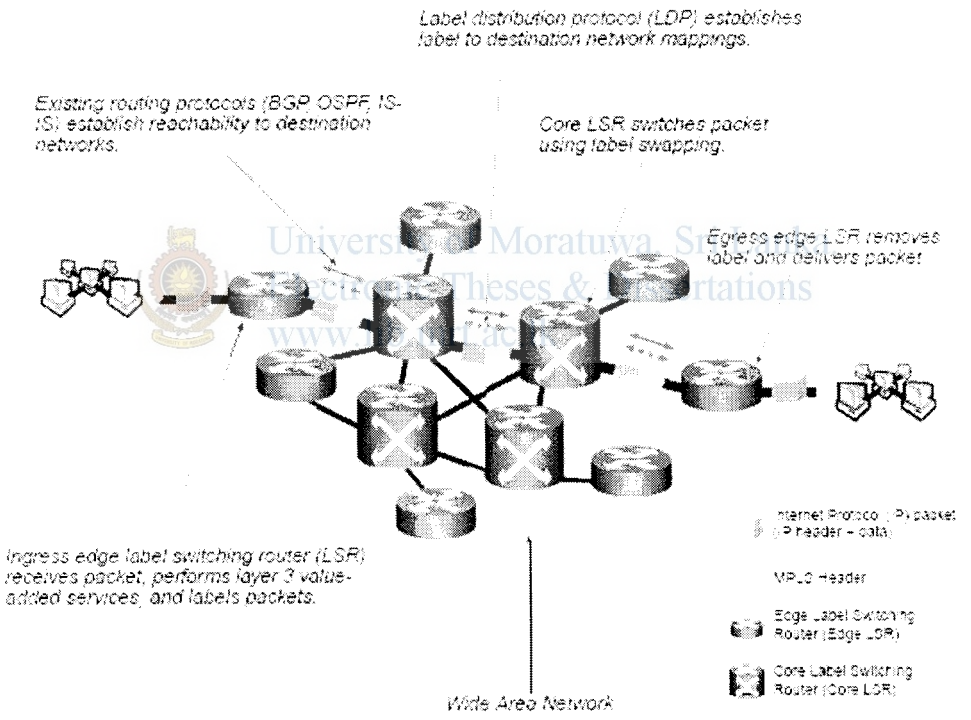


Figure 2.7: MPLS Operation [3]

Figure 2.7 illustrates the flow of a packet through an MPLS-enabled network. The source network is on the left and the destination network on the right. The large cloud in the center is the MPLS WAN cloud. Some times LERs are also called ingress/egress LSR

From the above diagram existing routing protocols OSPF, IS-IS establishes the reachability of the destination networks and LDP establishes label-to-destination network mappings. Ingress edge LSR receives a packet, performs layer-3 value-added services, and labels the packets. LSR switches the packet using label swapping and Egress edge LSR removes the label and delivers the packet to final destination. Figure 2.8 illustrates more detailed view of the MPLS operation.

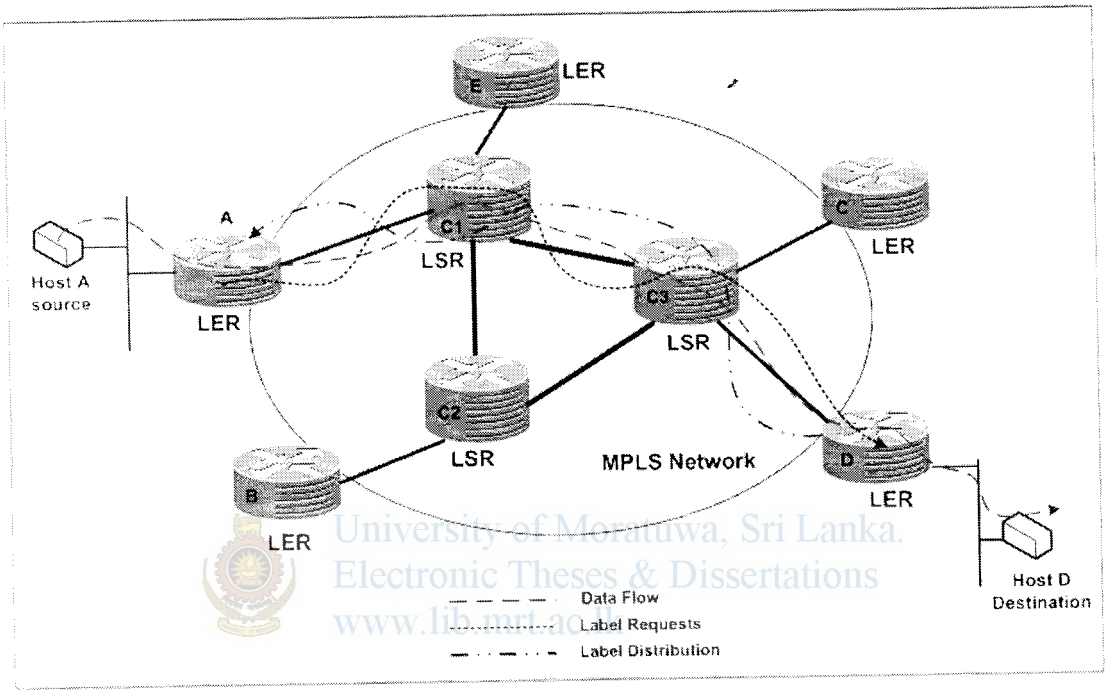


Figure 2.8: Packet Flow in MPLS

From the figure 2.8 the following steps must be taken for a data packet to travel through an MPLS cloud.

1. Label creation and distribution - Before any traffic begins the routers make the decision to bind a label to a specific Forward Equivalent Class (FEC) and build their tables. In LDP, downstream routers initiate the distribution of labels and the label/FEC binding.

2. Table creation at each router - On receipt of label bindings each LSR creates entries in the LIB. The contents of the table will specify the mapping between a

label and an FEC. The entries are updated whenever renegotiation of the label bindings occurs.

3. Label-switched path creation - The LSPs are created in the reverse direction to the creation of entries in the LIBs.

4. Label insertion/table lookup - The first router LER-A uses the LIB table to find the next hop and request a label for the specific FEC. Subsequent routers just use the label to find the next hop. Once the packet reaches the egress LER-D, the label is removed and the packet is supplied to the destination.

5. Packet forwarding – LER-A may not have any labels for this packet as it is the first occurrence of this request. In an IP network, it will find the longest address match to find the next hop. For example let LSR-C1 be the next hop for LER-A.
    a. LER-A will initiate a label request toward LSR-C1.This request will propagate through the network as indicated as "label requests" in diagram.
    b. Each intermediary router will receive a label from its downstream router starting from LER-E and going upstream till LER-A. The LSP setup is indicated as "label distribution" in the diagram using LDP or any other signaling protocol. If traffic engineering is required, constrained based (CR) LDP will be used in determining the actual path setup to ensure the QoS/CoS) requirements.
    c. LER-A will insert the label and forward the packet to LSR-C1
    d. Each subsequent LSR, i.e., LSR-C2 and LSR-C3 will examine the label in the received packet, replace it with the outgoing label and forward it.
    e. When the packet reaches LER-D, it will remove the label because the packet is departing from an MPLS domain and deliver it to the destination.
    f. The actual data path followed by the packet is indicated as "data flow" in the diagram.

2.7.1 Label Switch Routers (LSRs) or Label Edge Routers (LERs)

The devices those take participate in an MPLS operation from the above Figure 2.8 are Label Edge Routers (LER) and Label Switch Routers (LSR). A core router (C1, C2 or C3) is a high speed router having hardware Application Specific Integrated Circuits (ASICs) for which participates in the establishment of LSPs using appropriate Label signaling protocol for switching data traffic based on established paths.

An LER is a device that operates at the perimeter of the access and the MPLS networks supporting multiple ports connecting to dissimilar networks such as Ethernet, ATM, PPP, Frame relay and forwards those traffic on to MPLS after establishing the LSPs, using LDP at the ingress. This traffic then distributed to the egress and back to the access. A LERs main job is removal and assignment of labels for input and output traffic.

2.7.2 Forward Equivalent Class (FEC)

A group of IP packets which are forwarded in the same manner, for example over the same path, with the same forwarding treatment and all packets in such group are given same treatment routing to the destination. MPLS assigns a particular packet to a particular FEC once only as packet enters the network. FEC's are based on service requirements for a given set of packets. Each LSR builds a table to specify how the packet is forwarded which is known as Label Information Base (LIB) having FEC to label bindings.

2.7.3 Labels and Label Bindings

A label is the simplest form of path in which a packet traverses. A label is carried or encapsulated in a layer 2 header along with the packet. The receiving router examines the packet for its label details to determine the next hop. Once packet has been labeled the entire path it would take is based on label switching. These label values are local significance only which means they belong to hops between the LSRs only.

Once a packet has been classified as a new or existing FEC, a label is assigned to the packet and these label values are obtained from the underlying data link layer. The packets are then forwarded based on the label value. Labels are bound to FEC as a result of some

event or policy that indicates a need for such bindings. These events can be either data or event driven.

Label assignment could be based on several criteria such as destination unicast routing, traffic engineering, multicast, virtual private network or Quality of Service.

Generic MPLS header format is illustrated in figure 2.9. These labels can be inserted as a shim header between layer 2 and layer 3 headers or as a header of data link layer in case of ATM or Frame relay. A shim header is a special header placed between layer 2 and layer 3 of the OSI model. The shim header contains the label used to forward the MPLS packets. The Shim Header consists of 32 bits in four parts – twenty bits are used for the label, three bits for experimental functions, one bit for stack function, and eight bits for time to live (TTL).

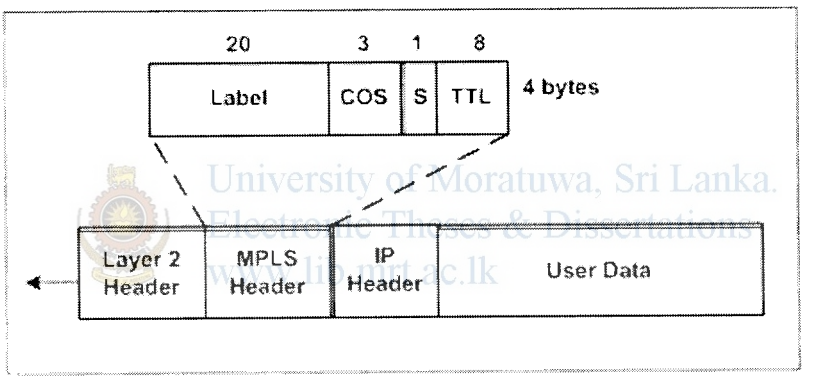


Figure 2.9: MPLS Header [11]

The 32 bit MPLS header contains the following fields,

a. Label - 20bits and carries the actual value of MPLS label
b. CoS – 3 bits and can affect the queuing and discard algorithms applied to packets when transmitted through the network
c. S – Stack 1 bit which supports hierarchical label stack
d. TTL – 8 bits, provides normal IP TTL functionality

2.7.4 Label Creation and Distribution

Labels can be created using several methods. Topology based method uses normal processing of routing protocols of OSPF and BGP. Request uses processing of request based control traffic such as RSVP. Traffic based method uses reception of packet to trigger assignment and label distribution. The first two are control driven bindings and the final one is data driven bindings.

There is variety of ways to signal label distribution. Existing routing protocol BGP have been enhanced to piggyback the label information within the contents of the protocol. RSVP also has been extended to support piggybacked exchange of labels. The IETF has defined a new protocol known as LDP to explicit signaling and management of label space. Extensions to LDP protocol have also been defined to support explicit based QoS and CoS requirements. These extensions are mentioned in the constraint based routing CR-LDP protocol definition.

Varies schemes are used for label exchange. LDP maps unicast IP destinations to labels. RSVP or CR-LDP is used for TE and resource reservation to effectively utilize the link capacity. Protocol Independent Multicast (PIM) is used for multicast states label mapping and BGP is used for external VPN labels.

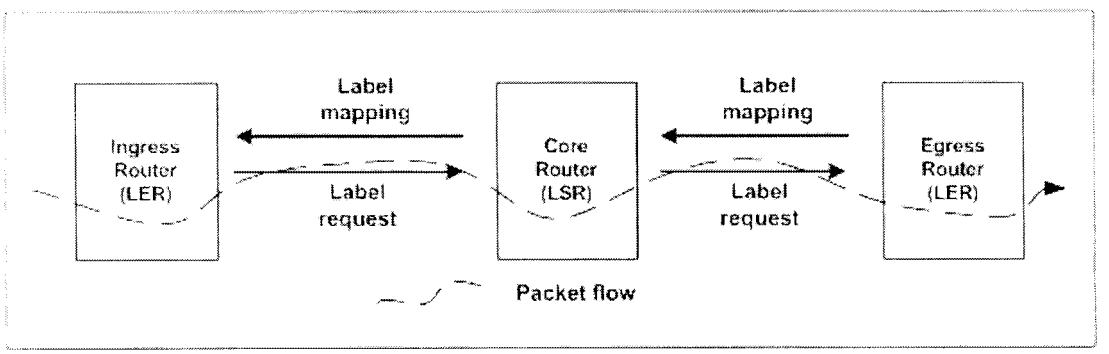


Figure 2.10: Label Request and Label Mapping

Labels are distributed using request and mapping mechanisms. Using label request mechanism, an LSR requests a label from its peer downstream neighbor so that it can bind to a specific FEC. This mechanism is implemented down the line of other LSR's until the egress LER where the packet exist the MPLS cloud. In response to label request downstream LSR will send a label to its initiator using label mapping mechanism. These requests are shown in figure 2.10.

LDP is a new application layer protocol for distributing label binding information to LSRs. It is used to map FEC tables which in turn create LSPs and LDP sessions are established between LDP peers in the MPLS network. Following types of messages are exchanged by peers.

1. **Discovery messages -** announce and maintain the presence of an LSR in a network
2. **Session messages -** establish, maintain, and terminate sessions between LDP peers
3. **Advertisement messages -** create, change, and delete label mappings for FECs
4. **Notification messages -**provide advisory information and signal error information

2.7.5 Label Switched Paths (LSPs)

A path is established before the data transmission starts in an MPLS cloud and this path is a representation of a FEC. MPLS provides two options to set up an LSP path described below. The LSP setup for an FEC is unidirectional. The return traffic must take another LSP path. Two ways of LSP creation by an LSR is described below.

Hop-by-Hop routing - Each LSR independently selects the next hop for a given FEC. LSRs support any available routing protocols (OSPF, ATM, etc). This is very similar that is used in current IP networks.

Explicit routing - Is similar to source routing. The ingress LSR where the data packet to the network first originates specifies the list of nodes through which the packet traverses. Along the path resources may be allocated to guarantee QoS to data traffic which eases TE throughout the network and differentiated services can be provided using flows based on policies.

Labels used by an LSR for FEC label bindings can be per platform or per interface. In first label values are unique across the whole network and labels are allocated form a common pool. Label distributed on different interfaces will not have same value. In per interface, label ranges are associated with interfaces and multiple labels pools are defined for interfaces. The labels provided in those interfaces are allocated from the separate pools and label values on different interfaces could be the same.

Chapter 3

MPLS Traffic Engineering and Techniques

3.1 Overview

TE which was mainly present in Asynchronous Transfer Mode (ATM) or Frame Relay networks is the ability to steer traffic through a network from edge to edge in the most optimal way. In earlier networks, virtual circuits were laid out to carry traffic from one edge point in the network to another and today most networks rely on a pure IP solution. With IP/MPLS-TE capabilities are integrated into layer 3, which optimizes the routing of IP traffic based, on the given constraints imposed by backbone capacity and topology. Traffic flows across a network are based on the resources available in the network. MPLS is an integration of layer 2 and layer 3 technologies and by making traditional layer 2 features available to layer 3 MPLS enables traffic engineering.

WAN links are an expensive resource in a service provider budget. Traffic engineering enables service provider's network traffic to route in such a way that these links are utilized efficiently in terms of throughput. TE modifies routing patterns to provide efficient mapping of traffic flows to network resources and this efficient mapping can reduce the occurrence of congestion and improves service quality in terms of the delay, jitter and loss that packets experience. Also it guarantees service levels to end users and reduces the impact of network failures thus increasing service availability.

MPLS-TE provides explicit routing capabilities to MPLS networks. An originating LSR or head-end edge node can set up a TE LSP to a terminating LSR or tail-end through an explicitly defined path containing a list of intermediate LSR's or midpoints. IP uses destination-based routing and does not provide a general and scalable method for explicitly routing traffic. Alternatively, MPLS networks can support destination-based and explicit routing simultaneously. MPLS-TE uses extensions to RSVP and the MPLS forwarding model to provide explicit routing. These enhancements provide a level of routing control that makes MPLS suitable for TE.

