QoS Performance Evaluation of Segment Routing Traffic Engineering- (SRTE)

By: Halefom Gebremedhin

Adviser: Sosina Mengistu(PhD).

A Thesis submitted to

School of Electrical and Computer Engineering

Addis Ababa Institute of Technology

In Partial Fulfillment of the Requirements for the Degree of Master of Science

(Telecommunication Engineering)

December 2021

Name: Halefom Gebremedhin

Advisor: Sosina Mengistu(PhD).

Addis Ababa, Ethiopia

December 2021

This is to certify that the thesis prepared by Halefom Gebremedhin, titled: QoS Performance Evaluation of Segment Routing Traffic Engineering (SRTE) and submitted in partial fulfillment of the requirements for the Degree of Master of Science in Computer Science complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the Examining committee:

Name **Signature** **Date**

Advisor: _____

Examiner: _____

Examiner: _____

DECLARATION

I, the undersigned, declare that the thesis is entirely my own work and adheres to internationally acknowledged standards. I have appropriately recognized and referred to all materials used in this thesis work.

Halefom Gebremedhin _____

Full Name Signature

Addis Ababa University

Addis Ababa Institute of Technology

School of Electrical and Computer Engineering

QoS Performance Evaluation of Segment Routing Traffic Engineering (SRTE)

Signed by the Examining Committee:

Internal Examiner_____ Signature _____Date_____

External Examiner _____ Signature _____Date_____

Advisor Sosina Mengstu (PhD) Signature _____Date_____

Co-Advisor _____ Signature _____Date_____

_____

Dean, School of Electrical and Computer Engineering

ACKNOWLEDGMENT

To begin, I would want to thank God and his holy virgin mother, St. Mary, for giving me the strength to finish my thesis work despite various challenges in my life. Next, I'd like to thank Dr. Sosina Mengstu (PhD), my supervisor dr., for his insightful comments, and mentoring throughout of this thesis. Her observations, unreserved advice, and continuous support were helpful and constructive. Mesfin Kifle (PhD) and Fitsum Assamnew (PhD) were my examiners, and I appreciate their helpful remarks and input during the development and examination of my thesis.

Finally, I want to express my heartfelt appreciation to all of my friends, especially Lwam Brhane and Hailemariam Abreha, for their unwavering support and encouragement throughout my years of study as well as during the research and writing of this thesis. Without them, this achievement might not have been possible. I appreciate it!

Abstract

Today's telecom services have rather high expectations for quality of service (QoS), especially as internet applications become increasingly sensitive to time and delays. Because they are real-time, the crucial nature of certain of these applications is more noticeable. These provide challenges to network operators and service providers; since they are required to not only deliver these services to users, but also to ensure the requirements for Quality of Service (QoS).

The majority of service providers and network operators run their networks using MPLS technology and label distribution protocols, which are complex to install, maintain, and troubleshoot. The IETF is standardizing an SR paradigm that is manageable and implemented on MPLS and is based on a simple control plane. SRTE implements the SR protocol and establishes a tunnel using TE constraints. In SR Policy, the Head-end learns multiple candidate paths from one or more segment lists, but only one path is instantiated in RIB/FIB. As a result, SR policy for TE is an effective method for engineering the packet path at the ingress router, and it is continually improving and enabling unprecedented control, as well as successfully leveraging the benefits of SR technology, which enhances more QoS requirements.

This research presents a comparative analysis of SRTE with SR in terms of average latency, jitter, and packet loss, and finds that SRTE has a 33% reduction in latency, a 7.3% reduction in packet loss, and a 15% reduction in jitter. Concerning the above attributes, the conclusion of the investigation revealed that SRTE appeared to be more capable in the optimization of traffic in Core Networks when implemented by service providers and network operators, based on the comparative results of network performance.

Keywords— MPLS, SRTE, SR, QoS, RTT, Jitter, Packet loss, FRR, TE, SPRING, SR Policy

Table of Contents

LIST OF FIGURES

LIST OF TABLES

ACRONYMS AND ABBREVIATIONS

ABR: Area Border Router

Adj-SID: Adjacency Segment

ARP: Address Resolution Protocol

AS: Autonomous System

ASBR: Autonomous System Boundary Router

BGP: Border Gateway Protocol

BGP-LS: BGP Link State

BGP-LU: BGP- Labeled Unicast

CE: Customer Edge

CLI: Command Line Interface

CR: Core Router

CSPF: Constrained SPF

DA: Destination Address

DiffServ: Differentiated Service

DSR: Dynamic Source Routing

eBGP: External BGP

ECMP: Equal-cost multi-path

FRR: Fast Reroute

iBGP: Internal BGP

ICMP: Internet Control Message Protocol

IETF: Internet Engineering Task Force

IGP: Interior Gateway Protocol

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

ISIS: IS-IS for IP Internets

ITU: International Telecommunication Union

LDP: Label Distribution Protocol

LER: Label Edge Router

LFIB: Label Forwarding Information Base

LSA: Link State Advertisement

LSR: Label Switching Routers

LSRR: Loose Source and Record Route

LLC: Logical Link Control

LSP: Label Switched Path

LSR: Label Switching Router

MPLS-TE: MPLS-Traffic Engineering

OSPF: Open Shortest Path First

OAM: Operation and Maintenance

PCC: Path Computation Clients

PCE: Path Computation Element

PCEP:	PCE communication Protocol
PE:	Provider Edge Router
Prefix-SID:	Prefix Segment
QoS:	Quality of Service
RSVP-TE:	RSVP-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
SPRING:	Source Packet Routing in Networking
SR:	Segment Routing
SRGB:	Segment Routing Global Block
SRMPLS:	Segment Routing-MPLS
SRTE:	Segment Routing Traffic Engineering
TCP:	Transmission Control Protocol
TI-LFA:	Topology independent loop-free alternate
TE:	Traffic Engineering
TED:	Traffic Engineering Database
UDP:	User Datagram Protocol

VPN: Virtual Private Network

VRF: Virtual Routing Function

WG: Working Group

CHAPTER ONE: INTRODUCTION

1.1 Background

In today's telecommunication industries, Network operators and Service Providers are facing extreme challenges to keep pace with the exponential network traffic growth of their customer's. Moreover, service provider customers are demanding more strict Quality of Service (QoS) requirements for their sensitive and mission critical applications and services such as telephony, medical, financial, and live-streaming application resulting in tightened Service Level Agreements. Accordingly, service providers need to meet QoS standard requirements by enhancing service providers' network scalability, flexibility, automation policy and automated traffic steering in service delivery using QoS parameters[1].

Due to a number of promised benefits of telecom industries such as cloud computing, personal and business applications migrate to the cloud, and the users demand for network bandwidth is accelerating. Consequently, service quality will become an important differentiator between providers. For that, service providers invest in project expansion, maintaining specialized their current transport network architectures, and management approaches to satisfy the increasing demands.

The majority of transport networks use Multiprotocol Label Switching (MPLS) technologies. However, as the MPLS control plane became more complex, requiring a variety of interconnected protocols developed by several standards working groups, making it difficult to maintain, troubleshoot, and evolve.

For such considerations, the IETF standardized the Source based Packet Routing in Networking (SPRING) technique for signaling MPLS paths, commonly known as Segment Routing (SR). The ability to specify TE paths through the network has become one of SPRING's advantages [28]. Its primary goal is to provide a simple and easy-to-manage control plane that improves QoS standards and meets user's performance expectations.

In support of a source packet routing model, segment routing policy for traffic engineering (SRTE) drastically simplifies the configuration model and eliminates soft state of networking requirements [27]. SRTE offers not only simplicity and scalability, but also an SR native method of constructing traffic-engineered (TE) paths that take use of IP's ECMP feature.

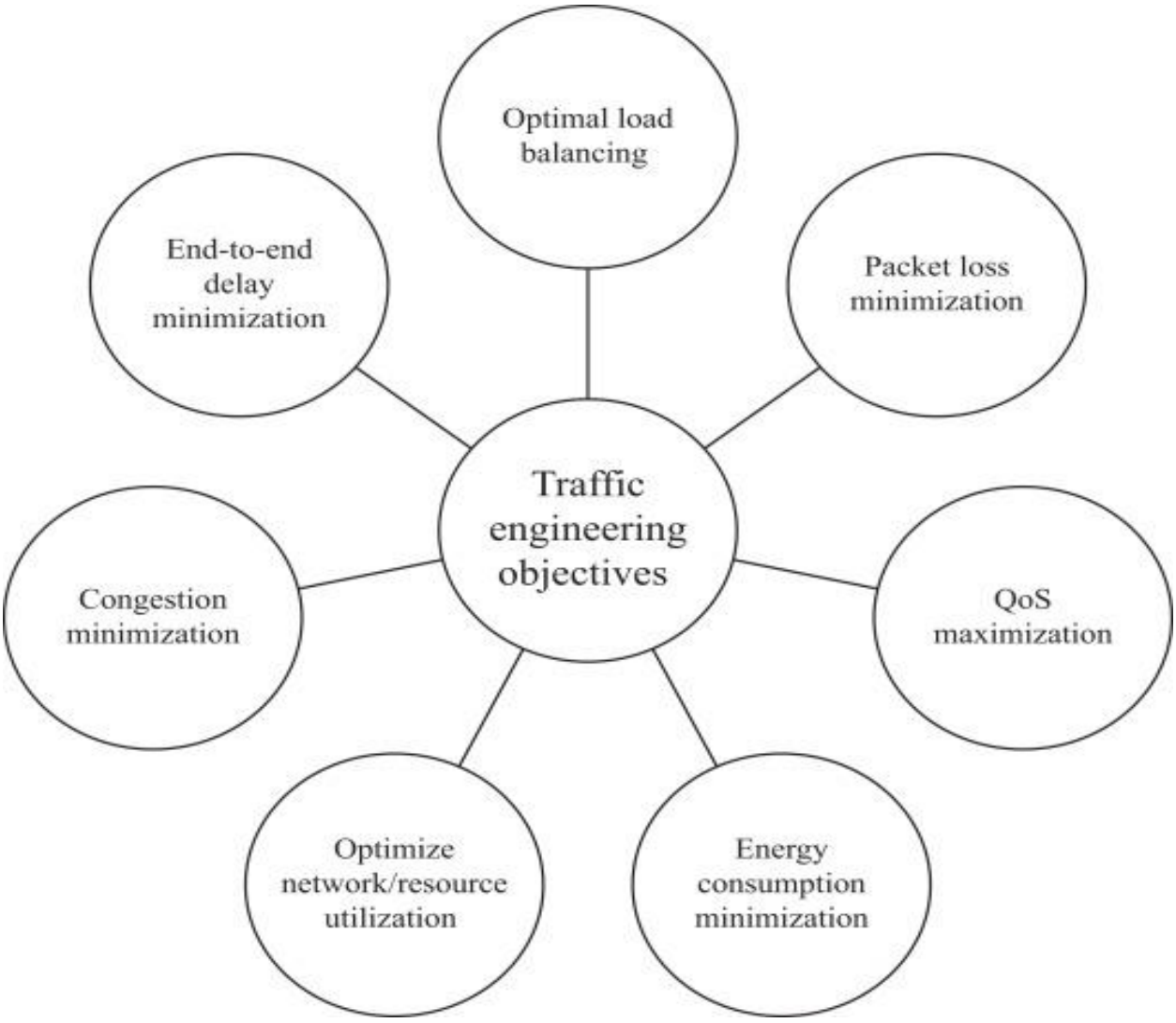

Figure 1. 1: Depicts the varied goals of implementing traffic-engineering techniques

The network's traffic complexity is further simplified because of the more advantage of automation provided by SR policy implementation and traffic steering. However, when used in conjunction with SR and MPLS, SRTE is a highly strong way for regulating the packet path at the source/ ingress router that is constantly developing and providing unprecedented control, allowing for higher QoS implementation.

1.2 Problem Statement

In reality, quality of service (QoS) is essential for optimally performing real-time applications over the Internet. The IETF has established numerous service models, policies, and mechanisms to meet

QoS standard requirements. The significant increase of real-time applications needs the provision of additional resources. The major challenge is to maximize resource utilization by implementing the sort of QoS that requires the validation of those QoS methods. As there are many hops between two core network elements, the subscriber's number & service demand has an impact on core network capacity and QoS performance[3]. Traffic engineering allows the optimal usage of network resources by including links that are not part of the least-cost path provided by IP routing. That means traffic engineering should provide the possibility to steer traffic through the network on paths different from the least-cost path [11]. Because of its control plane complexity, TE-MPLS and SRVP have been seldom used in service providers and network operators till now [3]. Segment Routing (SR) solely uses the source-routing paradigm based on IGP metrics and does not efficiently route network resources and traffic to offer QoS when the network is overloaded [28,32]. However, the network complexity of Traffic Engineering in SR is further decreased due to the added benefits provided by SR policy implementation and automated traffic steering in the network [27]. In the IPv4 context, most of the existing QoS techniques, including MPLS, MPLS-TE, and SR, have been analyzed to a greater extent. On the other hand, SR policy with TE is expected to be the future generation Internet Protocol, which has not yet been thoroughly examined or analyzed, that is my driving motivation. In general, this thesis will attempt to address the following Research Question:

What are the potential benefits of **Segment Routing Traffic Engineering (SRTE)** over an **SR-MPLS** network when QoS criteria are considered?

Hence, in SRTE, the candidate path from the head-end to the tail end instructs the intermediate routers to follow the specified path. Instead of IGP, a set of restrictions (TE Affinity, Disjoint, and Flexible Algorithm) and an optimization objective (TE & IGP metric) are used [27,31]. The SRTE optimize:

- Amount of traffic the network carries
- Utilization of resources (to avoid high utilized & low BW link.)
- The quality of service delivered

1.3 Aims and Objectives

The primary objective of this thesis work is to evaluate the performance of an end-to-end Segment Routing policy for Traffic Engineering SR-TE architecture using QoS parameters in IPv4 networks using Cisco IP SLA technology.

The specific aims of this study are-required functionality or service users to express quality of service performance and expectations in the form of Quality of Service parameters or attributes like delay or packet loss, and the network throughput to meet the requirement using various QoS techniques.

- Doing literature study about QoS, MPLS TE, SR, IPv4, and SRTE.
- To explore the technologies supported by SRTE
- Design network architecture with routers configured for SRTE and SR-MPLS networks.
- Collect the simulation results of SRTE architecture and SR-MPLS architecture from Cisco IP SLA Technology.
- Analyzing these performance parameters in QoS implemented SRTE network and its potential improvements on QoS.

1.4 Literature Review

The implementation and evaluation of QoS with the MPLS-TE and SRTE networks can improve the network's performance. For establishing QoS on a network, a variety of TE algorithms and SR policies can be utilized, which can affect the network's performance.

