Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Telecommunication Engineering Graduate Program

Analyzing Impact of Segment Routing MPLS on QoS

By

Kibrab Alemayehu

Advisor

Dr. Yalemzewd Negash

A Thesis Submitted to the School of Electrical and Computer Engineering in Partial Fulfillment of the Requirements for the Degree of Masters of Science in Telecommunication Engineering

December 2019

Addis Ababa, Ethiopia

Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

Analyzing Impact of Segment Routing MPLS on QoS

By: Kibrab Alemayehu

Approval by Board of Examiners

Dr. Yalemzewd Negash _____
Dean, School of Electrical & Computer Engineering Signature

Committee

Dr. Yalemzewd Negash _____
Advisor Signature

Dr. Murad Ridwan _____
Examiner Signature

Dr. Ephrem Teshale _____
Examiner Signature

Abstract

Multiprotocol Label Switching (MPLS) Segment Routing (SR), SR-MPLS in short, is an MPLS data plane-based source routing paradigm in which a sender of a packet is allowed to partially or completely specify the route the packet takes through the network by imposing stacked MPLS labels to the packet. SR-MPLS could be leveraged to realize a unified source routing mechanism across MPLS, IPv4 and IPv6 data planes by using an MPLS label stack as unified source routing instruction set while preserving backward compatibility with traditional MPLS networks.

The Segment Routing is a promising Traffic Engineering (TE) model that provides end-to-end communications. SR can observably improve the network utilization and control the routing path flexibly by encoding route information into a list of segments, i.e., the Segment List (SL). The key feature of SR is that it adopts the source routing paradigm, which implies the routing path followed by a packet is determined and written to the packet header by the first switch of SR networks (called Ingress SR switch).

The motivation of this thesis is to investigate and analyze the impact of implementing SR-MPLS on Quality of Service (QoS). The impact on QoS parameters is analyzed by using two scenarios; Traditional Unified MPLS integrating four domains into single MPLS domain and Segment Routing over Unified MPLS integrating four domains into a single MPLS domain. Simulation tools such as EVE-NG, Ostinato, Cisco IPSLA technology are used to compare performances of the two scenarios. The analysis results show that in SR-MPLS throughput is improved on average by 32%, latency is improved by 24%, packet loss is improved by 20.4% and jitter is improved by 12.6% compared to Label Distribution Protocol (LDP) based Unified MPLS. From the results, one can understand that any service provider can benefit from deploying Unified SR-MPLS. Segment Routing is a new routing paradigm that provide a better end-to-end QoS guarantee, making traditional MPLS network more efficient and scalable.

Keywords—IP, MPLS, Segment Routing, QoS, SR-MPLS domain, Latency, Jitter, Throughput, Packet loss, Performance

Declaration

I, the undersigned, declare that this thesis is my original work, has not been presented for a degree in this or any other university, and all sources of materials used for the thesis have been fully acknowledged.

Kibrab Alemayehu

Name Signature

Place: Addis Ababa

Date of Submission: December 2019

This thesis has been submitted for examination with my approval as a university advisor.

Dr. Yalemzewd Negash

Advisor's name Signature

Acknowledgment

First and foremost, I wish to thank my wife, Selamawit, who has stood by me through all my travails, my absences, my fits of pique and impatience. She gave me support and help, discussed ideas and prevented several wrong turns. She also supported the family during much of my graduate studies. Along with her, I want to acknowledge my two sons, Nathan and Nahom. They have never known their dad as anything but a student, it seems. Good boys, both, and great sources of love and relief from scholarly endeavor. In fact, all my family have been committed and supportive. My siblings and their families, my parents-in-law and brothers-in-law, and the vast extended family from both my side and my wife's side have all been wonderful and very patient.

Second, my deep gratitude goes to Dr. Yalemzewd Negash for his continuous follow-up and guidance during the course of this thesis. His observation, unreserved advice, and support were very useful and constructive.

Also, I would like to express my appreciation to AAiT in collaboration with Ethio Telecom for their devotion and sponsorship to make this postgraduate program fruitful.

Finally, I must express my very profound gratitude to all my friends specially Tsehaye Kindeya for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Table of Content

List of Figures

List of Tables

List of Abbreviations

ABR	Area Border Router
AN	Access Node
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Boundary Router
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BGP-LU	Border Gateway Protocol Labeled Unicast
CR	Core Router
CSPF	Constrained Shortest Path First
DiffServ	Differentiated Service
DoD	Downstream-on-Demand
eBGP	External Border Gateway Protocol
ECMP	Equal-cost multi-path
EPE	Egress Peering Engineering
EVE-NG	Emulated Virtual Environment Next Generation
FEC	Forwarding Equivalence Class
FTP	File Transfer Protocol
iBGP	Internal Border Gateway Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force

IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IS-IS	Intermediate System-Intermediate System
ITU	International Telecommunication Union
LDP	Label Distribution Protocol
LLC	Logical Link Control
LSP	Label-Switched Path
LSR	Label Switching Router
MLD	Multicast Listener Discovery
MPLS	Multiprotocol Label Switching
NNTP	Network News Transfer Protocol
OSPF	Open Shortest Path First
RSVP-TE	Resource Reservation Protocol for Traffic Engineering
RTSP	Real-Time Streaming Protocol
RTT	Round Trip Time
SDN	Software-Defined Networking
SID	Segment Identifier
SLA	Service Level Agreement
SPF	Shortest Path First
SR	Segment Routing
SIP	Session Initiation Protocol
SR-MPLS	Segment Routing Multiprotocol Label Switching

SR-TE	Segment Routing Traffic Engineering
TCP	Transmission Control Protocol
TI-LFA	Topology independent loop-free alternate
TE	Traffic Engineering
UDP	User Datagram Protocol
PCC	Path Computation Client
PHP	Penultimate Hop Popping
QoS	Quality Of Service
VPN	Virtual Private Network

1. Introduction

The need for timely delivery of real-time applications like telephony, video conferencing or guaranteed bandwidth for mission-critical applications has led to a high demand for end-to-end quality of service (QoS) guarantees such as delay, Jitter and packet loss [1] [4]. QoS requirements put new challenges to service providers. QoS does not create capacity, but only supports the priorities of traffic and allocation of resources under the terms of congestion [1] .

As content and applications migrate to the cloud, the demand for network bandwidth is accelerating, and users' quality-of-experience (QoE) [2] expectations are reaching new heights. At the same time, service provider networks are struggling to keep pace using their current transport architectures and management approaches [3]. To more easily and affordably meet demand and improve user experiences, service providers need a network transport solution that will provide greater control, agility, application awareness, and simplified traffic management for their networks. Operators can get all these capabilities with the segment routing solution [4].

Source Packet Routing in Networking (SPRING) Working Group (WG) is developing an Multi Protocol Label Switching (MPLS) source routing mechanism.The MPLS source routing mechanism can be leveraged to realize a unified source routing instruction that works across both IPv4 and IPv6 underlays in addition to the MPLS underlay [3][5].

Segment Routing (SR) is a new routing paradigm that aims to optimize, simplify, and improve the scalability of IP/MPLS based networks.Segment Routing utilizes source-based routing scheme where a network node directs a packet based on a list of instructions carried in the packet header (called "segments").The list of segments carried in the packet header provide a strict or a loose design of the required network path or tunnel removing the need for transit nodes to hold and maintain that path/tunnel information [4][6].

The standards for Segment Routing are supported by the Internet Engineering Task Force (IETF) SPRING Working Group which defines the specifications for network operations, applications, interoperability, and management. Segment Routing architecture is defined in RFC8402. The IETF SPRING WG collaborates with other IETF Working Groups on the extensions of existing protocols to support Segment Routing including OSPF/IS-IS, BGP, VPN services, Traffic Engineering, IPv6 and MPLS VPN [5][7].

Segment Routing can be directly applied to the MPLS architecture with no change to the forwarding plane. A segment is encoded as an MPLS label. An ordered list of segments is encoded as a stack of labels. The segment to process is on the top of the stack. Upon completion of a segment, the related label is popped from the stack [8].

SR can also be applied to the IPv6 architecture, with a new type of routing header. A segment is encoded as an IPv6 address. An ordered list of segments is encoded as an ordered list of IPv6 addresses in the routing header.The active segment is indicated by the Destination Address (DA) of the packet.The next active segment is indicated by a pointer in the new routing header [6][8].

Segment routing is a promising technology that can be seamlessly deployed in today's MPLS and ipv6 networks. The adaptability of the technology in terms of deployment (distributed versus centralized), network types (Data Centers (DC) or Wide Area Network (WAN)), diverse use cases makes it a good candidate for deployment in any kind of WAN, Data Center, access, metro or virtualized environment [9].

1.1.Motivation

Service Providers are facing extreme challenges to keep pace with the exponential growth of their customers' traffic. Moreover, customers are requesting stricter Quality of Service requirements for their sensitive applications such as medical, financial, real-time videos call and streaming application resulting in tightened Service Level Agreements (SLA). Consequently, service providers need to meet those requirements while reducing costs. One of the solutions they are adopting is simplifying their complex networks and rely more on software to reduce operational expense and capital expenditure.

Organizations operating in highly demanding environments such as banking, universities, industries, medical, etc. rely on dedicated Wide Area Network connections to connect their remote sites. Mainly because of the guaranteed QoS requirements such as bandwidth, protection, delay, etc. that the Service Providers (SPs) deliver. For that, service providers invest in building and maintaining specialized WANs to satisfy the increasing demands. The majority of these networks run on the MPLS network. However, over the years and with the increase of use cases the MPLS control plane grows increasingly complex, which required a variety of interconnected protocols built by different standardization working groups, thus making it hard to manage, troubleshoot and grow.

For the reasons mentioned above, the Internet Engineering Task Force SPRING working group has proposed the Segment Routing (SR) architecture. Its main objective is to have a simple and easy to manage control plane. It relies on an old networking paradigm known as source routing, where a packet carries in its header the path to reach its destination. This architecture has generated a lot of interest among service providers such as Orange [30], due to the simplification that it brings to their IP/MPLS networks. In fact, the instantiation of SR architecture over the MPLS data plane requires less control plane protocols: There is no need to pre-establish tunnels and the per-flow states are maintained only at the edges of the network. Therefore, no signaling protocols such as LDP and/or RSVP-TE (Resource Reservation Protocol for Traffic Engineering) are required. Consequently, the number of states maintained in the network is considerably reduced. However, as to the best of the researcher's knowledge, the impact of SR on QoS is not studied so far. And the lack of such an important use case makes the service providers hesitant to migrate their networks to SR. This thesis, tries to study the impact of Unified SR-MPLS on QoS in IP/MPLS networks.

This paper analyzes the impact of Segment Routing MPLS (SR-MPLS) on QoS. It starts with an introduction to the motivations for Segment Routing and an overview of its evolution and standardization. CISCO IP Service Level Agreements are used for active traffic monitoring to analyze IP service levels for IP applications and services.

1.2. Statement of the Problem

In its general sense this thesis tries to answer the following Research Question:

"What is the impact of SR-MPLS on QoS by taking four parameters of QoS into consideration relative to traditional MPLS, which is LDP based ?"

1.3. Objective

1.3.1. General Objective

The general objective of this thesis is to analyze the impact of an end-to-end Segment Routing MPLS architecture for enhancing service providers' IP network scalability and flexibility in service delivery using QoS parameters in comparison with the LDP based MPLS architecture.

1.3.2. Specific Objectives

The goal of this Theses is to emulate network architecture to analyze the impact (performance) of SR-MPLS and MPLS networks on QoS. It considers different traffic types between source and destination and the statistics related to SR-MPLS vs. MPLS are collected and analyzed.

The specific goals of the study are:

- To investigate the technologies supported by SR-MPLS
- To simulate and evaluate SR-MPLS architecture
- To compare SR-MPLS architecture with LDP based MPLS architecture and its potential improvements on QoS.
- Design a network architecture with routers configured for Unified SR-MPLS and Unified MPLS (LDP based) networks.
- Simulation all routers in the network architecture.
- Configure routers to permit background traffic.
- Emulate two scenarios: Scenario 1 with SR-MPLS and Scenario 2 With LDP-MPLS.
- Analyze the simulation results.
- To assess the impact of SR-MPLS on QoS parameters

1.4. Methodology

In this thesis state-of-the-art, related works and statements of the problem are used as a baseline to achieve the objectives. The methodology starts with investigating different technologies enabling SR-MPLS architecture. Then the methods of simulating and evaluating the architecture from a QoS perspective are followed. A theoretical study of SR-MPLS and QoS features are done thoroughly along with the evaluation of the limitations of the traditional MPLS (LDP based) architecture. SR-MPLS architecture & implementation scenarios with its benefits compared to LDP based MPLS architecture are explained.

In the implementation part, a practical environment is developed using a network simulation tool, EVE-NG (Emulated Virtual Environment Next Generation), and two scenarios are built in order to collect test results from the simulator. The two scenarios are built in such a way that the first LDP based Unified MPLS network is built. Then the same network topology is implemented with Segment Routing based Unified MPLS features and the test results are collected from the simulator using IP Service Level Agreement (Ipsla) technology for the two

scenarios. To make the scenarios similar to the real network, a network traffic generator called Ostinato is used to generate traffic into the network. Finally, the test results for the two scenarios are presented graphically for comparison and analysis with respect to QoS parameters.

1.5. Scopes and Limitations

1.5.1. Scopes of the Thesis

In Unified SR-MPLS large numbers of MPLS domains can be aggregated to a single domain. However, in this thesis four representative SR-MPLS domains are used for the implementation of Unified SR-MPLS, considering the results are equally applicable for the other domains. The four domains can be considered as two access, two pre-aggregations and two aggregation MPLS networks connected by a core SR-MPLS network. Also in the thesis, SR-MPLS IP unicast is considered and the performance analysis is independent of the type of traffic generated. So all network traffic entering the network is treated equally.

In general, in the scope of this thesis virtual network is implemented for testing SR-MPLS properties and its impact on QoS. In the network topology, Segment Routing was tested from different aspects. The work investigated Segment Routing performance capabilities, scalability properties and multi-domain application.

1.5.2. Limitations of the Thesis

The cisco virtual service routers used in the simulation requires three gigabytes of memory each. So due to memory limitations of personal computers and the process intensiveness of the simulation tools used. The number of virtual service provider routers used in the simulation environments is limited.

1.6. Contributions

Operators of IP/MPLS networks including Ethio telecom need to optimize their existing network infrastructure, increase the options available to existing services and potentially create new service offerings without adding additional resources. Segment Routing (SR) delivers the functionality required to meet these needs.

Many service providers, including Ethio telecom, have deployed mobile backhaul in addition to IP/MPLS core networks. The interconnection, as well as service provisioning among these

different domains, should be done seamlessly without introducing additional delay, additional signaling protocol overhead, flexibility problems, granted the ultimate end to end QoS and better resource utilization. This thesis aims to improve end-to-end network QoS performance by optimizing the Unified MPLS which is based on SR architecture using new emerging technologies. This minimizes limitations of the existing MPLS architecture and enhances the scalability, resource utilization and flexibility of service delivery in any telecommunication industry.

1.7.Literature Review

Recently IETF has proposed a traffic engineering technology that simplifies IP/MPLS operation and enables easier integration with centralized control architecture. Segment Routing is a new technology designed for the Software-defined networking (SDN) era [10] . Segment Routing does not depend on distributed signaling protocols and it easily fits the SDN concepts. However, even though is built with SDN in mind, Segment Routing is compatible with traditional IP/MPLS networks.