IP routing is based on leased cost routing strategy because IP networks are governed by the need to get traffic across the network to the destination as quickly as possible. Every

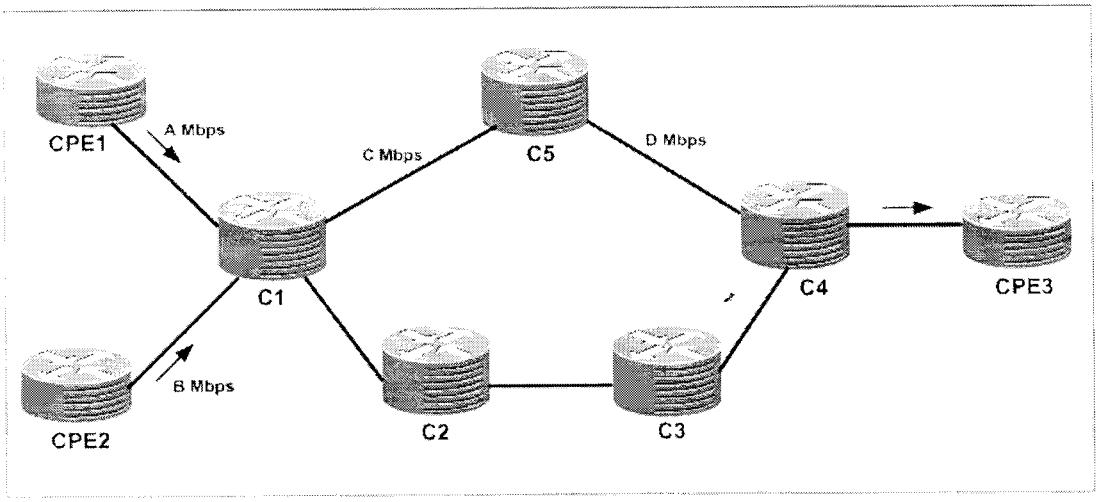


Figure 3.1: IP forwarding network

IP routing protocol has a cost associated with the links in the networks. The accumulation of the cost of every link of a path is used to calculate the smallest cost path to forward traffic through the network. This cost can be a single or composite based on the routing protocol used.

IP forwarding model is based on leased cost path and does not take into account bandwidth available on the link which might be different to the link cost. Therefore a router can keep forwarding IP traffic onto a link, even though that link is already dropping packets due to insufficient bandwidth to forward all the traffic flows for which the routing table sees a shortest path for that destination. This results shortest path links to be over utilized and alternate links to be underutilized. TE could solve this problem by utilizing the alternative paths to divert traffic.

From the figure 3.1 assuming all links have the same cost then preferred path between the customer premises equipments (CPE's) will take the least cost path C1 C5 C4 and the alternative path C1 C2 C3 C4 will be idle. For example in the event of CPE1 and CPE2 simultaneously sending traffic to CPE 3 and if bandwidth A+B Mbps exceeds C or D Mbps some packets would be dropped at C1 or C5. IP routing protocols can be used to

overcome this either by load balancing between both paths or by using routing protocol metrics steering CPE2 traffic along the C1 C2 C3 C4 path, but this would causing complexity in an service provider mesh network environment considering operational point of view. When MPLS-TE is implemented, the IP network shown figure 2.8 transforms into the label switched domain in which the TE label switched paths or TE tunnels Tunnel1 and Tunnel2 defined paths that can be used by traffic between C1 and C4. Here tunnel 1 may represent path C1 C5 C4 and tunnel 2 C1 C2 C3 C4.

The main advantage of implementing MPLS-TE is that it provides a combination of ATM's TE capabilities along with the class of service (CoS) differentiation of IP. Therefore, to avoid packet drops due to inefficient use of available bandwidth and to provide better performance, TE enables to steer some of the traffic destined to follow the optimal path to an alternate path to enable better bandwidth management and utilization between a pair of routers. MPLS-TE also provides a resilient design in which a secondary path can be used when the primary path fails between two routers in a network.

3.2 How MPLS-TE Operates

MPLS-TE operates using logically defined tunnels which are unidirectional per direction and each data flow between a specific source and destination will have properties or attributes associated with them. The attributes associated with a tunnel, in addition to the ingress (head end) and egress (tail end) points of the network, can include the bandwidth requirements and the CoS for data that will be forwarded utilizing this tunnel. Traffic is forwarded along the path defined as the TE tunnel assigned to a specific LSP from source to destination, which are usually edge routers. Unless configured explicitly, TE tunnels can reroute packets via any path through the network associated with an MPLS LSP. This path might be defined by the IGP used in the core network.

An IGP protocol such as OSPF or IS-IS with extensions for TE is used to carry information pertaining to the tunnel configured on a router and these extensions carry information on available resources for building a tunnel, like bandwidth on a link. As a result, if a link that does not have the requested resources (example bandwidth) it is not

chosen to be a part of the LSP tunnel or TE tunnel. Signaling in an MPLS-TE environment uses RSVP with extensions to support TE tunnel features.

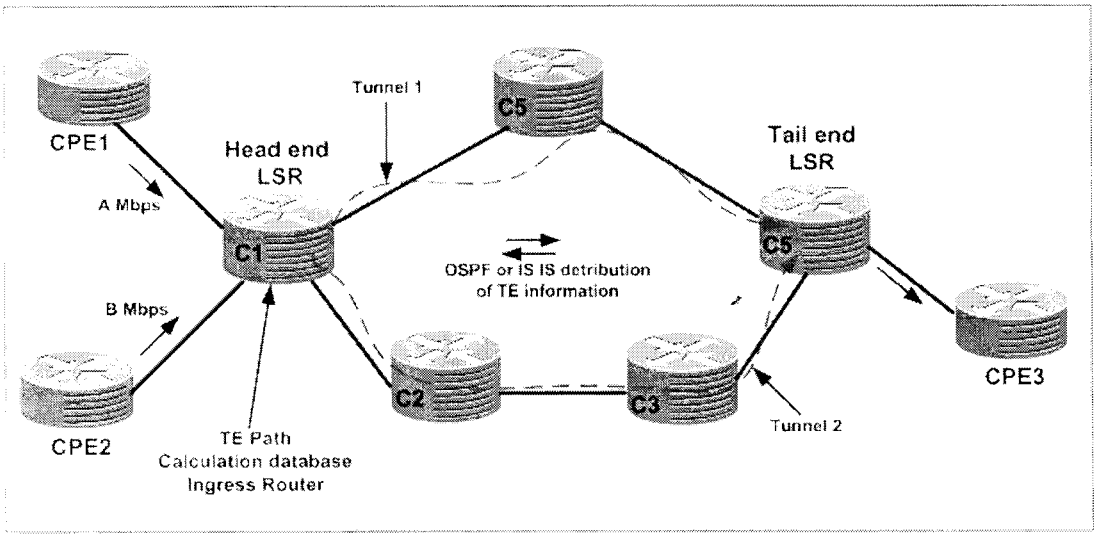


Figure 3.2: MPLS-TE Tunnels

Figure 3.2 illustrates the same example shown in figure 3.1; additionally showing the TE tunnels (Tunnel and Tunnel 2) which have been used to occupy the C1 C2 C3 C4 underutilized link. Ingress (head end) router C1 gathers information on all the available resources in the network along with the topology, which defines tunnels through the network between a set of MPLS-enabled routers using the flooded information in IGP updates. In IS-IS a new (TLV) (type 22) has been developed to transmit information pertaining to resource availability and link status (LS) in the LS-PDUs. In OSPF, the type 10 link state advertisements (LSA) provide resource and links status information.

Constraint Based Routing (CBR), which is the key mechanism in MPLS-TE which takes into account the possibility of multiple paths between a specific source and destination pair in a network. With CBR, the operation of an IP network is enhanced so the least cost routing can be implemented as well as variables to find paths from a source to destination. Resource availability and link status information are calculated using a Constrained Shortest Path Calculation (CSPF) calculation in which factors such as the bandwidth, policies, and topology are taken into consideration to define probable paths from a source to destination.

3.2.1 MPLS-TE Signaling Protocols

There are two signaling protocols for MPLS-TE. RSVP extension for TE (RSVP-TE) and constrained based LDP (CR-LDP). IETF consensus was reached to carry on with developing RSVP as the signaling protocol for MPLS-TE and to stop further development on CR-LDP. This was documented in RFC 3468.

RSVP reserves bandwidth along a path from a specific source to destination. RSVP messages are sent by the head-end router in a network to identify resource availability along the path from a specific source to destination. The head-end router is always the source of the MPLS-TE tunnel, and the tail-end router is the router that functions as the endpoint for the TE tunnel.

3.2.2 Resource Reservation protocol (RSVP) Extensions

RSVP-TE is used to establish MPLS LSPs when there are traffic engineering requirements. It is mainly used to provide QoS and load balancing across the core network. MPLS traffic engineering automatically establishes and maintains the tunnel across the backbone, using RSVP. The path used by a given tunnel at any point in time is determined based on the tunnel resource requirements and network resources, such as bandwidth. The four main messages used in implementation of RSVP for TE are described below.

1. **RSVP PATH message**— Generated by the head-end router and is forwarded through the network along the path of a future TE LSP. At each hop, the PATH message checks the availability of requested resources and stores this information thus RSVP PATH message functions as a label request in MPLS-TE domain.

2. **RSVP RESERVATION message**— Created by the tail-end router in the MPLS-TE domain and used to confirm the reservation request that was sent earlier with the PATH messages.

3. **RSVP error messages**— In the event of unavailability of the requested resources, the router generates RSVP error messages and sends them to the router from which the request or reply was received.

4. **RSVP tear messages**— RSVP creates two types of tear messages, namely, the PATH tear message and the RESERVATION tear message. These tear messages clear the PATH or RESERVATION states on the router instantaneously. The process of clearing a PATH or RESERVATION state on a router using tear messages enables the reuse of resources on the router for other requests.

RFC 3209 defines these RSVP TE extensions [12]. RSVP "Path" messages flow downstream with a collection of four objects which relates to EXPLICIT_ROUTE, LABEL_REQUEST, SESSION_ATTRIBUTE, and RECORD_ROUTE. The EXPLICIT_ROUTE object contains a hop list that defines the explicit routed path that the signaling will follow. The RECORD_ROUTE object collects hop and label information along the signaling path. The SESSION_ATTRIBUTE object lists the attribute requirements of the LSP (priority, protection etc.). RSVP "Resv" messages flow upstream and include two objects related to MPLS-TE (LABEL and RECORD_ROUTE).

3.2.3 Traffic Selection

Selection of traffic to the TE LSP can be done using different approaches which can be static or dynamic. For example, it can also depend on packet type such as IP or contents such as CoS. An MPLS network can make use of several traffic-selection mechanisms depending on the services it offers. Traffic can enter the TE LSP only at the head-end and therefore, the selection of the traffic is a local head-end decision. Thus MPLS-TE provides flexibility by separating TE LSP creation from the process of selecting the traffic that will use the TE LSP.

Chapter 4

MPLS and Quality of Service

4.1 Overview

QoS is a general term that, in the IP VPN environment, refers to the ability to set control mechanisms that allows data packets to be handled in a manner that guarantees certain levels of performance. It must be highlighted that QoS is not in itself a protocol or standard like TCP/IP or MPLS. Generally in a modern IP VPN environment, the preferred technical mechanism for establishing QoS is the Differentiated Services (DiffServ) standard. DiffServ allows for class-based traffic management.

The ability to differentiate one type of traffic from another as it passes from a non-MPLS edge to an MPLS core is essential to ensure that applications are assigned to the correct class of service. Only with precise classification can applications be treated according to their respective business importance. Businesses can use QoS to optimize their entire data or MPLS VPN network to ensure the consistent and cost effective delivery of critical communications. QoS also allows for efficient management in the event of unanticipated congestion or other network issues impacting on the applications. If you turn off QoS in sections of a network you may lose the ability to track end-to-end application session performance. Therefore QoS can optimize your network to ensure business critical communications are consistently delivered when and where they're needed [13].

4.2 Differentiated Services

Conventionally all packets are treated as best effort (BE) and routers forward Internet traffic on a first-in-first-out basis as long as the there is enough buffer capacity on the interface. As the amount of traffic on the Internet grows the network performance gradually decreases, causing network degradation, network delay or jitter, and packet loss. Applications such as Web access, email, and file transfer can typically withstand network delays, but delay-sensitive applications such as voice, video, and other real-time

applications cannot. To provide adequate service in a network, some level of intelligence must be built into the network so that packets are prioritized. A differentiated service

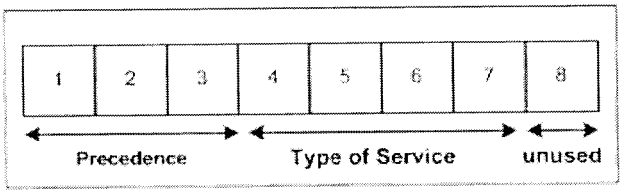


Figure 4.1: IP version 4 Type of Service (TOS) field

(DiffServ) is one of the QoS architectures which have proven to be scalable and widely used and defined in RFC 2475 [14].

Differentiated services has two major components, namely

- Traffic conditioning – Includes policing and shaping for the packets arriving at edge router or LER
- Per-Hop-Behaviors (PHB) – Includes queuing, scheduling and dropping of packets which is done at each hop

Initially packets have to be classified and matched against parameters from the IP header such as IP destination, IP source or differentiated service code point (DSCP) values. Originally, the TOS field in IP header had 3 precedence bits and 4 TOS bits and 1 unused bit. Precedence bits were used to make various decisions about a packet treatment and used of TOS bits was never well deployed. The precedence bits are set at edge of the network into 8 different classes. Figure 4.1 illustrates the TOS fields and their bit descriptions are mentioned below.

LSB bits are precedence values showing packet relative priority from 0 to 7:

0 – Routine

1 – Priority

2 – Immediate

3 - Flash

4 - Flash Override

5 – Critical

6 - Internet Control

7 - Network Control

TOS fields indicate packet classifications and 5 combinations are defined:

0 - Normal service

2 - Minimum monetary cost

2 - Maximum reliability

4 - Maximize throughput

5 - Minimize delay

IETF redefined RFC 2475 of DiffServ architecture defining 6 bits for Type-of-Services field to form 64 combinations for packet treatment. Remaining 2 bits are used for Explicit Congestion Notification (ECN). Table 4.2 shows the DSCP fields in decimal groups.

IP Precedence		DSCP	
Decimal	Bits	Decimal	Bits
0	000	0	000000
1	001	8	001000
2	010	16	010000
3	011	24	011000
4	100	32	100000
5	101	40	101000
6	110	48	110000
7	111	56	111000

Table 4.2: DSCP and IP Precedence mappings

From the above table, the 8 precedence values are called classes and DSCP bits mapped to them are called Class Sector Code Points (CSCP) and abbreviated as class selectors (CS). RFC 2597, 2598 defines additional 13 DSCP values known as Assured Forwarding (AF) and Expedited Forwarding (EF) which are shown in the table below 4.3. AF and EF are further explained in section 4.2 [15].

Class	DSCP decimal	DSCP bits
Default	0	000000
AF11	10	001010
AF12	12	001100
AF13	14	001110
AF21	18	010010
AF22	20	010100
AF23	22	010110
AF31	26	011010
AF32	28	011100
AF33	30	011110
AF41	34	100010
AF42	36	100100
AF43	38	100110
EF	46	101110

Table 4.3: DSCP AF and EF values

DiffServ provides a simple way to categorize and prioritize network traffic aggregates. In IP version 4, where every router looked at the address, protocol, and port number fields, and then applied classification rules to each packet on a per-hop basis and classification rules were applied to a 4-bit TOS field and then a forwarding decision was made. DiffServ takes the IP TOS field, as a differential services byte, and uses it to carry information about IP packet service requirements. It operates at layer 3 only and does not deal with lower layers. DiffServ relies on traffic conditioners sitting at the edge of the network to indicate each packet's requirements.

4.3 Per-Hop Behaviors (PHBs) and Codepoints

PHBs are applied by the traffic conditioner to traffic at a network ingress point according to pre-determined policy rules. The traffic may be marked at this point, routed according to the marking, and then unmarked at the network egress point. DiffServ provides a simple method of classifying services of various applications. There are currently two standard PHBs defined that effectively represent two traffic classes, namely,

a. Expedited Forwarding (EF) - is defined for low loss, low delay and low jitter service and any traffic that exceeds the defined policy will be discarded. The recommended DSCP value for this is 46.

b. Assured Forwarding (AF) - has four classes and three drop-precedence's within each class (equaling twelve code points). Excess AF traffic is not delivered with as high a probability as the traffic within the policy means it may be demoted but not necessarily dropped.

Drop Order	Class 1	Class 2	Class 3	Class 4
Low	AF11=001010	AF21=010010	AF31=011010	AF41=100010
Medium	AF12=001100	AF22=010100	AF32=011100	AF42=100100
High	AF13=001110	Af23=010110	AF33=011110	AF43=100110

Table 4.4: General drop order based on classes [8]

The packets are marked at the edge of the network, by setting the DSCP fields of the packets according to their differentiated service value. Packets are buffered and scheduled in accordance to their DSCP values throughout the network by Weighted Random Early Detection (WRED) and Weighted Round Robin (WRR). Important traffic such as network control traffic and from corporate customers will be forwarded with high priority. The DSCP 6 bits is used to queue and schedule packets. General drop order for classes is shown in table 4.4.

4.4 IP Service Level Agreements (SLAs)

In response to escalating performance requirements for critical applications, converged IP networks must become optimized for performance levels. Service Level Agreements (SLAs) that support application solutions are becoming an increasingly common requirement, and SLAs in the IP infrastructure are an essential part of optimizing the network for business. Network equipment must therefore verify service guarantees, validate network performance, improve network reliability, proactively identify network issues, and react to performance metrics with changes to the configuration and network.

