Farhan et al LGURJCSIT 2019

LGURJCSIT
ISSN: 2519-7991

LGU Research Jounral for
Computer Sciences & IT

Vol. 3 Issue 1, January - March 2019

A Comparative Analysis of Unicast Routing Protocols for MPLS-VPN

[1]Muhammad Farhan, [2]Muhammad Asif, [3]Maaz Bin Ahmad, [2]Khalid Maqsood
[1]Department of Computer Sciences, Lahore Leads University, Lahore, Pakistan
[2]Department of Computer Sciences, Lahore Garrison University, Lahore, Pakistan
[3]College of Computing and Information Sciences, PAF Karachi Institute of Economics and Technology, Karachi, Pakistan
hafizfarhan4@gmail.com, drmuhammadasif@lgu.edu.pk,
maaz@pafkiet.edu.pk, khalid.masood@lgu.edu.pk

Abstract:

MPLS-VPN technology is introduced to provide secure transmission with minimum propagation delay. This paper presents a comparative analysis of unicast routing protocols for MPLS-VPN enabled networks. The motive behind this analysis is to observe the consequence of unicast routing protocols on the performance of MPLS-VPN enabled networks and to choose most suitable routing protocol for such type of networks. To conduct the analysis, a test bed is established in GNS3 simulator. Three main unicast routing protocols i.e. Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) has been considered in this work. Round-Trip-Time, Jitter and Administrative-distance are used as performance measure metrics. The experimental analysis indicates that EIGRP is the most suitable protocol among the aforementioned protocols for MPLS-VPN.

Keywords: MPLS, VPN, ISP, IPSEC, GNS3

1. INTRODUCTION

Multiprotocol Label Switching (MPLS) protocol is de- signed with the goal to speed up and shape network traffic flow across service provider networks and enterprise wide area. It is presented by the Internet Engineering Task Force (IETF) for efficient routing, switching and forwarding of network traffic [1]. This mechanism allows data packet forwarding through labels (switching level) rather than the hop-by-hop IP based forwarding (routing level) [2]. It is basically a Wide Area Network (WAN) technology that is running at the backbone of Internet Service Providers (ISPs). ISPs used MPLS to enhance the quality of service (QoS) through Label-Switched Paths (LSPs) establishment that can fulfill particular Service Level Agreements (SLAs) on downtime, packet loss, jitter and traffic latency [2], [3], [4]. MPLS also provides numerous main features including traffic separation, virtual private networks (VPNs) creation, virtual leased lines (VLLs) and virtual private LAN services (VPLS). It works very well to select the right path to reach the destination without any downtime. In case of any fault, the whole network will not go down. It works on layer 2.5, means that it supports layer 2 and also layer 3 of open system Interconnection (OSI) reference Model [1].

Fig. 1 demonstrates the working of MPLS. It shows that when a packet enters to the service provider area, it gets a labeled from ingress router after that traffic forwarding through the network is done with the help of labels instead of IP. When the packet is reached at the egress router, it removes the label and forward IP packet to final destination [2]. In MPLS, label is used to follow the forwarding path LSP. LSP is automatically determined in service provider area to decide the best path for traffic flow within a private or public network

[5], [6].

It is observed that simple MPLS does not have any ad- vantage because of additional configuration load. It is highly suitable with its applications like VPN, QOS, VLL and etc. VPN is a very impressive application of MPLS that transforms a private system to an open system e.g internet [6]. It empowers the clients to send and get information across the public network as the intermediate devices or computing devices that are directly connected to the private network [7]. It is useful for security and administration arrangements of the private system [8]. A number of enterprises put the VPN in their backbone of network to facilitate or take advantages of number of services like IP-SEC, QOS and traffic engineering [9].

In this work, a comparative analysis is made to observe the effect of unicast routing protocols on the performance of MPLS-VPN enabled network and select the most appropriate protocol for such type of networks. Three main unicast routing protocols i.e. Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) is considered. The performance measure metrics use in this work includes Jitter, Round-Trip- Time and Administrative-distance. The experimental analysis portrays that EIGRP outperform the rest of unicast routing protocols in MPLS-VPN domain.

The rest of the paper is organized as follows: Background is covered in section II. Section III presents the simulation tools and parameters, testing environment and performance measure metrics. Experimental analysis is done in section IV. Finally, section V concludes the article.