In the scientific literatures, there is a limited number of works done regarding Segment Routing technology to the best of my knowledge. The work in [7] , discusses SR implementation in both SDN and traditional IP/MPLS network. Firstly, it examines the Segment Routing tunnel setup in an SDN environment where nodes are OpenFlow switches. They used SR-Controller that was developed from the RYU framework by adding new modules such as to request a handler, network tracker, per-flow monitor, and SR engine. The second network is not software defined but it has a centralized path computation entity (PCE) that creates the routes in traditional IP/MPLS network. Their scenario examines flow rerouting with the aim of better resource utilization. Both implementations were successfully utilized to demonstrate dynamic packet rerouting enabled by enforcing different segment lists at the ingress node. Flow reroute is performed without any signaling protocol and with no packet loss.

The problem of how to extend QoS capabilities across multiple provider domains has not been solved satisfactorily to date to the best of my knowledge. The source of the problem lies mainly with the autonomous nature of Internet Service Providers (ISP) and their loose partnership that forms the global Internet [11].

The paper in [1] tries to solve the problem of enhancing end-to-end QoS performance using Seamless MPLS by taking four important QoS parameter into consideration and got a very nice

result but the paper uses LDP as a signaling protocol and this protocol has its own limitation as it relies on IGP plus LDP signal to establish LSP and to converge. This limitation affects the result. What if ignore the additional LDP signal and uses the Interior Gateway Protocol (IGP) extension to send labels without adding or modifying the MPLS plane? What will be the impact on QoS ? This work tries to answer these quations.

The paper [12] Talked about the multimedia application categorization based on kind of interactions, one of them is interactive application which is a kind of human to human communication such as video conferencing and believe that Video conferencing had a quality issue and to resolve the quality issue even though there are several solutions as it stated in the study the author believe the most practical and utilized of them is QoS. QoS as mentioned is a general solution for multimedia application that was discussed from different viewpoints of 6 different layers (application, system, network). The paper focused on parameters of network level, such as bandwidth, jitter, and delay. While figuring the needs of multimedia applications to these parameters. IntServ and DiffServ were presented as two main ways for QOS implementation, as far as they are not perfect just, and can resolve each other limitations, their integration seemed to be a favorable solution. The paper state Gatekeeper as an evolving solution offering good facilities, like address translation and admission control. Due to some drawbacks such as bandwidth ignorance, it should be joint to previous solution to perform perfectly.

The paper in [14] focuses on supporting QoE in multimedia networks based on an SR mechanism. Two problems were identified. The first one is how to implement fine-grained routing in a complex network environment. To solve it efficiently, a MOMC-based optimization model was put forward as there are multiple limitations on QoE-driven routing in such a complicated network environment, including bandwidth, delay, packet loss rate, throughput, etc Simulations-based testing showed how the proposed solution outperforms existing alternative solutions in terms of diverse QoS performance parameters. But the paper does not consider end-to-end QoS performance in addition to multi-domain unified implementation.

Large networks [15][16] are often structured hierarchically by grouping nodes into different domains in order to deal with the scaling problem. In such networks, it is infeasible to maintain the detailed network information at every router. Therefore, topology information of domains are summarized before broadcasted. This process is called topology aggregation. Hierarchical

routing protocols are then used to find a route among the domains. [15][16] study several basic problems associated with hierarchical QoS routing, including how to make QoS-aware topology aggregation, how to represent the aggregated network state, and how to find an end-to-end route based on aggregated information.

As in [17], inter-domain routing is considered a challenging research area due to two reasons: First, the inter-domain routing protocol, BGP, currently used on the Internet has several limitations, but its replacement is not a realistic option due to its worldwide deployment. Second, inter-domain routing denotes routing among distinct domains or networks. These domains are completely autonomous entities, which perform their own routing management based on policies that only have local significance.

The document RFC8203 [18] describes a system as a functional component called MPLS Path Monitoring System (PMS) . The PMS uses capabilities for MPLS data-plane path monitoring. The use cases introduced here are limited to a single Interior Gateway Protocol MPLS domain. Although many use cases depict the PMS as a physical node, no assumption should be made, and the node could be virtual. This system is defined as a functional component abstracted to have many realizations. The terms "PMS" and "system" are used interchangeably here. The system applies to the monitoring of non-SR LSPs like Label Distribution Protocol as well as to the monitoring of SR LSPs.As compared to non-SR approaches, SR is expected to simplify such a monitoring system by enabling MPLS topology detection based on IGP-signaled segments. The MPLS topology should be detected and correlated with the IGP topology, which is also detected by IGP signaling. Thus, a centralized and MPLS-topology-aware monitoring unit can be realized in an SR domain. This topology awareness can be used for Operation, Administration, and Maintenance (OAM) purposes as described by the document.

The Internet Engineering Task Force (IETF) [19] standard in RFC 8402 [8] is aimed to address the drawbacks of traditional MPLS such as scalability and flexibility in service provisioning limitations. The scalability is achieved by directly applied Segment Routing to the MPLS architecture with no change to the forwarding plane. To enhance the flexibility in provisioning, label mapping information for a particular route is piggybacked in the same BGP update message that is used to distribute the route itself. A segment is encoded as an MPLS label. An ordered list of segments is encoded as a stack of labels. The segment to process is on the top of the stack. Upon completion of a segment, the related label is popped from the stack.

1.8. Thesis Layout

This thesis is composed of six chapters. Chapter one deals with the introduction to the thesis. It includes background information, statement of the problem, objectives of the study, the methods of how the objectives are achieved, scopes and limitations of the thesis, contributions of the thesis and related works.

Subsequent chapters describe in detail the scope of work performed and lessons learned from practical scenarios and they also point to the potential use of these results. Chapter 2 introduces the basic concepts in Segment Routing technology. It highlights the advantages of SR compared to other old technologies and the most common terminologies used in SR are briefly explained in this chapter.

Chapter 3 is a detail description of unified SR-MPLS. The architecture and key technologies supported in SR-MPLS along with the benefits this architecture brings are presented in this chapter.

Chapter 4 is all about IP QoS principles, parameters, and models used in the current IP/MPLS networks. The four QoS parameters such as throughput, latency, packet loss and jitter are discussed in detail and their recommended values are also listed.

Chapter 5 presents the simulation and result analysis part which describes the simulation tools used, simulation scenarios, network topology and analysis of the results obtained.

The final chapter concludes the thesis by drawing conclusions from the analysis part. A potential research area for future work is also included in this chapter. References and appendixes are also included at the end of this document.

2. Technology Overview

Segment Routing allows for agile definition of end-to-end paths within IGP topologies by encoding paths as sequences of topological sub-paths, called "segments". These segments are advertised by the link-state routing protocols (IS-IS and OSPF) [8]. Prefix segments represent an ECMP-aware shortest path to a prefix (or a node), as per the state of the IGP topology. Adjacency segments represent a hop over a specific adjacency between two nodes in the IGP. A prefix segment is typically a multi-hop path while an adjacency segment, in most of the cases, is a one-hop path. SR's control plane can be applied to both IPv6 and MPLS data planes and does not require any additional signaling (other than the regular IGP). For example, when used in MPLS networks, SR paths do not require any LDP or RSVP-TE signaling [20] . Still, SR can interoperate in the presence of Label Switched Paths (LSPs) established with RSVP or LDP.This chapter explains concepts and uses cases of Segment Routing in a more detailed manner. Moreover, one can find an analysis of all protocols and technologies necessary for Segment Routing deployment.

2.1.Source Routing

Routing is the process of selecting the best path through the network for incoming data flows [19]. Usually, the path is guided through the network according to its destination IP address. Such a routing method is called destination-based routing and it’s commonly used in traditional IP networks. Once a router receives a packet, the router checks the packet’s destination IP address and consults its routing information base (RIB). Once it finds a suitable IP address match, a router forwards a packet to a proper port and the packet is forwarded towards the destination IP address. In contrast to traditional destination-based routing, one could implement source routing in a network. Source routing is a method where a sender of a packet specifies the route that a packet should take through the network [20]. When the packet with source routing travels through the network, a transit router routes a packet by inspecting the path information encoded in the packet by source router. A source router must be aware of the network layout in order to specify the route to the destination. Source routing allows a router to determine a path partially or completely. When a sender determines the exact path that mechanism is called Strict Source and Record Routing (SSRR) [21]. This approach is rarely used. A common case of source routing is called Loose Source and Recorded Routing (LSRR),

where the sender provides one or more intermediate hops that packet must-visit on its path to the destination [5].

The main benefit of source routing is that intermediate nodes do not have to keep route information in RIB because the forwarding steps are specified in the data packet. Source routing enables easier network troubleshooting, enhances traceroutes and increases overall network performance [21] [22] [23].

2.2. Segment Routing

Segment Routing is a new source routing model intended to simplify existing routing techniques in traffic-engineered networks. It enables efficient packet guiding through a specific network path, rather than the natural shortest path that packet usually takes within a network. A source node leads incoming packet flow through the network by specifying a list of midway destinations that a packet must-visit on its way to the final destination. In Segment Routing, labels called segments to represent in-between path points. The main benefit of this technology is its simplicity, easier implementation and scalability [1] [22].

It is a technique that is enabled by a small number of extensions to routing protocols such as IGP, BGP and PCEP and it can be applied in MPLS and IPv6 architecture. Segment Routing does not require a lot of changes in the MPLS forwarding plane [24]. A segment is encoded as an MPLS label and a list of segments is equivalent to MPLS label stack. In IPv6 architecture, a segment is represented as an IPv6 address. This is enabled by introducing Segment Routing Extension Header that allows multiple IPv6 addresses to be encoded in source router, so multiple intermediate hops can be specified [8] [25]. The Segment Routing concepts are the same in both environments. However, some implementation details and protocol extensions differ between Segment Routing in MPLS and Segment Routing in IPv6 networks. This work puts focus on Segment Routing over MPLS architecture and details on Segment Routing in IPv6 networks will be skipped.

2.2.1. Segment Routing Concepts

Segment Routing leverages the source routing paradigm. A node steers a packet through an ordered list of instructions, called "segments". A segment can represent any instruction, topological or service-based. A segment can have a semantic local to an SR node or global

within an SR domain. SR provides a mechanism that allows a flow to be restricted to a specific topological path while maintaining a per-flow state only at the ingress node(s) to the SR domain [8] [26] .

2.2.1.1. Segment

One of the main concepts in SR architecture is the idea of segments. They represent different network components: physical (node, link, etc.) or logical (service/application). An identifier called Segment Identifier or SID is attributed to each segment [27]. The SID type and format depend on the fundamental data plane (an MPLS label or an IPv6 address as). According to the IETF RFC8402 [8], a segment is an instruction that node executes on the incoming packet. This instruction could be, for instance, forward the packet to a specific network node according to the shortest path, or forward packet through a specific interface, or deliver the packet to a given application or service. A segment is identified with Segment Identifier (SID) and in MPLS environment it is encoded in 32 bits MPLS label [28][24].

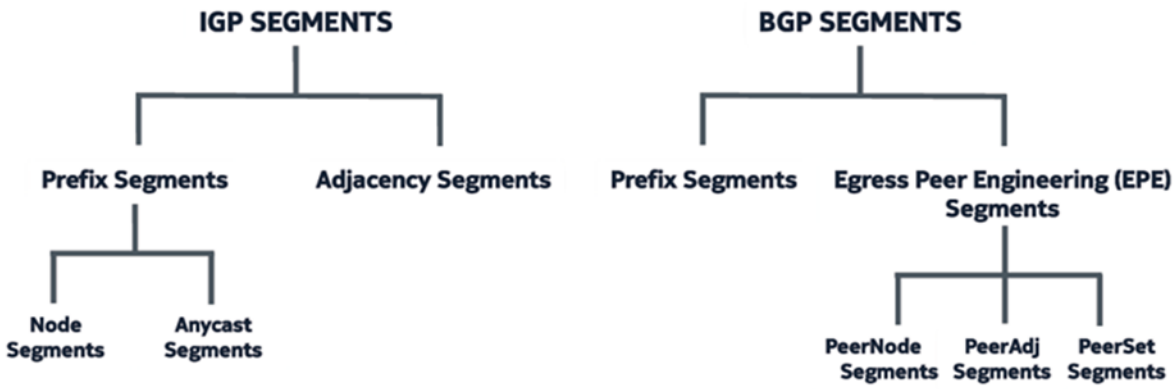


Figure 1. Tyeps of Segments

2.2.1.2. Segment Advertising

Segments are advertised using IGP and BGP routing protocols [29]. For both protocol types, Segment Routing extensions are defined to include Segment Routing information. In other words, routing protocols enable segments' signaling through the network. Let us now consider an autonomous system consisting of multiple IGP areas. Within each IGP area, either IS-IS or OSPF is running. They are responsible to advertise segments within an IGP domain [27]. However, in order to implement traffic engineering between an AS, segment exchanging

between BGP peers must be enabled. BGP is extended to advertise the segments related to the BGP-prefix [26] [30].

'Segment Routing' added few extensions to existing IGP protocols, wherein these extensions allowed distribution of labels across the network using the normal way of link-state distribution, without making any major change to existing IGP protocols. In other words, an IGP protocol can be another client of MPLS data plane, or it can now create an MPLS tunnel-like RSVP or LDP, a little less sophisticated way [31] [25].

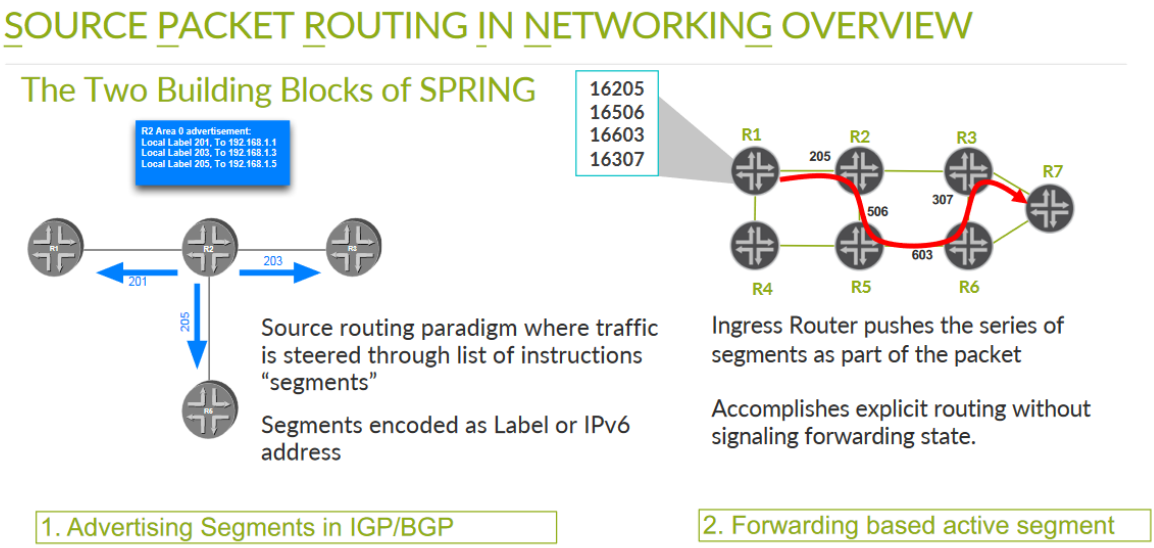


Figure 2: The Two Building Blocks of SPRING [22]

2.2.1.3. Global and Local Segments

A global segment is related to the instruction that is supported by all nodes in an IGP domain. A global segment must be unique within a domain. Any node in an IGP domain must have all global segments in its Forwarding Information Base (FIB). The value of the global segment identifiers is taken from the Segment Routing Global Block (SRGB). SRGB is a subspace of a 32bit SID space, and it takes values from 16000 up to 23999 [29] .