Traditional SLAs are layer 2 circuit-switched networks. These networks must meet a Committed Information Rate (CIR), or minimal guaranteed bandwidth, as well as a minimum guaranteed connectivity rate, which is expressed as a percentage (example: 99.9%). This SLA is a fixed point-to-point circuit in no way indicative of the end-to-end

experience of the end-user and their application. Moreover, the SLA goes with the customer following a migration from the legacy circuit(s) to other transport options. Therefore these traditional SLAs are limited and application-unaware.

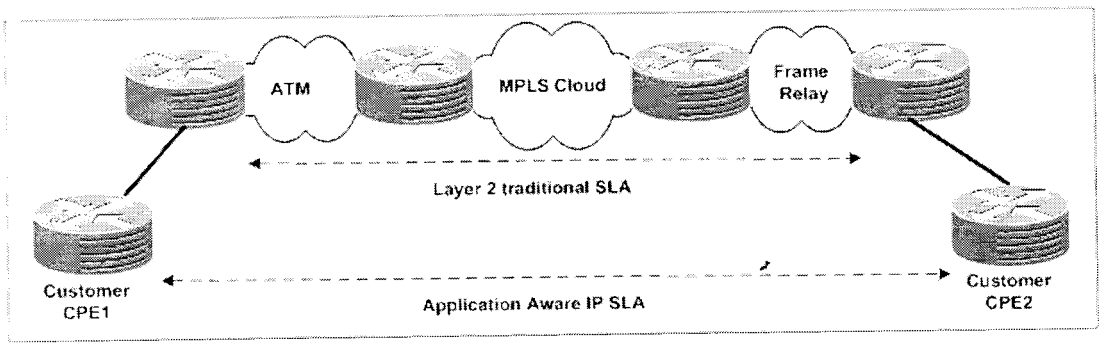


Figure 4.5: End to End IPSLA

IP networks are currently held accountable for carrying all types of applications that require networks and the Internet to provide the appropriate level of service for the appropriate application. These include integrated web, voice, video, and business-critical applications. In order to make real-time network decisions that ensure application QoS, it is important to measure end-to-end network performance statistics as data traverses the network. This end-to-end measurement is the only way to accurately assess whether the performance statistics are satisfactory enough to support the application(s). This is shown in figure 4.5 and some of the main market drivers for requirement of enhanced SLAs are,

1. **Business-Critical Applications -**
    a. These are individual needs of the customers. (example; Enterprise Resource Management (ERP), Customer Relationship Management (CRM), Material Requirements Planning (MRP), portals, and client-server applications etc.) In order to meet business objectives, service providers must deliver these applications with a high degree of network performance. This can only be accomplished with a dynamic network that measures, adjusts, warns and assists with problem identification and troubleshooting.

2. **Voice -**
    a. Dedicating a single converged network connection to voice, video, and data traffic reduces network complexity, resulting in measurable cost savings in hardware, software, and management while ensuring quality.

3. **Audio/Video Conferencing -**
    a. As virtual teams, global offices, and telecommuting are become more frequent, there is a corresponding increase in the importance of video and audio services. Examples of emerging applications include:
        i. Audio and web conferencing tools allow real-time meeting places.
        ii. Voice over IP (VoIP) phones in home offices enables telecommuters to traverse the company network.
        iii. Seamless interface for scheduling and hosting multimedia conferences.
        iv. Unified messaging which is integration of voice, email, fax, and scheduling into one interface accessible both via voice and online.
        v. All of these value-added applications depend on an IP network that can deliver an appropriate level of network performance.

4. **Virtual Private Networks (VPNs) -**
    a. Customers could easily upgrade their network traffic over the MPLS VPN circuits when the provider can ensure the requested bandwidth and QoS with confidence. The increasing frequency of MPLS VPNs with QoS guarantees requires providers to pay closer attention to network performance.

5. **Outsourcing Services-**
    a. Many enterprises outsource their network and services from service providers. In the agreement, pricing are based upon variety of criteria related to network uptime, mean-time-to-repair (MTTR), bandwidth, latency, packet loss, and jitter. The agreements can also be specific to traffic types like database application (Premium package), Internet (Silver package) and email (Bronze package) etc.

Network engineers can use a variety of benchmarks, including delay, packet loss, jitter, packet sequencing and connectivity, to measure the quality of service delivered to the end user. An IP infrastructure that supports these metrics ensures a successful network-wide rollout of business-critical applications.

Therefore, to ensure application delivery for customers, SLAs need to be tight. An IP SLA is an SLA that is set very precisely and thus provides a service level that is both realistic and high quality. Service Providers that support improved IP SLAs have the opportunity to increase their business and to successfully rollout new applications. In order to tighten network SLAs, service providers need technology that support metrics and accuracy within the IP infrastructure.

In this thesis, considering the need for IP SLA a software program has been developed based on JAVA and SNMP libraries which gather network performance metrics such as end-to-end delay, jitter, and availability and application performance (http) for each VPN customer circuits. The results are represented in graphs including summary which will ensure the service provider to deliver what customer expects. Standard SLA programs are much expensive asset in a service provider's CAPEX. Therefore this has been developed as a low cost solution which could be used as a tool until service provider's maturity.

SNMP is one of the most commonly used technologies when it comes to network bandwidth and performance monitoring. Collections of information of device statistics are represented hierarchically in the devices Management Information Base (MIB). Object Identifiers (OIDs) uniquely identify managed objects within MIB hierarchy and SNMP is used to access them. OIDs are represented as a tree structure and each vendor have their own OIDs under the "private" column in an OID Tree. Figure 4.6 shows an OID tree hierarchy for CISCO. For example a complete OID for CISCO router 7604 to obtain protocol information would be 1.3.6.1.4.1.9.9.42.1.2.2.1.1.X, where X is a number unique to a particular SLA which is used when configuring SLA in that device. The MIB used in this work is CISCO-RTTMON [16], [17] to query SLA details from CISCO devices.

This program uses SNMP JFreeChart to display graphs and SNMP4J libraries to query SNMP enabled devices and also uses Access database to store user information and performance mercies for each SLA types concerned. The program is tested with CISCO 7600 and 12000 series routers from a live MPLS network but can be customized for any equipment that supports SNMP and having their MIBs for the required OIDs to gather different SLAs. Figure 4.7 (a) and (b) shows the flow chart of the program operation using SNMP.

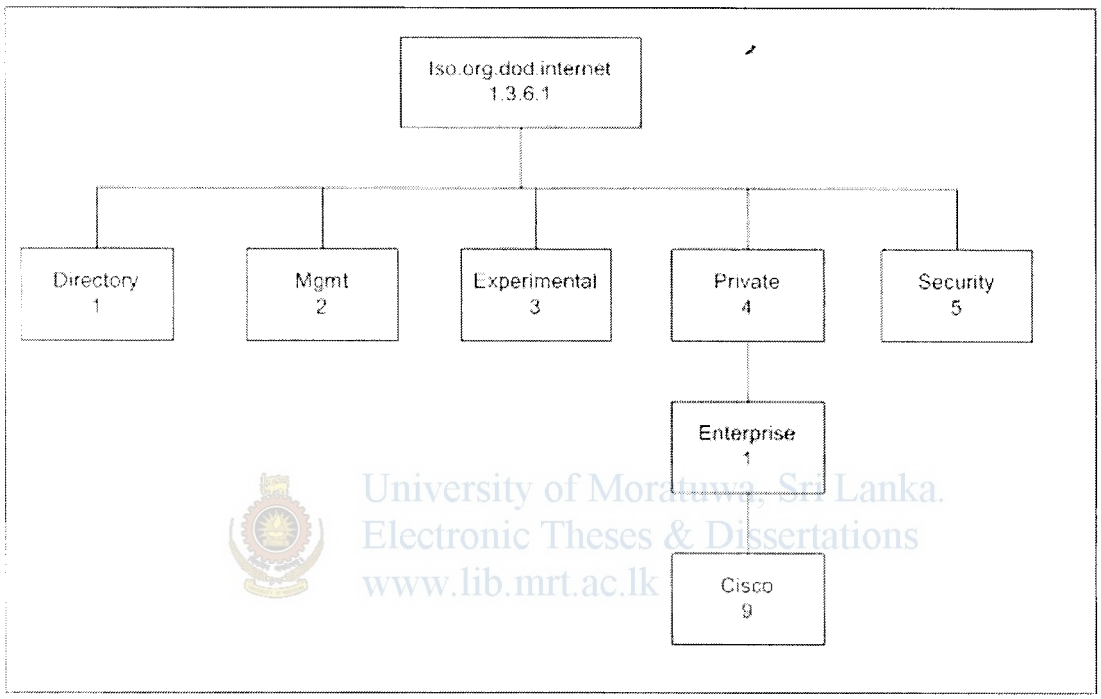


Figure 4.6: MIB tree for vendor CISCO (1.3.6.1.4.1.9.X.X.X.X.X) where "X" represents values specific to a product.

The flow chart below in figure 4.7 shows the operation of the program. Figure 4.7 (a) is the main polling program which uses SNMP to establish connection with SNMP enabled nodes and query configured SLA parameters in a sequence. Figure 4.7 (b) describes viewing of customer performance reports. Once a customer and SLA is selected, the program retrieves data from database, perform any calculation if necessary and populate results graphically.

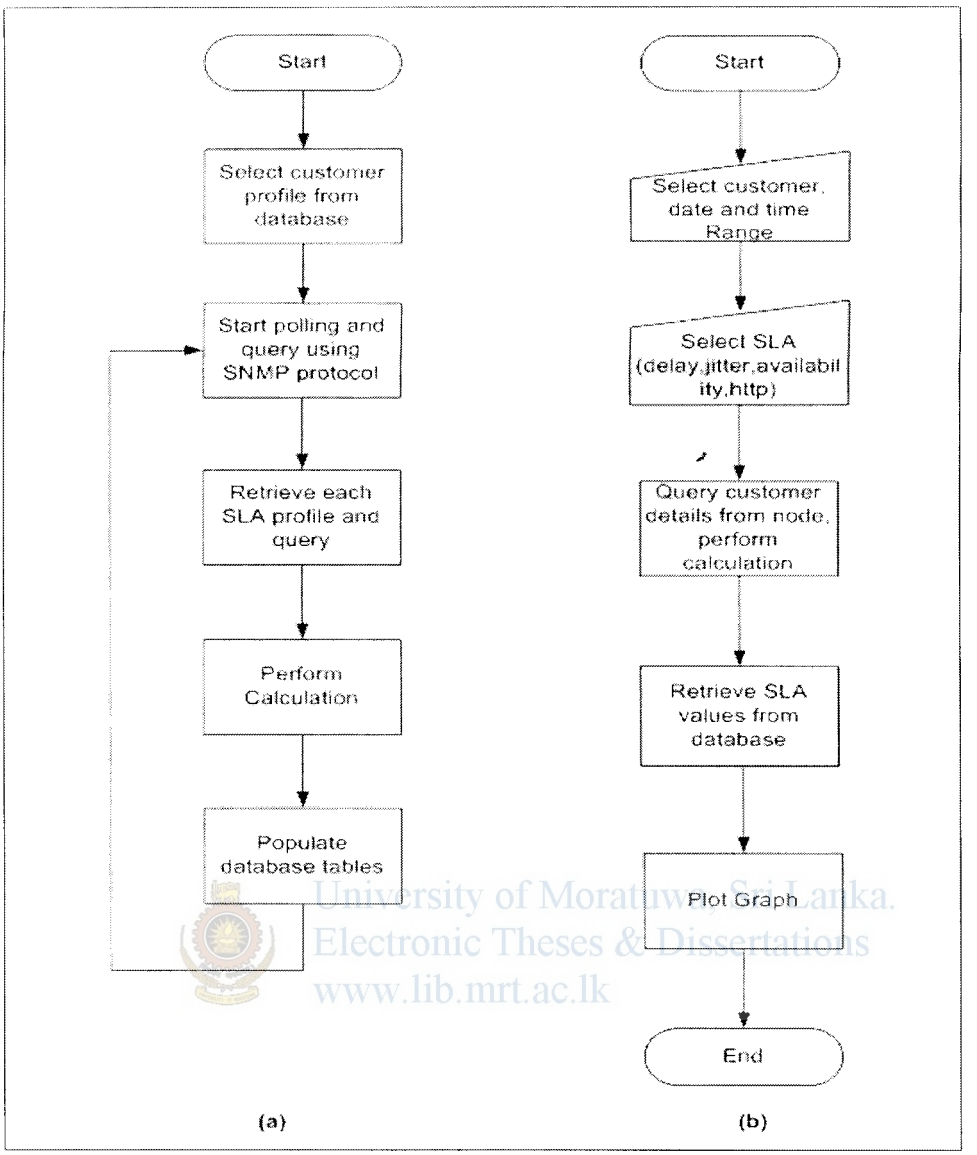


Figure 4.7: SLA program logic to generate performance reports.

Each SLA parameter is maintained in separate tables in an Access database. Average values are calculated from the returned values from the devices in response to a query from the program and database is updated periodically. The polling time is 10 minutes but this could be customized.

simulations, the model behavior will change each simulation according to the set of initial parameters assumed for the environment.

Several software packages exist for running computer-based simulation modeling of a network topology and there is limited number of simulation programs available commercially to do MPLS simulations which are very expensive. For example, MPLS module in OPNET simulator offers the most comprehensive and accurate performance predictions of networks that incorporate MPLS-TE technology and policies. Therefore an open source based network simulator known as "GNS3" [4] is used to setup and simulate the MPLS-TE tunnels initially and results are been captured in a real lab environment. The simulator is not used to capture or compare results with the real lab because of the extensive processing power it required and eventually delaying the response time of the routers and was difficult to obtain acceptable results. It was used to study and understand the concepts of MPLS-TE and the configurations were used in a real lab to obtain the results.

5.2 Setting up MPLS topology and assigning traffic via TE tunnels

In order to develop TE tunnels an MPLS network topology was implemented and tested in a real lab environment using vendor equipments from CISCO and results are obtained. Simulation demonstrates how TE is used to divert traffic in an underutilized alternative path using tunnels. The following equipments and parameters were considered

Simulation Parameters for the model,

1. Core and Edge routers in GNS3 simulation program – CISCO 3640 with IOS software release 12.3 (26)
2. Core and Edge routers in real test lab– CISCO 2800 IOS 12.4(15)
3. Frame Relay Switch – CISCO 2821 with 3 asynchronous ports of 128Kbps and IOS 12.4 (8a)
4. Links – 100 Mbps Ethernet for the whole topology using the GNS3 simulator and 128Kbps point to point 3 serial links for core routers in Lab environment via frame relay switch. The edge routed connected to core routers via 100Mbps Ethernet connections.

5. Routing Protocol – BGP and ISIS
6. "Iperf" tool is used to generate UDP traffic via the backbone to the other end from PC1 to PC3
7. Initial bandwidth reserved for each interface 96Kbps for the real lab and 512Kbps for the simulation.

Figure 5.1 shows the topology diagram simulated in GNS3 and figure 5.2 is the diagram for the real lab network. Router configurations are attached in appendix A and B. Routers C1, C2 and C3 are the core routers and PE1, PE2, and PE3 are the edge routers. MPLS is enabled on all core router interfaces and all edge router interfaces facing the core network side. The Interior Gateway Protocol (IGP) used is IS-IS within the core and customers routes are propagated using BGP peering with all edge routes using their loop back addresses. Customer-end networks used are 192.168.1.0, 192.168.2.0 and 192.168.3.0. By default IS-IS selects the shortest path C2 C3 to steer traffic and the link C2 C1 C3 is all most idle. One solution to occupy this idle link is to change default metric values of the protocol but this would be cumbersome in large complex service provider network. The viable solution is to implement TE for less critical traffic such as Internet and email which could be diverted via the longest path C2 C1 C3. Delay sensitive applications like voice, video or database access can be routed via the shortest path providing adequate end to end response time, jitter and delay.

In the real lab, tunnel 0 (T0) was setup to follow PE1 C2 C3 PE3 path and traffic destined to 192.168.3.0 was routed through T0. Traffic destined to 192.168.7.0 was routed through PE1 C2 C1 C3 PE3 tunnel 1 (T1) path. TE was enabled on interfaces of C1, C3 and C2 (except fast Ethernet 1/0) and on all fast Ethernet 0/0 of edge devices. Initial bandwidth reserved was 96K on each TE enabled interfaces.