2. BACKGROUND

A. Virtual Private Network (VPN)

VPN is the technology that is used to establish encrypted connection over pre-existing less secure network [2]. VPNs enable the optimal level of security for the organizations that do not afford to build an entirely private network server. Across the world, there are so many organizations that have their sub offices in different countries. Most of these organizations used Virtual Private Network (VPN) for the remote connectivity among these sub branches with the head office to reduce the propagation delay [6], [9]. VPN provides a mechanism for encapsulation and reliable communication between two branches and saves a lot of resources like money for installation of leased lines or purchasing some physical links for communication.

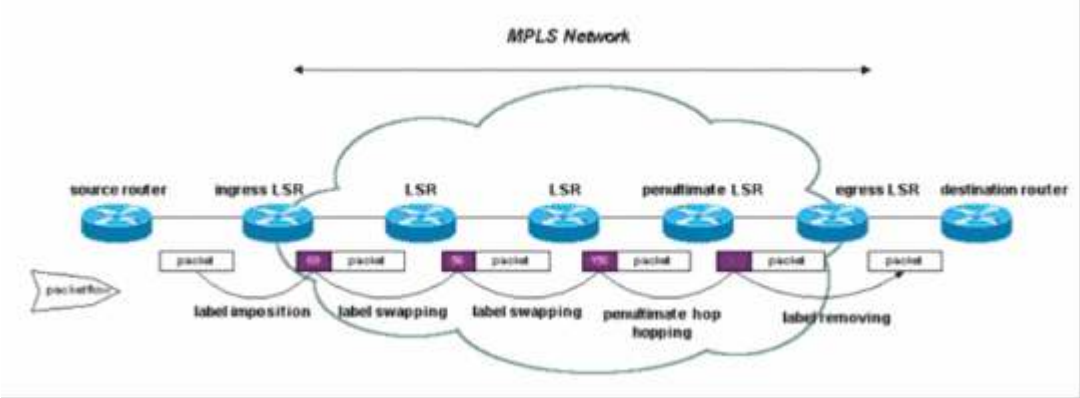

Fig. 1. MPLS Network

1) Types of VPN: It can be categorized into following two main types: Site-to-Site VPN:

- Site-to-Site VPN needs a fixed location of the customers that are connected through ISP and a virtual tunnel is created between these two sites to provide the secure transmission of the data [2], [9-10]. The Site-to-Site VPN is shown in Fig. 2.
- Remote VPN: It does not require any fixed location; user can be anywhere but need an internet connection for the centralized network communication. For this type of commun 4ication, VPN Tunneling protocols are used [2], [9-10].

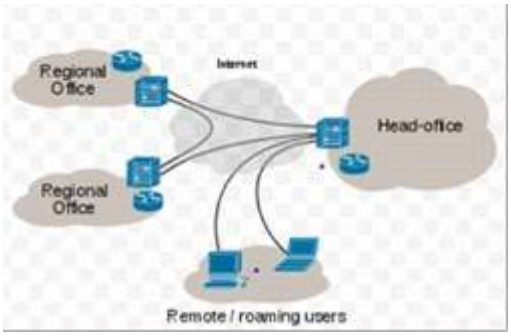

Fig. 2. Site-to-Site VPN

1) VPN Tunneling Protocols:

The following are the main tunneling protocols used in VPN:

- Point-to-Point Tunneling Protocol (PPTP): It does not provide any encapsulation mechanism, just follow the point-to-point protocol (PPP) to establish tunnel for data transmission.
- Layer 2 Tunneling Protocol (L2TP): It is almost similar to PPP and uses layer 2 for the data transmission and consolidation.
- Internet Protocol Security (IP-SEC): IP-SEC is used to encrypt and encapsulate the data packets and sends to the network. It is very popular VPN security protocol. It operates on two modes that include Tunnel mode and Transport mode. Fig. 3 shows the IP-SEC tunnels. In IP-SEC tunnel, data can be reached at the destination securely and no one can sniff the traffic and provides the maximum reliability. In this mode, there are some gateways that help to perform the encapsulation process. These gateways verify the incoming and outgoing packets [10].

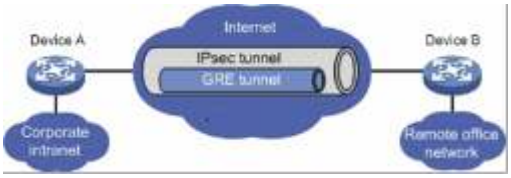

Fig. 3. IP-SEC Tunnels

An IPSEC Tunnel offers huge security benefits and ought to be utilized where information protection is required. On the other hand, Generic Routing Encapsulation (GRE) Tunnel is used when IP bundles needed to be sent from one system to other without being parsed by any mediating course.