The local segment is an instruction that is supported by the node originating it. Local segments take a value outside of the SRGB range. Since it has only local significance, its value is related only to local router FIB. A router is not aware of local segments of the other routers in a domain.

Moreover, the local SID values could be reused within an IGP domain, since a local SID value has local meaning for every single router [5].

2.2.2. Control Plane and Forwarding Plane

Segment Routing can be implemented using either MPLS or IPv6 forwarding plane. In MPLS case the segment is encoded as label and segment list as a stack of labels. Node processes the top segment (label) and when the segment is completed, the related label is popped. This means that Segment Routing can use the existing MPLS forwarding paradigm without any change [28].

Segment Routing IPv6 forwarding plane uses a new routing header where segments are encoded as IPv6 addresses. The destination address of the packet indicates the currently active segment. When a segment is completed, the segments left the field in the routing header are decremented and the destination address is updated to the next segment in the segment list [32].

Segment Routing uses existing IGPs IS-IS and OSPF for distributing segments within the IGP domain. These segments are called IGP segments and they are associated with prefixes and adjacencies in the IGP domain. IGP segment distribution is implemented using extensions for IS-IS and OSPF [29].

2.2.2.1. Segment Routing Signaling (Control Plane)

IGP protocols running between adjacent routers maintain session information and advertise IP Prefixes to enable routers to build a complete network topology. In addition, IGP protocols run the Shortest Path Algorithm on each router to determine the best route for each destination and then populate these routes in the routing table [33]. The structure of IGP protocols allows for extensions to enable the exchange of additional network attributes required to support advanced functions such as traffic engineering. For segment routing, these extensions include router capabilities, segment types, segment values, and forwarding options [7].

The control plane exchanges routing information and label with the adjacent routers. Routing information is advertised to any of the routers in the MPLS domain whereas label binding information is advertised to only adjacent routers by link-state routing protocols. It consists of two types of protocols namely routing protocols (e.g., RIP, EIGRP, OSPF, and BGP) and label exchange information protocols (e.g., LDP, TDP, RSVP, etc.) [34].

2.2.2.2. Segment Routing Packet Forwarding (Data Plane)

When an IP packet is inserted into an SR domain, the first router adds a segment or a list of segments based on the destination address and the local routing policy. The IP packet is then forwarded within the SR domain based on the type and value of the SR segment and the routing algorithm. The default routing algorithm within the SR domain is based on IGP ECMP-aware shortest path algorithm.

The ability to specify transit nodes or links for certain traffic flows or under certain conditions enables SR to support advanced protection algorithms that provide fast reroute function without an additional traffic engineering protocol (i.e., RSVP-TE.). The data plane has a forwarding plane that is based on the information attached to labels. There are two types of tables, namely the Label Information Base (LIB) and Label Forwarding Information Base (LFIB). LFIB is used by the data plane to forward the labeled packets. LIB table contains all the local labels and the mapping of the labels which is received from the adjacent routers. The information in LFIB and label value is used by the MPLS-enabled routers to make forwarding decisions [24].

2.3. SR Traffic Engineering (SR-TE)

The research and standardization activities on Segment Routing created mainly with the goal of overcoming some scalability issues and limitations that had been identified in the traffic-engineered Multi-Protocol Label Switching (MPLS-TE) solutions used for IP backbones [24]. In particular, it was observed that MPLS-TE requires an explicit state to be maintained at all hops along an MPLS path and this may lead to scalability problems in the control-plane and in the data-plane. Moreover, the per-connection traffic routing model of MPLS-TE does not easily exploit the load balancing offered by Equal Cost Multipath (ECMP) routing in plain IP networks. On the other hand, Segment Routing can steer traffic flows along traffic-engineered paths with no per-flow state in the nodes along the path and exploiting ECMP routing within each segment [14][35].

In the early 2010s, the IETF started the “Source Packet Routing in Networking” Working Group (SPRING WG) to deal with Segment Routing. The activity of the SPRING WG has included the identification of Use Cases and Requirements for Segment Recently, the WG has issued the “Segment Routing Architecture” document (RFC 8402) [5]. In particular, it was

observed that MPLS-TE requires an explicit state to be maintained at all hops along an MPLS path and this may lead to scalability problems in the control-plane and in the data-plane. Moreover, the per-connection traffic steering model of MPLS-TE does not easily exploit the load balancing offered by Equal Cost Multipath (ECMP) routing in plain IP networks. On the other hand, Segment Routing can steer traffic flows along traffic-engineered paths with no per-flow state in the nodes along the path and exploiting ECMP routing within each segment.

The implementation of the Segment Routing Architecture requires a Data Plane which is able to carry the segment lists in the packet headers and to properly process them. Control Plane operations complement the Data Plane functionality, allowing to allocate segments (i.e. associate a segment identifier to specific instruction in a node) and to distribute the segment identifiers within an SR domain.

As for the Data Plane, two instantiations of the SR Architecture have been designed and implemented, SR over MPLS (SR-MPLS) and SR over IPv6 (SRv6). With SR-MPLS, no change to the MPLS forwarding plane is needed [6]. SRv6 is based on a new type of IPv6 routing header called SR Header (SRH) [7]. As for the SR Control Plane operations, they can be based on a distributed, centralized or hybrid approach. In the centralized approach, an SR controller allocates the segments, takes the decision on which packets need to be associated with which segment lists and configures the nodes accordingly. Very often, a hybrid approach which consists in the combination of distributed and centralized approach is used .

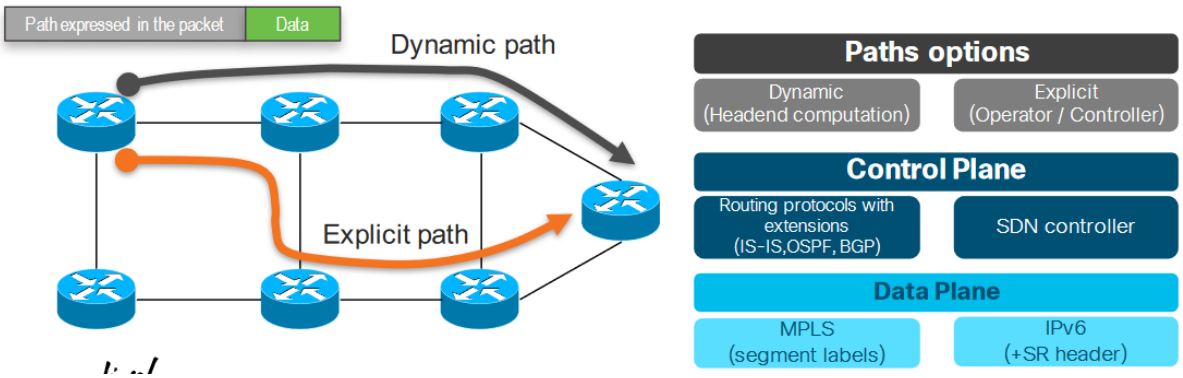


Figure 3: End to end forwarding behavior defined in the packet [35]

In the distributed approach, the routing protocols are used to signal the allocation of segments and the nodes take independent decisions to associate packets to the segment lists. In the

context of an IGP-based distributed control plane, two topological segments are defined: the IGP-Adjacency segment and the IGP-Prefix segment. In the context of a BGP-based distributed control plane, two topological segments are defined: the BGP peering segment and the BGP-Prefix segment. The headend of an SR Policy binds a SID (called a Binding segment or BSID) to its policy. When the headend receives a packet with an active segment matching the BSID of a local SR Policy, the headend steers the packet into the associated SR Policy.

SR-TE benefit

- **Simple, Automated and Scalable**
  - No Core State: state is in the packet header
  - No tunnel interface: “SR Policy”
  - On Demand policy instantiation
  - Automated Steering of packets
- **Multi-Domain**
  - SR Controller
  - Binding-SID for stitching multiple segments
- **SR-TE architecture applies to MPLS and IPv6 applications**
- **SR-TE next-hop** is a list or lists of SIDs that operator wants incoming traffic to use.

2.4. Different Flavors for SR

Table 1 presents the different flavors for Segment Routing.

Table 1: Different flavors for SR [22]

	SR-MPLS	**SRv6**	**SR-MPLS over UDP/IP**
IGP	IPv4, IPv6	IPv6	IPv4, IPv6
Segment Identifier	Label (20 bits)	IPv6 address (128 bits)	Label (20 bits)
Forwarding	Label Switching	IPv6, SRv6	IPv4, IPv6
Forwarding operation	Push, Pop, Swap	IPv6 header update	IP (v4/v6) over UDP
SRTE Path	Stack of Labels (20 bit SIDs)	Stack of IPv6 addresses	Stack of Labels
Entropy	Entropy Label	Flow Label	UDP source Port
Integration in to existing network	All nodes need SR	Seamless integration	Seamless integration
Draft	draft-ietf-spring-segment-routing-mpls	draft-ietf-6man-segment-routing-header	draft-ietf-mpls-sr-over-ip

To summarize: In Segment Routing, the path a packet follows is represented by a stack of labels pushed down to the packet by an edge router. Each label represents a segment - a particular forwarding instruction that determines how the packet will be forwarded.

A global segment is an ID value bearing significance inside the entire SR domain. This means that every node in the SR domain knows about this value and assigns the same action to the associated instruction in its LFIB. The reserved label range used for these purposes is <16000 - 23999>, it is called Segment Routing Global Block (SRGB) and it is a vendor-specific range, therefore, other vendors may use a different range.

A local segment, on the other hand, is an ID value holding local significance, and only the originating node (the router advertising it) can execute the associated instruction. As this

range is only relevant for that particular node, these values are not in the SRGB range but in the locally configured label range. Segment Routing recognizes many particular types of segments that belong either to the global or the local segment class. Let's have a look at some of them:

IGP Prefix Segment: A globally significant segment that is distributed by IGPs (IS-IS/OSPF) and whose path is computed as the shortest path towards that specific prefix. This also allows it to be ECMP-aware. The actual SID value of an IGP Prefix Segment is configured by the administrator on a per-interface basis, and it is also the administrator's responsibility to make sure that this value is unique in the entire SR domain. Typically, the SID would be configured on loopback interfaces to identify nodes in the cloud. An IGP Prefix Segment is very similar to a loose source routing hop.

IGP Adjacency Segment: A locally significant segment distributed by IGPs (IS-IS/OSPF) which describes a particular link - or better put, an IGP adjacency between two neighboring routers. As opposed to IGP Prefix Segments, the SID for an Adjacency segment would be assigned by the router itself and does not require an administrator's intervention. The instruction related to this segment can be explained as "Pop label and forward on the IGP adjacency".[36] .Pushing multiple labels representing segments of the same type onto a packet essentially provides exactly the same functionality as IP Source Routing does: Multiple IGP Prefix Segments are nothing else than Loose Source Routing; multiple IGP Adjacency segments are nothing else than Strict Source Routing - but here, based on MPLS labeling, and, provided with a sufficient MTU reserve, not limited anymore to just 9 explicit hops.What might not be obvious is that labels for both segment types can be freely combined and pushed onto a packet! Their combination is a superset of what plain IP Source Routing was able to accomplish and provides ample space for more complex source routing scenarios including backup paths and fast-reroute-alike detours where traffic can be steered through the network routing around a failure.

BGP Prefix Segment: Similar to IGP Prefix segment and holding global significance, BGP Prefix Segment represents the shortest path to a specific BGP prefix and, of course, is ECMP-aware. As opposed to IGP Prefix Segment that is advertised by an IGP, this segment is signaled by BGP.Since the Prefix segments (IGP Prefix and BGP Prefix segment types) have a global significance, it was necessary to consider that MPLS routers might reserve the same

range of label values for SR deployment, and it might not be possible to expect that all routers will be able to use the same label for the same segment. There are various reasons for that:

Different vendors might allocate different default ranges; gradual SR deployment into an existing MPLS network may face the obvious issue of the label range already partially used or label ranges configured differently on different routers. Therefore, Prefix segments introduce a level of indirection: Each router advertises its own range of labels reserved for Prefix segments in its link-state packets, and this range is called the Segment Routing Global Block (SRGB). Individual Prefix segment IDs are then advertised as offsets, or indexes, from the beginning of the label range, instead of absolute values. Typically, the SRGB range starts at 16,000, and this is what we call the default SRGB.this way traffic engineering algorithms for load balancing or, in case of failures, rerouting traffic can be used more efficiently [37] . While Segment Routing is based on core networks in which MPLS is used for routing, SRv6 aims to be an IPv6 header extension that is compatible with any IPv6-enabled software stack [38].

3. Segment Routing MPLS

3.1. Overview of SR-MPLS

The need for one converged packet network to deliver all fixed and mobile services, regardless of the access technology, advances from time to time. The success of MPLS in core networks and the benefits it brings have enabled the way for the technology to be implemented in aggregation and access networks as an alternative to ATM or legacy Ethernet-based aggregation. Now the mobile backhaul service has been deployed widely, the requirement of the integration of mobile backhaul networks and core networks has been proposed [30]. Deploying a service from one MPLS region to another requires provisioning at several intermediate points in the end-to-end network, making troubleshooting and fault recovery more complex. A preferred approach would be to deploy a single end-to-end service and transport network architecture [10].

The MPLS architecture RFC3031 defines a label distribution protocol as a set of procedures by which one Label Switched Router (LSR) informs another of the meaning of labels used to forward traffic between and through them. The MPLS architecture does not assume a single label distribution protocol. In fact, a number of different label distribution protocols are being standardized. Existing protocols have been extended so that label distribution can be piggybacked on them. New protocols have also been defined for the explicit purpose of distributing labels. The MPLS architecture discusses some of the considerations when choosing a label distribution protocol for use in particular MPLS applications such as Traffic Engineering RFC2702.

Segment Routing leverages the source routing paradigm. A node steers a packet through an SR Policy instantiated as an ordered list of instructions called "segments". A segment can represent any instruction, topological or service-based. A segment can have a semantic local to an SR node or global within an SR domain. SR supports per-flow explicit routing while maintaining a per-flow state only at the ingress nodes to the SR domain. A segment may be associated with a topological instruction. A topological local segment may instruct a node to forward the packet via a specific outgoing interface. A topological global segment may instruct an SR domain to forward the packet via a specific path to a destination. Different

segments may exist for the same destination, each with different path objectives (e.g., which metric is minimized, what constraints are specified) [8].

Segment Routing can be directly applied to the MPLS architecture with no change in the forwarding plane. This Chapter describes how Segment Routing operates on top of the MPLS data plane. Segment Routing, applied to the MPLS data plane, offers the ability to tunnel services (VPN, VPLS, VPWS) from an ingress PE to an egress PE, without any other protocol than ISIS or OSPF [17] and [18]. LDP and RSVP-TE signaling protocols are not required [39].