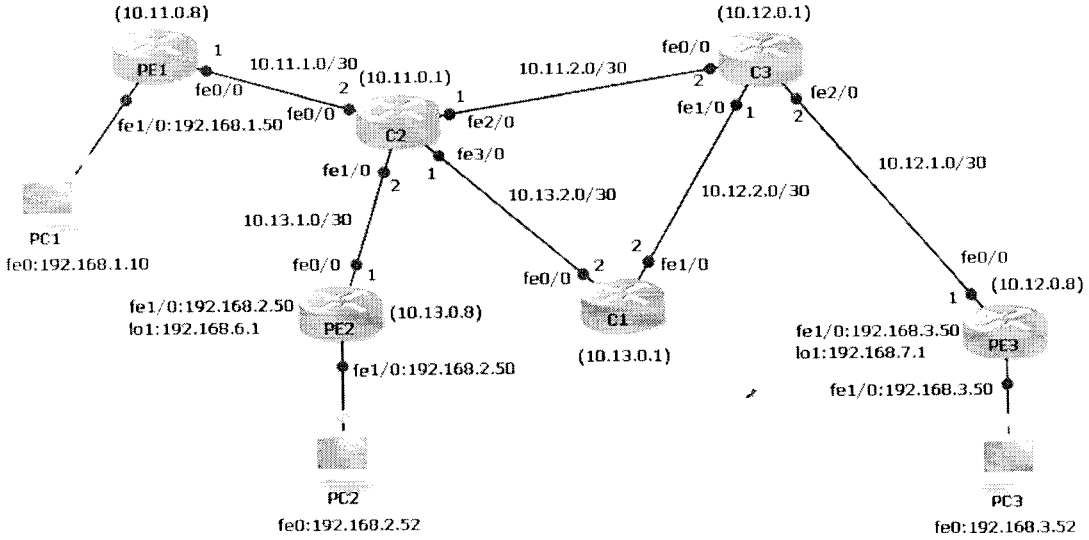


Figure 5.1: Initial Topology creations in GNS3, all routers are CISCO 3640 with IOS version 12.3(26)

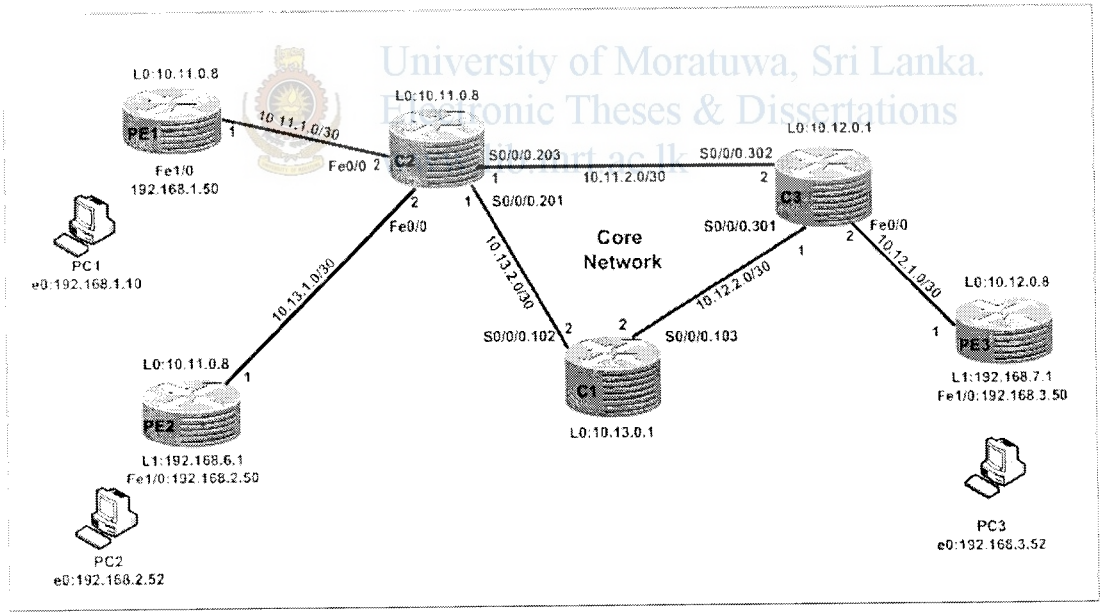


Figure 5.2: MPLS network Topology implemented in Lab, all routers are CISCO 2800 and core serial links are connected via a Frame Relay Switch

In real lab environment tunnels T0 and T1 were setup with 48Kbps (priority 7) and 32Kbps (priority 2) of bandwidth respectively. A tunnel of priority 2 has a better priority than a tunnel of priority 7 and this could be clearly seen in figure 5.8 (a).

Initial neighbor relation ship between the edge and core routers are shown below in figures 5.3 (a) to (f). All routers are peering with their loop back addresses L0 and customer routes 192.168.3.0, 192.168.7.0, 192.168.2.0 are been propagated on each edge node via BGP. Figure 5.4 shows the routing tables for these networks.

```
PE1#sh isis topology

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
C2                   10         C2                   Fa0/0       0017.9491.0a88
PE1                  --
C3                   20         C2                   Fa0/0       0017.9491.0a88
PE3                  30         PE3                  Tu1         *MPLS TE-Tunnel
                                PE3                  Tu0         *MPLS TE-Tunnel
C1                   20         C2                   Fa0/0       0017.9491.0a88
PE2                  20         C2                   Fa0/0       0017.9491.0a88
```

Figure 5.3 (a): Topology Information in Router PE1

```
PE2#sh isis topology

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
C2                   10         C2                   Fa0/0       0017.9491.0a89
PE1                  20         C2                   Fa0/0       0017.9491.0a89
C3                   20         C2                   Fa0/0       0017.9491.0a89
PE3                  30         C2                   Fa0/0       0017.9491.0a89
C1                   20         C2                   Fa0/0       0017.9491.0a89
PE2                  --
```


Figure 5.3 (b): Topology Information in Router PE2

```
PE3#sh isis topology

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
C2                   20         C3                   Fa0/0       0017.95bb.d968
PE1                  30         C3                   Fa0/0       0017.95bb.d968
C3                   10         C3                   Fa0/0       0017.95bb.d968
PE3                  --
C1                   20         C3                   Fa0/0       0017.95bb.d968
PE2                  30         C3                   Fa0/0       0017.95bb.d968
```

Figure 5.3 (c): Topology Information in Router PE3

```
C1#sh isis topology

IS-IS paths to level-2 routers
System Id           Metric     Next-Hop             Interface   SNPA
C2                  10         C2                   Se0/0/0.102 DLCI 102
PE1                 20         C2                   Se0/0/0.102 DLCI 102
C3                  10         C3                   Se0/0/0.103 DLCI 103
PE3                 20         C3                   Se0/0/0.103 DLCI 103
C1                  --
PE2                 20         C2                   Se0/0/0.102 DLCI 102
```

Figure 5.3 (d): Topology Information in Router C1

```
C2#sh isis topology

IS-IS paths to level-2 routers
System Id           Metric     Next-Hop             Interface   SNPA
C2                  --
PE1                 10         PE1                  Fa0/0       0017.95aa.61e0
C3                  10         C3                   Se0/0/0.203 DLCI 203
PE3                 20         C3                   Se0/0/0.203 DLCI 203
C1                  10         C1                   Se0/0/0.201 DLCI 201
PE2                 10         PE2                  Fa0/1       0017.95aa.7140
```

Figure 5.3 (e): Topology Information in Router C2

```
C3#sh isis topology

IS-IS paths to level-2 routers
System Id           Metric     Next-Hop             Interface   SNPA
C2                  10         C2                   Se0/0/0.302 DLCI 302
PE1                 20         C2                   Se0/0/0.302 DLCI 302
C3                  --
PE3                 10         PE3                  Fa0/0       0017.95aa.5fb8
C1                  10         C1                   Se0/0/0.301 DLCI 301
PE2                 20         C2                   Se0/0/0.302 DLCI 302
```


Figure 5.3 (f): Topology Information in Router C3

```
PE1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.32.0.0/24 is subnetted, 1 subnets
C       172.32.1.0 is directly connected, FastEthernet0/1.200
     10.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
C       10.11.1.0/30 is directly connected, FastEthernet0/0
i L2    10.11.0.1/32 [115/20] via 10.11.1.2, FastEthernet0/0
i L2    10.11.2.0/30 [115/20] via 10.11.1.2, FastEthernet0/0
i L2    10.12.2.0/30 [115/30] via 10.11.1.2, FastEthernet0/0
i L2    10.13.2.0/30 [115/20] via 10.11.1.2, FastEthernet0/0
i L2    10.13.1.0/30 [115/20] via 10.11.1.2, FastEthernet0/0
i L2    10.13.0.1/32 [115/30] via 10.11.1.2, FastEthernet0/0
i L2    10.12.1.0/30 [115/30] via 10.11.1.2, FastEthernet0/0
i L2    10.12.0.1/32 [115/30] via 10.11.1.2, FastEthernet0/0
C       10.11.0.8/32 is directly connected, Loopback0
i L2    10.12.0.8/32 [115/40] via 10.11.1.2, FastEthernet0/0
i L2    10.13.0.8/32 [115/30] via 10.11.1.2, FastEthernet0/0
B    192.168.7.0/24 [200/0] via 10.12.0.8, 01:30:58
C    192.168.1.0/24 is directly connected, FastEthernet0/1.50
B    192.168.2.0/24 [200/0] via 10.13.0.8, 00:57:16
C    192.168.100.0/24 is directly connected, FastEthernet0/1.100
B    192.168.3.0/24 [200/0] via 10.12.0.8, 01:05:28
```

Figure 5.4: IP routing table showing customer subnets and next hop addresses

The figures 5.5 (a) shows, all packets take the default shortest path identified by the shortest path algorithm and figure 5.5 (b) illustrates that's packet destined to 192.168.7.1 address can be steered via the alternative longest path using a tunnel T1. Each tunnel has their head-end originating from PE1 and tail- end at PE3. Figures 5.7 (a) and (b) shows tunnel status, allocated bandwidth and priority values. There are many ways to assign traffic to the tunnels. Here we use policy based routing at input interface of PE1 fast Ethernet 0/1.

```
*******************************Trace to destination without tunnels*********************

C:\>tracert 192.168.7.1

Tracing route to 192.168.7.1 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.1.50
  2    47 ms    47 ms    47 ms  10.11.1.2
  3    41 ms    37 ms    37 ms  10.11.2.2
  4    28 ms    28 ms    28 ms  192.168.7.1

Trace complete.


C:\>tracert 192.168.3.52

Tracing route to 192.168.3.52 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.1.50
  2    47 ms    47 ms    46 ms  10.11.1.2
  3    37 ms    37 ms    37 ms  10.11.2.2
  4    23 ms    23 ms    23 ms  10.12.1.1
  5    28 ms    27 ms    27 ms  192.168.3.52

Trace complete.
```

Figure 5.5 (a): Trace through PE1 to PE3 takes the shortest path always for 192.168.3.52 and 192.168.7.1 destination network

```
*******************************Trace to destination with tunnels*************************

C:\>tracert 192.168.3.52

Tracing route to 192.168.3.52 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.1.50
  2    47 ms    47 ms    47 ms  10.11.1.2
  3    37 ms    37 ms    42 ms  10.11.2.2
  4   156 ms    23 ms    23 ms  10.12.1.1
  5    28 ms    27 ms    27 ms  192.168.3.52

Trace complete.

C:\>tracert 192.168.7.1

Tracing route to 192.168.7.1 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.1.50
  2    70 ms    70 ms    70 ms  10.11.1.2
  3    61 ms    60 ms    60 ms  10.13.2.2
  4    51 ms    51 ms   185 ms  10.12.2.1
  5   213 ms    41 ms    41 ms  192.168.7.1

Trace complete.
```


Figure 5.5 (b): Trace through PE1 to PE3 for 192.168.7.1 takes the alternative path

```
PE1#sh ip rsvp interface
interface    rsvp  allocated  i/f max  flow max sub max
Fa0/0        ena   80K        96K      96K      0
```

Figure 5.6: Total bandwidth reservation by both tunnels at fast Ethernet 0/0 is 80Kbps at PE1

```
PE1#sh mpls traffic-eng tunnels tunnel 0

Name: PE1_t0                                (Tunnel0) Destination: 10.12.0.8
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 10, type explicit pathc2c3 (Basis for setup, path weight 30)

  Config Parameters:
    Bandwidth: 48       kbps (Global)  Priority: 7  7   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 48       bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled


  InLabel  : -
  OutLabel : FastEthernet0/0, 25
  RSVP Signalling Info:
       Src 10.11.0.8, Dst 10.12.0.8, Tun_Id 0, Tun_Instance 9
    RSVP Path Info:
      My Address: 10.11.1.1
      Explicit Route: 10.11.1.2 10.11.2.2 10.12.1.1 10.12.0.8
      Record   Route:   NONE
      Tspec: ave rate=48 kbits, burst=1000 bytes, peak rate=48 kbits
    RSVP Resv Info:
      Record   Route:   NONE
      Fspec: ave rate=48 kbits, burst=1000 bytes, peak rate=48 kbits
  Shortest Unconstrained Path Info:
    Path Weight: 30 (TE)
    Explicit Route: 10.11.1.2 10.11.2.2 10.12.1.1 10.12.0.8
  History:
    Tunnel:
      Time since created: 1 hours, 32 minutes
      Time since path change: 1 hours, 32 minutes
      Number of LSP IDs (Tun_Instances) used: 9
    Current LSP:
      Uptime: 1 hours, 32 minutes
    Prior LSP:
      ID: path option 10 [6]
```


Figure 5.7 (a): T0 reserved with 48Kbbps and priority 7 and explicit route shows the shortest path via C2 C3

```
PE1#sh mpls traffic-eng tunnels tunnel 1

Name: PE1_t1                                (Tunnel1) Destination: 10.12.0.8
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 20, type explicit pathc1c2c3 (Basis for Setup, path weight 40)

  Config Parameters:
    Bandwidth: 32       kbps (Global)  Priority: 2  2   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 32       bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 20 is active
    BandwidthOverride: disabled  LockDown: disabled  verbatim: disabled


  InLabel  :  -
  OutLabel : FastEthernet0/0, 26
  RSVP Signalling Info:
       Src 10.11.0.8, Dst 10.12.0.8, Tun_Id 1, Tun_Instance 14
    RSVP Path Info:
      My Address: 10.11.1.1
      Explicit Route: 10.11.1.2 10.13.2.2 10.12.2.1 10.12.1.1
                      10.12.0.8
      Record   Route:   NONE
      Tspec: ave rate=32 kbits, burst=1000 bytes, peak rate=32 kbits
    RSVP Resv Info:
      Record   Route:   NONE
      Fspec: ave rate=32 kbits, burst=1000 bytes, peak rate=32 kbits
  Shortest Unconstrained Path Info:
    Path Weight: 30 (TE)
    Explicit Route: 10.11.1.2 10.11.2.2 10.12.1.1 10.12.0.8
  History:
    Tunnel:
      Time since created: 1 hours, 32 minutes
      Time since path change: 1 hours, 32 minutes
      Number of LSP IDs (Tun_Instances) used: 14
    Current LSP:
      Uptime: 1 hours, 32 minutes
    Prior LSP:
      ID: path option 20 [7]
```


Figure 5.7 (b): T1 reserved with 32Kbps and priority 2 and explicit route shows the longest path hops via C2 C1 C3

From figure 5.8 (a) tunnel T1 with priority 2 consumes 32 Kbps and reservable bandwidth is 64Kbps (96-32) and any tunnel with priority less than 2 (3 to 7) sees reservable bandwidth as 64Kbps. Thus tunnel T0 with priority 7 consumes 48Kbps and reservable is 16Kbps. This shows important tunnels gets more resources.

```
PE1#sh mpls traffic-eng topology 10.11.0.8

IGP Id: 0100.1100.0008.00, MPLS TE Id:10.11.0.8 Router Node  (isis  level-2) id 2
      link[0]: Point-to-Point, Nbr IGP Id: 0100.1100.0001.00, nbr_node_id:1, gen:14
          frag_id 0, Intf Address:10.11.1.1, Nbr Intf Address:10.11.1.2
          TE metric:10, IGP metric:10, attribute flags:0x0
          SRLGs: None
          physical_bw: [128] (kbps), max_reservable_bw_global: [96] (kbps)
          max_reservable_bw_sub: 0 (kbps)

                                Global Pool       Sub Pool
                Total Allocated Reservable        Reservable
                BW (kbps)       BW (kbps)         BW (kbps)
                --------------- ----------        ----------
          bw[0]:              0         96                 0
          bw[1]:              0         96                 0
          bw[2]:             32         64                 0
          bw[3]:              0         64                 0
          bw[4]:              0         64                 0
          bw[5]:              0         64                 0
          bw[6]:              0         64                 0
          bw[7]:             48         16                 0
```