B. Unicast Routing Protocols

Unicast means the transmission of data form single source to single destination through network. Routing protocols are the rules and regulations how to find the shortest path form source to destination to send the information including text, audio, images, video and etc. The following are the three main unicast routing protocols used in this work:

1) Routing Information Protocol (RIP):

RIP is a distance vector routing protocol [11]. It is a type of interior gateway protocols. RIP broadcast its routing updates after 30 seconds that may affect the networks performance because of periodic route update information. It has more convergence time. It

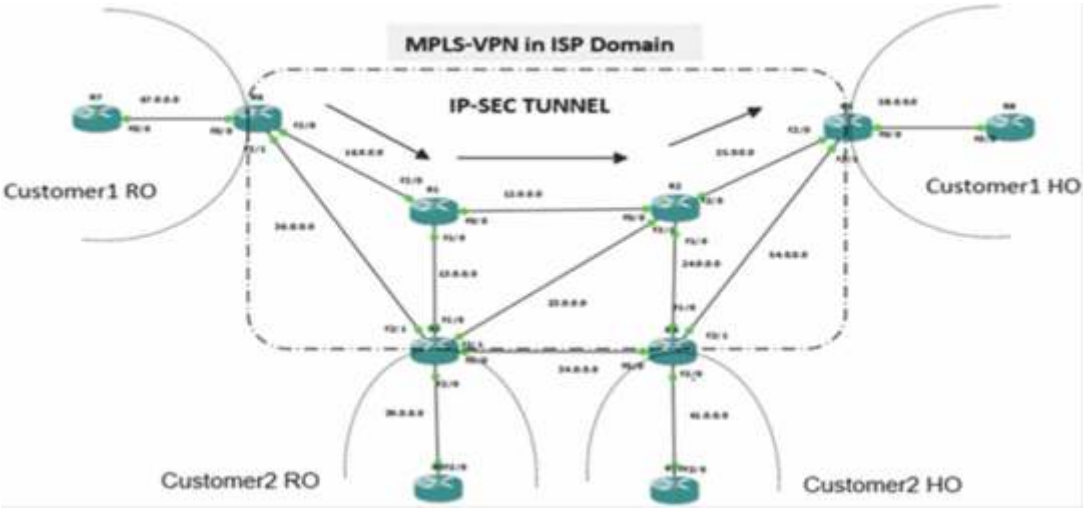

Fig. 4. Experimental Environment

uses a metric that is called hop count. It just supports the class full networks and is mostly used for the small autonomous system.

2) Open Shortest Path First (OSPF): OSPF is a link state routing protocol (LSRP) [11]. The routing updates of the OSPF are called LSA (Link State Advertisement). It multicast routing updates that decreases the route update traffic on the network. OSPF metric is cost that is tricky to handle. OSPF is designed for large autonomous system with no limit on number of hops. It has fast convergence.

3) Enhanced Interior Gateway Routing Protocol (EIGRP): EIGRP is a mixture of distance vector and link state protocol. It is developed by Cisco. It uses SHA-2 and MD5 encapsulation among two routers [11].

3. SIMULATION ENVIRONMENT

A. Simulation Parameters

In this work, Graphical Network Simulator (GNS3) is used for simulation of network [12-14]. GNS3 enables clients to plan and convey reenactment for complex network topologies. The simulation parameters are listed in Table 1.

Table 1. Simulation Parameters

Simulator	Graphical Network Simulator (GNS3)
Platform	Cisco IOS Router 7200 Enterprise Edition
Protocols	RIP , EIGRP and OSPF
Parameters	Jitter, Round-Trip-Time and Administrative Distance
Units of measurement	Milliseconds

B. Test Environment Setup

To build the experimental environment, a couple of sup- positions are made with a specific end goal to facilitate the examination and perception which are:

- Cisco C7200 routers are used to build the experimental setup.
- All the interfaces in setup are serial and have same cost.
- IP assignment is based on labels.

In this setup, there are two customers and each have two remote branches (Regional office RO and Head Office HO). They want to communicate with each other through MPLS-VPN networks. The experimental setup consists of 10 routers out off these 4 are the Customer Edge (CE) routers. Fig. 4 shows the experimental environment.

Customer 1 consists of router R7 and R8. On other hand, router R9 and R10 belong to customer 2. The main motive is to secure transmission between two sites with minimum packet loss and delay. In this topology, R5 (egress) and R6 (Ingress) are customer 1 edge routers that provide connectivity with service provider network. The routers R7, R8, R9 and R10 are the part of private networks and rest of the routers are belonged to ISP domain. The private networks do not have the influence in ISP domain. The MPLS is enabled on each interface.