3.2.MPLS Instantiation of Segment Routing

MPLS instantiation of Segment Routing fits in the MPLS architecture as defined in RFC3031 both from a control plane and forwarding plane perspective: From a control plane perspective, RFC3031 does not mandate a single signaling protocol. Segment Routing makes use of Link State IGPs since their flooding mechanism fits very well with label stacking on ingress.

From a forwarding plane perspective, Segment Routing does not require any change to the forwarding plane. When applied to MPLS, a Segment is an LSP and the 20 right-most bits of the SID are encoded as a label. This implies that, in the MPLS instantiation, the SID values are allocated within a reduced 20-bit space out of the 32-bit SID space [40]

The notion of an indexed global segment, defined in RFC8402 [8], fits the MPLS architecture RFC3031 as the absolute value allocated to any segment (global or local) can be managed by a local allocation process (similarly to other MPLS signaling protocols). Contrary to RSVP-based explicit routes where tunnel midpoints maintain states, SR-based explicit routes only require per-flow states at the ingress edge router where the traffic engineer policy is applied [41].

3.3. SCALABILITY ISSUES OF LDP AND RSVP-TE

LDP and RSVP-TE are the de-facto signaling and label distribution protocols in IP/MPLS network used for years, but are they scalable?

3.3.1. Control Plane Sessions

For LDP each router maintains sessions (LSPs state), which are equal to the number of LDP neighbors. For RSVP-TE, the number of sessions is equal to the total number of LSPs in which the router is involved (whether ingress, egress or transit). In the RSVP-TE case, if a topology includes N fully meshed routers, there will be a need to maintain a state of N x N (N square) LSPs in each router[39]. This quickly runs into an N square problem because of the number of N increases. From a control session perspective, RSVP-TE can run into scalability issues [42].

3.3.2. FORWARDING STATE

LDPs maintain forwarding state of all Forwarding Equivalence Class (FEC) in the network because each FEC is reachable by any other LDP router in a network. RSVP-TE only keeps the forwarding state of the LSPs that traverse through it and potentially their protection path. From a forwarding state perspective, LDP runs into scalability issues if a network becomes extremely large.

RSVP-TE can also perform traffic engineering in IP/MPLS networks; however, it involves complex tunnel configurations on interfaces and is difficult to troubleshoot. LDP cannot do traffic engineering, but it can lose synchronization of the LDP and IGP because LDP depends on IGP for route convergence [6] [7].

SR is scalable [6] because it does not rely on LDP/RSVP-TE, and there is no need of keeping thousands of labels in an LDP database. It avoids thousands of MPLS traffic engineering LSPs in the network. SR uses extensions to existing IGP protocols for signaling purposes. Relying on IGP has other benefits too; it can take advantage of Equal Cost Multi-Path Routing (ECMP) to load balance across multiple available paths in the network and gain better bandwidth utilization. This kind of flexibility does not exist in current RSVP-TE, which would need complex manual configurations for ECMP functionality [7].

3.4. Unified SR-MPLS

In the past, it was necessary to provide connectivity between the different domains and the core on per service level and not based on MPLS (e.g. by deploying native IP Routing or

Ethernet-based technologies between aggregation and core). In most cases service specific configurations on the border nodes between core and aggregation were required. New services led to additional configurations and changes in the provisioning tools. With Unified MPLS there are no technology boundaries and no topology boundaries for the services [14]. Network (or region) boundaries are for scaling and manageability and do not affect the service layer since the transport pseudowire (layer 2 VPN) that carries packets from the access node to the service node doesn't care whether it takes two hops or twenty, nor how many region boundaries it needs to cross. The network architecture is about network scaling, network resilience and network manageability; the service architecture is about optimal delivery: service scaling, service resilience (via replicated service nodes) and service manageability. The two are decoupled: each can be managed separately and changed independently [9].In the following subsections, key characteristics offered by Seamless MPLS is discussed [12].

Unified MPLS [43] provides the framework for taking MPLS end-to-end in a scalable fashion, extending the benefits of traffic engineering and guaranteed service-level agreements (SLAs) with deterministic network resiliency. In Seamless MPLS all forwarding of packets within a network, from the time a packet enters the network until it leaves the network, is based on MPLS labels [12].

The motivation of Unified MPLS is to provide an architecture which supports a wide variety of different services on a single MPLS platform fully integrating access, aggregation and core networks by the addition of extra features with classical/traditional MPLS and it gives more scalability, security, simplicity, manageability and flexible end-to-end service delivery. In order to obtain a highly scalable architecture, Seamless MPLS takes into account that typical access devices such as Digital Subscriber Line Access Multiplexer (DSLAM) and Multi-service access node (MSAN) are lacking some advanced MPLS features, and may have more scalability limitations. Hence access devices are kept as simple as possible [9]. Seamless MPLS is not a new protocol suite but describes the architecture by deploying existing protocols like BGP, LDP, OSPF and ISIS (Intermediate System-Intermediate System) [44].

Building on the success of MPLS technology, Segment Routing follows the same forwarding paradigm by using labels to direct traffic flows, but it achieves that with simplified control plane protocols. Segment Routing utilizes a source-based routing scheme that encodes the traffic paths as MPLS labels into the packet header (called segments). Each segment can

identify a node (transit or destination), link or service. Including these labels/segments in the packets removes the burden of establishing transport LSPs in advance. Also, by exchanging these segments via extensions of IGP protocols (which are already running on the IP network), segment routing eliminates the need for transport label signaling protocols (LDP and RSVP-TE). This simplifies the MPLS router configuration and enhances scalability due to the reduced burden on the routers [45].

Enhancing MPLS Fast Reroute Capabilities utilizing an advanced Fast Reroute algorithm: Topology Independent Loop-Free Alternate (TI-LFA). Routers identify failures of adjacent links and nodes and perform quick local repair via pre-calculated backup routes. Traditional fast reroutes schemes such as IP FRR (LFA or Remote LFA) or MPLS FRR may not provide optimal protection paths in certain topologies or scale due to a large number of RSVP-TE or LDP tunnels. Segment Routing TI-LFA calculates optimal post-convergence backup routes that are readily available upon failure detection. By using segment labels to reach selected transit nodes along the backup routes, segment routing eliminates the need for LDP or RSVP-TE tunnels further simplifying MPLS configuration and enhancing network router scalability [46].

Simplifying the Network Design and Operation of MPLS based network by consolidating signaling protocols and keeping the service and path setup at the edge of the network. Without the need to track transit tunnels, MPLS core routers can scale to support a larger number of paths and services. Additionally, keeping the network and services set up at the edge of the network allows for more efficient programming of traffic-engineered paths. This can be accomplished via a centralized application (or network controller) using the Path Computation Element (PCE) server, and this approach is aligned with the network centralization and automation objectives of Software Defined Networking (SDN).

Network transport infrastructure simplified leading to scalability, superior protection capabilities, coupled with compatibility with MPLS forwarding methods is a key tenant for the design of mission-critical networks. In conclusion, Segment Routing represents an evolution of IP/MPLS network architecture. The evolution embodying “Simplicity is prerequisite for reliability,” an adage by Edsger Dijkstra.

3.5. Unified SR-MPLS Transport Network Overview

The unified MPLS implements a divide-and-conquer strategy where the core, aggregation, and access networks are partitioned in different MPLS/IP domains that are isolated from Interior Gateway Protocol (IGP) perspective. The adoption of divide-and-conquer strategy reduces the size of routing and forwarding tables within each domain, which in turn leads to better stability and faster convergence. The SR enabled IGP is used for label distribution to build Label Switched Path (LSP) within each independent IGP domain. This enables a device inside an access, an aggregation, or a core domain to have reachability through intra-domain SR LSPs to any other device in the same region. Within a domain, both Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) are suitable choices of IGP protocols, but the protocol selection is based on operator's preference.

Reachability across domains is achieved either using RFC 3107 procedures whereby BGP-Labeled Unicast (BGP LU) is used to build inter-domain hierarchical LSPs across domains, or by a controller that pushes the segment list (SR label stack) for a particular service. This allows the link state database of the IGP in each isolated domain to remain as small as possible, leaving all external reachability information to be carried through BGP, which is designed to scale to the order of millions of routes.

In Single-AS multi-area designs, the interior Border Gateway Protocol (iBGP)-labeled unicast is used to build inter-domain LSPs. In Inter-AS designs, the iBGP-labeled unicast is used to build inter-domain LSPs inside the AS, while exterior Border Gateway Protocol (eBGP)-labeled unicast is used to extend the end-to-end LSP across the AS border. In both the cases, the unified MPLS transport across domains uses hierarchical LSPs that rely on a BGP-distributed label to transit across the isolated MPLS domains, and on SR segment within the domain to reach the inter-domain Border Router (BR) or Autonomous System Border Router (ASBR) corresponding to the labeled BGP next hop. If an IGP domain is not SR capable, the domain can run LDP instead of SR. Alternatively, a controller with visibility on the entire network can provide the end to end path for inter-domain reachability. Such visibility is attained through BGP Link State (BGP-LS) feeds from each domain providing topology and state information.In general, (as in the case of Cisco and Juniper) there are three transport options in SR-MPLS [47].

1. **Traditional BGP LU**:-This is a protocol driven transport that was also supported in the previous MPLS. It relies on BGP to build the end-to-end hierarchical LSP. Fast convergence across IGP boundaries is accomplished using BGP Prefix Independent Convergence (BGP PIC) feature. This model is suitable for networks such as traditional MPLS network.
2. **BGP LU with BGP Prefix SID:-**This is also a protocol driven transport. However, the BGP prefix SID feature enables to uniquely identify each IGP border node and service node in the network using a unique prefix segment ID (BGP prefix SID). This transport option requires end-to-end segment routing capability as well as BGP prefix SID capability at IGP border routers.
3. **Programmable Transport:-**This transport option is SDN driven. Each domain runs IGP/SR across the domain, and two IGP border routers in each domain uses BGP LS to feed topology, bandwidth, reliability, latency, SRLG and other transport states of the IGP domain to the SDN controller. The SDN controller uses the topology data and current state of the network, to build the best path and alternate disjoint path that satisfies a given service requirement and pushes the corresponding segment list to the service edge router.

3.6.Segment Routing MPLS Interworking with LDP

Segment Routing control plane can coexist with current label distribution protocols such as LDP [RFC5036].This document outlines the mechanisms through which SR interworks with LDP in cases where a mix of SR-capable and non-SR-capable routers coexist within the same network and more precisely in the same routing domain [8].

3.6.1. LDP Overview

LDP is a protocol defined for distributing labels. It is the set of procedures and messages by which Label Switched Routers (LSRs) establish Label Switched Paths (LSPs) through a network by mapping network-layer routing information directly to data-link layer switched paths[48]. These LSPs may have an endpoint at a directly attached neighbor (comparable to IP hop-by-hop forwarding), or may have an endpoint at a network egress node, enabling switching via all intermediary nodes.LDP associates a Forwarding Equivalence Class (FEC) RFC3031 with each LSP it creates. The FEC associated with an LSP specifies which packets

are "mapped" to that LSP. LSPs are extended through a network as each LSR "splices" incoming labels for a FEC to the outgoing label assigned to the next hop for the given FEC [8].

3.6.1.1. LDP Message Exchange

There are four categories of LDP messages:

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

3.6.2. LDP to SR Behavior

It has to be noted that no additional signaling or state is required in order to provide interworking in the direction LDP to SR. An SR node having LDP neighbors MUST create LDP bindings for each Prefix-SID learned in the SR domain by treating SR-learned labels as if they were learned through an LDP neighbor. In addition, for each FEC, the SR node stitches the incoming LDP label to the outgoing SR label. This has to be done in both LDP-independent and ordered label distribution control modes as defined in RFC5036 [8].

3.6.3. SR to LDP

This section defines the Segment Routing Mapping Server (SRMS). The SRMS is an IGP node advertising mapping between Segment Identifiers (SID) and prefixes advertised by other IGP nodes[49]. The SRMS uses a dedicated IGP extension (IS-IS, OSPFv2, and OSPFv3), which is protocol specific and defined in RFC8665, RFC8666, and RFC8667.The SRMS function of an SR-capable router allows distribution of mappings for prefixes not locally attached to the advertising router and therefore allows advertisement of mappings on behalf of non-SR-capable routers.The SRMS is a control-plane-only function that may be located anywhere in the IGP flooding scope. At least one SRMS server MUST exist in a routing domain to advertise Prefix-SIDs on behalf of non-SR nodes, thereby allowing non-LDP routers to send and receive labeled traffic from LDP-only routers. Multiple SRMSes may be

present in the same network (for redundancy). This implies that there are multiple ways a prefix-to-SID mapping can be advertised. Conflicts resulting from inconsistent advertisements are addressed by RFC8660 [8].

3.6.4. Segment Routing Mapping Server (SRMS)

The SRMS functionality allows assigning of Prefix-SIDs to prefixes owned by non-SR-capable routers as well as to prefixes owned by SR-capable nodes. It is the former capability that is essential to the SR-LDP interworking.The SRMS functionality consists of two functional blocks: the Mapping Server (MS) and Mapping Client (MC). An MS is a node that advertises an SR mappings. Advertisements sent by an MS define the assignment of a Prefix-SID to a prefix independent of the advertisement of reachability to the prefix itself. An MS MAY advertise SR mappings for any prefix whether or not it advertises reachability for the prefix and irrespective of whether that prefix is advertised by or even reachable through any router in the network [8].

An MC is a node that receives and uses the MS mapping advertisements. Note that a node may be both an MS and an MC. An MC interprets the SR-mapping advertisement as an assignment of a Prefix-SID to a prefix. For a given prefix, if an MC receives an SR-mapping advertisement from a Mapping Server and also has received a Prefix-SID Advertisement for that same prefix in a prefix reachability advertisement, then the MC MUST prefer the SID advertised in the prefix reachability advertisement over the Mapping Server Advertisement, i.e., the Mapping Server Advertisement MUST be ignored for that prefix. Hence, assigning a Prefix-SID to a prefix using the SRMS functionality does not prevent assigning the same or different Prefix-SID(s) to the same prefix using explicit Prefix-SID Advertisement such as the above-mentioned Prefix-SID sub-TLVs.For example, consider an IPv4 prefix advertisement received by an IS-IS router in the Extended IP reachability TLV (TLV 135). Suppose TLV 135 contained the Prefix-SID sub-TLV. If the router that receives TLV 135 with the Prefix-SID sub-TLV also received an SR-mapping advertisement for the same prefix through the SID/Label Binding TLV, then the receiving router must prefer the Prefix-SID sub-TLV over the SID/Label Binding TLV for that prefix. Refer to [8] for details about the Prefix-SID sub-TLV and SID/Label Binding TLV.

4. IP Quality of Service

QoS is defined as a mechanism or set of techniques that allows network applications or services can operate as expected. QoS can be defined as well as the ability to provide a performance guarantee in the network. Performance is the speed and reliability of the delivery of various types of load data in a communication system [50].

Network performance may vary due to several problems, such as the problem of packet loss, delay (latency), jitter and throughput, which can make a big enough effect for many applications. For example, voice communications (such as IP Telephony or VoIP) and video streaming can make users frustrated when the application is streaming data packets over the network when bandwidth is not enough, with a delay that cannot be predicted, or excessive jitter. Having regard to packet loss, delay (latency), jitter and throughput can be predicted and matched with the needs of the applications that are used in the existing network depending on the QoS capabilities and how the device is configured [34][51]:

- Prioritizing traffic over other traffic based on the type of protocol, a source or destination address, or a source or destination port number
- Filtering traffic upon ingress or egress
- Controlling the allowed bandwidth transmitted or received on the interfaces of the device
- Applying QoS behavior requirements in the packet header
- Controlling congestion and packet loss.