Figure 5.8 (a): Bandwidth allocation in PE1 at Fast Ethernet 0/0 interface of router PE1. BW (2) and BW (7) are the priorities of the tunnels.

```
PE1#sh mpls traffic-eng link-management bandwidth-allocation fastEthernet 0/0
System Information::
    Links Count:          1
    Bandwidth Hold Time:  max. 15 seconds
Link ID::  Fa0/0 (10.11.1.1)
    Local Intfc ID:        1
    Link Status:
      SRLGs:                    None
      Intfc Switching Capability Descriptors:
        Default:                Intfc Switching Cap psc1, Encoding ethernet
      Link Label Type:          Packet
      Physical Bandwidth:       [128] kbits/sec
      Max Res Global BW:        [96] kbits/sec (reserved: 0% in, 83% out)
      Max Res Sub BW:           0 kbits/sec (reserved: 100% in, 100% out)
      BW Descriptors:           2
      MPLS TE Link State:       MPLS TE on, RSVP on, admin-up, flooded, allocated
      Inbound Admission:        reject-huge
      Outbound Admission:       allow-if-room
      Admin. Weight:            10 (IGP)
      IGP Neighbor Count:       1
      Up Thresholds:            1 2 5
      Down Thresholds:          5 2 1
    Downstream Global Pool Bandwidth Information (kbits/sec):
      KEEP PRIORITY     BW HELD  BW TOTAL HELD   BW LOCKED  BW TOTAL LOCKED
                  0           0              0           0                0
                  1           0              0           0                0
                  2           0              0          [32]             32
                  3           0              0           0               32
                  4           0              0           0               32
                  5           0              0           0               32
                  6           0              0           0               32
                  7           0              0          [48]             80
    Downstream Sub Pool Bandwidth Information (kbits/sec):
      KEEP PRIORITY     BW HELD  BW TOTAL HELD   BW LOCKED  BW TOTAL LOCKED
                  0           0              0           0                0
                  1           0              0           0                0
                  2           0              0           0                0
                  3           0              0           0                0
                  4           0              0           0                0
                  5           0              0           0                0
                  6           0              0           0                0
                  7           0              0           0                0
```

Figure 5.8 (b): Bandwidth allocation by both tunnels T0 and T1 at Fast Ethernet 0/0 interface of router PE1

```
PE1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.32.0.0/24 is subnetted, 1 subnets
C       172.32.1.0 is directly connected, FastEthernet0/1.200
     10.0.0.0/8 is variably subnetted, 12 subnets, 2 masks
C       10.11.1.0/30 is directly connected, FastEthernet0/0
i L2    10.11.0.1/32 [115/20] via 10.11.1.2, FastEthernet0/0
i L2    10.11.2.0/30 [115/20] via 10.11.1.2, FastEthernet0/0
i L2    10.12.2.0/30 [115/30] via 10.11.1.2, FastEthernet0/0
i L2    10.13.2.0/30 [115/20] via 10.11.1.2, FastEthernet0/0
i L2    10.13.1.0/30 [115/20] via 10.11.1.2, FastEthernet0/0
i L2    10.13.0.1/32 [115/30] via 10.11.1.2, FastEthernet0/0
i L2    10.12.1.0/30 [115/30] via 10.11.1.2, FastEthernet0/0
i L2    10.12.0.1/32 [115/30] via 10.11.1.2, FastEthernet0/0
C       10.11.0.8/32 is directly connected, Loopback0
i L2    10.12.0.8/32 [115/40] via 10.12.0.8, Tunnel1
                     [115/40] via 10.12.0.8, Tunnel0
i L2    10.13.0.8/32 [115/30] via 10.11.1.2, FastEthernet0/0
B    192.168.7.0/24 [200/0] via 10.12.0.8, 01:30:58
C    192.168.1.0/24 is directly connected, FastEthernet0/1.50
B    192.168.2.0/24 [200/0] via 10.13.0.8, 00:57:16
C    192.168.100.0/24 is directly connected, FastEthernet0/1.100
B    192.168.3.0/24 [200/0] via 10.12.0.8, 01:05:28


PE1#sh ip route 10.12.0.8
Routing entry for 10.12.0.8/32
  Known via "isis", distance 115, metric 40, type level-2
  Redistributing via isis
  Last update from 10.12.0.8 on Tunnel0, 01:32:48 ago
  Routing Descriptor Blocks:
  * 10.12.0.8, from 10.12.0.8, via Tunnel1
      Route metric is 40, traffic share count is 2
    10.12.0.8, from 10.12.0.8, via Tunnel0
      Route metric is 40, traffic share count is 3
```


Figure 5.9: IP routing table after tunnels are been setup and PE3 (10.12.0.8) has two paths Tunnel T0 and T1

```
**************************UDP traffic (12Kbps) from PE1 to PE3 customer 192.168.7.0******


Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\1\iperf>iperf.exe -u -c 192.168.7.1 -t60 -i1 -b12K
------------------------------------------------------------
Client connecting to 192.168.7.1, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
[1716] local 192.168.1.10 port 1050 connected with 192.168.7.1 port 5001
[ ID] Interval       Transfer     Bandwidth
[1716]  0.0- 1.0 sec  2.87 KBytes  23.5 Kbits/sec
[1716]  1.0- 2.0 sec  1.44 KBytes  11.8 Kbits/sec
[1716]  2.0- 3.0 sec  1.44 KBytes  11.8 Kbits/sec
[1716]  3.0- 4.0 sec  1.44 KBytes  11.8 Kbits/sec
[
[1716] 59.0-60.0 sec  1.44 KBytes  11.8 Kbits/sec
[ ID] Interval       Transfer     Bandwidth
[1716]  0.0-61.8 sec  90.4 KBytes  12.0 Kbits/sec
```

Figure 5.10 (a): "Iperf" tool is sending 12Kbps UDP traffic to destination 192.168.7.1 from PC1

```
**************************UDP traffic (30KKbps) from PE1 to PE3 customer 192.168.3.0******

C:\1\iperf>iperf.exe -u -c 192.168.3.52 -t120 -i1 -b30K
------------------------------------------------------------
Client connecting to 192.168.3.52, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
[1716] local 192.168.1.10 port 1049 connected with 192.168.3.52 port 5001
[ ID] Interval       Transfer     Bandwidth
[1716]  0.0- 1.0 sec  4.31 KBytes  35.3 Kbits/sec
[1716]  1.0- 2.0 sec  4.31 KBytes  35.3 Kbits/sec
[1716]  2.0- 3.0 sec  2.87 KBytes  23.5 Kbits/sec
[1716]  3.0- 4.0 sec  4.31 KBytes  35.3 Kbits/sec

[1716] 118.0-119.0 sec  4.31 KBytes  35.3 Kbits/sec
[1716] 119.0-120.0 sec  4.31 KBytes  35.3 Kbits/sec
[ ID] Interval       Transfer     Bandwidth
[1716]  0.0-120.8 sec   442 KBytes  30.0 Kbits/sec
[1716] Server Report:
[1716]  0.0-120.8 sec   442 KBytes  30.0 Kbits/sec  1.165 ms    0/  308 (0%)
```

Figure 5.10 (b): "Iperf" tool is sending 30Kbps UDP traffic to destination 192.168.3.52 for 120 seconds from PC1

Above figures 5.10 (a) and (b) shows traffic of 12Lbps and 30Kbps been sent which could be seen at tunnel interfaces shown in figure 5.11 (a) and (b)


```
PE1#sh int tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of Loopback0 (10.11.0.8)
  MTU 1514 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 73/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.11.0.8, destination 10.12.0.8
  Tunnel protocol/transport Label Switching

  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output 00:16:07, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 29000 bits/sec, 2 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1396 packets output, 1290889 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Figure 5.11 (a): Tunnel 0 interface bandwidth 29Kbps

```
PE1#sh int tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of Loopback0 (10.11.0.8)
  MTU 1514 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 28/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.11.0.8, destination 10.12.0.8
  Tunnel protocol/transport Label Switching

  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output 00:00:48, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 11000 bits/sec, 1 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     462 packets output, 204562 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Figure 5.11 (b): Tunnel 1 interface bandwidth 11Kbps

Figure 5.12 represents the flooding during change in interface state of a tunnel 1 to the whole topology at C2. The state information is flooded in all 3 links of C2.

```
**********Tunnel 1 manually shutdown**********

*Jan 11 12:27:36.166: TE-LM-ADMIT: Admission control received RSVP Resv delete notification for 10.11.0.8 1_28 (10.
12.0.8)
*Jan 11 12:27:36.166: TE-LM-RSRC: TagRM Delete Downstream:: dest: 10.12.0.8/1, src: 10.11.0.8/28, Fa0/0 --> Se0/
0/0.201
*Jan 11 12:27:36.170: TE-LM-RSRC: TagRM Response: Downstream: op: 3, dest: 10.12.0.8/1, src: 10.11.0.8/28, up_tag:
4294967294, down_tag: 4294967294, Error: 0
*Jan 11 12:27:36.170: TE-LM-BW: link Se0/0/0.201 (Downstream): unlocking Global Pool 32 kbits/sec at keep-priority 2
*Jan 11 12:27:36.170: TE-LM-BW: link Se0/0/0.201 (Downstream): held Global Pool 0 [0]; locked 0 [0] at keep-priority 2
*Jan 11 12:27:36.170: TE-LM-ADV: LSA: link Se0/0/0.201: Downstream Global Pool bandwidth change at keep_priority, 7,
triggering flooding
*Jan 11 12:27:36.170: TE-LM-ADV: area isis  level-2: *** Flooding node information ***
*Jan 11 12:27:36.170:   System Information::
*Jan 11 12:27:36.170:     Flooding Protocol:    ISIS
*Jan 11 12:27:36.170:   Header Information::
*Jan 11 12:27:36.170:     IGP System ID:        0100.1100.0001.00
*Jan 11 12:27:36.170:     MPLS TE Router ID:    10.11.0.1
*Jan 11 12:27:36.170:     Flooded Links:        3
*Jan 11 12:27:36.170:   Link ID::  0 (FastEthernet0/0)
*Jan 11 12:27:36.170:     Link Subnet Type:     Point-to-Point
*Jan 11 12:27:36.170:     Link IP Address:      10.11.1.2
*Jan 11 12:27:36.170:     Neighbor:             ID 0100.1100.0008.00, IP 10.11.1.1
*Jan 11 12:27:36.170:     TE metric:            10
*Jan 11 12:27:36.170:     IGP metric:           10
*Jan 11 12:27:36.170:     SRLGs:                None
*Jan 11 12:27:36.170:     Physical Bandwidth:   128 kbits/sec
*Jan 11 12:27:36.170:     Res. Global BW:       96 kbits/sec
*Jan 11 12:27:36.170:     Res. Sub BW:          0 kbits/sec
*Jan 11 12:27:36.170:     Downstream::
*Jan 11 12:27:36.170:                                 Global Pool   Sub Pool
*Jan 11 12:27:36.170:                                 -----------   ----------
*Jan 11 12:27:36.170:       Reservable Bandwidth[0]:          96           0 kbits/sec
*Jan 11 12:27:36.170:       Reservable Bandwidth[1]:          96           0 kbits/sec
*Jan 11 12:27:36.170:       Reservable Bandwidth[2]:          96           0 kbits/sec
*Jan 11 12:27:36.170:       Reservable Bandwidth[3]:          96           0 kbits/sec
*Jan 11 12:27:36.170:       Reservable Bandwidth[4]:          96           0 kbits/sec
*Jan 11 12:27:36.170:       Reservable Bandwidth[5]:          96           0 kbits/sec
*Jan 11 12:27:36.170:       Reservable Bandwidth[6]:          96           0 kbits/sec
*Jan 11 12:27:36.170:       Reservable Bandwidth[7]:          96           0 kbits/sec
*Jan 11 12:27:36.174:     Attribute Flags:      0x00000000
```


Figure 5.12: Triggered flooding at C2 during T1 shutdown at PE1. The highlighted portion shows T1 bandwidth 32Kbps been released during tunnel shutdown and this information is flooded to all TE enabled three links at router C2.

5.3 QoS Marking using Differentiated Services Code Point (DSCP)

The generated UDP packets were classified based on the table 5.13 below at the edge router PE1 as premium and silver service levels. Premium service is for UDP sessions marked with priority value AF21 (18) at the input are queued with a priority bandwidth of 48kbps at the output fast Ethernet0/0 to the sever 192.168.3.10. Silver service is for UDP sessions with the server at 192.168.7.10 and the packets are marked with AF11 (10) at the input and queued with a priority bandwidth of 32kbps at fast Ethernet 0/0. Any other packets are classified as default service with no priority and rate limited to 64kbps at the output interface fast Ethernet0/0. Servers 192.168.3.10 and 192.168.7.10 are located in PE3 and 192.168.2.50 is the Ethernet interface of router PE2 in the figure 5.2.

Without QoS control and TE all packets destined to customers at PE3 would take the default shortest path of PE1, C2, C3, and PE3 thus idling the alternate path PE1, C2, C1, C3 and PE3 . The backbone capacity of core router C2 serial interface0/0/0 is limited to 128Kbps and when the bit rate exceeds 128kbps, figure 5.14 shows packet drops at this interface. Figure 5.16 shows the UDP traffic generated to each network. By applying strict QoS control to low priority best effort data at the edge router PE1 output interface Ethernet0/0 and only allowing premium and silver traffic to use the shortest path, packet drops are avoided at C2 serial interface0/0/0 as shown in figure 5.15. The best effort data still continues to reach customer at 192.168.2.50 at PE2 from PE1 but excess of 64kbps traffic is dropped at PE1 as shown in figure 5.16. Premium and silver class traffic after queuing at the output interface can be routed via any tunnels T0 or T1 to destination networks at PE3 as described in section 5.2.

Service	DSCP Markings	Destination network
Premium	AF21 (18)	192.168.3.10
Silver	AF11 (10)	192.168.7.10
Best Effort	NIL	192.168.2.50

Table 5.13: Classifying of packets based on DSCP marking


```
C2#sh int serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 17/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  LMI enq sent  98, LMI stat recvd 97, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 2/64, broadcasts sent/dropped 774/0, interface broadcasts 740
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters 00:16:19
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 196
  Queueing strategy: fifo
  Output queue: 40/40 (size/max)
  5 minute input rate 5000 bits/sec, 1 packets/sec
  5 minute output rate 105000 bits/sec, 22 packets/sec
     2332 packets input, 1033028 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     14706 packets output, 10469224 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Figure 5.14: Packet drops at C2 serial interface 0/0/0, Queue type is FIFO

```
C2#sh int serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 12/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  LMI enq sent  416, LMI stat recvd 416, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 1023  LMI type is CISCO  frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 3237/0, interface broadcasts 3099
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 01:09:22
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 4000 bits/sec, 0 packets/sec
  5 minute output rate 76000 bits/sec, 12 packets/sec
     4868 packets input, 1929186 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

Figure 5.15: Packet drops are avoided at C2 serial interface 0/0/0 after QoS at PE1 router

```
C:\1\iperf>iperf.exe -u -c  192.168.3.10 -t1800 -i1 -b40K
------------------------------------------------------------
Client connecting to 192.168.3.10, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
[1716] local 192.168.1.10 port 1665 connected with 192.168.3.10 port 5001
[ ID] Interval       Transfer     Bandwidth
[1716]  0.0- 1.0 sec  5.74 KBytes  47.0 Kbits/sec
[1716]  1.0- 2.0 sec  4.31 KBytes  35.3 Kbits/sec


C:\2>iperf.exe -u -c 192.168.7.10 -t1800 -i1 -b30K
------------------------------------------------------------
Client connecting to 192.168.7.10, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
[1712] local 192.168.1.10 port 1666 connected with 192.168.7.10 port 5001
[ ID] Interval       Transfer     Bandwidth
[1712]  0.0- 1.0 sec  4.31 KBytes  35.3 Kbits/sec
[1712]  1.0- 2.0 sec  4.31 KBytes  35.3 Kbits/sec


C:\1\iperf>iperf.exe -u -c 192.168.2.50 -t1800 -i1 -b150K
------------------------------------------------------------
Client connecting to 192.168.2.50, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
[1724] local 192.168.1.10 port 1670 connected with 192.168.2.50 port 5001
[ ID] Interval       Transfer     Bandwidth
[1724]  0.0- 1.0 sec  18.7 KBytes   153 Kbits/sec
[1724]  1.0- 2.0 sec  18.7 KBytes   153 Kbits/sec
```


Figure 5.16: UDP packet generation using "iperf" tool

```
PE1#sh policy-map interface fastEthernet 0/0
 FastEthernet0/0

  Service-policy output: oubound

    queue stats for all priority classes:
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 156/122460

    Class-map: premium (match-all)
      10631 packets, 16036812 bytes
      30 second offered rate 41000 bps, drop rate 0 bps
      Match: qos-group 1
      Match:  dscp af21 (18)
      Priority: 48 kbps, burst bytes 1500, b/w exceed drops: 0


    Class-map: silver (match-all)
      8039 packets, 12121882 bytes
      30 second offered rate 30000 bps, drop rate 0 bps
      Match: qos-group 2
      Match:  dscp af11 (10)
      Priority: 32 kbps, burst bytes 1500, b/w exceed drops: 0


    Class-map: class-default (match-any)
      26012 packets, 37159506 bytes
      30 second offered rate 156000 bps, drop rate 92000 bps
      Match: any

      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 2314/822106
      police:
          cir 64000 bps, bc 2000 bytes
        conformed 10626 packets, 15880369 bytes; actions:
          transmit
        exceeded 13226 packets, 20050616 bytes; actions:
          drop
        conformed 61000 bps, exceed 92000 bps
```


Figure 5.17: marked packets are queued into their appropriate queues and excess low priority are dropped at class-default

```
PE1#sh queue fastEthernet 0/0
 FastEthernet0/0 queue size 0, 0 bytes
        pkts output 0, wfq drops 0, nobuffer drops 0
 WFQ: aggregate queue limit 25000 max available buffers 25000

     Class 1: bandwidth 48 exceed drops 0
     Class 2: bandwidth 32 exceed drops 0
     Priority Queue: limit 64 qsize 0 packets, 0 bytespkts output 0 drops 0
```

Figure 5.18: Class based queue at PE1 output interface

```
PE1#sh policy-map interface fastEthernet 0/1

  service-policy input: SETDSCP

    Class-map: voice (match-all)
      58 packets, 82176 bytes
      5 minute offered rate 4000 bps, drop rate 0 bps
      Match: access-group 101
      QoS Set
        qos-group 1
          Packets marked 58
        dscp af21
          Packets marked 58

    Class-map: data (match-all)
      15 packets, 16988 bytes
      5 minute offered rate 2000 bps, drop rate 0 bps
      Match: access-group 102
      QoS Set
        qos-group 2
          Packets marked 15
        dscp af11
          Packets marked 15

    Class-map: class-default (match-any)
      88 packets, 113629 bytes
      5 minute offered rate 4000 bps, drop rate 0 bps
      Match: any


PE1#sh access-lists

Standard IP access list r0
Extended IP access list 101
    10 permit ip any host 192.168.3.10 (157 matches)
Extended IP access list 102
    10 permit ip any host 192.168.7.10 (45 matches)
```

Figure 5.19: Packets are matched at the input interface PE1 and marked accordingly to DSCP markings

Classified packets are queued using a classed based queuing as shown in figure 5.17. Figures 5.18 and 5.19 show the outbound policy map "OUBOUND"" and the inbound policy map "SETDSCP" at the interfaces Ethernet 0/0 and 0/1 at PE1 respectively. The packets are matched against access control lists at the input marked using DSCP values and queued at the outbound interface to queues.