In[4], a Quality-of-Service (QoS) based Flow Assignment method for MPLS-TE in SDN was developed and implemented, allowing the computation of end-to-end paths for traffic flows promising QoS requirements such as bandwidth, end-to-end delay, and packet loss probability. In[5], by utilizing the characteristics of SDN, which proposed QoS sensitive, routing for available bandwidth by using segment routing (SR). It has focused on monitoring flow entries among switches and finding the feasible path over a QoS-based routing scheme. The routing algorithm found the path, which was feasible to meet the desired QoS data flows. If the required QoS cannot

provide for the requested flow, the controller determines how to calculate depending on the request from the switch. If the initial path will not be able to achieve the available bandwidth, the algorithm reroutes the higher bandwidth flow using Open Network Operating System (ONOS) controller with OpenFlow protocol. The research in [6] presented a work propose of Evolutionary Computation approach that supports Path Computation Element (PCE) to optimize label switching paths for congestion avoidance while using at the most three labels to configure each label switching path. In [7] has worked to evaluate end-to-end QoS performance using Seamless MPLS based on four important QoS parameters. However, the legacy MPLS uses a signaling protocol that has its own limitation. Hence, it relies on IGP plus LDP signal to establish LSP that affects the QoS performance.

Segment Routing (SR) can operate in a centralized, distributed, or hybrid arrangement. IGP (IS-IS, OSPF) or BGP are used in a distributed situation to assign and signal segments. An SR controller allocates and instantiates the segments in a centralized situation (SDN controller). Though centralized and distributed intelligence can be mixed in a hybrid model, distributed intelligence can also be utilized within the same IGP domain and single ASN. The SR controller can compute a source based routed policy of an IGP node when the destination is outside IGP domain [8].

In [9], mainly focused on two important segment routing use cases: dynamic traffic recovery and multi-domain traffic engineering. Indeed, when compared to typical Internet Protocol (IP)/MPLS methods, segment routing can greatly simplify network operation in both use scenarios. Both approaches are compared, with a simulative study of the segment list depth (based on software-defined networking). A segment can encapsulate topological or service-based instructions that provide for the enforcement of a flow over any topological path while just keeping a per-flow state at the SR domain's head-end router. The SR architecture can be implemented directly to the MPLS data plane without requiring any changes to the forwarding plane as the SR works in a network with LDP and when SR and non-SR-capable nodes coexist [28][29].

In this research, a technique for transitioning from a pure IP network to a full Segment Routing (SR) network studied. It is based on the design of a Segment Routing Domain (SRD), a subset of SR capable nodes, and a MILP optimization framework to select the best SRD in terms of congestion reduction; additionally, a technique to manage routing in the hybrid IP/SR network.

The performance analysis showed that the SRD generated by addressing the SR Domain Design problem might significantly reduce maximum link consumption, delivering performance comparable to that of a full SR network even when the percentage of SR nodes is low; at the same time, the number of flow states in the flow tables of the SR competent nodes reduced [3].

In particular, according to SR, packet flows are enforced through a specific path by applying, at the ingress node, a specifically computed stack of SIDs [29]. In [10] has investigated and analyzed the impact of implementing SR-MPLS over traditional MPLS on Quality of Service (QoS) in two scenarios. In spite of the analysis, results showed SR-MPLS has better QoS, SR has mainly focused on label encoding algorithms, without carefully addressing some key aspects of SR in terms of the overall SR policies and TE and its effects on the QoS performance.

1.5 Methodology

This study attempts to develop the analysis based on simulation experimental results. This simulation, as well as the analysis report, can be used to draw inferences and draw conclusions. Due to the lack of a real SRTE network for this research, the simulation has been used as an alternative. Without a review of the literature and the selection of articles, the research cannot achieve its goal. Figure 1.1 shows the work follow of the research.

- Review the documents for understanding and determining the QoS parameters, which consider for the analysis.
- To investigate different technologies to enable SRTE architecture.
- Designing a model for the simulation using the simulation tool GNS3 for both scenarios (SRTE and SR).
- Ostinato is a traffic generator tool that is used to generate traffic into the network.
- Justify the research using the simulated data collected from IP-SLA as a measure for QoS analysis.
- Finally, the test results are presented graphically for comparison and analysis with respect to QoS parameters.

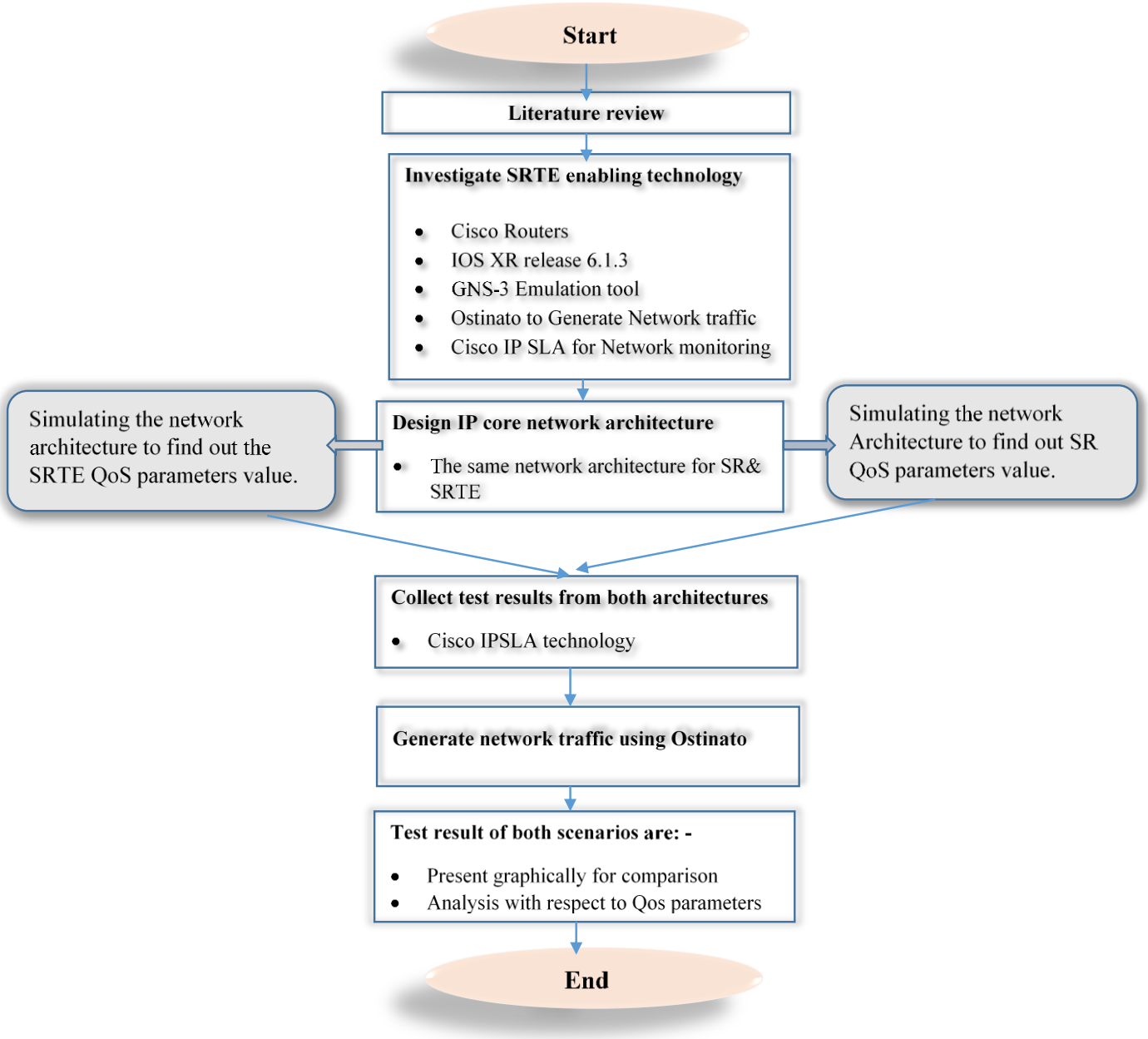

Figure 1. 2: Flow chart -Methodology on SRTE and SR on QoS.

1.6 Deliverables

Today, most of the service providers, network operators and enterprises are operated as a single network infrastructure to support and increase the number of services. Network operators have been exploring different engineering solutions to deal with the exponential growth in traffic. So segment routing traffic engineering (SRTE) is now worth the edition of the traffic engineering world. SRTE has the capabilities of optimizing the network infrastructure, control network routing, control data traffic and improve the end-to-end network QoS performance. SRTE has become the undisputed solution to deliver better quality of service and network resources utilization.

1.7 Scopes and Limitations

1.7.1 Scopes of the Thesis

This research covers the technical challenges and aspects that must be considered for the implementation of performance analysis QoS in the CORE Network, as well as the difficult issues of optimizing network traffic utilizing Segment Routing Policy and Traffic Engineering regardless of the type of traffic generated. In the experiment, two representative IGP domains (OSPF multi-area) are utilized for both scenarios, with the results applying to the other domains as well. They are two PE (provider edge) networks linked by a P (provider) network. As a result, all network traffic entering the network is treated the same. The routing techniques, features, and design parameters of the SRTE and SR networks are described in this research, as well as the SR policies and TE implementation.

1.7.2 Limitations of the Thesis

Each of the Cisco routers in the GNS3 simulation requires minimum Two gigabytes of RAM (Cisco IOS XRv Router). The Cisco IOS XR Software for SRTE and SR is limited by the memory constraints of computers and the process taken into account in determining of the simulation tools. The number of SRTE enabling routers is limited in simulation scenarios. However, it should be emphasized that increasing the number of routers used for testing and analysis has no effect on the final outcome.

1.8. Thesis Layout

The outline of this thesis paper is organized as follows; The introduction, motivation, aims and objectives, review of the state of the art, research methodology, and contribution of this research are described in chapter one of this thesis paper. It also describes the thesis paper's research question and scope.

Chapter 2 gives a detail overview on Network Traffic Engineering, SR Policy and TE. Topics like Introduction to Network Traffic Engineering, Traffic Engineering with MPLS, Introduction to segment routing, SRTE Policy Overview, SRTE LSP Instantiation, Instantiation of an SR Policy, Candidate Path, Binding Segment ID (BSID), Benefits of SRTE policy. In addition, Quality of Service (QoS) Background, and the overview of Service Level Agreement (SLA) and SLA metrics.

Chapter 3 is presents simulation tools used and QoS principles, QoS parameters, and technologies, which are used in IP/MPLS/SR networks. The four QoS parameters such as throughput, latency, packet loss and jitter are discussed in detail and their recommended values.

Chapter 4 presents the simulation and result analysis part, which describes the 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.

CHAPTER TWO: OVERVIEW OF TECHNOLOGIES

2.1 Introduction to segment routing

The IETF's SPRING Working Group created segment routing technology to make traffic engineering easier by extracting network state information from transit nodes and storing it in packet headers at the "source" or ingress node (i.e. where the data enters the network). By removing the status information from the network, the millions of labels that must be held on routers are less likely to overload it. This gives up a slew of new opportunities for network scalability and efficiency [8, 28].

Segment Routing is a source-based routing technique that involves stacking a list of unique segment identifiers in order of arrival along a traffic channel. It improves on the existing MPLS data plane by encoding a SID in each MPLS label, resulting in a stack of labels in the packet header that instructs each network element along the path to process the information contained in the segments upon receipt and transmit it to the next node [29]. This technology can be used to optimize network resources, delivering essential performance goals such as latency while also increasing operational efficiency in areas such as capacity reporting and change control management through automation and the usage of a controller.

2.1.1 Segment routing architecture

The main components of the SR Architecture are described in this section. Two different components of the architecture must be described in order to implement the SR framework.

To begin, the SR data-plane specifies how to represent the sequence of segments to be applied to a packet, as well as the segment forwarding semantics (how each device should process a packet based on a segment). The SR operation described here is independent of the protocol used to convey the information in the SR header.

Second, the SR control plane determines how segment identifiers are distributed among network devices and how network devices are commanded to apply a certain sequence of segments to a flow [14, 28].

1. Data-plane SR

A SR header uses a list of segments and a pointer to the active segment of the packet, which is the instruction that must be performed by the device processing the packet, from an abstract perspective. Following the execution of the active segment, the next segment in the list becomes active. A segment ID (SID) is a number that uniquely identifies a segment. A SID can have domain-wide relevance or simply have local significance to the router processing it, depending on its kind.

The following are the most common segment types:

Node SID: The Node SID forwarding strategy is to send the packet on the shortest path possible to the Node associated with that Segment ID. Each router in the network is given a domain-wide unique Node segment ID by the operator. This can be handled manually or with the help of a centralized controller.

Adjacency SID: An Adjacency SID's forwarding logic is to send the packet over the related adjacency. For each of its IGP adjacencies, each router will assign a locally significant segment ID.

Service SID: A Service SID's forwarding logic is to send a packet to the matching service provided by the node processing the packet. For each service it provides to the network, each node will assign a locally significant segment ID.

An SR-enabled node can perform the following data-plane operations:

- ✓ Continue Operation - Based on the active segment, a forwarding action is taken.
- ✓ Push Operation - Add a segment ahead of the packet's SR header and make it the active segment.
- ✓ Next Operation - Mark the next segment as the active segment.

2 Control-plane SR

The SR control-plane determines how segment ID information is exchanged among network devices. The link state IGP protocol will be used to advertise Node and Adjacency SIDs in an SR network. The most widely used IGP protocols in service provider networks, OSPF and ISIS, have been updated to facilitate the dissemination of segment IDs [14][15].

Any router can keep a database of all nodes and adjacency segments due to IGP protocol extensions. The segment database on each router can also be promptly updated after any topology change by exploiting the sub-second convergence properties of both IGPs. End-to-end encapsulation can be achieved in the network utilizing these extensions without the need to enable and manage another protocol, such as LDP.

Another aspect of the SR control plane is how an ingress router is informed to choose the SR path that a packet should take. For this objective, the following methods can be used:

1. Distributed Constrained SPF (CSPF) Calculation. In this technique, an headend router calculates the shortest path to a destination while ensuring that it meets certain criteria. The path is then encoded by a sequence of node and adjacency segments.
2. Software Defined Networking (SDN) controller-based technique. SR delivers a scalable and resilient data plane while maintaining the control flexibility that SDN systems are known for. Because of this, certain SDN-oriented controllers are expected to include SR support in their designs. The Path Computation Element Protocol (PCEP), for example, is supported by OpenDaylight for controlling SR[16].
3. Statically defined by the operator. Because of obvious scaling, resiliency, and administration constraints, static tunnel setup may be utilized for specific reasons such as testing or troubleshooting, but it is normally not recommended for long-term network operation.

Based on the applications and scenarios they want to support, an operator can use any of these ways. It's worth noting that the three techniques can coexist in a network. Static tunnels could be used for troubleshooting or other specific but infrequent uses. The CSPF technique requires a balance between optimization and automation when it comes to connectivity. For networks with TE objectives for which contradictory judgments could be made if executed in a dispersed manner

(e.g. demand placement for capacity engineering purposes), the enormous flexibility provided by centralized techniques makes it appealing.