The routing protocols including (RIP, EIGRP and OSPF) are configured on routers (R1, R2, R5, R6, R7 and R8) in the same scenario one by one. After that, IP-SEC tunnel is created between edge routers R5 (egress) and R6 (Ingress) to provide the secure transmission between them. When an IP packet enters in router R6, a label will be assigned that hides the IP address. After that, forwarding will be done on basis of labels instead of IP address. When the packet reaches to R1, it will assign a new label for further forwarding to R2 and then R2 will assign new label to transfer it to the router R5.

R5 is a customer edge router and it will remove the label and the pure IP traffic will forward to R8. In this work, BGP (Border gateway routing protocol) is configured on the routers R3 and R4 because the traffic will transform between different autonomous systems.

IP-SEC tunnel is used at both customer sites, after using the IP-SEC the IP packet will be protected because the original packet will hide inside a new header and then send it to the second site of VPN tunnel. It is usually used between gateways and the gateway acts as proxy of host behind it. After all the configurations have been done, the environment is ready to conduct the experimental analysis.

C. Performance Measure Metrics

The following performance measure metrics are used to evaluate the performance of aforementioned routing protocols in MPLS-VPNS.

1) ***Round-Trip-Time (RTT):***

RTT is the time needed to transfer data packet from a source to a destination and back to the source through the network. It is one of a few variables important metrics that

demonstrate the network performance. In this work, is measured in millisecond.

2) Jitter:

It is an average variation in the delay of received packets. During network communication, sender transmits data in a continuous stream of evenly spaced packets. Some of the data packets take longer time to travel from source to destination while others take less time. Jitter is an important network performance measure metric that give average variation in the latency on a packet flow between two systems. Route changes, network congestion and timing drift are the major causes of jitter. It adversely affects the real-time audio and video applications like IP telephony and video conferencing [15]. In this work, Jitter is measured in millisecond.

3) Administrative-Distance:

It is the attribute that routers utilize to pick the optimum route from two or more different paths to the same destination determine by two dissimilar routing protocols. It is used to prioritize each routing protocol from most to least reliable. The administrative distance can also be calculated from routing table of a router. It is a unit less quantity and is measured in decimal value.

4. EXPERIMENTAL ANALYSIS

A. Round-Trip-Time (RTT)

Fig. 5 shows EIGRP outperform the rest of the routing protocols in context of RTT. To compare the performance, minimum, maximum and average value of RTT is calculated against each protocol.

B. Jitter

To compare the performance of three unicast routing protocols, minimum, maximum and average value of jitter is calculated against each protocol. Fig. 6 shows the performance of RIP is worst than OSPF and EIGRP in context of jitter. The behavior of OSPF and EIGRP is almost similar.

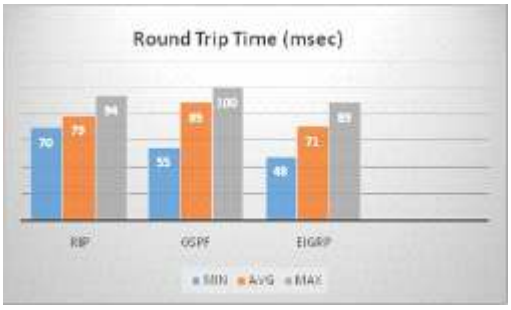

Fig 5: Performance comparison in terms of RTT (Millisecond)

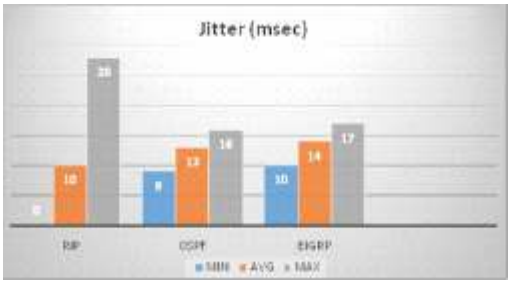

Fig 6: Performance comparison in terms of Jitter (Millisecond)

C. Administrative Distance

Fig. 7 demonstrates the performance of three routing proto- cols in terms of Administrative Distance. It depicts that EIGRP has minimum Administrative Distance value, RIP has maximum Administrative Distance value and OSPF has average Administrative Distance value. The EIGRP outperform rest of the routing protocols on the bases of Administrative Distance value.