5.4 IP Service Level Agreements (SLA) customer reports

The figures 5.20 (a) to (d) shows reports for a test "customer-A" of an operational test network from a customer end CISCO 1841 router to the nearest edge router 7604, the variation of round trip response time, jitter, availability and http transaction time for a test VPN "customer A". Results are queried every 10 minutes except availability from the customer nodes up-to the MPLS VPN network Availability calculated hourly bases.

Other parameters used are,

- Source to destination link – WiMAX access
- LINK signal levels at time of testing – uplink / downlink SNR is 25.4 / 29 dB
- Shortest estimated distance from customer to base station is approximately - 500m
- Link bandwidth – 128Kbps (access)
- Source IP address (customer router) – 119.235.6.42
- Destination IP address (edge router) – 119.235.6.41
- Test Customer layer 3 VPN name – COL3-TEST2-128K-ILL

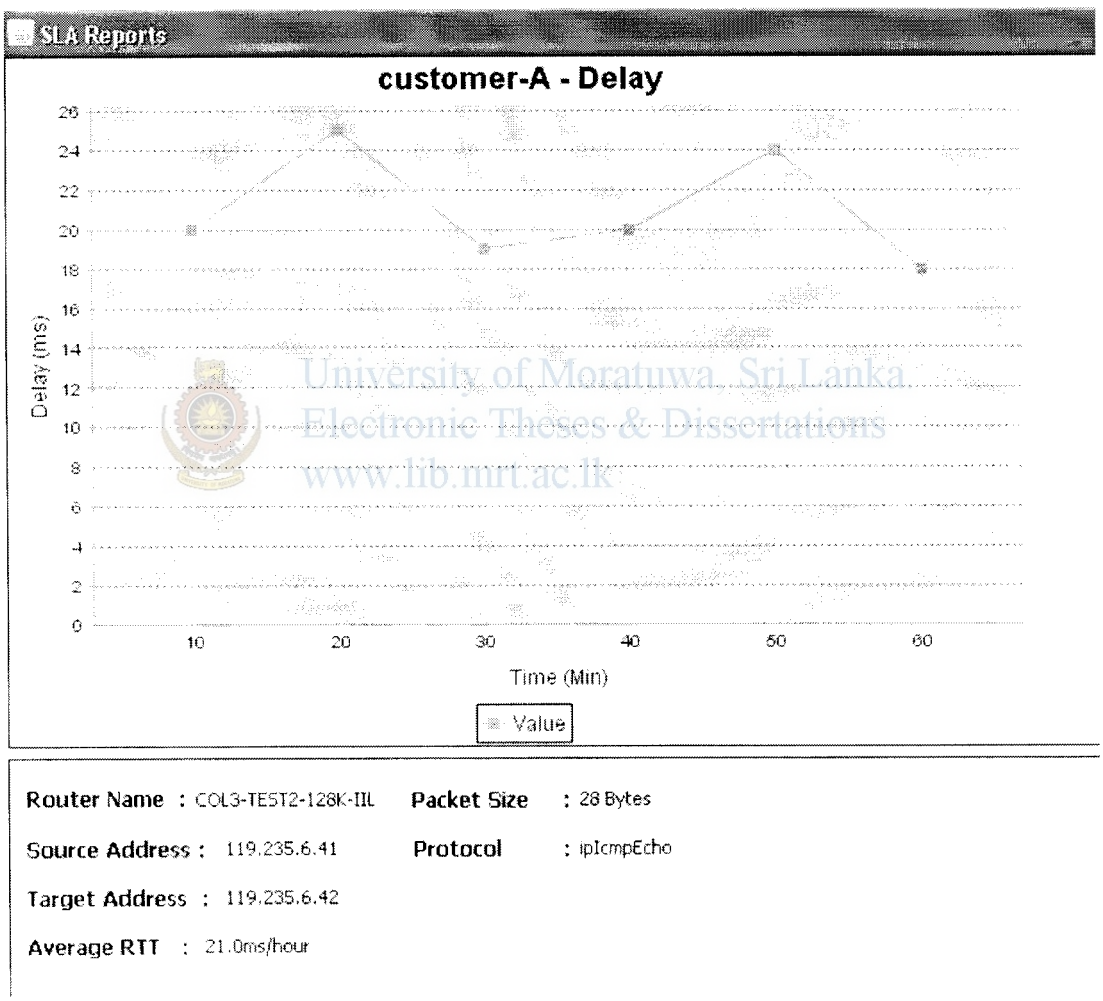
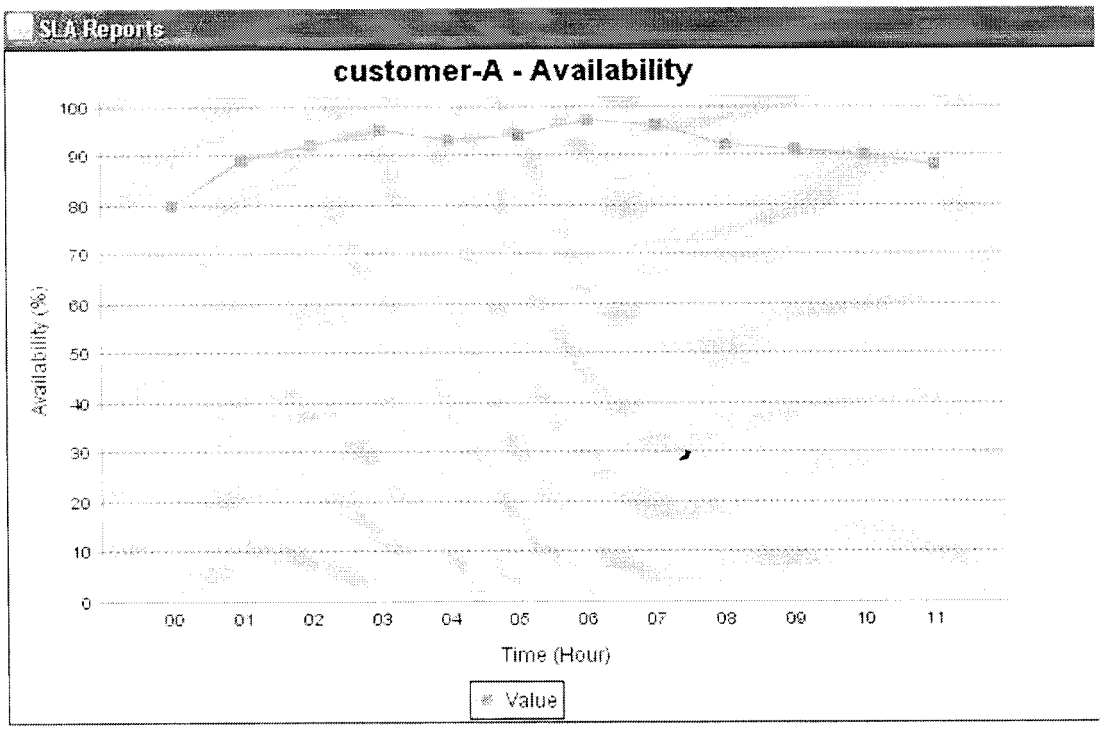


Figure 5.20 (a): Round trip time (RTT) response using "icmpecho" protocol



Router Name : COL3-TEST2-128K-IIL

Source Address : 119.235.6.41

Target Address : 119.235.6.42

Avg Availability : 91.42%

Figure 5.20 (b): Availability of link from source to destination. Average availability is 91.42%

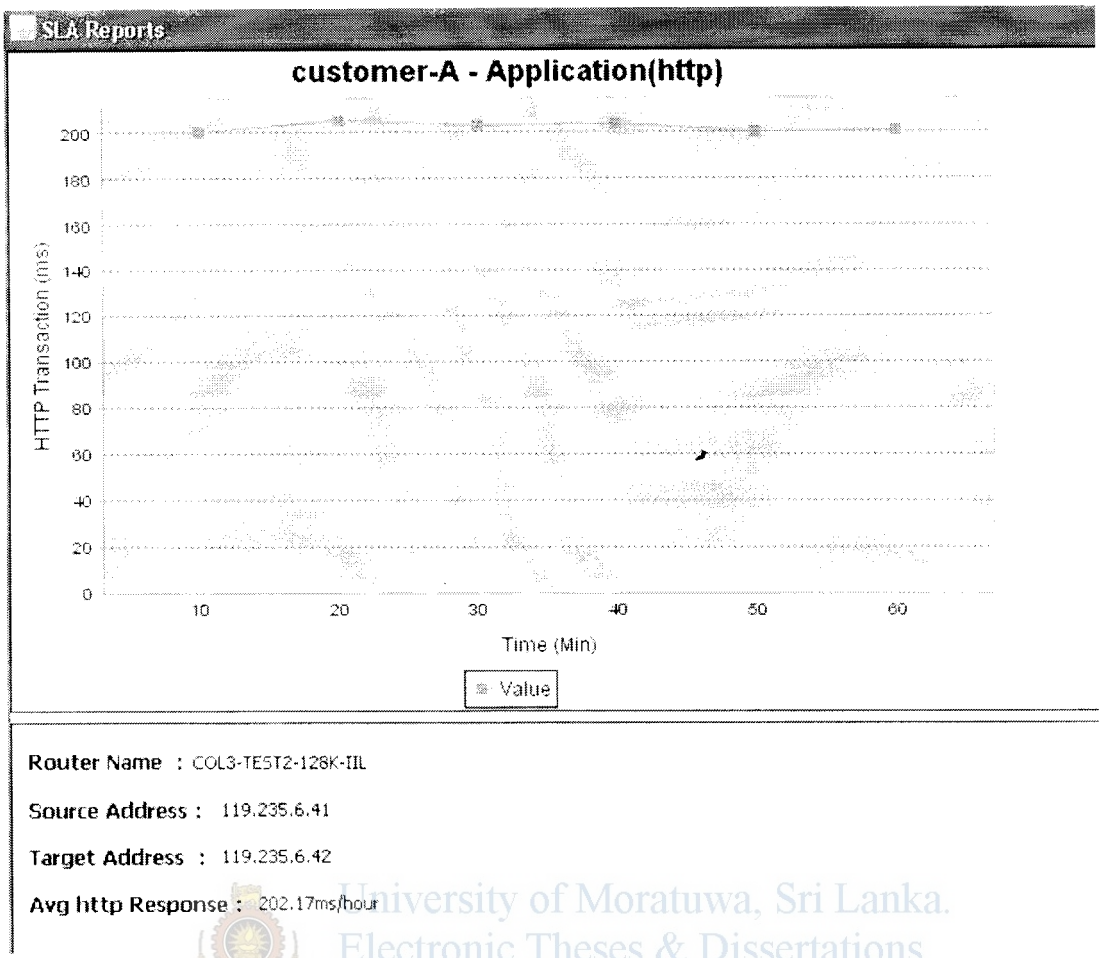
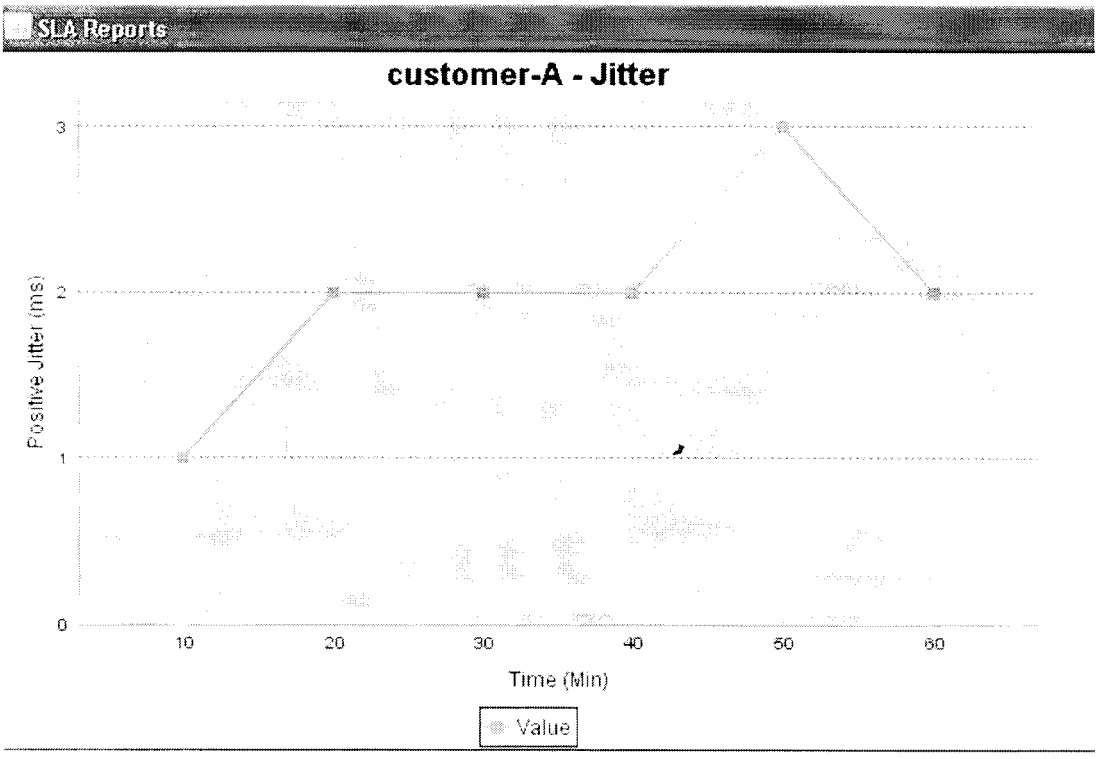


Figure 5.20 (c): HTTP transaction time to a web-server. Average time is 202.17 ms/hour



Router Name : COL3-TEST2-128K-IIL

Source Address : 119.235.6.41

Target Address : 119.235.6.42

Avg Jitter : 2.0ms/hour

Figure 5.20 (d): Source to Destination positive Jitter. Average positive source to destination jitter is 2ms/hour

Chapter 6

Conclusion

In this thesis the integration of TE tunnels in the IP core together with IP SLA program to produce performance metrics to guarantee and ensure end to end QoS for customers is analyzed. The test results showed that critical traffic can be given a priority queue if QoS is implemented and the best way to implement QoS is to use differentiated services markings due to the broader classification of classes available. Thus combined use of MPLS-TE and QoS for multiservice traffic in an IP network, service providers can ensure end to end guaranteed services and SLAs can be ensured to their customers by providing SLA performance reports using the IP SLA program. This program can be a feasible tool for growing service providers without any initial investment compared to commercial expensive software available. Also efficient use of backbone bandwidth in a fair way can be achieved. Summary of the project results is discussed below.

Discussion of Results

Core backbone WAN links are an expensive resource in a service provider's OPEX and MPLS-TE is one of the best ways to efficiently utilize them. The problem with routing a packet based on destination involves that every hop packet takes along the route is decided based on routing table and generally this path is the routing protocol's shortest path which may not be the best path always. For any reason if this forwarding path is experiencing longer delays or become congested, critical traffic may experience packet drops.

Two tunnels were created to divert certain traffic through alternative path and results show both backbone links are utilized. This was shown by tunnel with priority 2 reserved 32Kbps from the 96Kbps pool and tunnel with priority 7 reserved 48Kbps from 64Kbps pool. This also demonstrates more important tunnels (lower priority number) are free to push other tunnels and are allowed to get the required bandwidth from the total reserved pool. Both tunnels occupied 83% of the reserved bandwidth of 96Kbps using the reservation protocol. The generated UDP traffic of 30Kbps and 12Kbps were routed accordingly in proper tunnels. The routing table also correctly showed both tunnels T0 and

T1 for the desired destination as two alternative physical paths. It is further shown in the debug messages, that any change in tunnel states (T1) caused triggered flooding of the link states to all connected TE enabled links at router C2 regardless of periodic flooding. The classification of packets based on DSCP classes showed that they are class based queued accordingly at the output interface of PE1 and the packet drops at C2 serial interface were avoided. The best effort data packets which exceeded rate of 64kbps were dropped at PE1 output interface. The IP SLA performance report program for the test Customer-A on an operational network generated accurate average acceptable results for round trip delay, availability, jitter (source to destination) and http transaction time.