2.1.2 Topology Independent Loop Free Alternate (TI-LFA)

Topology Independent Loop Free Alternate Fast Re-route (TI-LFA) aims at providing protection of node and adjacency segments within the Segment Routing network architecture. The fast reroute (FRR) path selection method, which establishes protection over the anticipated post-convergence paths from the point of local repair, is a basic feature of TI-LFA. Despite the fact that the node is in the SID list to be visited, the TI-LFA FRR path may skip it. Furthermore, TI-LFA is designed to minimize performance degradation when routers encounter a topology change caused by a link or node failure. Rapid failure repair (less than 50 msec) is accomplished by using pre-calculated backup paths that are loop-free and safe to use until the dispersed network convergence procedure is completed[17][9]. The optimal repair route that traffic will finally take when the IGP has converged. This is referred to as the post-convergence path. For the following reasons, this path is preferred:

- Optimal for capacity planning — During the network's capacity planning phase, a link's capacity is provided while taking into consideration that it will be used if other links fail.
- Simple to operate – There's no need to make case-by-case adjustments to get the optimal LFA from a pool of candidates.
- Fewer traffic transitions – The traffic only changes paths once because the repair path is equal to the post-convergence path.

The following protection is supported by TI-LFA:

- ✓ Link protection – During the post-convergence backup path computation, the link is skipped.
- ✓ Node protection – During the post-convergence backup path calculation, the adjacent node is ignored.
- ✓ SRLG (Shared Risk Link Groups) protection – SRLG refers to cases where network links share a common fiber (or a common physical attribute). These relationships have a common risk: if one fails, the rest of the group may fail as well. The TI-LFA SRLG protection tries to find a post-convergence backup path that doesn't include the protected

link's SRLG. All local links that have an SRLG in common with the protective link are disqualified.

When link protection is enabled, node protection, SRLG protection, or both can be enabled, and a tiebreaker priority can be specified if there are multiple LFAs [32].

2.1.3 Segment Routing Mapping Server (SRMS)

The mapping server is a critical component of the interoperability of LDP and segment routing. It allows SR-enabled nodes to communicate with LDP nodes. On behalf of other non-SR-capable nodes, the mapping server promotes Prefix-to-SID mappings in IGP.

Cisco IOS XR segment routing's mapping server feature assigns prefix-SIDs to some or all of the recognized prefixes. A router must be capable of acting as both a mapping server and a mapping client.

A router that operates as a mapping server allows the user to configure SID mapping entries to specify the prefix-SIDs for certain or all prefixes. The local SID-mapping policy is created as a result of this. Non-overlapping SID-mapping entries are found in the local SID-mapping policy. The mapping server informs the mapping clients about the local SID-mapping policy [32].

To build remote SID-mapping entries, a router that acts as a mapping client receives and parses SIDs from the mapping server.

A router that serves as both a mapping server and a mapping client constructs a non-overlapping consistent active mapping policy using both remotely learned and locally configured mapping entries. The active mapping policy is used by the IGP instance to calculate the prefix SIDs of some or all prefixes [2][29].

The mapping server (SRMS) maintains the insertions and deletions of mapping entries automatically, resulting in an active mapping policy with non-overlapping consistent SID-mapping entries at all times.

The mapping server takes as input the locally configured mapping policy as well as remotely learnt mapping entries from a specific IGP instance and chooses a single mapping entry among overlapping mapping entries based on the preference criteria for that IGP instance. As a result, an

active mapping policy with non-overlapping consistent mapping entries is created. At steady state, all routers must have similar active mapping rules, at least within the same area or level.

2.2 Binding Segment ID (BSID)

Segment Routing-SR to provide greater network scalability, network opacity, and telecom service independence uses a Binding Segment ID (BSID). The BSID is associated with an SR Policy, that can be created using a list of segment identifiers -SIDs. Any packets with an active segment-ID equal to BSID are steered to the SR Policy that is bound.

A local or global SID can be used for a BSID. If the SRLB is local, a BSID must be assigned. If the BSID is to be global, it must be assigned from the SRGB.

Using a BSID allows the policy instantiation (the SID list) to be stored solely on the node or nodes that need to apply the segment routing policy. Imposition of the BSID is all that is required to direct traffic to a node that supports the SR policy. If the policy changes, only the nodes that implement the policy need to be updated. The policy's users are unaffected [2].

2.2.1 Binding SID of a candidate path

A candidate path is a packet-forwarding path that can be used by an SRTE policy. Multiple candidate paths with the same BSID can exist in an SRTE policy. Two SRTE policies, on the other hand, cannot share the same candidate path. Different SR policies' Candidate Paths cannot have the same BSID [30][31].

2.2.2 Binding SID of an SR Policy

An SR Policy's BSID is the BSID of its active candidate path. When the active candidate path has a specified BSID, the SR Policy utilizes that BSID if that value is available (i.e., not associated with any other usage, such as to another MPLS client, another SID, or another SR Policy). In addition to checking that the active path's BSID is available, a headend may also check that it is available within that SID range, as defined in [27].

An alarm message must be generated if the supplied BSID is not available (or is not in the SRLB). So when an SR Policy does not have a BSID available, the Policy can automatically bind a BSID to itself. Outside the SRLB, dynamically bound BSID should use an existing SID.

As a result, the association of an SR Policy with a BSID may change over the period of the SR Policy's lifetime (e.g., upon active path change). As a consequence, the BSID should not be utilized to identify an SR Policy.

2.3 SRTE Policy Overview

A SR policy is used to guide traffic through the network by a segment routing policy for traffic engineering. A segment ID (SID) list identifies the path of an SR-TE policy, which is a list of segments. Each segment is a complete path from ingress to egress that encourages network routers to take that path rather than the IGP's shortest path [27]. The ingress router adds the Segment-ID list to a packet when it is directed into an SR policy. All other intermediate routers in the network between the tunnel headend execute the instructions in the SID list and the tunnel tail end, a Traffic Engineered tunnel container of LSPs. One or more SR-TE LSPs that are associated with the same TE tunnel can be instantiated by a TE tunnel. The SR-TE LSP path to a destination node may or may not follow the same IGP path. In this situation, the SR-TE path can be specified using a collection of prefix-SIDs, adjacency-SIDs of nodes, or both, as well as the connections that the SR-TE LSP will traverse [17][18].

In service provider and enterprise networks, an SR-TE controller is a type of controller that provides centralized or distributed path calculation, traffic engineering, granular visibility, and traffic flow control for SR forwarding planes. The SR-TE controller allows network operators to improve their infrastructure via proactive monitoring and planning, as well as dynamically routing huge traffic loads depending on defined limitations[3].

2.3.1 Benefits of SRTE policy

Due to the necessity to construct a large number of tunnel configurations for TE policies, RSVP-TE, the protocol for traffic engineering in IP/MPLS, is not widely used. Because of these limitations, it quickly runs into scaling issues.

The core of SRTE is kept minimal and scalable (as core is stateless). Both explicit and constraints-based routing, such as RSVP-TE, are supported by SRTE. Flexible policies can be developed automatically in centralized and distributed contexts using constraints-based routing based on latency, disjoints, and preferred pathways, among other factors.

SRTE is multi-domain capable and designed to work with or without a centralized controller in a multi-domain network. The SRTE process maintains an SRTE-DB that can run flexibly in a headend router or a centralized controller to validate paths and compute dynamic paths. IGP, BGP-LS, or NETCONF can be used to discover the associated domain topology. BGP-LS or NETCONF can be used to learn a nonattached (remote) domain topology[9][17].

Automated PCE support in a centralized environment can create end-to-end uniform policy-based limitations such as latency, disjoints, and SRLGs.

2.4 SRTE LSP Instantiation

A Traffic Engineered (TE) tunnel is a container for one or more Traffic Engineered LSPs that have been instantiated. Configuring ‘segment-routing' on the path-option of the TE tunnel creates an SR-TE LSP. The traffic destined for the tunnel is routed through the primary SR-TE LSP [31].

Under the same tunnel, many path options can be defined. Each path-option has a preference index or path-option index that is used to assess which path-option is the best for instantiating the major LSP—the lower the preference index, the better the path-option. Other less desirable path-options inside the same TE tunnel are referred to as secondary path-options, and they can be employed if the currently used path-option is invalidated (for example, due to a path failure)[15].

If the head-end detects a failure on any link in a TE tunnel with an existing instantiated SR-TE LSP, the head-end assumes that a fault has happened on that link. Local repair protection, such as the IP FRR, kicks in this situation. After an adjacency is lost for a period, the IGPs maintain the protected adjacency label and associated forwarding. This provides adequate time for the head-ends to divert the tunnels onto alternate paths that are not affected by the same problem. When the head-end detects a connection failure, it starts a tunnel invalidation timer to try to reroute the tunnel to other available path-options with valid pathways[9].

2.4.1 SR-TE Tunnel Establishment

Segment Routing Traffic Engineering (SR-TE) implements the SR protocol and creates a tunnel using TE constraints [30].

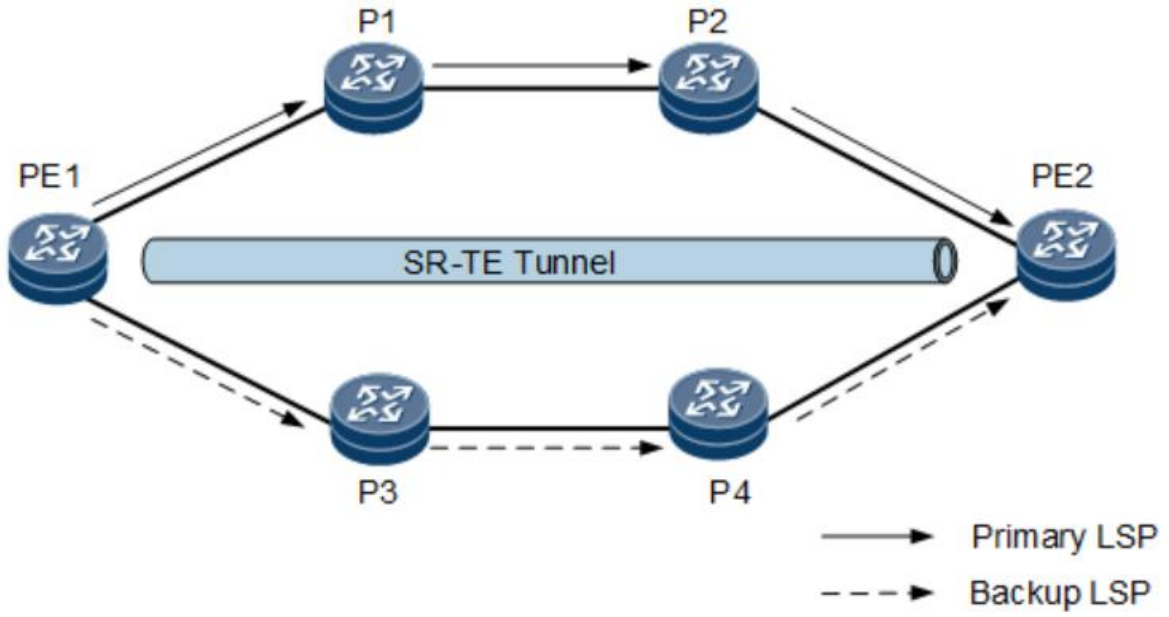

Figure 2.1: SRTE Tunnel

In Figure 2.1, a primary LSP is formed along the link PE1->P1->P2->PE2, and a backup path is established along the link PE1->P3->P4->PE2. The two LSPs each have the same SRTE tunnel ID. The LSP starts at the ingress, continues through transit nodes, and ends at the egress.

Configuring and establishing an SR-TE tunnel is part of the SR-TE tunnel setup. To perform network layer connectivity, assign labels, and gather network topology information, IS-IS/ OSPF neighbor relationships between forwarders must be established before an SR-TE tunnel can be formed. Forwarders transmit the controller label and network topology information, which the controller uses to calculate routes. Enable the CSPF path computing function on the ingress of an SR-TE tunnel if no controller is available, so that a forwarder can use CSPF to compute a path.

To construct tunnels, SRTE tunnel properties are used. A controller or a Head-end can configure an SRTE tunnel.

- On a controller, an SR-TE tunnel is configured.

To deliver tunnel attributes to a forwarder, the controller executes NETCONF. The forwarder to delegate tunnel management to the controller uses PCEP. The forwarder runs PCEP to delegate LSPs to the controller after the SR-TE tunnel configuration is received. The controller determines paths, creates labels, and keeps the SR-TE tunnels running.

- On a forwarder/head-end, an SR-TE tunnel is manually configured.

A forwarder/head-end manually configures an SR-TE tunnel. The forwarder provides LSPs to the controller for management.

2.4.2 SR-TE Tunnel Re-optimization

When the head-end determines that a better path than the one currently in use is available, TE tunnel re-optimization occurs. In the event of a failure along the SR-TE LSP path, for example, the head-end might detect the failure and revert to a more ideal path by triggering re-optimization. Tunnels that use the SR-TE LSP can re-optimize without disrupting the traffic that passes through the tunnel[17].

Re-optimization can occur because:

1. When the primary SR-TE LSP explicit path's explicit path hops have been changed.
2. Because of a topology path disconnect or a missing SID in the SID database indicated in the explicit-path, the head-end determines that the already used path-option is invalid.
3. A more suitable path (lower index) becomes available.

The invalidation timer is started when the head-end router detects a failure on a protected SR adjacency-SID that is crossed by an SR-TE LSP. The tunnel state is brought ‘down' if the timer expires and the head-end is still utilizing the unsuccessful way because it is unable to redirect on a new path. This prevents a null route from being sent with the traffic. Once the tunnel is deactivated, the tunnel's services converge to follow a different path [27].

2.5 Instantiation of an SR Policy

An SR-TE controller is a type of controller that provides centralized or distributed path computation. The SRTE controller enables network operators and service providers to optimize network infrastructure through proactive monitoring and planning [30].

At the source router, an SR policy for traffic engineering is instantiated, or implemented and using the following segment routing instantiation mechanisms:

2.5.1 On-Demand SR Policy – SR On-Demand Next-Hop

On-Demand Next Hop (ODN) with Automated Steering is a feature that uses BGP color communities to identify prefixes and automatically direct packets from a head-end to a tail-end on demand, without the need for elaborate policies on every Provider Edge(PE) router. Instead of configuring SR policy ahead of time, SRTE provides an innovative means of instantiating it on demand. Based on BGP Next Hop, an SR policy can be instantiated on demand. As a result, policies can be applied in a very dynamic, flexible, and automated manner. Not only can the policy be instantiated on demand, but traffic can also be steered automatically (thanks to BSID) based on the forwarding plane specified by the on-demand SR policy [27].