4.1. QoS Parameters

QoS is a traffic management strategy that allows allocating network resources based on traffic characteristics. These traffic characteristics must be controlled and managed on a hop by hop basis in order to achieve the QoS needed by the traffic. The core QoS parameters which influence the traffic in the IP network are throughput, delay, jitter and packet loss [36, 37] [2]. The factors affecting QoS parameters and the implementation of performance recommendations are shown in the below Figure 4.

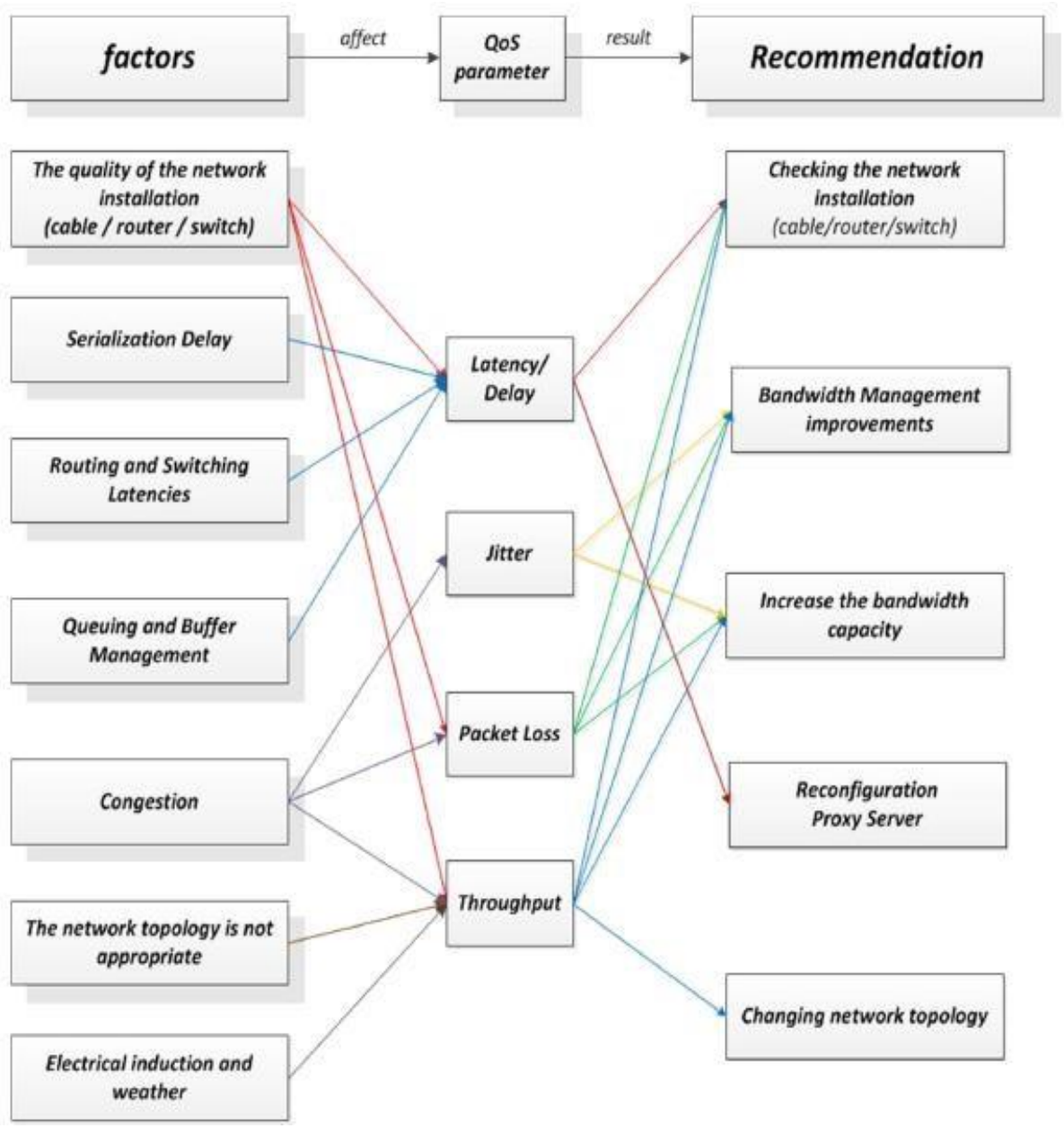


Figure 4. Recommendations for QoS parameters [51]

4.1.1. Throughput

Throughput is a measure of how many units of information a system can process in a given amount of time. Given the dynamic nature of traffic flow across a network, different resources can become bottlenecks at different times [52]. Some of the factors that determine the bandwidth and throughput are network devices, network topology, and a number of network users, etc. The formula for calculating throughput value is shown in

Equation 1

$$\textbf{Throughput} = \frac{\sum \boldsymbol{sent\ data\ (bit)}}{\boldsymbol{time\ data\ delivery\ (s)}}\ [\boldsymbol{bps}]$$

Throughput refers to how much data can be transferred from one location to another in a given amount of time. It is used to measure the performance of hard drives and RAM, as well as the Internet and network connections.

Table 2. Quality standards for throughput [53]

Throughput standard	**Category**	**Throughput/Bandwidth**
	Excellent	100%
	Good	75%
	Medium	50%
	Poor	< 25%

4.1.2. Delay

RFC 7679 defines a metric for measuring one-way delay as the difference in the time at which the datagram crosses two reference points. The delay of a datagram experienced within a service provider network is defined as the difference in the time at which the datagram enters the network and the time at which it leaves the network. It is also commonly referred to as latency [54]. Each element through which a datagram flows in a traffic path will increase the delay experienced by the datagram. From an SLA perspective, the delay is the average fixed delay that an application's traffic will experience within the service provider's network. Delay in TCP/IP networks can be classified as packetization delay, queuing delay, propagation delay, transmission delay and processing delay [35]. The formula for transmission delay is as shown in Equation 2.

Equation 2

$$\boldsymbol{Delay} = \frac{\boldsymbol{packet\ length\ (bit)}}{\boldsymbol{link\ bandwidth}\ (\frac{\boldsymbol{bit}}{\boldsymbol{s}})}\ [\boldsymbol{second}]$$

Table 3. Quality standards ITU-T G.114 for delay [53]

	Category	Delay (ms)
Delay standard	Good	0-150
	Medium	150-400
	Poor	>400

4.1.3. Jitter

RFC 3393 has defined a metric for measuring one-way jitter. Jitter is the variation in the network delay experienced by datagrams. More specifically, it is measured as the delay variation between two consecutive datagrams belonging to a traffic stream. In order to avoid dropping datagrams when a resource is temporarily congested, buffer space is made available in network nodes and the datagrams are queued. Queuing within a network node introduces delay variation between different datagrams of a traffic stream. Although queuing is the main cause of traffic jitter, lengthy reroute propagation delays and additional processing delays can also affect traffic jitter. The formula for calculating jitter value is shown in Equation 3.

Equation 3

$$\boldsymbol{Jitter} = \frac{\sum \boldsymbol{variation\ delay}}{\sum \boldsymbol{packet\ recived}}\ [\boldsymbol{second}]$$

Table 4. Quality standards ITU-T G.114 for jitter [53]

	Category	Jitter (ms)
Jitter standard	Good	0 - 20ms
	Medium	20 - 50ms
	Poor	>50ms

4.1.4. Packet Loss

Packet loss characterizes the datagram drops that occur in the path of one-way traffic flow between a source and destination node. Having buffer space to temporarily queue datagrams in network nodes helps reduce datagram loss, but it cannot be completely eliminated. Some of the factors that contribute to datagram loss are[53] [55]:

- Congestion - Bursty traffic can cause queue overflows resulting in datagram loss.
- Traffic rate-limiting - In order to ensure customer traffic is conforming to a negotiated SLA, service providers may rate-limit incoming traffic and drop non conforming datagrams.
- Physical layer errors - Noise in physical layers can cause bit errors. As a result, upper-layer protocols may drop datagrams.
- Network element failures—Network element failures may cause datagrams to drop until the failure is detected and the connectivity is restored. The formula for calculating the percentage of packet loss value is shown in Equation 4.

Equation 4

$$\textbf{Packets loss} = \frac{\textbf{packets sent} - \textbf{packets recived}}{\textbf{packets sent}} \times \textbf{100}\ \%$$

Table 5. Quality standards for packet loss [53]

	Category	Packet loss
Packet-loss standard	Excellent	0%
	Good	3%
	Medium	15%
	Poor	25%

4.2. QoS Models

How are QoS indicators defined within proper ranges to improve network service quality? The QoS model is involved. The QoS model is not a specific function, but an E2E QoS scheme. For example, intermediate devices may be deployed between two connected hosts. E2E service quality guarantee can be implemented only when all devices on a network use the same QoS service model. International organizations such as the IETF and ITU-T designed QoS models for their concerned services. The following describes three main QoS service models [38] [56] .

4.2.1. Best-Effort

Best-Effort is the default service model for the Internet and applies to various network applications, such as the File Transfer Protocol (FTP) and email. It is the simplest service model, in which an application can send any number of packets at any time without notifying the network. The network then tries its best to transmit the packets but provides no guarantee of performance in terms of delay and reliability. The Best-Effort model is suitable for services that have low requirements for delay and packet loss rate.

4.2.2. Integrated Services (IntServ)

In the IntServ model, an application uses a signaling protocol to notify the network of its traffic parameters and apply for a specific level of QoS before sending packets. The network reserves resources for the application based on the traffic parameters. After the application receives an acknowledgment message and confirms that sufficient resources have been reserved, it starts to send packets within the range specified by the traffic parameters. The network maintains a state for each packet flow and performs QoS behaviors based on this state to guarantee application performance [57].

The IntServ model uses the Resource Reservation Protocol (RSVP) for signaling. The RSVP protocol reserves resources such as bandwidth and priority on a known path, and each network element along the path must reserve required resources for data flows requiring QoS guarantee. That is, each network element maintains a soft state for each data flow. A soft state is a temporary state that is periodically updated through RSVP messages. Each network element checks whether sufficient resources can be reserved based on these RSVP messages.

The path is available only if all involved network elements can provide sufficient resources [58].

4.2.3. Differentiated Services (DiffServ)

Differentiated Services is based on an architecture [RFC 2475] that pushes complex decision making to the edge routers. The DiffServ model classifies packets on a network into multiple classes and takes different actions for each class. When network congestion occurs, packets of different classes are processed based on their priorities, resulting in different packet loss rates, delay, and jitter. Packets of the same class are aggregated and sent as a whole to ensure consistent delay, jitter, and packet loss rate.

Unlike the IntServ model, the DiffServ model does not require a signaling protocol. In this model, an application does not need to apply for network resources before sending packets. Instead, the application sets QoS parameters in the packets, through which the network can learn the QoS requirements of the application. The network provides differentiated services based on the QoS parameters of each data flow and does not need to maintain a state for each data flow. DiffServ takes full advantage of IP networks' flexibility and extensibility and transforms information in packets into per-hop behaviors (PHBs), greatly reducing signaling operations. DiffServ is the most commonly used QoS model on current networks. QoS implementation described in the subsequent sections is based on this model. The DiffServ model involves the following QoS mechanisms:

Traffic classification and marking:-Traffic classification and marking are prerequisites for differentiated services. Traffic classification divides packets into different classes or sets different priorities. Traffic marking sets different priorities for packets and can be implemented through priority mapping and re-marking.

Traffic policing, traffic shaping, and interface-based rate limiting:-Traffic policing and traffic shaping control the traffic rate within a bandwidth limit. Traffic policing drops excess traffic when the traffic rate exceeds the limit, whereas traffic shaping buffers excess traffic. Traffic policing and traffic shaping can be performed on an interface to implement interface-based rate limiting.

Congestion management and congestion avoidance:-Congestion management buffers packets in queues upon network congestion and use a scheduling algorithm to determine the forwarding order. Congestion avoidance monitors network resource usage and drops packets to mitigate network overload if congestion worsens. Traffic classification and marking are the basis of differentiated services. Traffic policing, traffic shaping, interface-based rate limiting, congestion management, and congestion avoidance control network traffic and resource allocation to implement differentiated services.

5. Simulation Results and Analysis

This chapter presents a brief introduction of simulation tools used in analyzing the impact of SR-MPLS on quality of service. Then simulation scenarios and network topologies used for the analysis follow. In the end, simulation results and analysis of the results is discussed.

5.1. Overview of Simulation Tools

5.1.1. Emulated Virtual Environment – Next Generation (EVE-NG)

EVE-NG is a clientless network emulator that provides a user interface via a browser. Users may create network nodes from a library of templates, connect them together, and configure them. Advanced users or administrators may add software images to the library and build custom templates to support almost any network scenario. EVE-NG supports pre-configured multiple hypervisors on one virtual machine. It runs commercial network device software on Dynamips and IOU and runs other network devices, such as open-source routers, on QEMU. EVE-NG is an open-source project Since it runs in a virtual machine, EVE-NG may be set up on any operating system such as Windows, Linux, or Mac OS [9][59] .

5.1.2. IP Service Label Agreement (IP SLA)

Cisco IP SLAs uses active traffic monitoring--the generation of traffic in a continuous, reliable, and predictable manner--for measuring network performance. IP SLAs sends data across the network to measure performance between multiple network locations or across multiple network paths. It simulates network data and IP services and collects network performance information in real-time. The information collected includes data about response time, one-way latency, jitter (inter-packet delay variance), packet loss, voice quality scoring, network resource availability, application performance, and server response time. IP SLAs performs active monitoring by generating and analyzing traffic to measure performance either between Cisco devices or from a Cisco device to a remote IP device such as a network application server [60] [61].

Measurement statistics provided by the various IP SLAs operations can be used for troubleshooting, for problem analysis, and for designing network topologies. Using IP SLAs, service provider customers can measure and provide service level agreements, and enterprise

customers can verify service levels, verify outsourced service level agreements, and understand network performance for new or existing IP services and applications. IP SLAs uses unique service level assurance metrics and methodology to provide highly accurate, precise service level assurance measurements.

Depending on the specific IP SLAs operation, statistics of delay, packet loss, jitter, packet sequence, connectivity, path, server response time, and download time can be monitored within the Cisco device and stored in both CLI and SNMP MIBs. The packets have configurable IP and application layer options such as a source and destination IP address, User Datagram Protocol (UDP)/TCP port numbers, a type of service (ToS) byte (including Differentiated Services Code Point [DSCP] and IP Prefix bits), a Virtual Private Network (VPN) routing/forwarding instance (VRF), and a URL web address. Being Layer-2 transport-independent, IP SLAs can be configured end-to-end over disparate networks to best reflect the metrics that an end-user is likely to experience. Performance metrics collected by IP SLAs operations include the following:

- Delay (both round-trip and one-way)
- Jitter (directional)
- Packet loss (directional)
- Packet sequencing (packet ordering)
- Path (per-hop)
- Connectivity (directional)
- Server or website download time
- Voice quality scores .