6.1 Future Works

When dealing with network growth and expansion TE engineering plays a significant role. Manual intervention is required to change reservation bandwidth and therefore detailed information on traffic patterns are required to correctly size the tunnel. More efficient use of tunnel bandwidth can be obtained by TE auto-bandwidth option which watches the traffic rate on a tunnel interface and periodically resizes the bandwidth on the tunnel interface to more closely align with the traffic that's actually going down the tunnel. As tunnels are set up and torn down across interfaces, the amount of available bandwidth on an interface changes in accordance with the reservations across an interface and when to advertise this changes to entire topology is a major concern. This could potentially be a tremendous amount of flooding enough to consume bandwidth on the network and significant processing on the router in large TE network having several tunnels. Therefore further analysis can be done to optimize flooding of TE tunnel changes for the particular IGP protocol used. Also, to maximize the efficiency and performance of traffic types advance TE features such as fast reroute, and DiffServ-aware TE can be deployed. Furthermore the deployment of MPLS-TE in mobile access network could lead to several improvements compared to traditional mobile IP transport. The SLA program could be further developed to incorporate more specific application performance parameters such as database access response times. Since new technologies are emerging all the time there would be different concepts and methods to tackle the growing volumes of different traffic types in the core backbone.

APPENDIX A

GNS3 Simulator configuration for initial TE tunnels setup

```
******Router C1***********

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$2Uk3$DmT2/2VblPBpELm2H6XqU1
!
no aaa new-model
ip subnet-zero
!
ip cef
mpls label protocol ldp
mpls traffic-eng tunnels
!
interface Loopback0
 description **** Management ****
 ip address 10.13.0.1 255.255.255.255
!
interface FastEthernet0/0
 description **** Conencted to C2 FE3/0 ****
 ip address 10.13.2.2 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls traffic-eng tunnels
 tag-switching ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 512
!
interface FastEthernet1/0
 description **** Conencted to C3 FE1/0 ****
 ip address 10.12.2.2 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls traffic-eng tunnels
 tag-switching ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 512
!
router isis TestLab
```

```
 net 49.0001.0100.1300.0001.00
 is-type level-2-only
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
 passive-interface Loopback0
!
ip http server
ip classless
!
line con 0
line aux 0
line vty 0 4
 login
!
end

******Router C2***********

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$T3xy$X4ZHL0/W3sge1ewng0Pyx.
!
no aaa new-model
ip subnet-zero
!
ip cef
mpls label protocol ldp
mpls traffic-eng tunnels
tag-switching tdp router-id Loopback0
!
interface Loopback0
 description **** Management ****
 ip address 10.11.0.1 255.255.255.255
!
interface FastEthernet0/0
 description **** Connected to PE1 FE0/0 ****
 ip address 10.11.1.2 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls traffic-eng tunnels
 tag-switching ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 512
!
interface FastEthernet1/0
```

```
 description **** Connected to PE2 FE0/0 ****
 ip address 10.13.1.2 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls label protocol ldp
 tag-switching ip
 isis circuit-type level-2-only
 isis network point-to-point
!
interface FastEthernet2/0
 description **** Connected to C3 FE0/0 ****
 ip address 10.11.2.1 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls traffic-eng tunnels
 tag-switching ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 512
!
interface FastEthernet3/0
 description **** Connected to C1 FE0/0 ****
 ip address 10.13.2.1 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls traffic-eng tunnels
 tag-switching ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 512
!
router isis TestLab
 net 49.0001.0100.1100.0001.00
 is-type level-2-only
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
 passive-interface Loopback0
!
ip http server
ip classless
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

```
******Router C3***********

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C3
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$/0Yw$fb2B32DRT8ppITnZh3iFs1
!
no aaa new-model
ip subnet-zero
!
!
ip cef
mpls label protocol ldp
mpls traffic-eng tunnels
!
interface Loopback0
 description **** Management ****
 ip address 10.12.0.1 255.255.255.255
!
interface FastEthernet0/0
 description **** Conencted to C2 FE2/0 ****
 ip address 10.11.2.2 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls traffic-eng tunnels
 tag-switching ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 512
!
interface FastEthernet1/0
 description **** Conencted to C1 FE1/0 ****
 ip address 10.12.2.1 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls traffic-eng tunnels
 tag-switching ip
 isis circuit-type level-2-only
 isis network point-to-point
```

```
 ip rsvp bandwidth 512
!
interface FastEthernet2/0
 description **** Conencted to PE3 FE0/0 ****
 ip address 10.12.1.2 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls traffic-eng tunnels
 tag-switching ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 512
!
router isis TestLab
 net 49.0001.0100.1200.0001.00
 is-type level-2-only
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
 passive-interface Loopback0
!
ip http server
ip classless
!
line con 0
line aux 0
line vty 0 4
 login
!
End

******Router PE1***********

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE1
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 errors
enable secret 5 $1$nC0F$jA3OhQ02.w/2XcqLaeu1B.
!
no aaa new-model
ip subnet-zero
!
ip cef
```

```
mpls label protocol ldp
mpls ldp neighbor 10.13.0.8 targeted ldp
mpls ldp neighbor 10.12.0.8 targeted ldp
mpls traffic-eng tunnels
tag-switching tdp router-id Loopback0
!
interface Loopback0
 description **** Management ****
 ip address 10.11.0.8 255.255.255.255
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel destination 10.12.0.8
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth  256
 tunnel mpls traffic-eng path-option 10 explicit name pathc1c2c3
!
interface Tunnel1
 ip unnumbered Loopback0
 tunnel destination 10.12.0.8
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth  256
 tunnel mpls traffic-eng path-option 20 explicit name pathc2c3
!
interface FastEthernet0/0
 description **** Connected to C2 FE0/0 ****
 ip address 10.11.1.1 255.255.255.252
 ip router isis TestLab
 ip flow ingress
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls traffic-eng tunnels
 tag-switching ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 512
!
interface FastEthernet1/0
 description **** Conencted to PC ****
 ip address 192.168.1.50 255.255.255.0
 duplex auto
 speed auto
!
router isis TestLab
 net 49.0001.0100.1100.0008.00
 is-type level-2-only
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
 passive-interface Loopback0
!
router bgp 65001
```

```
 bgp router-id 10.11.0.8
 bgp log-neighbor-changes
 neighbor 10.12.0.8 remote-as 65001
 neighbor 10.12.0.8 description **** Location C PE3 ****
 neighbor 10.13.0.8 remote-as 65001
 neighbor 10.13.0.8 description **** Location A PE2 ****
 neighbor 10.13.0.8 update-source Loopback0
 !
 address-family ipv4
 neighbor 10.12.0.8 activate
 neighbor 10.13.0.8 activate
 neighbor 10.13.0.8 send-community extended
 no auto-summary
 no synchronization
 network 192.168.1.0
 exit-address-family
!
no ip http server
ip classless
!
ip explicit-path name pathc1c2c3 enable
 next-address 10.11.1.2
 next-address 10.13.2.2
 next-address 10.12.2.1
 next-address 10.12.1.1
!
ip explicit-path name pathc2c3 enable
 next-address 10.11.1.2
 next-address 10.11.2.2
 next-address 10.12.1.1
!
access-list 101 permit ip any host 192.168.3.50
route-map voice permit 10
 match ip address 101
 set interface Tunnel1
!
line con 0
line aux 0
line vty 0 4
 login
!
end


******Router PE2***********

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE2
!
boot-start-marker
boot-end-marker
!
```

```
enable secret 5 $1$8uMM$814bHiOOOTv73k63buRjk1
!
no aaa new-model
ip subnet-zero
!
ip cef
mpls label protocol ldp
mpls ldp neighbor 10.11.0.8 targeted ldp
mpls ldp neighbor 10.12.0.8 targeted ldp
tag-switching tdp router-id Loopback0
!
interface Loopback0
 description **** Management ****
 ip address 10.13.0.8 255.255.255.255
!
interface Loopback1
 ip address 192.168.6.1 255.255.255.0
!
interface FastEthernet0/0
 description **** Conencted to C2 FE1/0 ****
 ip address 10.13.1.1 255.255.255.252
 ip router isis TestLab
 ip flow ingress
 duplex auto
 speed auto
 mpls label protocol ldp
 tag-switching ip
 isis network point-to-point
 ip rsvp bandwidth 512 512
!
interface FastEthernet1/0
 description **** LAN ****
 ip address 192.168.2.50 255.255.255.0
 duplex auto
 speed auto
!
router isis TestLab
 net 49.0001.0100.1300.0008.00
 is-type level-2-only
 metric-style wide
 passive-interface Loopback0
!
router bgp 65001
 bgp router-id 10.13.0.8
 bgp log-neighbor-changes
 neighbor 10.11.0.8 remote-as 65001
 neighbor 10.11.0.8 description ****Location A PE1 ****
 neighbor 10.11.0.8 update-source Loopback0
 neighbor 10.12.0.8 remote-as 65001
 neighbor 10.12.0.8 description **** Location C PE3 ****
 !
 address-family ipv4
 neighbor 10.11.0.8 activate
 neighbor 10.11.0.8 send-community extended
 neighbor 10.12.0.8 activate
 no auto-summary
 no synchronization
```

```
 network 20.20.20.0 mask 255.255.255.0
 network 192.168.2.0
 network 192.168.6.0
 exit-address-family
!
no ip http server
ip classless
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

******Router PE3***********

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE3
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$0hXT$J.9iYW18JBgPFXJqXqW0p0
!
no aaa new-model
ip subnet-zero
!
ip cef
mpls label protocol ldp
mpls ldp neighbor 10.11.0.8 targeted ldp
mpls ldp neighbor 10.13.0.8 targeted ldp
mpls traffic-eng tunnels
tag-switching tdp router-id Loopback0
!
interface Loopback0
 description **** Management ****
 ip address 10.12.0.8 255.255.255.255
!
interface Loopback1
 ip address 192.168.7.1 255.255.255.0
!
interface Tunnel0
 ip unnumbered Loopback0
 shutdown
 tunnel destination 10.11.0.8
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
```

```
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth  256
 tunnel mpls traffic-eng path-option 10 explicit name pathc3c1c2
!
interface FastEthernet0/0
 description **** Connected to C3 FE2/0 ****
 ip address 10.12.1.1 255.255.255.252
 ip router isis TestLab
 ip flow ingress
 duplex auto
 speed auto
 mpls label protocol ldp
 mpls traffic-eng tunnels
 tag-switching ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 512
!
interface FastEthernet1/0
 description **** LAN ****
 ip address 192.168.3.50 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2/0
 description **** LAN1 ****
 ip address 203.143.36.1 255.255.255.0
 duplex auto
 speed auto
!
router isis TestLab
 net 49.0001.0100.1200.0012.00
 is-type level-2-only
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
 passive-interface Loopback0
!
router bgp 65001
 bgp router-id 10.12.0.8
 bgp log-neighbor-changes
 neighbor 10.11.0.8 remote-as 65001
 neighbor 10.11.0.8 description **** Location A PE1 ****
 neighbor 10.11.0.8 update-source Loopback0
 neighbor 10.13.0.8 remote-as 65001
 neighbor 10.13.0.8 description **** Location A PE2 ****
 neighbor 10.13.0.8 update-source Loopback0
 !
 address-family ipv4
```

```
 neighbor 10.11.0.8 activate
 neighbor 10.13.0.8 activate
 no auto-summary
 no synchronization
 network 192.168.3.0
 network 192.168.7.0
 network 203.143.36.0
 exit-address-family
!
ip http server
ip classless
!
ip explicit-path name pathc3c1c2 enable
 next-address 10.12.1.2
 next-address 10.12.2.2
 next-address 10.13.2.1
 next-address 10.11.1.1
!
ip explicit-path name pathc3c2 enable
 next-address 10.12.1.2
 next-address 10.11.2.1
 next-address 10.11.1.1
!
line con 0
line aux 0
line vty 0 4
 login
!
End
```

APPENDIX B

Real Lab Simulated configuration for initial TE tunnels setup

```
******Router C1***********

=~=~~= PuTTY log 2009.01.13 08:46:48 =~=~=~=~=~=
C1#wr t
Building configuration...

Current configuration : 1912 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$W28n$CaVSz6MOf2zFbBwLzMOU6/
!
no aaa new-model
!
dot11 syslog
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip cef
!
no ipv6 cef
!
multilink bundle-name authenticated
!
mpls traffic-eng tunnels
mpls label protocol ldp
!
voice-card 0
 no dspfarm
!
archive
 log config
  hidekeys
!
interface Loopback0
 ip address 10.13.0.1 255.255.255.255
 ip router isis TestLab
!
interface FastEthernet0/0
 ip address 172.25.103.185 255.255.252.0
 duplex auto
 speed auto
 mpls ip
```

```
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 encapsulation frame-relay
 no fair-queue
 clock rate 128000
!
interface Serial0/0/0.102 point-to-point
 ip address 10.13.2.2 255.255.255.252
 ip router isis TestLab
 snmp trap link-status
 mpls traffic-eng tunnels
 mpls ip
 frame-relay interface-dlci 102
 isis circuit-type level-2-only
 ip rsvp bandwidth 96
!
interface Serial0/0/0.103 point-to-point
 ip address 10.12.2.2 255.255.255.252
 ip router isis TestLab
 snmp trap link-status
 mpls traffic-eng tunnels
 mpls ip
 frame-relay interface-dlci 103
 isis circuit-type level-2-only
 ip rsvp bandwidth 96
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router isis TestLab
 net 49.0001.0100.1300.0001.00
 is-type level-2-only
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
mpls ldp router-id Loopback0
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password XXXX
```

```
 login
!
scheduler allocate 20000 1000
end

******Router C2***********

=~=~=~PuTTY log 2009.01.13 08:52:42 =~=~=~=~=~=~=~
C2#wr t
Building configuration...

Current configuration : 2546 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C2
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$31O7$mIPKBVETTxFCMvXnSuo3a/
!
no aaa new-model
!
dot11 syslog
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip cef
!
no ipv6 cef
!
multilink bundle-name authenticated
!
mpls traffic-eng tunnels
mpls label protocol ldp
!
voice-card 0
 no dspfarm
!
archive
 log config
  hidekeys
!
interface Loopback0
 ip address 10.11.0.1 255.255.255.255
 ip router isis TestLab
!
interface FastEthernet0/0
 description *********** Link to PE1-f0/0 ***********
 ip address 10.11.1.2 255.255.255.252
 ip router isis TestLab
 duplex auto
```

```
 speed auto
 mpls traffic-eng tunnels
 mpls traffic-eng flooding thresholds up 25 50 100
 mpls traffic-eng flooding thresholds down 100 50 25
 mpls ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 96
!
interface FastEthernet0/1
 description **** Connected to PE2 FE 0/0 ****
 ip address 10.13.1.2 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls traffic-eng tunnels
 mpls ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 96
!
interface Serial0/0/0
 no ip address
 encapsulation frame-relay
 no fair-queue
 clock rate 128000
!
interface Serial0/0/0.201 point-to-point
 description *********** Link to C1-s0/0/0.102  ***********
 ip address 10.13.2.1 255.255.255.252
 ip router isis TestLab
 snmp trap link-status
 mpls traffic-eng tunnels
 mpls ip
 frame-relay interface-dlci 201
 isis circuit-type level-2-only
 ip rsvp bandwidth 96
!
interface Serial0/0/0.203 point-to-point
 description *********** Link to C3-s0/0/0.302  ***********
 ip address 10.11.2.1 255.255.255.252
 ip router isis TestLab
 snmp trap link-status
 mpls traffic-eng tunnels
 mpls ip
 frame-relay interface-dlci 203
 isis circuit-type level-2-only
 ip rsvp bandwidth 96
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router isis TestLab
 net 49.0001.0100.1100.0001.00
 is-type level-2-only
```

```
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
mpls ldp router-id Loopback0
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password XXXX
 login
!
scheduler allocate 20000 1000
end

******Router C3***********

=~=~=~=~= PuTTY log 2009.01.13 08:54:23 =~=~=~=~=
C3#wr t
Building configuration...