BGP route coloring is used in conjunction with low-based SR-MPLS Traffic Engineering. The traffic is routed through the SR Policy, where it is allocated a traffic class value based on DSCP marks or a 5-tuple ACL match, and then sent to the specified destination. Another advantage is that SR-TE, when used in conjunction with a centralized controller, can provide end-to-end dynamic pathways across several autonomous systems, increasing network size.

2.5.2 Manually Provisioned SR Policy

On the head-end/ingress router, manually provisioned Segment routing (SR) policies are configured. Dynamic or explicit paths can be used in these policies. For details on manually providing an SR policy utilizing dynamic or explicit paths.

The following are features of a candidate path:

- It has a preference – If two policies have the same (Preference/color, endpoint) but different preferences, the one with the higher preference is chosen.
- It is associated with a single binding SID (BSID) - A BSID conflict occurs when multiple SR policies share the same BSID. In this situation, the first-installed policy receives the BSID and is preferred.
- If it can be used, it is valid.

When a path is valid and its preference is the best among all candidate paths for a policy, it is preferred.

2.6 Candidate Path

2.6.1 Explicit Candidate Path

An explicit candidate path is related to a Segment-List or a set of Segment-Lists that can be delivered either directly by the operator or through a controller. The SR Policy headend is not involved in the computation that leads to the selection of the Segment-List. The Segment-List is not computed by the SR Policy headend. Its validity is only confirmed by the SR Policy headend. An explicit candidate path may consist of a single explicit Segment-List with just an implicit-null label to indicate pop-and-forward behavior [27]. The BSID is popped, and traffic is forwarded depending on the inner label or an IP lookup if unlabeled IP packets are received. This explicit path can function as a fallback or path of last resort for traffic steered into an SR Policy through its BSID.

2.6.2 Dynamic Candidate Path

A dynamic candidate path is defined by an optimization objective and constraints. The policy's headend uses its SR database to generate a Segment-List ("solution Segment-List") that solves this optimization problem. When the problem's inputs change, the headend re-computes the solution Segment-List (e.g., topology changes). When local computation is either impossible or undesirable (for example, when a policy's tail-end is outside the topology known to the headend), the headend may transmit a path computation request to a PCE that supports the PCEP extension.

The dynamic candidate path must be considered invalid if no solution to the optimization objective and constraints can be identified [30].

2.7 Quality of Service (QoS) Background

In the world of telecommunications industry, quality of service (QoS) is defined as a collection of particular needs that a network operator and service provides to satisfy their customers or service users. An application's required functionality or service has to meet and quality of the service and the performance expectations has expressed in terms of Quality of Service parameters like delay or packet loss, and the throughput to meet the requirement using various QoS methods. Each service model has its own set of quality-of-service parameters[19][20].

In the commercial environment, service quality can be a factor. Its parameters and metrics are required to provide an indicator of how well a service is performing, and hence should be considered when comparing services offered by other service providers [34]. When service features and rates are comparable, quality becomes the factor for consumers, and service providers can leverage quality to present an image of being a "respected" provider.

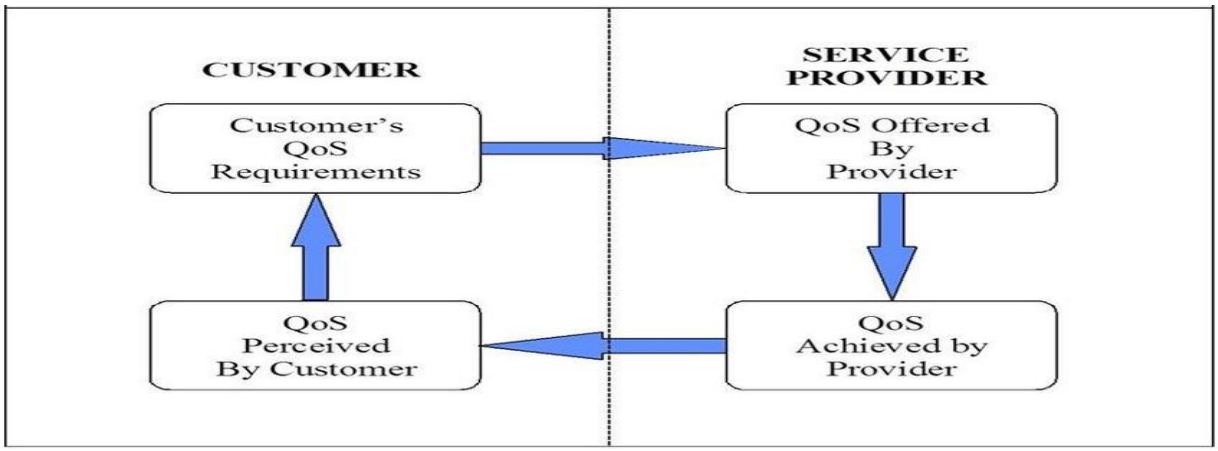

Figure 2. 2: ITU-T Four Views QoS Perspective[20]

The following are some of the challenging scenarios that lead QoS degradation:

1. Traffic congestion happened due to overflowing traffic (bottlenecks).
2. Delays or RTT/Latency effect of low performance of networking equipment in high-volume scenarios, as well as distance/ retransmission of lost packets;
3. Incidents and long delays or latency are typical on shared communication channels or bandwidth, and
4. Networks with limited bandwidth and ineffective and low capacity management.

As shown in Figure 2.3, the end-to-end QoS is influenced by the contributions made by the components.

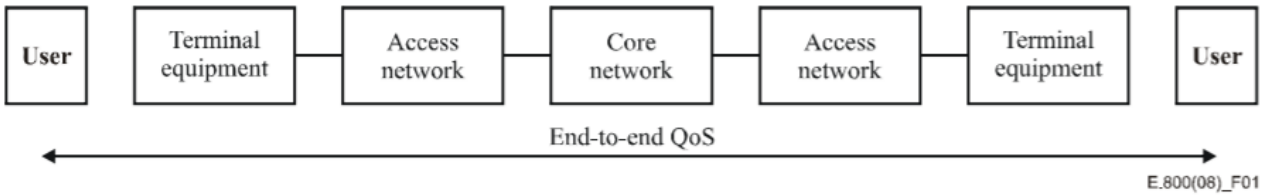

Figure 2. 3: Schematic contributions to end-to-end QoS[20]

2.8 Service Level Agreement (SLA)

Service Level Agreement Management (SLAM) has recently gotten a lot of interest from telecom companies and customers. Service Level Agreement (SLA) management is the most demanding functionality due to advancement in QoS service provisioning and dynamic interactive monitoring and control of telecommunication infrastructure. SLAM is another layer in the telecommunication network infrastructure, working over the monitoring and resource control levels and delivering a more generic and consistent perspective of service provided to end-users. It is the next inevitable step in the evolution of these systems, linking the technical aspects of system infrastructure operation with the telecom industry's market and user-driven strategic goals [22][23]. SLAs, in principle, specify end-user demands for the quality of services delivered, which are defined as quite aggregated metrics determined for the selected time of service delivery. Complications of SLA contract metrics representation and on-line, bidirectional transition of the business standpoint to the overall technical system parameters cause difficulties in SLAM creation and implementation as shown in Figure3.3.

Figure 2. 4: Information flow in SLAM framework[22]

The SLA outlines the requirements for all parties engaged in the delivery of the service in a customer-friendly manner, with measurable and easy-to-observe and-prove requirements. SLAs are performed to establish end-to-end QoS because they describe how services will be delivered,

accessed, what is permitted, and the charge for services offered. Penalties for failing to satisfy service requirements, additional assistance alternatives, incentive awards for exceeding service levels, and so on[23]. SLAs are divided into three categories:

- Customer service level agreements (SLAs): specify the services (product or service offerings) provided to the customer. This is a contract between the customer and the operator that is written in easy-to-understand words and focuses on the end-to-end delivery of the product's components.
- Supplier Service Level Agreement (SLA): Describes how specific performance criteria for third-party resource and service components will be accomplished. It is generally collected from the service provider's and operator's contractual agreement.
- Internal Service Level Agreement (SLA): This sort of SLA focuses on resources and which is used to manage a set of services and service components which are already defined by one of the two types of SLAs described above. Agreements between organizational roles within the operator's business are required.

2.8.1 SLA Metric

Service level agreements are used to formally establish the performance parameters that a provider guarantees to achieve. The defined parameters are monitored after a SLA has been agreed upon in order to detect agreement breaches. One of the most important aspects of developing a SLA is defining methods for measuring specific service criteria that must be agreed upon by both contracting parties. When a SLA breach is discovered, a suitable remediation mechanism (also described in the contract) is implemented. In addition, the consumer is entitled to compensation from the supplier. Identifying the offenses and determining the penalties could be difficult. A SLA contract [22] can be considered of as a logical product of predicates based on the outcomes of monitoring specific service metrics. The SLA can be represented as a hierarchy of sub-contracts that will eventually be defined as policy based on measurement-based predicates to make it more intelligible. The SLA Management System (SLAM) is driven by a monitoring database that receives data from attribute measurements. The SLAM systems' responsibilities are to:

- In the context of agreements signed by a certain provider, evaluate data provided by a monitoring. This feature also involves warning the provider of unexpected events that may result in a SLA breach before they occur.

- provide the customer with regular reporting on the SLA parameters.
- provide data to external systems for the purpose of determining compensation for SLA violations.

In the event of a contract breach, the compensation is usually conveyed in the form of refunds or payment-free periods of services provided for the customer. Although the agreement covers the computation specifics, and the SLAM system isn't designed to compute fines, a few elements related to the computations were taken into account throughout the design phase to identify the data that should be given to the computation subsystem. On the one hand, fine-grained output appears to be essential to offer maximum flexibility in penalty calculations. On the other aspect, the SLAM is not expected to replace the monitoring system. A method was chosen to establish an interface between SLAM and the monitoring system(s) that would be utilized to provide fine-grained data if necessary[9][24].

CHAPTER THREE: EVALUATION METHODOLOGY

3.1. Overview of Simulation Tools

3.1.1. Emulated Virtual Environment –GNS3

Graphical Network Simulation 3 (GNS3) is the tool used to emulate the network topologies. GNS3 is a free and open-source network software simulator that can be used to simulate, configure, test, and troubleshoot virtual and real-world networks.

GNS3's most recent versions support a variety of network elements, including Cisco virtual switches, Cisco ASAs, Brocade vRouters, Cumulus Linux switches, Docker instances, HPE VSRs, various Linux appliances, and more [25]. Furthermore, the number of devices supported by GNS3 is unrestricted. The CPU and RAM of the hardware that runs it are the only possible constraints.

GNS3 simulates a device's hardware and runs real images in the virtual device, enabling it to be used to design and simulate complicated networks. It requires the images or IOS of the network element to be emulated because it runs actual images.

GNS3 provides a variety of appliances on its official website that come with a pre-configured image that may be used to simulate a device.

For the realization of the experimentation, it is required an image/ IOS for the routers and another image for the hosts.

3.1.2 GNS3 Architecture

GNS3 consists of two software components [25]:

- Client part: The GNS3-all-in-one software (GUI)
- Server part: The GNS3 virtual machine (VM)

The GNS3-all-in-one is the graphical user interface (GUI) where the network topologies can be created. When the topologies are formed, the network elements are hosted and run by a server process.

The following options are available for the server part:

- Local GNS3 server: run on the same computer where the GUI is installed.
- Local GNS3 VM: run on the same PC using virtualization tool such as VMware or Virtualbox.
- Remote GNS3 VM: run remotely using VMware ESXi or in the cloud.

For this experiment, the host devices on the GNS3 VM using VMware which is the recommende d option.

3.1.3. Cisco IP Service Label Agreement (IP SLA)

Cisco IPSLAs is a Cisco IOS (Cisco operating system) integrated tool that measures network performance by actively monitoring traffic generation in a continuous, reliable, and predictable manner. IPSLAs sends data over the network to monitor performance across multiple network path. It emulates network traffic and IP services while also collecting real-time network performance data. Response time, one-way latency, jitter, packet loss, voice quality scoring, network resource availability, application performance, and server response time are among the collected data. IPSLAs conducts ongoing monhitoring by generating and analyzing traffic in order to evaluate performance between Cisco devices or between Cisco devices and a distant IP device including a network application server. The various IP SLAs operations provide measurement statistics that can be utilized for troubleshooting, problem analysis, and planning network topologies[23][24].

Cisco IP SLA Benefits:

- IP Service Level Agreements (SLAs) monitoring
  - ✓ Provides SLA monitoring, measurement, and verification.
- Monitoring of network performance
  - ✓ Provides, reliable, and predictable measurements of jitter, latency, or packet loss in the network.
- Troubleshooting of network operation
  - ✓ Consistent, reliable measurement that instantly identifies problems and reduces troubleshooting time.

3.1.4 Ostinato

Ostinato is an open-source network traffic and packet generator with packet modification and analysis capabilities. To do the same operations, it offers a very easy GUI. It supports the most of network protocols and has a Python API for automating operations. A stream of packets can also be generated, any fields of the protocol specified can be configured, and the stream can be transported over any network connected - wireless or Ethernet. Another prominent feature is cross-platform compatibility that is related to the architecture. As a result, there is no need to be concerned about using Ostinato with a device that supports on a different platform. There are also the following features[26]:

- Stream rates and packet count configuration
- Open and modify packet capture (PCAP) files, then customize and rerun them as needed.
- Frameworks built in to construct new protocols that aren't currently supported

Ostinato is compatible with the following protocols:

- ✓ Ethernet / 802.3/ LLC SNAP
- ✓ Switching/ layer 2 protocols VLAN (with Q in Q)
- ✓ Network layer protocols such as ARP, IP Version4, IP version6, IP-in- IP
- ✓ Transport layer protocols -TCP/ UDP,
- ✓ Application layer protocols such as HTTP, SIP, RTSP, NNTP etc.

3.2 QoS Parameters

To offer and sustain quality of service (QoS), inventory management or resource management must be implemented in accordance with QoS standards. While allocating resources, the following QoS criteria might be considered for the network inventory management system:

- Network resource availability(NRA);
- Policies for resource management, such as Service Level Agreements (SLA);
- QoS requirements of applications and services are computed with respect to QoS parameters (PDV/Jitter, RTT, and Packet Loss …).

The QoS parameters must be monitored and available network resources reassigned in accordance to system anomalies in order to keep track of whether the contracted QoS is being fulfilled or not meet SLA or QoS requirments. Prior to the reservation of resources, the application layer must guarantee that the appropriate QoS parameters can be satisfied (through QoS negotiation signaling). To optimize the communication network resources at the traffic level, researchers consider some of the traffic-oriented performance measurements related with end-to-end QoS criteria. Latency, packet loss, and jitter are examples of these issues.