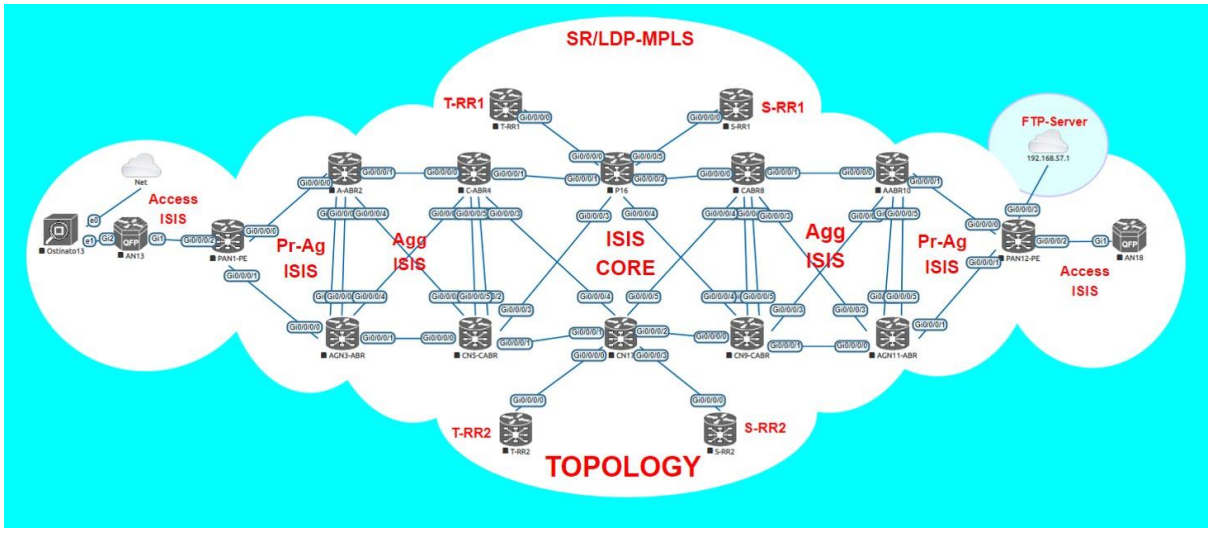
5.1.3. Ostinato

Ostinato is a user-level traffic generation tool with a friendly GUI. It is supported by Windows, Linux, BSD and Mac OS X. The common standard protocols supported by Ostinato are Ethernet/802.3/LLC SNAP; ARP, IPv4, IPv6, IP-in-IP, IP Tunneling (6over4, 4over6, 4over4, 6over6); TCP, UDP, ICMPv4, ICMPv6, IGMP, MLD and many text-based protocols like HTTP, SIP, RTSP, NNTP etc. It also supports client-server architecture. It can create and configure sequential and interleaved streams of different protocols at different rates.

5.2. Simulation Scenarios and Network Topology

In the implementation part, a practical environment is developed using EVE-NG and two scenarios are built in one topology in such away that LDP-prefered and SR-preferd are implemented, In order to test the performance of LDP unified MPLS and Unified SR-MPLS. The two scenarios are built in such a way that first a usual traditional unified MPLS network is built.Then the same network topology is implemented with Unified SR-MPLS technologies.

In both cases, Ostinato , Cisco IP-Sla and background Internet are used for generating network traffic in order to test the performance of the networks with respect to four QoS metrics.Three network traffic generators are implemented in such a way that the first traffic (IP-Sla) injects the required amount of traffic into the network for end-to-end performance analysis while the second which is Ostinato generator injects random network traffic and the last one which is the background Internet traffic injected to create a computation. The last two traffic are not directly used for testing and analysis purpose rather it is to create competition for resources among the network traffics. Finally, the test results are collected from the simulator using Cisco IP-Sla technology for the two scenarios. Figure 5 show LDP/SR based Unified MPLS architecture. In both scenarios, four MPLS domains are used where core, aggregation, pre-agregation and access are indifferent IGP domain.These topologies are representative of today's MPLS architecture supporting any typen of network traffic end-to-end.



SR-MPLS TOPOLOGY

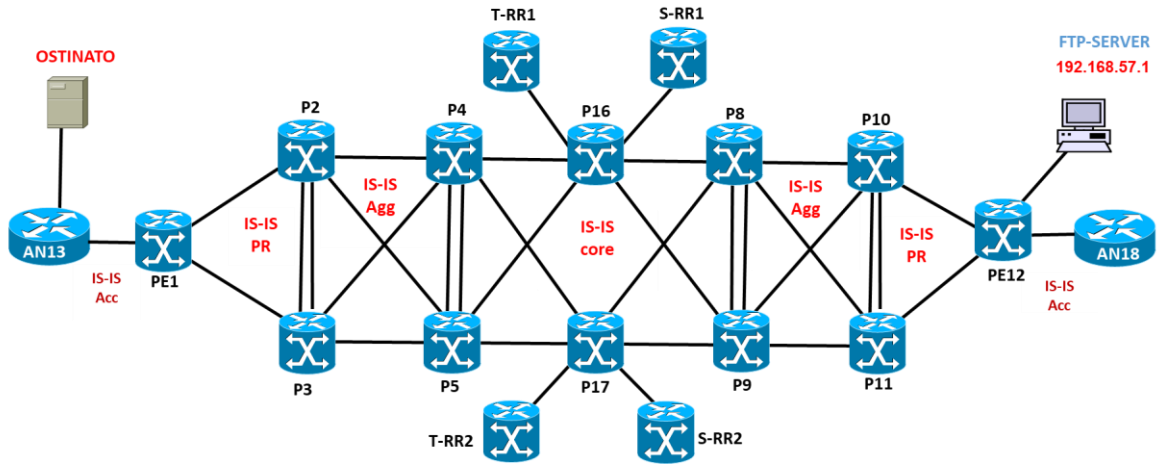


Figure 5. SR/LDP-MPLS TOPOLOGY for the scenario1& 2

5.2.1. Network Topology Design

Figure 5 shows a detailed view of the Simulation network to test, with access, pre aggregation, and aggregation domains in one BGP autonomous system.

The above figure 5 describes the various access domains interconnected through pre-aggregation, aggregation, and core domains using access technologies including MPLS with SR/LDP, each region runs separate IGP domains with SR/LDP, that are interconnected through BGP LU.

Partitioning these network layers into independent and isolated IGP domains helps to reduce the size of routing and forwarding tables on individual routers in these domains, which, in turn, leads to better stability and faster convergence within each of these domains. Intra-domain Label-Switched Paths (LSPs) within the core, LSPs across the core, aggregation, pre-aggregation and access domains are based on BGP labeled-unicast, whereas internal BGP (iBGP) labeled-unicast is used within each autonomous system, and exterior BGP (eBGP) labeled-unicast is used to extend the LSP across autonomous system boundaries [47]. This model is applicable to scenarios where the operator's network needs to be broken into several independent domains to achieve the geographical area and concentration of the customers. Typically, you can scale this network from tens of thousands of nodes to hundred thousand nodes. The network is divided into access, pre-aggregation, aggregation and core domains. Each domain is running a separate IGP (ISIS) domain with segment routing/LDP. The inter-domain nodes such as those between access and pre-aggregation domains, or pre-aggregation and aggregation domains, or aggregation and core domains, act as inline route reflectors that perform BGP labeled unicast (BGP-LU). In the core network, the dedicated transport route reflectors complete the end-to-end advertisements of service edge (SE) to SE reachability information, while the dedicated service route reflectors enable the propagation of service specific routes to the SE nodes. This deployment model achieves a highly scalable network architecture that uses simple building blocks.

All domains are running ISIS with segment routing / LDP, to exchange the internal routes and labels. This is an intra-AS deployment, so that all domains are in single-AS, AS100. All the domains are integrated through BGP labeled unicast, which enables the end-to-end distribution of addresses and associated labels of service edge nodes. To support in the delivery, the following configurations are done:

- Dedicated transport route reflectors such as T-RR1 and T-RR2 and dedicated service route reflectors such as S-RR1 and S-RR2 are implemented in the core.
- Inline route reflectors are configured on the inter-domain nodes
- All these inline route reflectors are configured with next-hop-self, which is used to override the next-hop address of the advertised routes with the local address to enable forwarding towards the destination within each domain. The transport route reflector establishes BGP-LU session with the service route reflector, to advertise all the addresses of the service edge, so that service route reflector has reachability to all the service edge nodes end-to-end.
- For all the relevant services, the client routes are distributed site-to-site through two centralized service route reflectors such as S-RR1 and S-RR2, that peer directly with all the service edge nodes. The service route reflectors also peer with related pre-aggregation and aggregation nodes, for hierarchal services.
- All nodes are running IGP with segment routing / LDP and topology-independent loop-free alternate (TI-LFA) for faster convergence.

5.2.2. Design Considerations:

- **MPLS Access** Node: In this part, the access node is part of an MPLS access network, which could be SR or traditional LDP based MPLS access network.
- **IGP Configuration: -**Two separate IGP instances are configured on each node, for example the core ABR nodes towards the core and aggregation domains. The segment routing (LDP) and TI-LFA are enabled for both the instances.
- **BGP Configuration:-** The BGP configuration in general implemented with the following:
  - BGP-LU session

- BGP-LU session with transport route reflector (core ABR)
- BGP-LU session with service route reflector.
- BGP Prefix-Independent Convergence (BGP-PIC)
- Redistribution of ABR's loopback into BGP.

5.3. Simulation Parameters Analysis

5.3.1. Throughput Analysis

Throughput is one of the QoS parameters which measures how many units of information a system can process in a given amount of time. To compute the throughput, we need to know the amount of data transferred and how long it takes to complete the file transfer. IPsla is used to generate traffic in both scenarios (LDP-MPLS and SR-MPLS). AN13 and FTP-server(Ftp://192.168.57.1/) are used as IPSla-agent/client and IPsla-Server respectively and the file is downloaded from the server to the client at different file sizes using FTP. During the simulation, IP sla collects relevant information including average round trip time required to complete the file download for each file size. Table 6. shows the output of IP sla for both LDP and SR for different FTP file size.For example ftp file size of 300 Kbytes for LDP the RRT is 15.30 sec. so the, throughput is computed as the ratio of the file downloaded to the average of round trip time i.e. (300Kbytes*8bits/byte)/15.30sec = 156.83 Kbps. Using the same procedure for SR file size of 300KB the throughput is (300Kbytes*8bits/byte)/9.80sec = 244.92 Kbps For different file sizes, the test results are tabulated for both scenarios as shown in Table 6.and the throughput is computed and put in the Table 7.

Table 6. Collected Result using IP sla

Collected Result using IP sla		
FTP-KB	LDP-RTT-sec	SR-RTT-sec
100	11.07	7.80
200	12.93	8.34
300	15.30	9.80
400	16.52	10.75
500	16.61	13.15
600	18.32	15.46
800	24.03	19.37
1100	29.81	25.05

Table 7. Throughput for LDP and SR MPLS at different file sizes

FTP(Kbyte)	**Label Distribution Protocol**	**Segment Routing**	Diffrence b/n them	Diffrence In %
100	72.29	102.55	30.26	41.87
200	123.76	191.89	68.13	55.05
300	156.83	244.92	88.09	56.17
400	193.75	297.70	103.95	53.65
500	240.85	304.09	63.24	26.26
600	262.02	310.46	48.44	18.49
800	266.29	330.37	64.08	24.07
1100	295.21	351.34	56.13	19.01
500	201.38	266.67	65.29	32.42
On average				**32.4%**

Figure 6 shows the graph of simulation results of throughput versus FTP file size while downloading the file from the server (FTP-server(Ftp://192.168.57.1/)) to the client (AN13). As can be seen in the throughput graph, at all FTP file size the performance of Unified SR-MPLS is better than that of LDP-MPLS. For example, if we take a file size of 300Kbytes for comparison, the throughput difference is about 88.09Kbps which is 56.17%. There are different reasons for the better throughput of SR-MPLS over LDP-MPLS. Among these : -

- In SR_MPLS forwarding state (segment) is established by IGP unlike LDP (IGP + LDP)

  - SR requires only 1 label per node in the IGP domain which is insignificant: < 1% of label space
- No complex LDP/IGP synchronization
  - One less protocol to operate
- Direct ISIS/OSPF extension

Unlike RSVP and Label Distribution Protocol (LDP), SR requires no MPLS control plane signaling and imposes no changes to the MPLS data plane. SR requires only ingress label edge routers to keep per-service state. State management requirements from the midpoint (label switch routers) and tail end (egress label edge routers) are removed. In the SR domain, nodes and links are assigned segment identifiers (SIDs), which are advertised into the domain by each SR router using extensions to intermediate system-intermediate system/open shortest path first. These SIDs allow an ingress node to select a path through the network using either a single SID to represent the destination node or using a series of SIDs, called a segment list, which specifies a particular path through the network that an SR tunnel should traverse. As a result, it is possible to route paths that are completely independent of the IGP shortest path. Segment Routing accomplishes the same thing as MPLS but is less complex. Better yet, it leverages existing MPLS services and hardware, meaning it does not require new infrastructure and provides an easy migration path. Segment Routing makes the network more scalable and intelligent while improving capacity utilization, leading to lower cost and greater user satisfaction.

The architecture of Segment Routing is based on the source-routing paradigm. It leverages source routing by providing a simple, stateless mechanism to program the path a packet takes through the network. Because the application has complete control over the forwarding path and steers the packet through the network by encoding an ordered list of segments in the packet header, there is no need for path signaling. Therefore, Segment Routing does not create any per-flow state and can scale infinitely and without any limitations. Large service providers, enterprises and financial and federal institutions will for the foreseeable future need high-speed backbone networks that require high throughput with guaranteed delivery and fast convergence for mission-critical real-time systems.

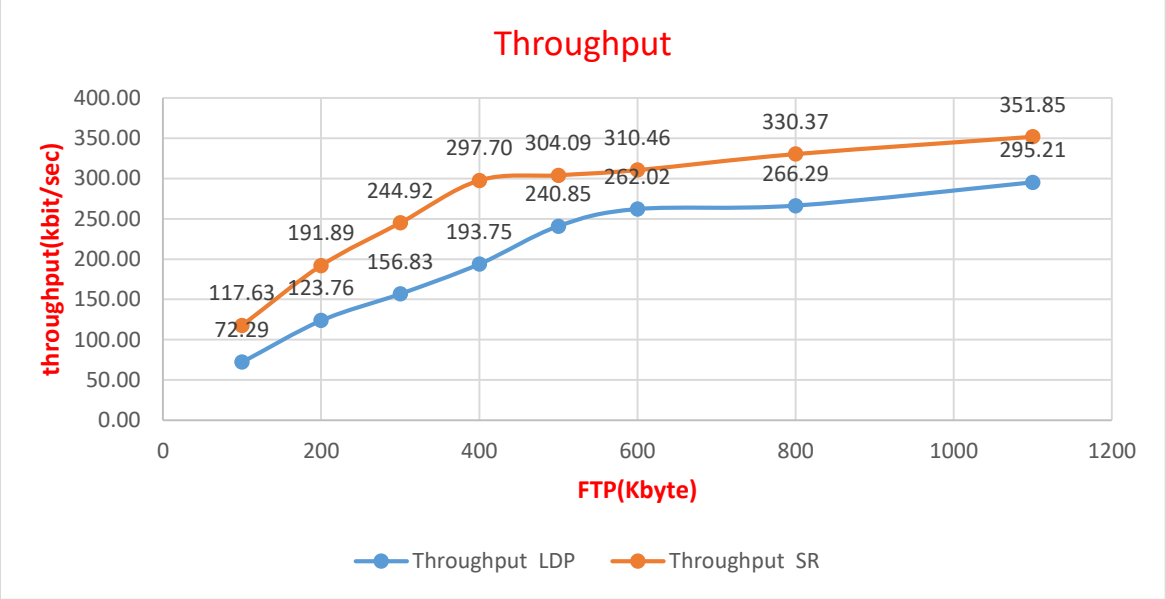


Figure 6. Graph of throughput for scenarios 1 & 2

5.3.2. Latency Analysis

The same topology setup as in the throughput analysis is used for latency analysis, the test instances implemented. The data that is obtained from the throughput analyses is used to calculate the latency shown in Table 8. Network traffic is generated end-to-end and Cisco IP-SLA collects the minimum, maximum and average delay of sending a test message from AN13 to Ftp-Server and vice versa. The latency output of different file size test messages collect using IP sla for both LDP and SR are shown in Table 8.