Fig 7: Performance comparison in terms of Administrative Distance

Table. 2 lists the experimental results on basis of RTT, Jitter and Administrative distance. EIGRP protocol has small RTT and Administrative Distance value as compared to restof the two algorithms. In context of Jitter, the behavior of EIGRP is comparable with OSPF while better than RIP. From the experimental analysis it can be concluded that EIGRP is most suitable routing protocols for the MPLS-VPN

networks as compared to RIP and OSPF.

TABLE 2. SIMULATION PARAMETERS

Protocols	RTT (Min/Avg/Max) millisecond	Jitter (Min/Avg/Max) millisecond	Administrative Distance (AD)
RIP	70/79/94	0/10/28	120
OSPF	55/89/100	9/13/16	110
EIGRP	48/71/89	10/14/17	90

5. CONCLUSION

This work presented a comparative analysis of unicast routing protocols for MPLS-VPN enabled networks to choose most suitable protocol for such type of networks. The experimental results indicate that EIGRP is the most suitable protocol as compared to OSPF and RIP for MPLS-VPN networks on the basis of Round trip time, Jitter and Administrative distance.

6. REFERENCES

[1] R. Q. Shawl, R. Thaker and Er. J. Singh, "A Review: Multiprotocol Label Switching (MPLS)", International Journal of Engineering Research and Applications, vol. 4, no. 1, pp. 66-70, 2014.

[2] Understanding the Importance of Multiprotocol Label Switching (MPLS) for Virtual Private Network Connectivity: https://www.volico.com/understanding-importance-multiprotocol-label- switching-mpls-virtual-private-network-connectivity/, Accessed: March 26, 2019.

[3] H. M. I. Yusof, S. Zainuddin, M. Kassim and Ruhani Ab Rehman, "A Comparative Analysis of Packet Fragmentation with MPLS Unicast IP Routing and OSPF in an IP-based Network", vol. 8, no. 3, 2016.

[4] N. Charles, "A Comparative Simulation Study of IP, MPLS, MPLS- TE for Latency and Packet Loss Reduction over a WAN", International Journal of Networks and Communications, vol. 6, no.1, pp.1-7, 2016.

[5] R .Ab Rahman, F. A. Alias, M. Kassim, M. I. Yusof and H. Hashim, "Implementation of high availability concept based on traffic segregation over MPLS-TE", ARPN Journal of Engineering and Applied Sciences, vol. 10, no. 3, pp.1295-301, 2015.

[6] M. Zhang and ZP Tao, "Application Research of MPLS VPN All-in-one Campus Card Network based on IPSec", IEEE International Conference on Computational and Information Sciences, 2012.

[7] F. Bensalah, N. Kamoun, A. Bahnasse, "Analytical Performance and Evaluation of the Scalability of Layer 3 Tunneling Protocols: Case of Voice Traffic Over IP", International Journal of Computer Science and Network Security (IJCSNS), vol. 17, no. 4, 2017.

[8] A. Bahnasse, M. Talea, A. Badri, F. E. Louhab, "New smart platform for automating MPLS virtual private network simulation", IEEE In- ternational Conference on Advanced Communication Technologies and Networking (CommNet), 2018.

[9] R. Ab Rahman, M. Kassim and N. Ariffin, "Performance Analysis on Wan Optimizations: Bandwidth Management in Multi Protocol Level Switching (MPLS) VirtualPrivate Network (VPN)", International Con- ference on Future Information Technology, IPCSIT ,vol.13, 2011.

[10] F. Palmieri, "VPN scalability over High Performance Backbones Eval- uating MPLS VPN against Traditional Approaches", Eighth IEEE Inter- national Symposium on Computers and Communication. pp: 975-981, 2003.

[11] P. Rakheja, P. Kaur, A. Gupta and A. Sharma, "Performance Analysis of RIP, OSPF, IGRP and EIGRP Routing Protocols in a Network," International Journal of Computer Applications, vol. 48, no. 16, pp. 6-11, 2012.

[12] Graphical Network Simulator-3: https://en.wikipedia.org/wiki/ Graphical Network Simulator-3, Accessed March 26, 2019.

[13] Y. Wang and J. Wang "Use gns3 to simulate network laboratory", Computer Programming Skills and Maintenance, 2010.

[14] L.Faxun "The Application of GNS3 in Network Experiments," Com- puter and telecommunication, pp.10:032, 2010.

[15] F. Bensalah, N. El Kamoun, A. Bahnasse, "Evaluation of tunnel layer impact on VOIP

performances (IP-MPL S-MPLS VPN-MPLS VPN Ipsec)", International Journal of Computer Science and Network Security (UC-SNS), vol. 17, no. 3, 2017.