In telecommunication networks, QoS is important to increased network resource capacity when service providers lunch new applications and services. Another advantage of QoS is that it supports the service providers in the management of congestion and avoidance mechanisms or network traffic management. It aids us in increasing revenue by acting as a primary backbone for shared structures. It aids in the management of multimedia that has an impact on the network,[21][19]

Depending on the required and management method, QoS is measured using characteristics or QoS standard parameters such as latency, jitter, packet loss, throughput, and many more. The general QoS parameters most considered in IP Core Networks are summarized below:

3.2.1 Latency:

Latency is defined as the time taken for a data packet to transit across a end-to-end network connection. The terminology latency and end-to-end delay are interchangeable in communication network context. Many network interactive applications and services, such as VoIP and video teleconferencing, are extremely sensitive to latency or delay [35]. One-way latency (the entire time from the source/ ingress router that transmits a packet to the destination/ egress that receives it) or round-trip time (RTT) latency (the one-way latency from end-to-end plus the one-way latency/ delay from the destination back to the source) can be measured. Because the “Ping” command can determine roundtrip time(RTT) from a single point, it is commonly utilized. Because it removes the time spent by a destination system processing the packet, the round trip delay is a generally accurate technique of measuring delay. The “Ping” command does not process packets. When it gets a packet, it merely responds with a response. In order to have a more precise roundtrip time measurement, both points of the network must be measured. The result is the shortest possible delay time for transmitting a packet from a source to a destination via that link. As a result, one of the most important tasks of QoS approaches is to provide end-to-end delay requirements [20][21].

3.2.2 Jitter:

Jitter or packet delay variation (PDV) is a term that describes the variation of latency/RTT across a specified period. Packets are used to convey information from one device to another inside a network. Packets are data chunks that are transmit to other devices to transport data within communication network. Latency is the length of time it takes for these packets to arrive at their destination.

The jitter value is the variance in latency above a specific threshold or substantial of jitter imply poor network performance and packets arrive out of sequence and are irrelevant. Jitter can be caused by a variety of factors, however there are a few typical causes that are responsible for the majority of jitter problems. These are some of them:

- Network congestion - Networks that are congested with traffic suffer from poor performance because active devices require too much bandwidth.
- Poor Hardware Performance - while working over an old network with out-of-date equipment, the jitter can be experienced due to hardware. The difference between a network with jitter and one that functions effectively can be as simple as an incompatible router, switch, or cable.

The level of network jitter that is tolerable on a network is determined by the services being provided. Some apps and services have a higher jitter tolerance than others. For example, jitter has less of an impact on sending emails than it does on voice calls [35].

When using low-tolerance applications like VoIP, jitter must be maintained below 30 milliseconds. Because the consequences of jitter will be minor, any rate of jitter below this level will be acceptable. Users will be able to understand the person on the other end of the line with minimal jitter[21].h

3.2.3 Packet Loss:

Packet loss occurs when one or more data packets passing through the internet or a computer network fail to arrive at their destination. IP networks cannot guarantee that packets or best effort approach; the packet may or may not be delivered at all. Other factors that cause packet loss include loads on network links, corrupted packets being deleted, and network element defects.

The UDP is a connectionless protocol commonly used to transport packets over the network for real-time services and applications (or more specifically the RTP protocol, which runs on top of UDP) [35]. Due to the significant latency sensitivity of real-time applications, standard TCP retransmission techniques are ineffective in this circumstance. The disadvantage of the connectionless/UDP protocol is that it cannot guarantee the delivery of all packets or that it does not provide feedback/ acknowledgement. Packets can be lost under peak loads or periods of congestion, and data packets lost during a network session are known as packet loss. In other words, packet loss refers to the number of packets that never reach it to their intended destination. Packet loss is one of the QoS standard parameters, which must be kept below a specific threshold for an application to function properly. Some Voice over IP (VoIP) QoS applications, for example, define the following QoS services [CA02]:

- < 0.2 % - GOLD service
- 5 % - SILVER service
- 10 % - BRONZE service

Packet losses greater than 10 percent are usually intolerable[21].

CHAPTER FOUR: SIMULATION RESULTS AND EVALUATION

This chapter provides a brief overview of network topology / simulation scenario, network model ing & simulation, results, and an analysis of the SR policy for TE on quality of service results.

4.1 Simulation Scenarios

Graphical Network Simulator-3 (GNS3) is used for simulation analysis in the implementation section, and both scenarios (scenario 1 and 2) are developed in the same topology such that SR-MPLS and SR policy for TE are implemented.

1. Scenario 1: SR-MPLS Network.
2. Scenario 2: SRTE Network.

Ostinato and Cisco IP-Sla are used in both scenarios to generate network traffic in order to measure network performance versus three QoS criteria. The first traffic generator (IP-Sla) injects the desired amounts of traffic into the network for end-to-end performance evaluation, while the second traffic generator (Ostinato) injects random network traffic to create a computation. The Ostinato generated traffic is not utilized for testing and analysis, but rather to create competition for resources among network traffics. Finally, using Cisco IP-Sla technology, the test results for the two different scenarios are retrieved from the emulator. Figure 5 shows an architecture based on SR-MPLS/SRTE. In both scenarios, there are two network domains with different IGP domains: Provider Area and Provider Edge. These architectures are typical of today's IP core network design, which can support any type of network traffic from end-to-end.

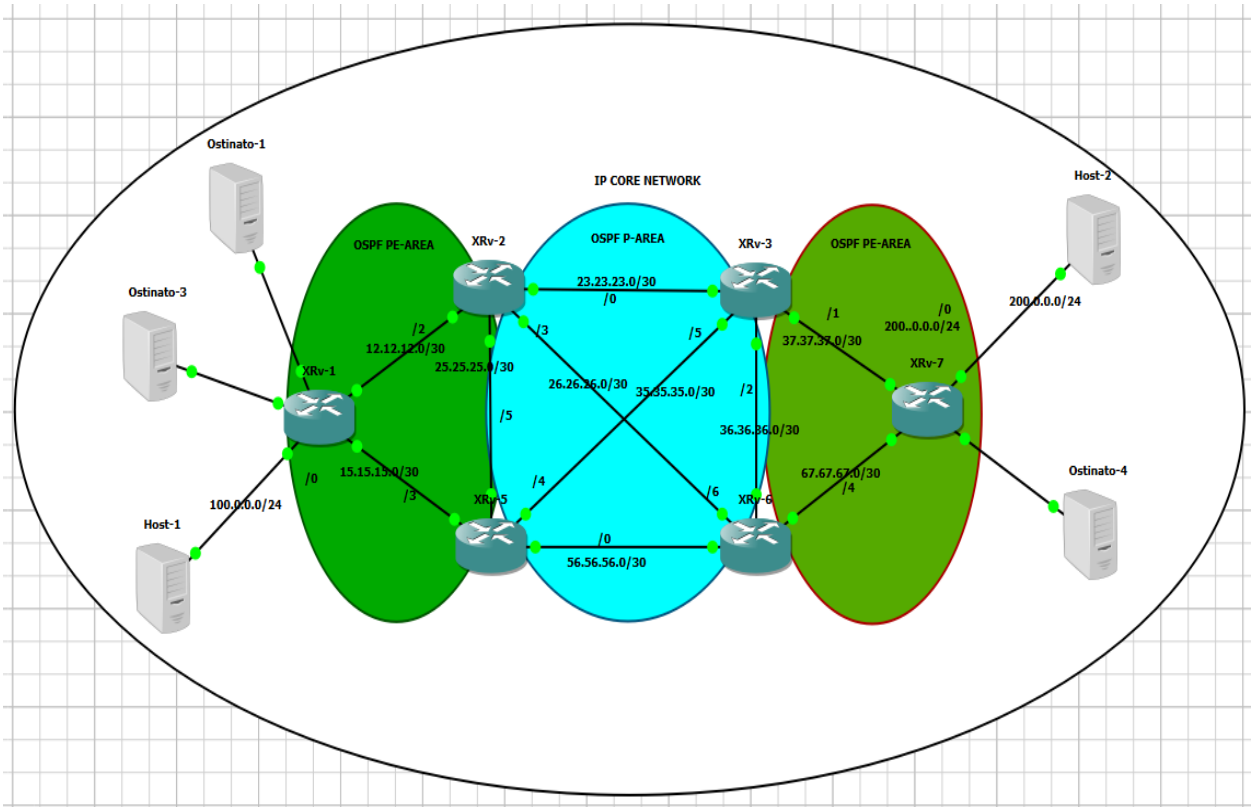

Figure 4.1: IP Core Network Architecture

4.1.1. Network Topology Design

Figure 4.1 shows the test network, which includes provider and provider edge domains that each run their own IGP domains (OSPF Multi-area) in a single BGP autonomous system.

The segmentation of these network layers into distinct and separate IGP domains facilitates:

- Smaller routing tables - Because network addresses can be aggregated between areas, there are fewer routing table entries.
- SPF computation frequency has been reduced - Within a given area; the influence of a topological change is localized. Because LSA flooding ends at the area boundary, it reduces the impact of routing updates.
- Link-state update overhead is reduced - Since there are fewer network elements exchanging LSAs, processing and memory costs are reduced.
- Network instability is limited to a single area of the network.

The provider and provider edge domains implement OSPF multi-area with segment routing / SRTE to interchange internal routes and SIDs. This is an intra-domain deployment, so both domains are part of the same autonomous system (AS), AS 1500. All of the domains are linked together using BGP labeled unicast, which allows for the end-to-end deployment of service edge node addresses and SID.

Each SR policy is expressed by a three-value tuple (head-end, color and end point). It is possible to establish explicit and dynamic paths, assign different preferences to various candidate paths, configure metrics, load sharing criteria, and many other features within the SR TE policy. SRTE policy with dynamic option has been configured in this simulation. To prepare the IP Core Network for segment routing policy for TE configuration, both scenarios must have some basic things configured, such as IGP with segment routing enabled, mpls traffic engineering enabled on all routers, and ingress egress routers.

4.2. Simulation Parameters Analysis

From these experiments, statistics on SR policy for traffic engineering and SR-MPLS have gathered in order to examine and discuss the data collected from Cisco IPSLA technology in order to validate simulation results using graphs and analysis of both scenarios and its QoS support. The IP core network of two scenarios QoS has shown, at different data sizes by examining the three parameters listed below:

1. Packet loss is the number of packets dropped during a network session or packets that never reach their intended destination.

2. Latency / Round Trip Time (RTT): The amount of time it takes a packet to traverse from head-end to tail-end.

3. Jitter is the variation in inter-packet arrival rate or the absolute value of the difference between two adjacent packets' arrival times minus their departure times.

4.2.1 Packet Loss Analysis

Figure 4.2 presents the results of experimentation and findings of packet loss. The average packet loss for SR-MPLS traffic is 16.6 percent, and 10.5 percent for SRTE traffic. The SR-MPLS and SRTE are experiencing a significant difference in this condition. Because the traffic that is passed at different packet sizes and delays has a significant impact on packet loss. Packet loss is primarily caused by delay. It ultimately runs out of time. A new packet is delivered in its place. A retransmission timeout occurs when this happens (RTO). When a packet is lost during delivery (in the form of speech data or video), the recipient hears the sound of breaking or poor streaming video images.

Table 4. 1: packet loss for both scenarios - SR and SRTE

Packet loss Comparison for SRTE and SR at different frame size Traffic			
Data Size(Byte)	Packet Loss SRTE (%)	Packet Loss SR (%)	Difference (%)
100	0	0	0
1000	0	1	0
2000	4	7	3
4000	7	11	4
6000	9	15	6
8000	12	18	6
10000	15	22	7
12000	17	25	8
14000	18	29	11
16000	20	34	14
18000	21	41	20
Average	11.2	18.5	7.3

Table 4.1 and Figure 4.2 show that when the links are not congested, there is no packet loss in either scenario at data sizes of 100 and 1000bytes. However, as data amount increases, the networks become congested and packet drop increases.

SRTE network architecture provides significantly better QoS than the SR-MPLS network architecture. In SR-MPLS, for example, there is 15percent less packet loss for a data size of 18000 bytes.

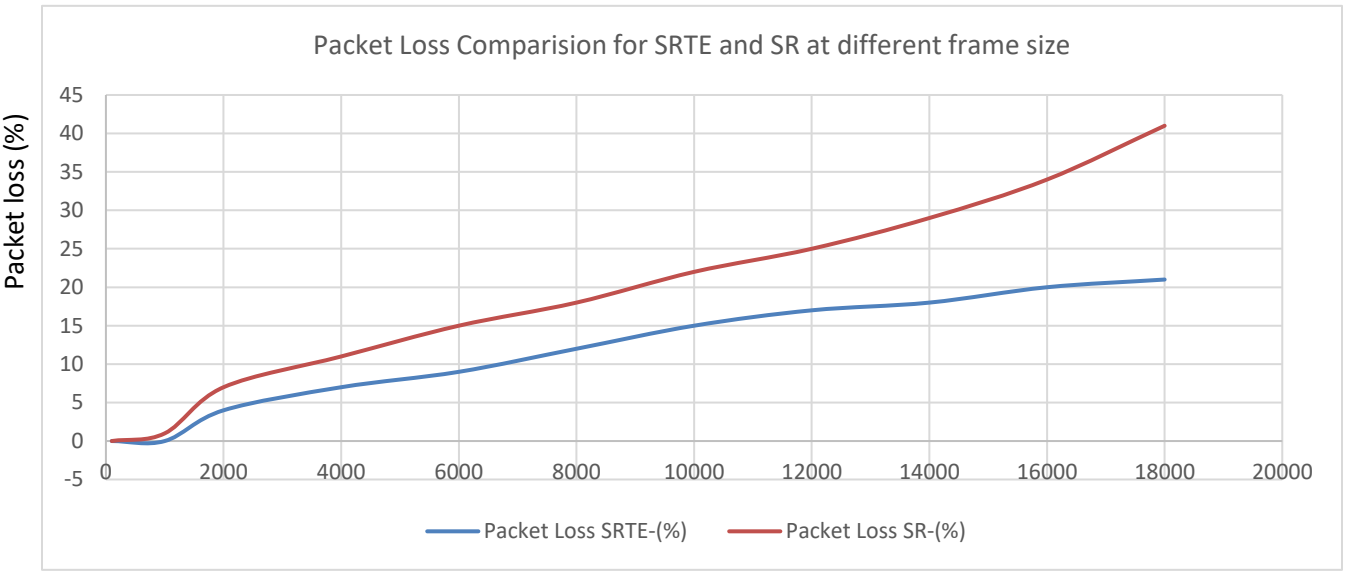

Figure 4. 2*: Packet loss- SRTE Vs SR*

4.2.2 Latency Analysis

Latency is a networking term referring to the roundtrip time or the duration of a data packet to travel from the head-end to the tail-end. When a data packet is sent and returned to its source, the time spent for the round trip is known as latency. Using Cisco IPSLA technology, the roundtrip time measures the minimum, maximum, and average latency of a test message from Host-1 to Host-2 and vice versa. Table 4.2 shows the delay/latency result of various data size test messages from collected using monitoring tool for both circumstances.