Table 8. Latency in sec

Data-size(Kbyte)	LDP	SR
100	11.07	7.80
200	12.93	8.34
300	15.30	9.80
400	16.52	10.75
500	16.61	13.15
600	18.32	15.46
800	24.03	19.37
1100	29.81	25.05

To increase the accuracy of the values for each of the latencies, the average of about 60 sample tests are used. For the simulation three congestion levels are considered: data rate less than link bandwidth, data rate equal to link bandwidth and data rate greater than link bandwidth. For the different congestion levels, the average values of simulation results are tabulated in Table 9.

Table 9: : Output of latency for scenarios 1 & 2

FTP(Kbyte)	LDP-Latency-s	SR-Latency-s	Latency -Diffrence-s	Latency -Dif In %
100	11.07	7.80	3.27	29.51%
200	12.93	8.34	4.59	35.50%
300	15.30	9.80	5.50	35.97%
400	16.52	10.75	5.77	34.92%
500	16.61	13.15	3.45	20.80%
600	18.32	15.46	2.86	15.60%
800	24.03	19.37	4.66	19.40%
1100	29.81	25.05	4.76	15.98%
500	18.07	13.72	4.36	24.11%

The latency versus data size graph in Figure 7 shows that the Traditional MPLS (Scenario 1) has higher latency than SR-MPLS (Scenario 2). On average the latency difference between the two scenarios is about 24.11%. That is the latency of SR-MPLS is improved on average by 4.36s (i.e. 24.11%) compared to the MPLS counterpart. This is a significant improvement because a 1ms decrease in latency will increase the data rate by 4000bps. Typically, on the traditional MPLS that the additional LDP protocol plus IGP creates additional latency.in the

case of SR-MPLS, the Assigned label is distributed by the IGP protocol (IS IS) and the label is global so during congestion the SR-MPLS is better.

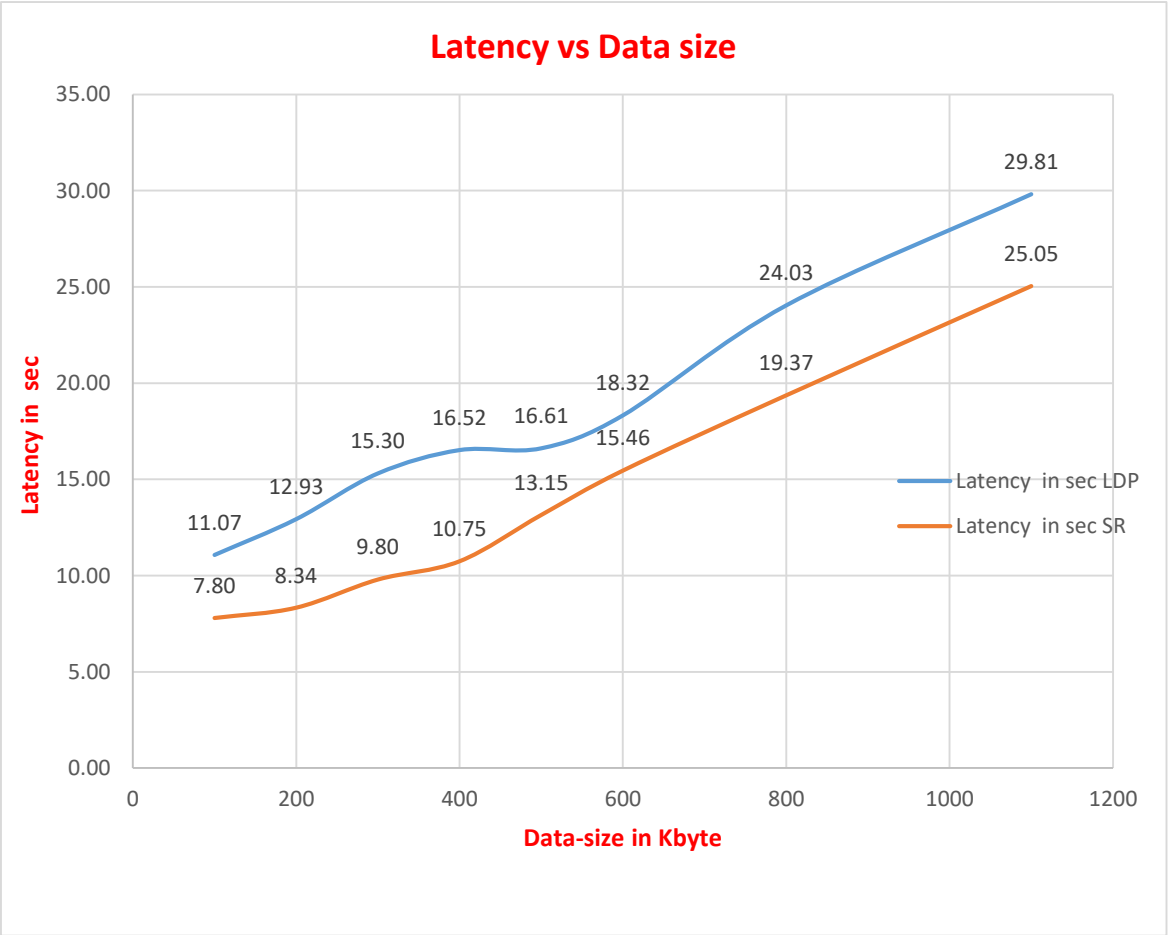


Figure 7: graph of latency test

5.3.3. Packet Loss Analysis

As already discussed in Section 4.1.4 some of the factors contributing to packet loss are congestion, traffic rate-limiting, physical link errors and network element failures. In ITU standards the recommended value for packet loss is less than 3%. For this packet loss analysis, congestion is selected to be a factor for packet loss i.e. the links in the network are deliberately congested by injecting more network traffic into the network using the network traffic generators. This enables us to compare the tolerance of both network scenarios towards congestion. ICMP test type is used to send test probes at three conditions i.e. data rate less than link bandwidth, data rate equal to link bandwidth and data rate greater than link bandwidth. The output of simulation result colleceted using IP sla is tabulated in Table 10..

Packet loss occurs in networks when data packets are lost during transmission or individual data packets arrive late at their destination. Before being sent, data is packaged into several layers.These packets travel through a variety of different hubs (copper cables, fiber optics, wireless, etc.) to reach their destination. In these hubs, TCP packets get lost or become delayed. Once sent, each packet is marked with a timestamp.

This value specifies the amount of time the sender must wait before obtaining confirmation of receipt. If a packet gets lost or is delayed, it eventually “times out”. When this happens, a new packet is sent in its place. This is known as a retransmission timeout (RTO). The result Data packets arrive late and performance suffers.

Table 10: The output of packet loss for scenarios 1 & 2

Data-size(byte)	LDP-paket-loss)	SR-packet-loss	Diffrence b/n them
1000	16	3	13
5000	19	9	10
6000	28	10	18
7000	37	14	23
10000	42	19	23
15000	45	21	24
16000	49	23	26
18024	50	24	26
Average preformance			**20.375**

The other method by which SR-MPLS minimizes the effects of congestion and link failure is by using fast reroute and pre-computed alternative routes. These mechanisms help to use alternative paths and nodes in a sub-second to reduce packet loss. The performance of SR MPLS is much better than that of LDP based MPLS. For example, at a data size of 16000 bytes, there is 26% less packet loss in SR-MPLS. Reason : - fewer protocols to operate, fewer protocol interactions, avoid directed LDP sessions between routers, Deliver automated FRR for any topology .

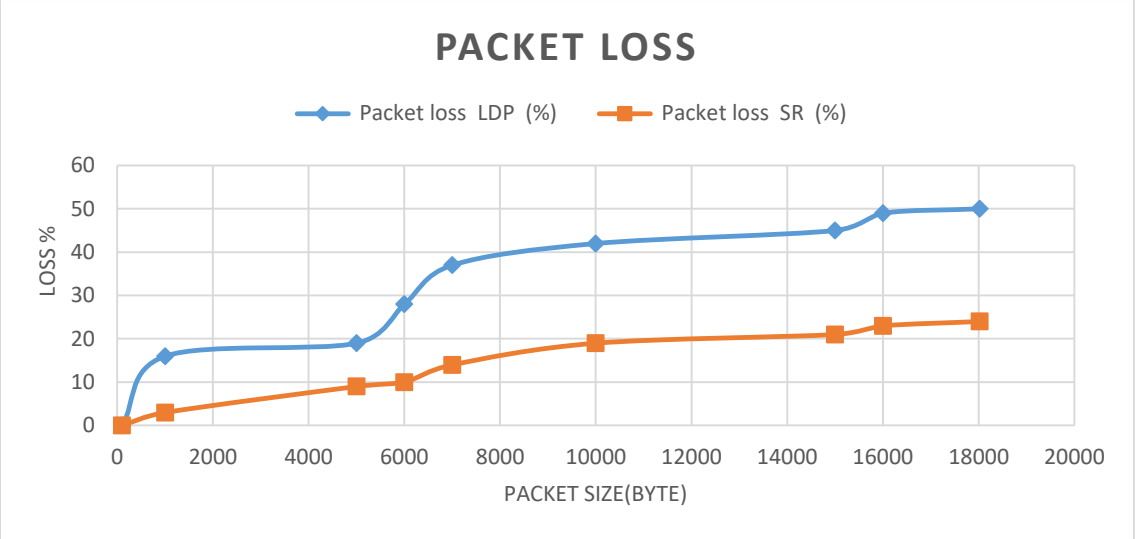


Figure 8. Graph of packet loss for scenarios 1 & 2

5.3.4. Jitter Analysis

Recall that Jitter is a variation in the delay of received packets. At the transmitting side, packets are sent in a continuous stream with the packets spaced evenly apart. Due to network congestion, improper queuing, or configuration errors, the delay between each packet can vary instead of remaining constant. In IP data network packets can take different alternative routes to a destination and may arrive at a different time and this causes variation of delay or jitter.

Table 11. Jitter collected using IP sla for LDP & SR

Data-in-Byte	LDP	SR
500	27	12
1000	90	30
5000	229	207
10000	502	428
15000	684	640
16384	780	703

Using the same procedures and scenarios as for the other parameters, we can simulate and measure the jitter values. In our network topology, there are redundant and alternative routes

to a destination so that packets of one stream can take different alternative routes with variable delay. Since network congestion is a common factor for jitter, our simulation has mainly considered it for jitter analysis. Though the test results can provide us with average jitter from a source node, AN13, to destination node, AN18, independently, The paper used the average jitter for the round trip path to compare the performance of the scenarios as shown in Table 11. As shown in Figure 9, the simulation results of average jitter for SR-MPLS is smaller than that of traditional Unified MPLS. On average, the jitter difference is about 48ms (i.e. 12.6%). This performance difference between the two scenarios has a significant impact on jitter sensitive real-time traffic such as voice, video conference, live streaming, etc. Unlike LDP which is locally significant to peers SR-MPLS maintain (and advertise to its peers) more than one route to a given destination, due to its label global significant. The use of these multiple routes reduce the effects of congestion in the network and hence reduce the jitter.

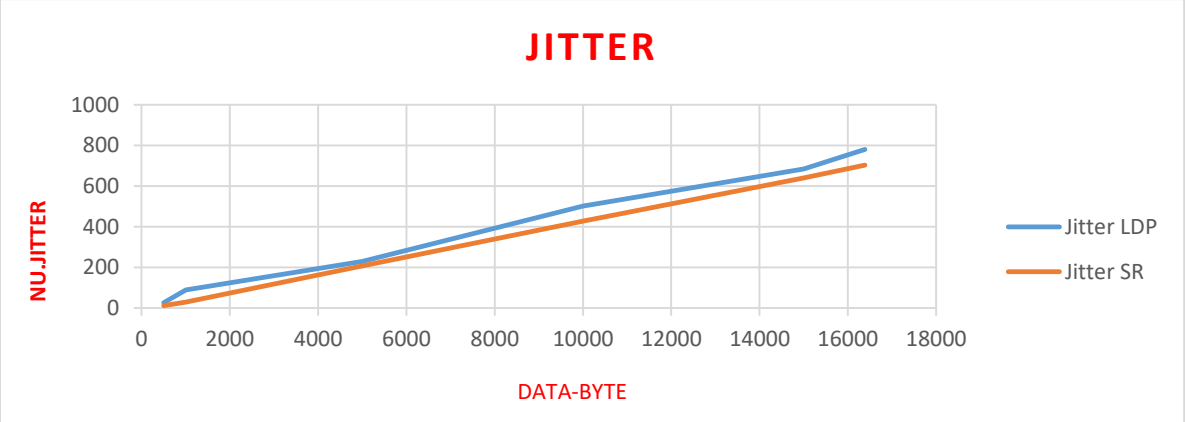


Figure 9. Graph of jitter for scenarios 1 & 2

- The performance of SR MPLS is much better than that of LDP based MPLS.
- On average 12.6% Jitter improvement

Here, we can summarize why the performances of LDP by stating its characteristics as follows:

- The forwarding mechanism of LDP depends on IGP completely and does not maintain any status. The forwarding behavior is similar to IGP.
- The label is valid locally.

- No traffic optimization method: Since the forwarding mode of LDP is the same as IP forwarding, the path is selected only based on the cost value, but not based on other complex conditions such as bandwidth and latency.

In general, to sum up, things LDP relies on IGP state, and features like the Label Distribution Protocol - Interior Gateway Protocol (LDP-IGP) sync were introduced so that they always remain in sync, reducing the possibility of traffic blackholing. With label distribution directly done by IGP, this issue is now unlikely In Segment Routing, nodes and prefixes have globally unique labels assigned throughout the domain, whereas in LDP, these labels are locally significant, assigned a unique value at every hop. Global labels significantly reduce the data plane state at every network hop. Depending on vendor implementation choice, an implementation with LDP independent LSP control mode can multiply unnecessary control and data plane state, resulting in scaling challenges.

Service providers need to reduce current complexities in their networks to compete efficiently with the web-scale over-the-top providers. Network owners have only two options: either continue to grow with the complexities and lose more on capital expense and operational expense or think outside of the box with Segment Routing to solve these issues.

6. Conclusion and Future Work

6.1. Conclusion

In this thesis impact analysis of an end-to-end Unified SR-MPLS architecture is done in comparison with traditional Unified MPLS (LDP based) using four QoS parameters. This work has investigated the limitations in network architecture with traditional untied MPLS domains with additional LDP signaling protocol and explores the possibility of extending SR-MPLS end-to-end by integrating access, pre-aggregation, aggregation and core network layers into single domain through the implementation of Unified SR MPLS architecture without additional protocol like LDP.