Current configuration : 2236 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname C3
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$E664$pPwAbAOZvr5K6aXbGuhNn/
!
no aaa new-model
!
dot11 syslog
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip cef
!
no ipv6 cef
!
multilink bundle-name authenticated
!
mpls traffic-eng tunnels
mpls label protocol ldp
!
```

```
voice-card 0
 no dspfarm
!
archive
 log config
  hidekeys
!
interface Loopback0
 ip address 10.12.0.1 255.255.255.255
 ip router isis TestLab
!
interface FastEthernet0/0
 description ********** Link to PE3- f0/0  **********
 ip address 10.12.1.2 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls traffic-eng tunnels
 mpls ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 96
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 encapsulation frame-relay
 no fair-queue
 clock rate 128000
!
interface Serial0/0/0.301 point-to-point
 description ********** Link to C1-s0/0/0.103  **********
 ip address 10.12.2.1 255.255.255.252
 ip router isis TestLab
 snmp trap link-status
 mpls traffic-eng tunnels
 mpls ip
 frame-relay interface-dlci 301
 isis circuit-type level-2-only
 ip rsvp bandwidth 96
!
interface Serial0/0/0.302 point-to-point
 description ********** Link to C2-s0/0/0.203  **********
 ip address 10.11.2.2 255.255.255.252
 ip router isis TestLab
 snmp trap link-status
 mpls traffic-eng tunnels
 mpls ip
 frame-relay interface-dlci 302
 isis circuit-type level-2-only
 ip rsvp bandwidth 96
!
```

```
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router isis TestLab
 net 49.0001.0100.1200.0001.00
 is-type level-2-only
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
mpls ldp router-id Loopback0
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password XXXX
 login
!
scheduler allocate 20000 1000
end

******Router PE1**********

=~=~=~= PuTTY log 2009.01.13 08:55:31 =~=~=~=~=~=~=
wr t
Building configuration...

Current configuration : 4052 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$S3Yk$gKLwOR/qgbHwhZ7bB8GmX0
!
no aaa new-model
!
dot11 syslog
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip cef
```

```
!
no ipv6 cef
!
multilink bundle-name authenticated
!
!
mpls traffic-eng tunnels
mpls label protocol ldp
!
voice-card 0
 no dspfarm
!
archive
 log config
  hidekeys
!
class-map match-all data
 match access-group 102
class-map match-all silver
 match qos-group 2
 match  dscp af11
class-map match-all voice
 match access-group 101
class-map match-all premium
 match qos-group 1
 match  dscp af21
!
policy-map SETDSCP
 class voice
  set qos-group 1
  set dscp af21
 class data
  set qos-group 2
  set dscp af11
policy-map oubound
 class premium
    priority 48
 class silver
    priority 32
 class class-default
    police 64000 exceed-action drop
interface Loopback0
 ip address 10.11.0.8 255.255.255.255
 ip router isis TestLab
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel destination 10.12.0.8
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 48
 tunnel mpls traffic-eng path-option 10 explicit name pathc2c3
 no routing dynamic
!
interface Tunnel1
 ip unnumbered Loopback0
```

```
 tunnel destination 10.12.0.8
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth 32
 tunnel mpls traffic-eng path-option 20 explicit name pathc1c2c3
 no routing dynamic
!
interface FastEthernet0/0
 description *********** Link to C2 - f0/0  ***********
 ip address 10.11.1.1 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls traffic-eng tunnels
 mpls traffic-eng flooding thresholds up 1 2 5
 mpls traffic-eng flooding thresholds down 5 2 1
 mpls ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 96
 service-policy output oubound
!
interface FastEthernet0/1
 description **** LAN ****
 ip address 192.168.1.50 255.255.255.0
 ip policy route-map voice
 service-policy input SETDSCP
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router isis TestLab
 net 49.0001.0100.1100.0008.00
 is-type level-2-only
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
router bgp 65001
 bgp router-id 10.11.0.8
 bgp log-neighbor-changes
 neighbor 10.12.0.8 remote-as 65001
 neighbor 10.12.0.8 update-source Loopback0
 neighbor 10.13.0.8 remote-as 65001
 neighbor 10.13.0.8 update-source Loopback0
 !
```

```
 address-family ipv4
  neighbor 10.12.0.8 activate
  neighbor 10.12.0.8 send-community extended
  neighbor 10.13.0.8 activate
  neighbor 10.13.0.8 send-community extended
  no auto-summary
  no synchronization
  network 192.168.1.0
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.12.0.8 activate
  neighbor 10.12.0.8 send-community extended
  neighbor 10.13.0.8 activate
  neighbor 10.13.0.8 send-community extended
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip explicit-path name pathc2c3 enable
 next-address 10.11.1.2
 next-address 10.11.2.2
 next-address 10.12.1.1
!
ip explicit-path name pathc1c2c3 enable
 next-address 10.11.1.2
 next-address 10.13.2.2
 next-address 10.12.2.1
 next-address 10.12.1.1
!
ip explicit-path name pathc2pe1 enable
 next-address 10.11.1.2
 next-address 10.13.1.1
!
access-list 101 permit ip any host 192.168.3.52
access-list 102 permit ip any host 192.168.7.1
!
route-map voice permit 10
 match ip address 101
 set interface Tunnel0
!
route-map voice permit 20
 match ip address 102
 set interface Tunnel1
!
mpls ldp router-id Loopback0
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password XXXX
 login
!
```

```
scheduler allocate 20000 1000
end

******Router PE2**********

=~=~=~=~ PuTTY log 2009.01.13 08:56:02 =~=~=~=~=~=~=
wr t
Building configuration...

Current configuration : 2805 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE2
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$gRwA$O47Ue.pap5G07Zjpywb.P.
!
no aaa new-model
!
dot11 syslog
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip cef
!
no ipv6 cef
!
multilink bundle-name authenticated
!
mpls traffic-eng tunnels
mpls label protocol ldp
!
voice-card 0
 no dspfarm
!
archive
 log config
  hidekeys
!
interface Loopback0
 description **** Management ****
 ip address 10.13.0.8 255.255.255.255
 ip router isis
!
interface FastEthernet0/0
 description **** connected to C2 FE 0/1 ****
 ip address 10.13.1.1 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
```

```
 mpls traffic-eng tunnels
 mpls ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 96
!
interface FastEthernet0/1
 description ******** LAN**********
 ip address 192.168.2.50 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router isis TestLab
 net 49.0001.0100.1300.0008.00
 is-type level-2-only
 metric-style wide
 passive-interface Loopback0
!
router isis
 is-type level-1
!
router bgp 65001
 bgp router-id 10.13.0.8
 bgp log-neighbor-changes
 neighbor 10.11.0.8 remote-as 65001
 neighbor 10.11.0.8 description ****Location A PE1 ****
 neighbor 10.11.0.8 update-source Loopback0
 neighbor 10.12.0.8 remote-as 65001
 neighbor 10.12.0.8 description **** Location C PE3 ****
 neighbor 10.12.0.8 update-source Loopback0
 !
 address-family ipv4
  neighbor 10.11.0.8 activate
  neighbor 10.11.0.8 send-community extended
  neighbor 10.12.0.8 activate
  neighbor 10.12.0.8 send-community extended
  no auto-summary
  no synchronization
  network 192.168.2.0
  network 192.168.6.0
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.11.0.8 activate
  neighbor 10.11.0.8 send-community extended
  neighbor 10.12.0.8 activate
```

```
  neighbor 10.12.0.8 send-community extended
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password XXXX
 login
!
scheduler allocate 20000 1000
end

******Router PE3**********

=~=~=~=~= PuTTY log 2009.01.13 08:56:47 =~=~=~=~=
PE3#wr t
Building configuration...

Current configuration : 3076 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE3
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$u687$wIoiSANYFvSH4Htv0CJbB1
!
no aaa new-model
!
dot11 syslog
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
ip cef
!
no ipv6 cef
!
multilink bundle-name authenticated
!
mpls traffic-eng tunnels
mpls label protocol ldp
!
voice-card 0
 no dspfarm
!
```

```
archive
 log config
  hidekeys
!
interface Loopback0
 ip address 10.12.0.8 255.255.255.255
 ip router isis TestLab
!
interface Loopback1
 ip address 192.168.7.1 255.255.255.0
!
interface FastEthernet0/0
 description ********** Link to C3 - f0/0  **********
 ip address 10.12.1.1 255.255.255.252
 ip router isis TestLab
 duplex auto
 speed auto
 mpls traffic-eng tunnels
 mpls ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 512
!
interface FastEthernet0/1
 description **** LAN ****
 ip address 192.168.3.50 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router isis TestLab
 net 49.0001.0100.1200.0012.00
 is-type level-2-only
 metric-style wide
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
router bgp 65001
 bgp router-id 10.12.0.8
 bgp log-neighbor-changes
 neighbor 10.11.0.8 remote-as 65001
 neighbor 10.11.0.8 update-source Loopback0
 neighbor 10.13.0.8 remote-as 65001
 neighbor 10.13.0.8 update-source Loopback0
 !
 address-family ipv4
  neighbor 10.11.0.8 activate
```

```
  neighbor 10.11.0.8 send-community extended
  neighbor 10.13.0.8 activate
  neighbor 10.13.0.8 send-community extended
  no auto-summary
  no synchronization
  network 192.168.3.0
  network 192.168.7.0
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.11.0.8 activate
  neighbor 10.11.0.8 send-community extended
  neighbor 10.13.0.8 activate
  neighbor 10.13.0.8 send-community extended
 exit-address-family
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
mpls ldp router-id Loopback0
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 password XXXX
 login
!
scheduler allocate 20000 1000
end

******Frame Relay Switch**********

~=~=~=~PuTTY log 2009.01.13 08:47:32 =~=~=~=~=~=

FR-SW#wr t
Building configuration...

Current configuration : 2158 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname FR-SW
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
resource policy
!
ip cef
```

```
!
frame-relay switching
!
voice-card 0
 no dspfarm
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000

interface Serial1/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial1/1
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 102 interface Serial1/2 201
 frame-relay route 103 interface Serial1/3 301
!
interface Serial1/2
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 201 interface Serial1/1 102
 frame-relay route 203 interface Serial1/3 302
!
interface Serial1/3
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 301 interface Serial1/1 103
 frame-relay route 302 interface Serial1/2 203
!
interface Serial1/4
 bandwidth 64
 no ip address
```

```
!
interface Serial1/5
 bandwidth 64
 no ip address
!
interface Serial1/6
 bandwidth 64
 no ip address
!
interface Serial1/7
 bandwidth 64
 no ip address
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
!
End
```

References

[1] S. Blake et al.,"An Architecture of Differentiated Services", RFC 2475, Dec 1998.

[2] D. Awduche, et al, "Requirements for Traffic Engineering over MPLS," RFC2702, Sep 1999.

[3] E. Rosen, A. Viswanathan, R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, Jan 2001.

[4] F. Le Faucheur, et al, "MPLS Support of Differentiated Services," RFC3270, May 2002.

[5] S. Ganti et. Al., "MPLS Support of Differentiated Services using E-LSP," IETF Draft, Apr. 2001.

[6] Danial O. Awduche,"MPLS Traffic Engineering in IP Networks",UUNET (MCI Worldcom), IEEE Communication Magazine, Dec 1999

[7] Xipeng Xiao, Lionel M.Ni, "Internet QoS:A Big Picture", Michigan State University, IEEE Network, Mar/Apr 1999

[8] Joevans, "MPLS Tutorial RIPE- Label Switching Timeline", Bologna, http://www.ripe.net/ripe/meetings/ripe-39/presentations/mpls-arch/sld007.html, Slide 7, Apr 2001.

[9] "Enhancing MPLS Network Performance", White Paper, Packeteer, http://www.packeteer.com.

[10] Altera Corporation, "Implementing Multiprotocol Label Switching with Altera PLDs", Application note, Ver 1.0 132, Jan 2001.

[11] L. Andersson, P. Doolan, N. Feldman, A. Fredette, B. Thomas, "LDP Specification", RFC 3036, Jan 2001

[12] D.Awduche, L.Berger, D, Gan, T.Li, V.Srinivasan, G.Swallow, "Extensions to RSVP for LSP Tunnels", RFC3209, Dec 2001.

[13] Victoria Fineberg, "QoS Support in MPLS Networks", MPLS/Frame Relay Alliance White Paper, MPLS Forum, May 2003.

[14] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, W. Weiss, "An Architecture for Differentiated Services", RFC 2475, Dec 1998.

[15] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, "Assured Forwarding PHB Group", RFC 2597, Jun 1999.

[16] "CISCO-MIB Compilers and Loading MIBs", mibcompilers.pdf, document ID: 26015, Jul 13, 2007.

[17] Cisco IOS IP SLAs Overview, http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsoverv.pdf, Dec 8, 2005.

[18] Victoria Fineberg, "QoS Support in MPLS Networks", MPLS/Frame Relay Alliance White Paper, http://www.ipmplsforum.org/tech/MPLSQOSWPMay2003.pdf, May 2003.

[19] D. Grossman," New Terminology and Clarifications for Diffserv", RFC 3260, Apr 2002

[20] Yakov Rekhter,Bruce Davie,Eric Rosen,George Swallow,Dino Farinacci,Dave Katz,"Tag Switching Architecture Overview", rekhter.pdf, Dec 4, 1997

Bibliography

[1] P.Trimintzios, L.Georgiadis, G.Pavlou, D.Griffin, C.F.Cavalcanti, P.Georgatsos, "Engineering the Multi-Service Internet: MPLS and IP-based Techniques", IEEE ICT'01 Bucharest, Romania, pg-ict2001.pdf, 4-7 Jun 2001.

[2] CISCO,"SLA Compilers and Loading SLAs", Document ID 26015, Updated July 2007.

[3] Andrew G. Malis, "The Converged Network Vision", The MPLS/FR Alliance", mplsfra_pp7.ppt, Updated July 2003.

[4] Mike Fuszner, "Graphical Network Simulator –version 1.0", http://www.gns3.net.

[5] X. Xiao, A. Hannan, B. Bailey, "Traffic Engineering with MPLS in the Internet", IEEE Network, Mar/Apr 2000.

[6] Henk Smit, Tony Li, "IS-IS extensions for Traffic Engineering", http://tools.ietf.org/html/draft-ietf-isis-traffic-01, May 2009.

[7] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus, work in progress" Requirements for Traffic Engineering Over MPLS",draft-ietf-mpls-traffic-eng-00.txt.

[8] R.W. Callon, "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, Dec. 1990.

[9] Der-Hwa Gan, Tony Li, George Swallow,Lou Berger, Vijay Srinivasan, Daniel Awduche "Extensions to RSVP for LSP Tunnels", 29th Sept 1999 .

[10] Bruce Davie, Pasi Vaananen, Liwen Wu,Francois Le Faucheur, Pierrick Cheval, Ram Krishnan, Shahram Davari "MPLS Support of Differentiated Services", Oct 11, 1999.

[11] Y. Rekhter, B. Davie, D. Katz, E. Rosen, G. Swallow," Cisco Systems' Tag Switching Architecture Overview", RFC 2105, http://www.faqs.org/rfcs/rfc2105.html , Feb 1997.

[12] Chuck Semeria," Multiprotocol Label Switching- Enhancing Routing in the New Public Network", part Number: 2000001-002, http://www.juniper.net/solutions/literature/white_papers/200001.pdf, Sep 27, 1999.

[13] Braden, R., Zhang L., Berson, S., Herzog, S., Jamin, S., "Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification", draft-ietf-rsvp-spec-16.txt, Internet Draft, Jun 1997.

[14] Yakov Rekhter,Bruce Davie, Eric Rosen, George Swallow, Dino Farinacci, Dave

Katz, Juniper, "Tag Switching Architecture Overview", Dec 4, 1997.

[15] Dr. Thomas Bauschert,"IP Network Engineering Challenges", ITG_110501_final.ppt, Nov 5, 2001.

[16] MFA Forum,"Converged Network Services Using MPLS", Public Interoperability Event, Paris, 2006.

[17] MPLS Forum, "Large Scale Multi-Vendor layer 2 VPNs with MPLS", Public Interoperability Event, Paris, 2005.

[18] T. Li, G. Swallow, and D. Awduche, "IGP Requirements for Traffic Engineering with MPLS," draft-li-mpls-igp-te-00.txt, IETF Internet Draf, Feb, 1999.

[19] Eric C. Rosen, et al, "BGP/MPLS VPNs," draft- ietf-ppvpn-rfc2547bis-03.txt, Oct 2002.

[20] D.Katz, K.Kompella, D.Yeung, "Traffic Engineering (TE) Extensions to OSPF Version 2", RFC 3630, http://www.rfc-archive.org/getrfc.php?rfc=3630, Sept 2003.

[21] B. Fortz, J. Rexford, and M. Thorup. "Traffic Engineering with Traditional IP Routing Protocols", IEEE Communications Magazine, 40(10):118—124, Oct 2002.

[22] Callon, R., Rosen, E., and Viswanathan, A. "Multiprotocol Label Switching Architecture," work in progress. http://www.ietf.org/html.charters/mpls-charter.html, Jul 2000.

[23] Internet Engineering Consortium, "An MPLS Tutorial", http://www.iec.org/tutorials/mpls/topic03.html, 2007.

[24] Osborne, E., and A. Simha,"Draft-ietf-mpls-soft-preemption-03 – MPLS Traffic Engineering Soft Preemption Traffic Engineering with MPLS", Cisco Press; 2003.

[25] H. Smit, T. Li, "IS-IS extensions for Traffic Engineering", RFC 3784, Jun 2004.

[26] F. Le Faucheur, Ed., "Protocol extensions for support of Differentiated-services-aware MPLS Traffic Engineering", RFC 4124, Jun 2005.

[27] D.Mitra, K.G.Ramakrishnan, "A case study of multiservice, multipriority traffic engineering design for data networks," Proc. of IEEE GLOBCOM, Rio de Janeiro, , PP.1087-1093, Dec 1999

[28] D.Awduche, J.Malcolm,J.Agogbua,M. O'Dell,J. McManus,"Multiprotocol Label Switching Architecture", RFC 2702, Sep 1999