Table 4. 2 Latency for both scenarios - SR and SRTE

Latency Comparison for SRTE and SR at different frame size Traffic				
Data Size(Byte)	*SRTE-Latency(ms)*	*SR-Latency(ms)*	*Difference(ms)*	*Difference (%)*
100	22	23	1	4
1000	24	29	5	17
2000	27	35	8	23
4000	29	41	12	29
6000	32	47	15	32
8000	36	53	17	32
10000	38	58	20	34
12000	41	63	22	35
14000	43	70	27	39
16000	47	76	29	38
18000	50	80	30	38
Average	35	52	17	33

Figure 4.3 shows the latency against the data size graph, which illustrates that SR-MPLS (Scenario 1) has a higher latency (RTT) than the SR-TE (Scenario 2). The difference of latency between the two cases is 33 percent on average. That is, when compared to the SR on the same network architecture, simulation tool and computer, the latency of different data sizes SR-TE is improved on average by 35ms (i.e. 33%).

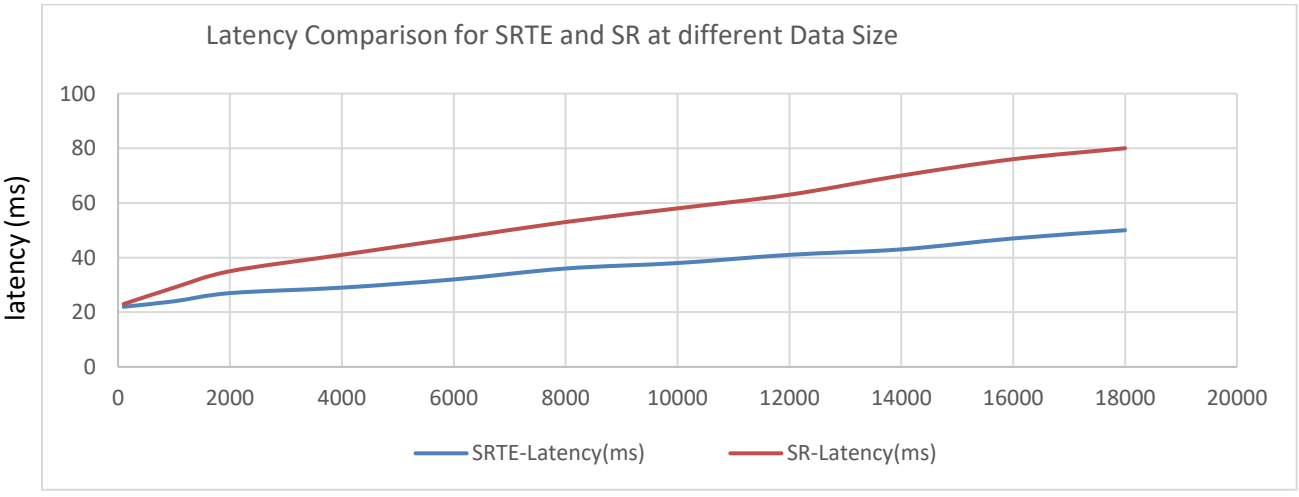

Figure 4. 3: Latency - SRTE Vs SR

4.2.3 Jitter Analysis

Aside from delay and packet loss, there is another metric to measure network performance: jitter. Jitter is the difference in time between the arrival of data packets caused by network congestion or route changes. Packets in IP networks can take several alternate paths to a destination and arrive at different times, resulting in variations in delay or jitter. Jitter degrades audio quality as data packets take longer to transport. Jitter is typically measured in milliseconds (ms). If the receiving jitter is greater than 20ms, this may increase delay and cause packet loss, resulting in a loss in audio quality. Table 4.3 and Fig. 4.4 show the jitter comparison of both network scenarios against different data sizes.

Table 4. 3: Jitter for both scenarios - SR and SRTE

Jitter Comparison for SRTE and SR at different frame size Traffic				
Data Size(Byte)	SRTE-Jitter(ms)	SR-Jitter(ms)	Difference(ms)	Difference (%)
100	3	4	1	25
1000	4	6	2	33
2000	5	7	2	29
4000	7	9	2	22
6000	8	10	2	20
8000	10	12	2	17
10000	13	15	2	13
12000	15	18	3	17
14000	18	20	2	10
16000	20	24	4	17
18000	23	26	3	12
Average	11	13	2	15

There are alternative routes in the experimentation network architecture, and average jitter for the round trip path has utilized to compare the performance of both scenarios. As illustrated in Figure 4.4, the simulation results of average jitter for SR-TE are lower than for SR. The jitter difference is 11ms on average (i.e. 15 percent). This performance between both scenarios has a substantial influence on jitter-sensitive real-time traffic like voice, video conferencing, and live streaming.

Figure 4. 4*: Jitter - SRTE Vs SR*

CHAPTER FIVE: CONCLUSION AND FUTURE WORK

5.1 Conclusion

This study's main goal is to provide a response to the research question "WHY" and "HOW" the Segment Routing policy for Traffic Engineering can be more capable in traffic optimization than the Segment Routing-MPLS protocol. And "how" these can be accomplished is mostly through the use of segment routing policies and traffic engineering (TE) to enable traffic optimization and network resource constraints. In an SR network configuration, routers in the network architecture only follow the specified path and the IGP's shortest path computation. However, as compared to MPLS, SR provides a significant improvement in overall performance, with latency increased by 24%, packet loss reduced by 20%, and jitter reduced by 12%. In order to answer these important questions, it is required to conduct extensive research in order to be able to respond in a more technical and convincing manner.

Three QoS performance measures, such as latency, packet loss, and jitter, are used to analyze and compare SR and SRTE. First, using the Cisco ISP router and GNS-3 emulator with appropriate configuration files, two scenarios are set up on the same network. Then, using Ostinato and Cisco IP-SLA technology (at different data sizes), network traffic is generated, and simulation data is collected using Cisco IP-SLA technology.

SRTE scenario demonstrates (using IOS XR 6.2.1) how to instantiate a Dynamic intra domain network architecture under a single ASN and the SR policy from a locally configured tunnel-te interface. The SR policy path has computed locally at the ingress/ source router and that learns network topology information via IGP (OSPF V2) protocol.

The SRTE path computation apply using the following methods:

- TE metric—SRTE optimizes the cumulative TE metric by using the TE metric in its path computations.
- IGP metric—SRTE optimizes reachability by using the IGP metric in its path computations.

- LSP Disjointness—SR-TE computes a pair of disjoint LSPs using path computation techniques.

As expected, the SR policy for the TE network improves packet transfers (in terms of packet loss 7.3%, Latency 33%, and jitter 15%). Although the chosen parameters are disputed when traffic congestion becomes worse, the traffic engineering technique and SR policies can improve the service provider network's performance.

According to the findings of the study, SRTE is better to SR for the following reasons.

- It provides high levels of service quality such as low packet losses,
- It minimizes congestion in the Core networks architecture
- Improves the overall jitter
- Has the shortest possible delay

In general, internet service providers and network providers appear to have used SR policies and TE to provide necessary flexibility for a wide range of services, simplify network architecture, provide reliable services, and overcome some existing infrastructure limitations.

5.2. Future Work

The primary objective of future work could be to validate the described approach in a real-world IP Core network scenario. From this perspective, future work directions might be thought of as:

- Study the impact of implement SR -TE on service-based performance evaluation of quality of service.
- Study the impact of implement SR-TE on SDN Controller-based performance evaluation of quality of service.
- Study the impact of implement SR-TE on network resource utilization and QoS improvement over RSVP-TE.
- Study the impact of implement SR-TE on IPV6 performance evaluation of quality of service.

References

[1] I. Ikram, *Traffic Engineering with MPLS and QOS*. .

[2] B. M. Sc, E. Cordeiro, and A. Reuter, "Source Packet Routing in Networking (SPRING)," no. May, pp. 31–37, 2017, doi: 10.2313/NET-2017-05-1.

[3] A. Cianfrani, M. Listanti, and M. Polverini, "Incremental Deployment of Segment Routing Into an ISP Network : a Traffic Engineering Perspective," pp. 1–15, 2017.

[4] L. P. Thiruvasakan, Q. V. B, and J. Loo, *A QoS-Based Flow Assignment for Traffic Engineering in Software-Defined*, vol. 1. Springer International Publishing, 2020.

[5] O. M. Mon and M. T. Mon, "Quality of Service Sensitive Routing for Software Defined Network Using Segment Routing," *2018 18th Int. Symp. Commun. Inf. Technol.*, no. Iscit, pp. 180–185, 2018.

[6] V. Pereira, M. Rocha, and P. Sousa, "ScienceDirect Optimizing Optimizing Segment Segment Routing Routing using using Evolutionary Evolutionary Computation Computation," *Procedia Comput. Sci.*, vol. 110, no. 2016, pp. 312–319, 2017, doi: 10.1016/j.procs.2017.06.100.

[7] H. Kumera, "Analysing Impact of Seamless MPLS on QoS Analysing Impact of Seamless MPLS on QoS," 2018.

[8] R. Mota, "Segment Routing with Use Cases," no. September, 2018, doi: 10.13140/RG.2.2.27036.13446.

[9] A. Giorgetti, A. Sgambelluri, F. Paolucci, F. Cugini, and P. Castoldi, "Segment Routing for Effective Recovery and Multi-Domain Traffic Engineering," no. February, pp. 0–11, 2017, doi: 10.1364/JOCN.9.00A223.

[10] K. Alemayehu, "No Title," no. December, 2019.

[11] "All About MPLS Traffic Engineering."

[12] D. T. Engineering and F. Reroute, “MPLS TE Technology Overview.”

[13] A. Nemtur, R. U. Wkh, and G. Ri, “Thesis / Dissertation Acceptance.”

[14] C. Filsfils, N. K. Nainar, C. Pignataro, J. C. Cardona, and P. Francois, “The Segment Routing Architecture.”

[15] C. Technologies *et al.*, “Models and Algorithms for Network Optimization with Segment Routing Thesis Commitee :,” no. February, 2020.

[16] B. R. P. Ays, D. E. L. A. L. Oire, and I. M. T. A. Tlantique, “Hese de doctorat de,” 2018.

[17] F. Name and F. Information, “Benefits of Using Segment Routing Traffic Engineering With OSPF,” pp. 1–22.

[18] S. Olivier and R. Olivier, “Managing future networks : a case study with Fibbing and Segment Routing,” 2017.

[19] F. C. De Gouveia and T. Magedanz, “QUALITY OF SERVICE IN TELECOMMUNICATION M ES PL C E O – M ES PL C E O –,” vol. II.

[20] T. Service and S. Operation, “ITU-T,” 2008.

[21] S. By, “A Traffic Engineering System for DiffServ/MPLS Networks,” no. October, 2003.

[22] J. Kosi and P. Nawrocki, “SLA Monitoring and Management Framework for Telecommunication Services SLA Monitoring and Management Framework for Telecommunication Services AGH University of Science and Technology,” no. April, 2008, doi: 10.1109/ICNS.2008.31.

[23] F. Published and S. Jose, “IP SLAs Configuration Guide,” no. 6387, 2012.

[24] F. Bensalah, N. El Kamoun, and A. Bahnasse, “Evaluation of tunnel layer impact on VOIP performances (IP – MPLS – MPLS VPN – MPLS VPN IPsec),” vol. 17, no. 3, pp. 87–92, 2017.

[25] W. Kellerer, “Master ’ s Thesis,” no. April, 2019.

[26] B. R. Patil, “Ostinato - A powerful traffic generator,” *2017 2nd Int. Conf. Comput.* Syst. Inf. Technol. Sustain. Solut., pp. 1–5, 2017.

[27] Z. Ali, B. Canada, S. Lin, and A. Bogdanov, “No Title,” pp. 1–50, 2018.

[28] C. Filsfils, S. Previdi, and L. Ginsberg, “No Title,” pp. 1–32, 2018.

[29] A. Bashandy, “RFC 8660 Segment Routing with the MPLS Data Plane Abstract,” pp. 1–29, 2019.

[30] R. Bhatia, F. Hao, M. Kodialam, T. V Lakshman, B. Laboratories, and C. Hill, “Optimized Network Traffic Engineering using Segment Routing,” pp. 657–665, 2015.

[31] R. Guedrez, “To cite this version : HAL Id : tel-02301017,” 2019.

[32] B. De Graaff, “Segment Routing in Container Networks,” 2017.

[33] J. Korhonen and H. Tschofenig, “No Title,” pp. 1–12, 2009.

[34] A. Gide, “**済無**No Title No Title No Title,” Angew. Chemie Int. Ed. 6(11), 951–952., pp. 5–24, 1967.

[35] A. Banguela and L. Hernández, “No **主観的健康感を中心とした在宅高齢者における健康関連指標に関する共分散構造分析**Title,” Biotechnol. Apl., vol. 23, no. 3, pp. 202–210, 2006.

Appendix

QoS Performance Evaluation of Segment Routing Traffic Engineering-(SRTE)

Halefom Gebremedhin Tesfay
Addis Ababa Institute of Technology
Addis Ababa Universtiy, Addis Ababa, Ethiopia
halefomgt@gmail.com

Sosina Mengistu(PhD)
Addis Ababa Institute of Technology
Addis Ababa University, Addis Ababa, Ethiopia
lesosinamg@gmail.com

***Abstract*-**

Today's telecom services have rather high expectations for quality of service (QoS), especially as internet applications become increasingly sensitive to time and delays. Because they are real-time, the crucial nature of certain of these applications is more noticeable. These provide challenges to network operators and service providers; since they are required to not only deliver these services to users, but also to ensure that they meet QoS requirements.

The majority of service providers and network operators run their networks using MPLS technology and label distribution protocols, which are complex to install, maintain, and troubleshoot. The IETF is standardizing an SR paradigm that is manageable and implemented on MPLS and is based on a simple control plane. SRTE implements the SR protocol and establishes a tunnel using TE constraints. In SR Policy, the Head-end learns multiple candidate paths from one or more segment lists, but only one path is instantiated in RIB/FIB. As a result, SR policy for TE is an effective method for engineering the packet path at the ingress router, and it is continually improving and enabling unprecedented control, as well as successfully leveraging the benefits of SR technology, which enhances more QoS requirements.

This research presents a comparative analysis of SRTE with SR in terms of average latency, jitter, and packet loss, and finds that SRTE has a 33% reduction in latency, a 7.3% reduction in packet loss, and a 15% reduction in jitter. Concerning the above attributes, the conclusion of the investigation revealed that SRTE appeared to be more capable in the optimization of traffic in Core Networks when implemented by service providers and network operators, based on the comparative results of network performance.