To do the analysis and comparison of traditional Unified MPLS and Unified-SR MPLS, four QoS performance metrics such as throughput, latency, packet loss, and jitter are used. First, two scenarios are set up on the same network topology (the one with LDP preference and the other SR-preferred) using the Cisco ISP router and EVE-NG emulator with required configuration files. Next network traffic is generated using Ostinato and Cisco IP-SLA tecnology with additional background internet traffic and then simulation data are collected using Cisco IP-SLA technology and finally the results are presented as a graph using excel 2016. From the study and simulation results the following conclusions can be drawn:

- SR MPLS can improve network performance and reduce the number of Protocols.
- Implementation of QoS in the Unified MPLS network (LDP based) alone does not guarantee end-to-end QoS.
- Segment routing utilizes the network bandwidth more effectively than traditional MPLS networks and offers lower latency.
- Compared to traditional Unified MPLS, Unified SR-MPLS improves the throughput of transferring files from one end of a network to another end of a network by 32.4% on average in the range of file size used in the simulation.
- Unified SR-MPLS improves end-to-end packet delay on average by 24.11% compared to traditional Unified MPLS.
- At the same congestion levels Unified SR MPLS reduces packet loss by 20.4% and jitter by 12.6%.

- Any service provider, including Ethio telecom, Can implement SR MPLS at the same time integrate the separated network domains such as mobile backhaul and IP core networks into single SR MPLS domain and reduce additional protocol overhead with minimum cost and simplified management to enhance QoS requirement and hence improves customer satisfaction, Guaranteed SLA and Network Efficiency.
- Defined as a modern variant of source routing, segment routing simplifies the network by removing network state information from intermediate routers and placing path state information into packet headers. When a packet arrives at an SR ingress node, the ingress node subjects the packet to policy. The policy associates the packet with an SR path to its destination. The SR path is an ordered list of segments that connects an SR ingress node to an SR egress node. This SR path can be engineered to satisfy any number of constraints (e.g., link bandwidth, minimum path latency).
- Besides greater simplicity and reduced operations costs, the real force driving adoption of segment routing is the coming of 5G. New 5G services will have various requirements for bandwidth, latency, reliability, and security that can be served by placing computing engines underlying network fabric that can be wisely engineered to deliver those tough requirements without adding operational overhead.

Segment routing is a Simplified Approach to Traffic Forwarding. It simplifies operations and reduces resource requirements in the network by removing network state information from intermediate routers and placing path information into packet headers at the ingress node. With the implementation of new technologies like 5G, the Internet of Things (IoT), and Artificial Intelligence (AI), the need for increased computing capacity at the network edge is growing. This growth is putting increased strain on the IP connectivity and protocols that "glue" the Internet together. The instantiation of SR architecture over the MPLS data plane requires less control plane protocols: There is no need to pre-establish tunnels and the per-flow states are maintained only at the edges of the network. Therefore, no signaling protocols such as LDP and/or RSVP-TE are required. Consequently, the number of states maintained in the network is considerably reduced and improved QoS.

6.2. Future Work

Although the thesis has achieved all the objectives set in Chapter one, there are some issues to be addressed in the future. These issues are:

- Study the effect of interconnecting SR-domain with LDP only capable routers on end-to-end QoS as most of the router especially in the access domain may not be SR-MPLS capable this can include the case of Ethio-telecom. But First, it is better to identify types of the router (or devices) used in the access domain. The access devices must be tested if they can support MPLS and SR-MPLS.
- Implement and analyze Segment Routing Traffic Engineering (SR-TE) on unified SR-MPLS networks to further enhance QoS.
- Analyze the effect of using SR-TE on resource utilization and further improvement of QoS relative to RSVP-TE.

References

[1] H. Kumera, “Analysing Impact of Seamless MPLS on QoS,” AAiT, 2018.

[2] B. De Graaff and M. Kaat, “Segment Routing in Container Networks,” System and Network Engineering , Univesity of Amsterdam, 2017.

[3] S. Bryant, D. Bernier, B. Canada, and J. Tantsura, “Service Chaining using Unified Source Routing Instructions draft-xu-mpls-service-chaining-03,” pp. 1–13, 2017.

[4] T. Hoßfeld, R. Schatz, M. Varela, and C. Timmerer, “Challenges of QoE management for cloud applications,” *IEEE Communications Magazine*, vol. 50, no. 4, pp. 28–36, 2012.

[5] B. M. Sc, E. Cordeiro, and A. Reuter, “Source Packet Routing in Networking (SPRING),” no. May, pp. 31–37, 2017.

[6] C. Filsfils, P. Camarillo, J. Leddy, D. Voyer, S. Matsushima, and Z. Li, “SRv6 Network Programmingsegmentlist,”draft-ietf-spring-srv6-network-programming-00, pp. 1–42, 2019.

[7] B. Informatica, “Informatica — Universiteit van Amsterdam On Service Chaining and Segment Routing,” no. June, 2018.

[8] Clarence Filsfils and Stefano Previdi and Les Ginsberg and Bruno Decraene and Stephane Litkowski and Rob Shakir, “Segment Routing Architecture,” 8402, 2018.

[9] C. Campana, “Introduction to Segment Routing Use cases and its applicability,” in *Introduction to Segment Routing Use cases and its applicability*, 2018, p. 74.

[10] S. Yang, C. Xu, L. Zhong, J. Shen, and G. M. Muntean, “A QoE-Driven Multicast Strategy With Segment Routing--A Novel Multimedia Traffic Engineering Paradigm,” *IEEE Transactions on Broadcasting*, 2019.

[11] R. El-Haddadeh, G. A. Taylor, and S. J. Watts, “Towards scalable end-to-end QoS provision for VoIP applications,” *IEE Conference Publication*, no. 2004–10492, pp. 132–135, 2004.

[12] N. Z. H. Ahmad Khalifeh,Ashkan Gholamhosseinian, "QOS For Multimedia Applications with Emphasize onVideo Conferencing.," Modern Communication System and Networks, 7.5 hp Halmstad University, February 2011.

[13] A. A. Simiscuka, M. Bezbradica, and G. M. Muntean, "Performance analysis of the Quality of Service-aware NETworking Scheme for sMart Internet of Things gatewayS," *2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC 2017*, pp. 1370–1374, 2017.

[14] S. Bidkar, A. Gumaste, P. Ghodasara, A. Kushwaha, J. Wang, and A. Somani, "Scalable segment routing-a new paradigm for efficient service provider networking using carrier ethernet advances," *Journal of Optical Communications and Networking*, vol. 7, no. 5, pp. 445–460, 2015.

[15] H. Wang, T. Du, F. Ding, Y. Liu, S. Huang, and J. Tao, "An end-to-end QoS guarantee scheme in heterogeneous networks," *Proceedings - 3rd International Conference on Instrumentation and Measurement, Computer, Communication and Control, IMCCC 2013*, no. 2009, pp. 384–389, 2013.

[16] K. S. Lui, K. Nahrstedt, and S. Chen, "Hierarchical QoS routing in delay-bandwidth sensitive networks," *Conference on Local Computer Networks*, pp. 579–588, 2000.

[17] M. P. Howarth *et al.*, "End-to-end quality of service provisioning through inter-provider traffic engineering," *Computer Communications*, vol. 29, no. 6, pp. 683–702, Mar. 2006.

[18] Job Snijders and Jakob Heitz and John Scudder, "BGP Administrative Shutdown Communication," 8203, 2017.

[19] J. Zhou, Z. Zhang, and N. Zhou, "A segment list management algorithm based on segment routing," in *2019 IEEE 11th International Conference on Communication Software and Networks, ICCSN 2019*, 2019, pp. 297–302.

[20] L. Bruno, "Segment Routing: Technology deep-dive and advanced use cases," in *BRKRST-3122*, vol. 53, no. 9, 2019, pp. 1689–1699.

[21] N. Slabakov, "Source Routing 2.0."

[22] A. Kaul, “SPRING FORSERVICE PROVIDER NETWORKS,” in *SANOG34*, 2019, p. 132.

[23] A. Abdelsalam, F. Clad, C. Filsfils, S. Salsano, G. Siracusano, and L. Veltri, “Implementation of virtual network function chaining through segment routing in a linux-based NFV infrastructure,” in *2017 IEEE Conference on Network Softwarization: Softwarization Sustaining a Hyper-Connected World: en Route to 5G, NetSoft 2017*, 2017.

[24] S. Bryant, A. Farrel, and J. Drake, “MPLS Segment Routing in IP Networks.” pp. 1–13, 2019.

[25] G. Maila, I. Marius, and C. Victor, “Segment Routing,” in *2017 10th International Symposium on Advanced Topics in Electrical Engineering, ATEE 2017*, 2017, pp. 34–38.

[26] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-defined networking: A comprehensive survey,” *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.

[27] Nagendra Kumar and Carlos Pignataro and Faisal Iqbal and Sasha Vainshtein, “Clarification of Segment ID Sub-TLV Length for RFC 8287,” 8690, 2019.

[28] A. Kaul, “SPRING FOR,” no. August, 2019.

[29] R. Bonica, “A Segment Routing (SR) Tutorial AKA : SPRING,” 2017.

[30] E. Moreno, A. Beghelli, and F. Cugini, “Traffic engineering in segment routing networks,” *Computer Networks*, vol. 114, pp. 23–31, Feb. 2017.

[31] A. I. Basuki, D. Krisnandi, R. Wardoyo, and D. Syamsi, “Sub-Second Path Restoration for Stateful-based Segment Routing,” *2018 International Conference on Computer, Control, Informatics and its Applications: Recent Challenges in Machine Learning for Computing Applications, IC3INA 2018 - Proceeding*, pp. 98–103, 2019.

[32] A. Giorgetti, A. Sgambelluri, F. Paolucci, F. Cugini, and P. Castoldi, “Segment routing for effective recovery and multi-domain traffic engineering,” *Journal of Optical*

Communications and Networking, vol. 9, no. 2, pp. A223–A232, Feb. 2017.

[33] T. Schuller, N. Aschenbruck, M. Chimani, M. Horneffer, and S. Schnitter, "Traffic Engineering Using Segment Routing and Considering Requirements of a Carrier IP Network," *IEEE/ACM Transactions on Networking*, vol. 26, no. 4, pp. 1851–1864, Aug. 2018.

[34] Juniper Networks. Inc, "Junos ® OS MPLS Applications Feature Guide," pp. 1237–1240, 2018.

[35] Hernán Contreras G., "No Network Programming with SRv6."

[36] R. Reflection *et al.*, "Description of BGP Route Reflection," no. Mcid.

[37] S. Bidkar, A. Gumaste, P. Ghodasara, A. Kushwaha, J. Wang, and A. Somani, "Scalable segment routing-a new paradigm for efficient service provider networking using carrier ethernet advances," *Journal of Optical Communications and Networking*, vol. 7, no. 5, pp. 445–460, May 2015.

[38] B. De Graaff, "Segment Routing in Container Networks," 2017.

[39] M. Baldi, "Multiprotocol Label Switching," *Convergence of Mobile and Stationary Next-Generation Networks*, pp. 541–579, 2010.

[40] S. (Cisco) Dasgupta, "Segment Routing – Introduction," pp. 1–34, 2014.

[41] E. Moreno, A. Beghelli, and F. Cugini, "Traffic engineering in segment routing networks," *Computer Networks*, vol. 114, pp. 23–31, 2017.

[42] R. Steenbergen, "MPLS for Dummies," *Nlayer Communications*, p. 64, 2015.

[43] S. X. X. (Huawei) A. F. J. D. (Juniper N. Bryant, "A Unified Approach to IP Segment Routing," *draft-bryant-mpls-unified-ip-sr-00*, vol. draft-brya, p. 14.

[44] H. T. Co, "Segment Routing Technology White Paper Huawei Technologies Co ., Ltd .," Bantian, Longgang Shenzhen 518129 People's Republic of China, 2018.

[45] P. L. Ventre *et al.*, "Segment Routing: a Comprehensive Survey of Research Activities, Standardization Efforts and Implementation Results," pp. 1–28, 2019.

[46] R. Guedrez, O. Dugeon, S. Lahoud, and G. Texier, "A new method for encoding MPLS segment routing TE paths," *Proceedings of the 2017 8th International Conference on the Network of the Future, NOF 2017*, vol. 2018-Janua, pp. 58–65, 2017.

[47] Cisco Systems Inc., *Cisco Evolved Programmable Network Transport Design Guide, Release 5.0*, Release 5. CA 95134-1706: Cisco Systems, Inc.

[48] E. B. Fgee, W. J. Phillips, S. Sivakumar, and W. Robertson, "Comparing IPv4 end-to-end QoS capabilities with QoS techniques using RSVP and MPLS," *Canadian Conference on Electrical and Computer Engineering*, vol. 3, pp. 1455–1460, 2002.

[49] C. Systems, C. Headquarters, and S. Jose, "Cisco Live 2014 San Francisco," no. 6387, 2014.

[50] E. Quality, C. Networks, and D. S. Performance, "Quality of Service Quality of Service," 2005.

[51] M. P. Howarth *et al.*, "End-to-end quality of service provisioning through inter-provider traffic engineering," *Computer Communications*, vol. 29, no. 6, pp. 683–702, 2006.

[52] Y. Gang, P. Zhang, X. Huang, and T. Yang, "Throughput maximization routing in the hybrid segment routing network," in *ACM International Conference Proceeding Series*, 2018, pp. 262–267.

[53] W. Sugeng, J. E. Istiyanto, K. Mustofa, and A. Ashari, "The Impact of QoS Changes towards Network Performance," *International Jurnal of Computer Networks and Communications Security*, vol. 3, no. 2, pp. 48–53, 2015.

[54] B. Nleya and A. Mutsvangwa, "Enhanced congestion management for minimizing network performance degradation in OBS networks," *SAIEE Africa Research Journal*, vol. 109, no. 1, pp. 48–57, 2018.

[55] D. A. Popescu, "Latency-driven performance in data centres," 2019.

[56] V. Joseph and B. Chapman, "Cisco IOS and IOS-XR Quality-of-Service Implementation for MPLS Layer 3 VPN Services," *Deploying QoS for Cisco IP and Next Generation Networks*, pp. 241–313, 2009.

[57] P. Ahlawat, “Comparison between Traditional IP Networks / Routing and MPLS,” *international Journal of Scientific Engineering and Research (IJSER)*, vol. 3, no. 3, 2015.

[58] M. Yampolskiy, W. Hommel, B. Lichtinger, W. Fritz, and M. K. Hamm, “Multi-domain end-to-end (E2E) routing with multiple QoS parameters considering real world user requirements and service provider constraints,” *Proceedings - 2nd International Conference on Evolving Internet, Internet 2010, 1st International Conference on Access Networks, Services and Technologies, Access 2010*, pp. 9–18, 2010.

[59] M. Doe, *EVE-NG Community Cookbook*. EVE-NG LTD.

[60] Cisco, “Catalyst 4500 Series Switch Cisco IOS Command Reference,” vol. 1, no. 2, pp. 1–1216, 2011.

[61] S. Jose, “IP SLAs Configuration Guide , Cisco IOS XE Gibraltar 16 . 11 . x (Cisco NCS 4200 Series),” no. 6387, 2019.