Keywords— *MPLS, SRTE, SR, QoS, RTT, Jitter, Packet loss, FRR, TE, SPRING, SR Policy*

I. INTRODUCTION

In today's telecommunication industries, Service Providers are facing extreme challenges to keep pace with the exponential growth of their customer's traffic. Moreover, clients are demanding more strict Quality of Service (QoS) requirements for their sensitive and mission-critical applications such as telephony, video conferencing, medical, financial, and streaming application resulting in tightened Service Level Agreements (SLA). Accordingly, service providers need to meet those requirements by enhancing service providers' network scalability, flexibility, automation policy and automated traffic steering in service delivery using QoS parameters [1].

Due to a number of promised benefits of cloud computing, personal and business applications migrate to the cloud, and the demand for network bandwidth is accelerating. Consequently, service quality will become an important differentiator between providers. For that, service providers invest in building, maintaining specialized their current transport architectures, and management approaches to satisfy the increasing demands.

The majority of transport networks use Multiprotocol Label Switching (MPLS). However, as the MPLS control plane became more complex, requiring a variety of interconnected protocols developed by several standards working groups, making it difficult to maintain, troubleshoot, and evolve.

For such considerations, the IETF standardized the Source Packet Routing in Networking (SPRING) technique for signaling MPLS paths, commonly known as Segment Routing (SR). The ability to specify TE paths through the network has become one of SPRING's advantages [28]. Its primary goal is to provide a simple and easy-to-manage control plane that improves QoS standards.

In support of a source packet routing model, segment routing policy for traffic engineering (SRTE) drastically simplifies the configuration model and eliminates soft state requirements [12]. SRTE offers not only simplicity and scalability, but also an SR native method of constructing traffic-engineered paths that take use of IP's ECMP feature.

The network's complexity is further simplified because of the more advantage of automation provided by SR policy implementation and automated traffic steering. However, when used in conjunction with SR-MPLS, SRTE is a highly strong way for regulating the packet path at the source that is constantly developing and providing unprecedented control, allowing for higher QoS implementation.

II. Problem Statement

In reality, quality of service (QoS) is essential for optimally performing real-time applications over the Internet. The IETF has established numerous service models, policies, and mechanisms to meet QoS requirements. The significant increase of real-time applications needs the provision of additional resources. The major challenge is to maximize resource utilization by implementing the sort of QoS that requires the validation of those QoS methods. As there are many hops between two core network elements, the subscriber's number & service demand has an impact on core network capacity and QoS performance[3]. Traffic engineering allows the optimal usage of network resources by including links that are not part of the least-cost path provided by IP routing. That means traffic engineering should provide the possibility to steer traffic through the network on paths different from the least-cost path [11]. Because of its complexity, traffic engineering in MPLS has been seldom used in service providers and network operators till now [3]. Segment Routing (SR) solely uses the source-routing paradigm based on IGP metrics and does not efficiently route network resources and traffic to offer QoS when the network is overloaded [8,3]. However, the network complexity of Traffic Engineering in SR is further decreased due to the added benefits provided by SR policy implementation and automated traffic steering in the network [7]. In the IPv4 context, most of the existing QoS techniques, including MPLS, MPLS-TE, and SR, have been analyzed to a greater extent. On the other hand, SR policy with TE is expected to be the future generation Internet Protocol, which has not yet been thoroughly examined or analyzed, that is my driving motivation. In general, this thesis will attempt to address the following Research Question:

What are the potential benefits of **Segment Routing Traffic Engineering (SRTE)** over an **SR-MPLS** network when QoS criteria are considered?

Hence, in SRTE, the candidate path from the head-end to the tail end instructs the intermediate routers to follow the specified path. Instead of IGP, a set of restrictions (TE Affinity, Disjoint, and Flexible Algorithm) and an optimization objective (TE & IGP metric) are used [9,11]. The SRTE optimize:

- Amount of traffic the network carries
- Utilization of resources (to avoid high utilized & low BW link.)
- The quality of service delivered

III. Literature Review

The implementation and evaluation of QoS with the MPLS-TE and SRTE networks can improve the network's performance. For establishing QoS on a network, a variety of TE algorithms and SR policies can be utilized, which can affect the network's performance.

In[4], a Quality-of-Service (QoS) based Flow Assignment method for MPLS-TE in SDN was developed and implemented, allowing the computation of end-to-end paths for traffic flows promising QoS requirements such as bandwidth, end-to-end delay, and packet loss probability. In[5], by utilizing the characteristics of SDN, which proposed QoS sensitive, routing for available bandwidth by using segment routing (SR). It has focused on monitoring flow entries among switches and finding the feasible path over a QoS-based routing scheme. The routing algorithm found the path, which was feasible to meet the desired QoS data flows. If the required QoS cannot provide for the requested flow, the controller determines how to calculate depending on the request from the switch. If the initial path will not be able to achieve the available bandwidth, the algorithm reroutes the higher bandwidth flow using Open Network Operating System (ONOS) controller with OpenFlow protocol. The research in [6] presented a work propose of Evolutionary Computation approach that supports Path Computation Element (PCE) to optimize label switching paths for congestion avoidance while using at the most three labels to configure each label switching path. In [7] has worked to evaluate end-to-end QoS performance using Seamless MPLS based on four important QoS parameters. However, the legacy MPLS uses a signaling protocol that has its own limitation. Hence, it relies on IGP plus LDP signal to establish LSP that affects the QoS performance.

Segment Routing (SR) can operate in a centralized, distributed, or hybrid arrangement. IGP (IS-IS, OSPF) or BGP are used in a distributed situation to assign and signal segments. An SR controller allocates and instantiates the segments in a centralized situation (SDN controller). Though centralized and distributed intelligence can be mixed in a hybrid model, distributed intelligence can also be utilized within the same IGP domain. The SR controller can compute a source-routed policy on behalf of an IGP node when the destination is outside IGP domain [8].

In [9], mainly focused on two important segment routing use cases: dynamic traffic recovery and multi-domain traffic engineering. Indeed, when compared to typical Internet Protocol (IP)/MPLS methods, segment routing can greatly simplify network operation in both use scenarios. Both approaches are compared, with a simulative study of the segment list depth (based on software-defined networking). A segment can encapsulate topological or service-based instructions that provide for the enforcement of a flow over any topological path while just keeping a per-flow state at the SR domain's head-end router. The SR architecture can be implemented directly to the MPLS data plane without requiring any changes to the forwarding plane as the

SR works in a network with LDP and when SR and non-SR-capable nodes coexist [8][9].

In this research, a technique for transitioning from a pure IP network to a full Segment Routing (SR) network studied. It is based on the design of a Segment Routing Domain (SRD), a subset of SR capable nodes, and a MILP optimization framework to select the best SRD in terms of congestion reduction; additionally, a technique to manage routing in the hybrid IP/SR network. The performance analysis showed that the SRD generated by addressing the SR Domain Design problem might significantly reduce maximum link consumption, delivering performance comparable to that of a full SR network even when the percentage of SR nodes is low; at the same time, the number of flow states in the flow tables of the SR competent nodes reduced [3].

In particular, according to SR, packet flows are enforced through a specific path by applying, at the ingress node, a specifically computed stack of SIDs [2]. In [10] has investigated and analyzed the impact of implementing SR-MPLS over traditional MPLS on Quality of Service (QoS) in two scenarios. In spite of the analysis, results showed SR-MPLS has better QoS, SR has mainly focused on label encoding algorithms, without carefully addressing some key aspects of SR in terms of the overall SR policies and TE and its effects on the QoS performance.

IV. METHODOLOGY

This study attempts to develop the analysis based on simulation experimental results. This simulation, as well as the analysis report, can be used to draw inferences and draw conclusions. Due to the lack of a real SRTE network for this research, the simulation has been used as an alternative. Without a review of the literature and the selection of articles, the research cannot achieve its goal.

Figure 1.1 shows the work follow of the research.

- Review the documents for understanding and determining the QoS parameters, which consider for the analysis.
- To investigate different technologies to enable SRTE architecture.
- Designing a model for the simulation using the simulation tool GNS3 for both scenarios (SRTE and SR).
- Ostinato is a traffic generator tool that is used to generate traffic into the network.
- Justify the research using the simulated data collected from IP-SLA as a measure for QoS analysis.
- Finally, the test results are presented graphically for comparison and analysis with respect to QoS parameters

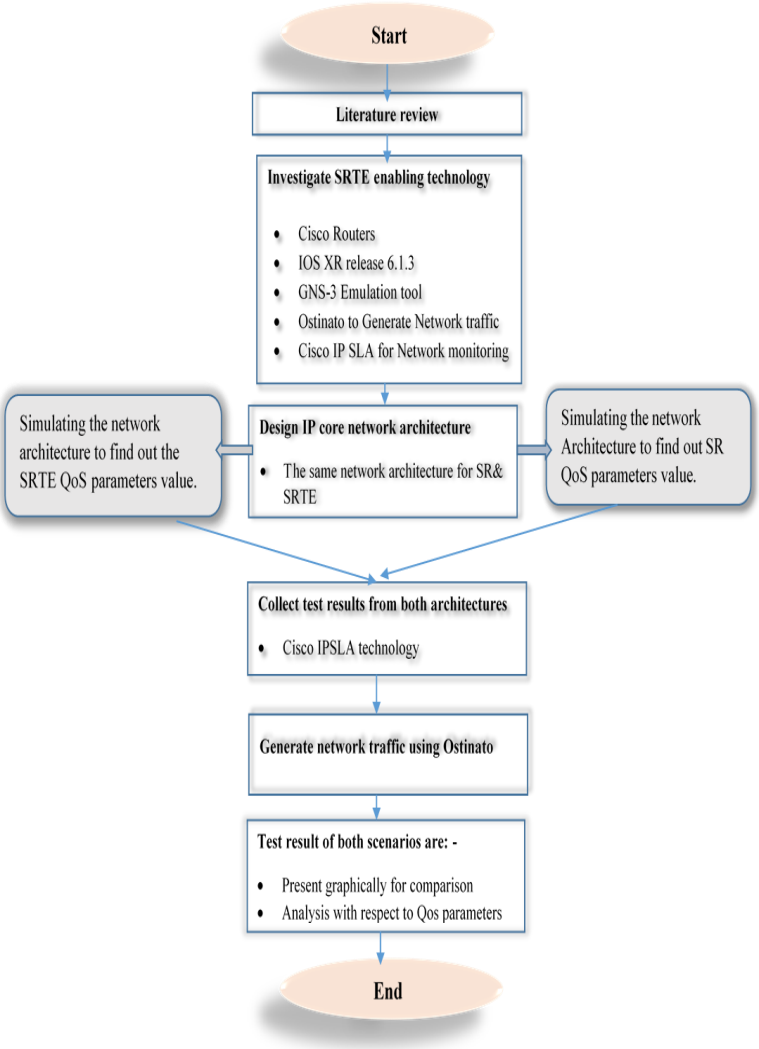

Figure 1.1: Flow chart -Methodology on SRTE and SR on QoS.

V. SIMULATION AND QOS PARAMETERS

1) simulation scenarios

Graphical Network Simulator-3 (GNS3) is used for simulation analysis in the implementation section, and both scenarios (scenario 1 and 2) are developed in the same topology such that SR-MPLS and SR policy for TE are implemented.

1. Scenario 1: SR-MPLS Network.
2. Scenario 2: SRTE Network.

Ostinato and Cisco IP-Sla are used in both scenarios to generate network traffic in order to measure network performance versus three QoS criteria. The first traffic generator (IP-Sla) injects the desired amounts of traffic into the network for end-to-end performance evaluation, while the second traffic generator (Ostinato) injects random network traffic to create a computation. The Ostinato

generated traffic is not utilized for testing and analysis, but rather to create competition for resources among network traffics. Finally, using Cisco IP-Sla technology, the test results for the two different scenarios are retrieved from the emulator. Figure 2 shows an architecture based on SR-MPLS/SRTE. In both scenarios, there are two network domains with different IGP domains: Provider Area and Provider Edge. These architectures are typical of today's IP core network design, which can support any type of network traffic from end-to-end.

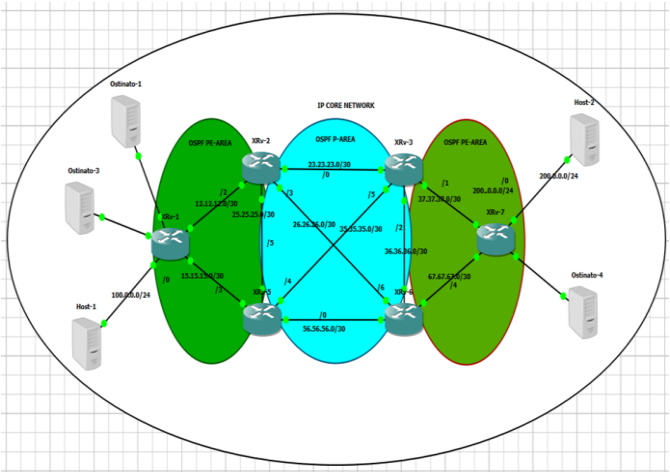

Figure 2: Network Architecture

The provider and provider edge domains implement OSPF multi-area with segment routing / SRTE to interchange internal routes and SIDs. This is an intra-domain deployment, so both domains are part of the same autonomous system (AS), AS 1500. All of the domains are linked together using BGP labeled unicast, which allows for the end-to-end deployment of service edge node addresses and SID.

Each SR policy is expressed by a three-value tuple (head-end, color and end point). It is possible to establish explicit and dynamic paths, assign different preferences to various candidate paths, configure metrics, load sharing criteria, and many other features within the SR TE policy. SRTE policy with dynamic option has been configured in this simulation. To prepare the IP Core Network for segment routing policy for TE configuration, both scenarios must have some basic things configured, such as IGP with segment routing enabled, mpls traffic engineering enabled on all routers, and ingress egress routers.

2. QoS Parameters

To provide and maintain quality of service (QoS), resource management must be QoS-driven. Different parameters can be considered by the resource management system while allocating resources:

- Network resource availability;
- Policies for resource management, such as Service Level Agreements (SLA);
- QoS requirements of applications and services, which are computed by QoS parameters (e.g. Jitter, Delay, and Packet Loss).

The QoS parameters must be monitored and resources reassigned in accordance to system anomalies in order to keep track of whether the contracted QoS is being fulfilled. Prior to the reservation of resources, the application layer must guarantee that the appropriate QoS parameters can be satisfied (through QoS negotiation signaling). To optimize the network at the traffic level, researchers consider some of the traffic-oriented performance measurements related with end-to-end QoS criteria. Latency, packet loss, and jitter are examples of these issues.

The main benefit of QoS in networks comes because of increased network capacity when new applications and services are introduced. Another advantage of QoS is that it supports the service providers in the management of congestion and avoidance mechanisms. It aids us in increasing revenue by acting as a primary backbone for shared structures. It aids in the management of multimedia that has an impact on the network,[6][1]

Depending on the required and management method, QoS is measured using characteristics such as latency, jitter, packet loss, throughput, and many more. The general QoS parameters most considered in IP Core Networks are summarized below:

A.Latency

Latency is defined as the time required for a data packet to transit across a network connection. It is, in reality, the end-to-end delay of a data packets. The terminology latency and end-to-end delay are interchangeable in this context. Many network interactive applications, such as VoIP and video teleconferencing, are extremely sensitive to latency [5]. One-way latency (the entire time from the source that transmits a packet to the destination that receives it) or round-trip latency (the one-way latency from source to destination plus the one-way latency from the destination back to the source) can be measured. Because the “Ping” command can determine roundtrip time from a single point, it is commonly utilized. Because it removes the time spent by a destination system processing the packet, the round trip delay is a generally accurate technique of measuring delay. The “Ping” command does not process packets. When it gets a packet, it merely responds with a response. In order to have a more precise delay measurement, both points of the network must be measured. The result is the shortest possible delay time for transmitting a packet from a source to a destination via that link. As a result, one of the most important tasks of QoS approaches is to provide end-to-end delay requirements [13][15].

B.Jitter

Jitter is a term that describes the variation of latency across a specified period. Packets are used to convey information from one device to another inside a network. Packets are data chunks that are transmit to other devices to transport data. Latency is the length of time it takes for these packets to arrive at their destination.

The jitter value is the variance in latency. Jitter levels beyond a certain threshold imply poor network performance and packet delivery delays. When there is a significant of jitter, packets arrive out of sequence and are irrelevant.

Jitter can be caused by a variety of factors, however there are a few typical causes that are responsible for the majority of jitter problems. These are some of them:

- Network congestion - Networks that are congested with traffic suffer from poor performance because active devices require too much bandwidth.
- Poor Hardware Performance - while working over an old network with out-of-date equipment, the jitter can be experienced due to hardware. The difference between a network with jitter and one that functions effectively can be as simple as an incompatible router, switch, or cable.

The level of network jitter that is tolerable on a network is determined by the services being provided. Some apps and services have a higher jitter tolerance than others. For example, jitter has less of an impact on sending emails than it does on voice calls [16].

When using low-tolerance applications like VoIP, jitter must be maintained below 30 milliseconds. Because the consequences of jitter will be minor, any rate of jitter below this level will be acceptable. Users will be able to understand the person on the other end of the line with minimal jitter[13].

C. Packet Loss

Packet loss occurs when one or more data packets passing through the internet or a computer network fail to arrive at their destination. IP networks cannot guarantee that packets may or may not be delivered at all. Other factors that cause packet loss include loads on network links, corrupted packets being deleted, and network element defects.

The UDP protocol is commonly used to transport packets over the network for real-time applications (or more specifically the RTP protocol, which runs on top of UDP) [4]. Due to the significant latency sensitivity of real-time applications, standard TCP retransmission techniques are ineffective in this circumstance. The UDP protocol has the drawback of not being able to ensure the delivery of all packets. During peak loads or periods of congestion, packets can be lost. The data packets lost during a network session is referred to as packet loss. In other words, packet loss refers to the number of packets that never reach it to their intended destination. Packet loss must be kept below a specific threshold for an application to function properly. Some Voice over IP (VoIP) QoS applications, for example, define the following QoS services [CA02]:

- < 0.2 % - GOLD service
- 5 % - SILVER service
- 10 % - BRONZE service

Packet losses greater than 10 percent are usually intolerable[14].

VI. RESULTS AND DISCUSSION

A. *Latency Analysis*

Latency is a networking term referring to the entire amount of time it takes for a data packet to travel from the head-end to the tail-end. When a data packet is sent and returned to its source, the time spent for the round trip is known as latency. Cisco IPSLA measures the minimum, maximum, and average delays of transmitting a test message from Host-1 to Host-2 and vice versa. Table 1 shows the latency result of various data size test messages collected using IP sla for both circumstances.

Table 1: Latency for both scenarios - SR and SRTE

Data Size(B)	*SRTE-RTT(ms)*	*SR-RTT(ms)*	*D/f (ms)*	*D/f (%)*
100	22	23	1	4
1000	24	29	5	17
2000	27	35	8	23
4000	29	41	12	29
6000	32	47	15	32
8000	36	53	17	32
10000	38	58	20	34
12000	41	63	22	35
14000	43	70	27	39
16000	47	76	29	38
18000	50	80	30	38
Average	35	52	17	33

Figure 3 shows the latency against the data size graph, which illustrates that SR-MPLS (Scenario 1) has a higher latency (RTT) than the SR-TE (Scenario 2). The variation in latency between the two cases is 33 percent on average. That is, when compared to the SR on the same network architecture, the latency of different data sizes SR-TE is improved on average by 35ms (i.e. 33%).

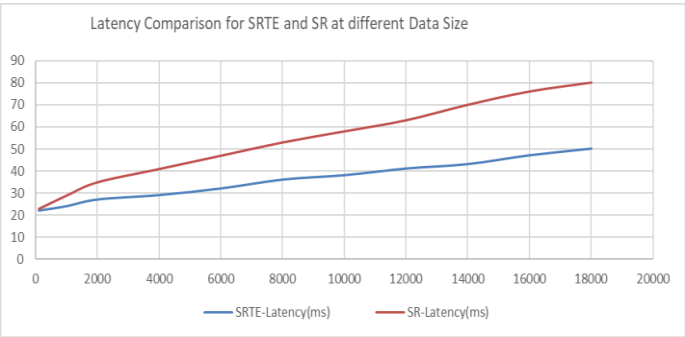

Figure 3: Latency - SRTE Vs SR

B. *Jitter Analysis*

Aside from delay and packet loss, there is another metric to measure network performance: jitter. Jitter is the difference in time between the arrival of data packets caused by network congestion or route changes. Packets in IP networks can take several alternate paths to a destination and arrive at different times, resulting in variations in delay or jitter. Jitter degrades audio quality as data packets take longer to transport. Jitter is typically measured in milliseconds (ms). If the receiving jitter is greater than 20ms, this may increase delay and cause packet loss, resulting in a loss in audio quality. Table 2 and Fig. 4 show the jitter comparison of both network scenarios against different data sizes.

Table 2: Jitter for both scenarios - SR and SRTE

Data Size(B)	SRTE-Jitter(ms)	SR-Jitter(ms)	D/f(ms)	D/f (%)
100	3	4	1	25
1000	4	6	2	33
2000	5	7	2	29
4000	7	9	2	22
6000	8	10	2	20
8000	10	12	2	17
10000	13	15	2	13
12000	15	18	3	17
14000	18	20	2	10
16000	20	24	4	17
18000	23	26	3	12
Average	11	13	2	15

There are alternative routes in the experimentation network architecture, and average jitter for the round trip path has utilized to compare the performance of both scenarios. As illustrated in Figure 4, the simulation results of average jitter for SR-TE are lower than for SR. The jitter difference is 11ms on average (i.e. 15 percent). This performance between both scenarios has a substantial influence on jitter-sensitive real-time traffic like voice, video conferencing, and live streaming.

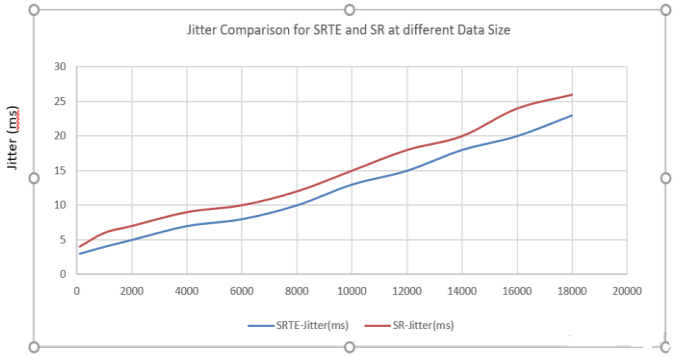

Figure 4: Jitter - SRTE Vs SR

C.*Packet Loss Analysis*

Figure 5 presents the results of experimentation and findings of packet loss. The average packet loss for SR-MPLS traffic is 16.6 percent, and 10.5 percent for SRTE traffic. The SR-MPLS and SRTE are experiencing a significant difference in this condition. Because the traffic that is passed at different packet sizes and delays has a significant impact on packet loss. Packet loss is primarily caused by delay. It ultimately runs out of time. A new packet is delivered in its place. A retransmission timeout occurs when this happens (RTO). When a packet is lost during delivery (in the form of speech data or video), the recipient hears the sound of breaking or poor streaming video images.

Table 3: packet loss for both scenarios - SR and SRTE

Data Size(Byte)	Packet Loss SRTE-(%)	Packet Loss SR-(%)	D/f(%)
100	0	0	0
1000	0	1	0
2000	4	7	3
4000	7	11	4
6000	9	15	6
8000	12	18	6
10000	15	22	7
12000	17	25	8
14000	18	29	11
16000	20	34	14
18000	21	41	20
Average	11.2	18.5	7.3

Table 3 and Figure 5 show that when the links are not congested, there is no packet loss in either scenario at data sizes of 100 and 1000bytes. However, as data amount increases, the networks become congested and packet drop increases.

SRTE network architecture provides significantly better QoS than the SR-MPLS network architecture. In SR-MPLS, for example, there is 15percent less packet loss for a data size of 18000 bytes.

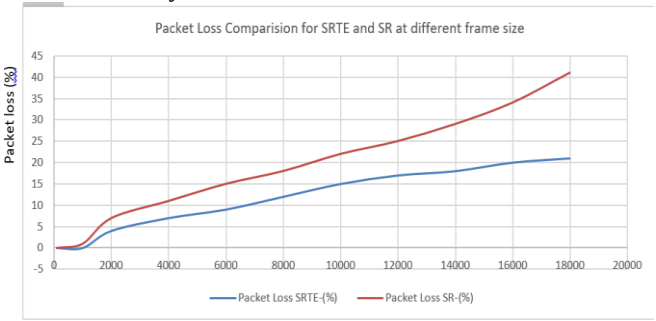

Figure 5*: Packet loss- SRTE Vs SR*

VII. CONCLUTSION

This study's main goal is to provide a response to the research question "WHY" and "HOW" the Segment Routing policy for Traffic Engineering can be more capable in traffic optimization than the Segment Routing-MPLS protocol. And "how" these can be accomplished is mostly through the use of segment routing policies and traffic engineering (TE) to enable traffic optimization and network resource constraints. In an SR network configuration, routers in the network architecture only follow the specified path and the IGP's shortest path computation. However, as compared to

MPLS, SR provides a significant improvement in overall performance, with latency increased by 24%, packet loss reduced by 20%, and jitter reduced by 12%. In order to answer these important questions, it is required to conduct extensive research in order to be able to respond in a more technical and convincing manner.

Three QoS performance measures, such as latency, packet loss, and jitter, are used to analyze and compare SR and SRTE. First, using the Cisco ISP router and GNS-3 emulator with appropriate configuration files, two scenarios are set up on the same network. Then, using Ostinato and Cisco IP-SLA technology (at different data sizes), network traffic is generated, and simulation data is collected using Cisco IP-SLA technology.

SRTE scenario demonstrates (using IOS XR 6.2.1) how to instantiate a Dynamic intra-domain SR policy from a locally configured interface tunnel-te. The SR policy path can be computed locally on the head-end and that learns topology information by way of IGP (OSPF V2).

SR-TE may compute paths using the following methods:

- TE metric—SR-TE optimizes the cumulative TE metric by using the TE metric in its path computations.
- IGP metric—SR-TE optimizes reachability by using the IGP metric in its path computations.
- LSP Disjointness—SR-TE computes a pair of disjoint LSPs using path computation techniques.

As expected, the SR policy for the TE network improves packet transfers (in terms of packet loss 7.3%, Latency 33%, and jitter 15%). Although the chosen parameters are disputed when traffic congestion becomes worse, the traffic engineering technique and SR policies can improve the service provider network's performance.

According to the findings of the study, SRTE is better to SR for the following reasons.

- It provides high levels of service quality such as low packet losses,
- It minimizes congestion in the Core networks architecture
- Improves the overall jitter
- Has the shortest possible delay

In general, internet service providers and network providers appear to have used SR policies and TE to provide necessary flexibility for a wide range of services, simplify network architecture, provide reliable services, and overcome some existing infrastructure limitations.

REFERENCES

[I] Ikram, *Traffic Engineering with MPLS and QOS*. .

[2] B. M. Sc, E. Cordeiro, and A. Reuter, "Source Packet Routing in Networking (SPRING)," no. May, pp. 31–37, 2017, doi: 10.2313/NET-2017-05-1.

[3] A. Cianfrani, M. Listanti, and M. Polverini, "Incremental Deployment of Segment Routing Into an ISP Network : a Traffic Engineering Perspective," pp. 1–15, 2017.

[4] L. P. Thiruvasakan, Q. V. B, and J. Loo, *A QoS-Based Flow Assignment for Traffic Engineering in Software-Defined*, vol. 1. Springer International Publishing, 2020.

[5] O. M. Mon and M. T. Mon, "Quality of Service Sensitive Routing for Software Defined Network Using Segment Routing," *2018 18th Int. Symp. Commun. Inf. Technol.*, no. Iscit, pp. 180–185, 2018.

[6] V. Pereira, M. Rocha, and P. Sousa, "ScienceDirect Optimizing Optimizing Segment Segment Routing Routing using using Evolutionary Evolutionary Computation Computation," *Procedia Comput. Sci.*, vol. 110, no. 2016, pp. 312–319, 2017, doi: 10.1016/j.procs.2017.06.100.

[7] H. Kumera, "Analysing Impact of Seamless MPLS on QoS Analysing Impact of Seamless MPLS on QoS," 2018.

[8] R. Mota, "Segment Routing with Use Cases," no. September, 2018, doi: 10.13140/RG.2.2.27036.13446.

[9] A. Giorgetti, A. Sgambelluri, F. Paolucci, F. Cugini, and P. Castoldi, "Segment Routing for Effective Recovery and Multi-Domain Traffic Engineering," no. February, pp. 0–11, 2017, doi: 10.1364/JOCN.9.00A223.

[10] K. Alemayehu, "No Title," no. December, 2019.

[11] "All About MPLS Traffic Engineering."

[12] D. T. Engineering and F. Reroute, "MPLS TE Technology Overview."

[13] A. Nemtur, R. U. Wkh, and G. Ri, "Thesis / Dissertation Acceptance."

[14] C. Filsfils, N. K. Nainar, C. Pignataro, J. C. Cardona, and P. Francois, "The Segment Routing Architecture."

[15] C. Technologies *et al.*, "Models and Algorithms for Network Optimization with Segment Routing Thesis Commitee :," no. February, 2020.

[16] B. R. P. Ays, D. E. L. A. L. Oire, and I. M. T. A. Tlantique, "Hese de doctorat de," 2018.