INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Deployment of Carrier supporting Carrier (CsC) Network Providing MPLS-VPN Services to End Customers

Merline Johndoss[1]*, **T Pramananda Perumal**[1]

1 Presidency College, Chennai, 600 005, Tamil Nadu, India

OPEN ACCESS

Received: 28-09-2023

Accepted: 18-10-2023

Published: 20-12-2023

Citation: Johndoss M, Perumal TP (2023) Deployment of Carrier supporting Carrier (CsC) Network Providing MPLS-VPN Services to End Customers. Indian Journal of Science and Technology 16(46): 4445-4455. https://doi.org/10.17485/IJST/v16i46.2456

* **Corresponding author**.

merlinjohndoss@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: A small service provider intends to connect its customers who are geographically apart and to give Multi Protocol Label Switching-Virtual Private Networks (MPLS-VPNs) services. But, the small service provider does not have direct connectivity between the locations. The end customers want very secure, fast and scalable network connectivity. To provide the requirements of the end customers, a comprehensive solution viz. Carrier supporting Carrier (CsC) network model is proposed. **Methods**: A topology for CsC network implementation is designed with Backbone Carrier routers, Customer Carrier routers and Customer routers. This CsC network is deployed with Customer Carrier providing MPLS-VPN services to its customers. MPLS is built on both Customer Carrier and Backbone Carrier service providers' IP networks. Interior Gateway Protocols (IGPs) are run for ensuring reachability. Over these IP networks, MPLS and Label Distribution Protocol (LDP) are run and the packets are switched using labels. VPNs are provided by using the concept of Virtual Routing and Forwarding (VRF) and using Multi Protocol-interior Border Gateway Protocol (MP-iBGP). By using MP-iBGP, it is ensured that the service providers' core routers are BGP free and the labelled packets from Customer Carrier is taken across Backbone Carrier. **Findings**: The proposed method is simulated using GNS3 network simulator. Carrier supporting Carrier topology is deployed in the GNS3 simulator and reachability from Customer PC of user site-1 to Customer PC of user site-2 is tested using ICMP ping command. It is successful. Also, traffic generator tool Ostinato is used to generate TCP and UDP traffic. Additionally, Wireshark, a network Monitoring and Analysing tool, is used to analyse the performance of the CsC network. From the deployed CsC topology and its implementation, it is found that MPLS-VPN services, provided by the Customer Carrier to its customers, are working fine. In the performance analysis of the CsC network using ICMP Extended ping command, it is seen that the average round trip time is around 240 ms which shows that Carrier supporting Carrier is working fine and consistent. Additionally, in UDP transmission, it is observed that on an average 1250 packets per second are transmitted and received and the average transmitted bit rate and received bit rate are 380 bits/second. In TCP transmission, it is observed

that on an average of 1000 packets per second are transmitted and received per second and the average throughput is 35 Mbps. Hence, UDP and TCP traffic transmissions confirm the consistency and performance accuracy of the proposed model. **Novelty:** In the Telecommunication Networks, currently IP based inter-Autonomous System (AS) routing is used. Conventionally, IP based routing faces lots of challenges in providing enhanced and scalable services. By implementing CsC, inter-AS MPLS-VPNs are provided through label exchanging method in order to switch labelled packets. There are three ways of exchanging labels in a MPLS VPN networks viz. i) using IGP+LDP, ii) using BGP and iii) BGP-LU. In this study, deployment of CsC is done through IGP+LDP label exchange method. By adopting and optimising the CsC model, labelled packets can be switched/forwarded across both of the AS networks. This CsC model adds value to next generation 5G networks which include networks densification, capacity expansion and rural coverage.

Keywords: MPLS Label; VRF; LDP; CsC; MPLS-VPN

1 Introduction

Multi Protocol Label Switching (MPLS) is a data-carrying mechanism/technology in computer networking and telecommunications. It is largely used by service providers to give Virtual Private Networks (VPNs)[1,2]. VPNs connect customer location which are geographically separated. MPLS based networks are cost effective for service providers as well as customers. It enhances the customer networking security, quality and scalability. Initially point-to-point circuits have been provided between customer locations or sites, also known as physical VPNs or L1 VPNs. In this method, in 'n' customer locations need to be connected and optimal traffic flow to happen, n(n-1)/2 links have to be provided. So adding new sites is not easily possible. In MPLS-VPN services, customers need to provide only one connection from their office router to the Service Provider point of presence, i.e., Provider edge router. The service provider forwards/routes the packets optimally to the destination of customer location. MPLS technology is used by Service Providers to use their IP based backbone network to provide secure, fast, scalable, VPNs to its customers[1].

Small service providers' network infrastructure will be limited to certain geographical areas. The customers of such small service providers will need MPLS-VPN services[3]. Such small service providers get the help of large service providers who has infrastructure in wider areas. Carrier supporting Carrier helps to carry the MPLS-VPN data traffic of customers of small service providers (Customer Carriers) through the larger service providers (Backbone Carriers) in a secure manner. Carrier supporting Carrier is a hierarchical VPN model[4] which seamlessly carries labelled VPN traffic across user sites of Customer Carrier locations. For Service providers, building an infrastructure in a big geographical area, providing cost effective, reliable and secured connectivity to its customers is challenging. The capital and operation expenditures are huge. Also, maintaining a big network is cumbersome. The solution for this is sharing the infrastructure of another service provider. But while doing so, many parameters are to be considered. Carrier supporting Carrier methods can help to solve this issue[4].

The main objective of this study is to enable smaller service providers, i.e., Customer Carriers to connect the parts of their networks which are not directly connected. When their customers need MPLS-VPN connectivity to a location, where their own point of presence is not available, Customer Carrier has to take the services of another Service provider which has its point of presence in that location.

In the Telecommunication Networks, currently IP based inter-Autonomous System (AS) routing is used. Conventionally, IP based routing faces lots of challenges in providing enhanced, secured and scalable services. By implementing CsC, inter-AS MPLS-VPNs are provided through label exchanging method in order to switch labelled packets. There are three ways of exchanging labels in a MPLS VPN networks viz. i) using IGP+LDP[4,5], ii) using BGP and iii) BGP-LU[6,7]. In this study, deployment of CsC is done through IGP+LDP label exchange method. By adopting and optimising the CsC model, labelled packets can be switched/forwarded across both of the AS networks.

2 Methodology

2.1 Deployment of Carrier supporting Carrier

Carrier supporting Carrier (CsC)[4,6] is used to expand the reachability of a Service provider (SP) using another Service providers' services. Carrier supporting Carrier is implemented in situations where small service providers can use the transport services of larger service provider. The end users or customers will be connected to the smaller SP known as Customer Carrier. The Customer Carrier will use the transport services of the larger SP i.e., Backbone Carrier. The CsC architecture is the solution which clearly defines the modalities by not compromising the security of the data of the users, Customer Carrier and the Backbone Carrier. CsC is where one service provider allows another service provider to use a segment of its backbone network. The service provider that shares the infrastructure of the backbone network to the other provider is called the Backbone Carrier. The service provider that uses the infrastructure of the backbone network is called the Customer Carrier. The Backbone Carrier offers Multi Protocol Label Switching (MPLS) -VPN services.

Traditionally in IP networks, when data is sent from one service provider to another service provider, the IP data packets are routed. In CsC networks, using MPLS, the labelled data packets are switched and the labels exchange is implemented by IGP-LDP method. In our study, this IGP-LDP method is used whereas in the reference[6], labels exchange is implemented by BGP-LU method in their study.

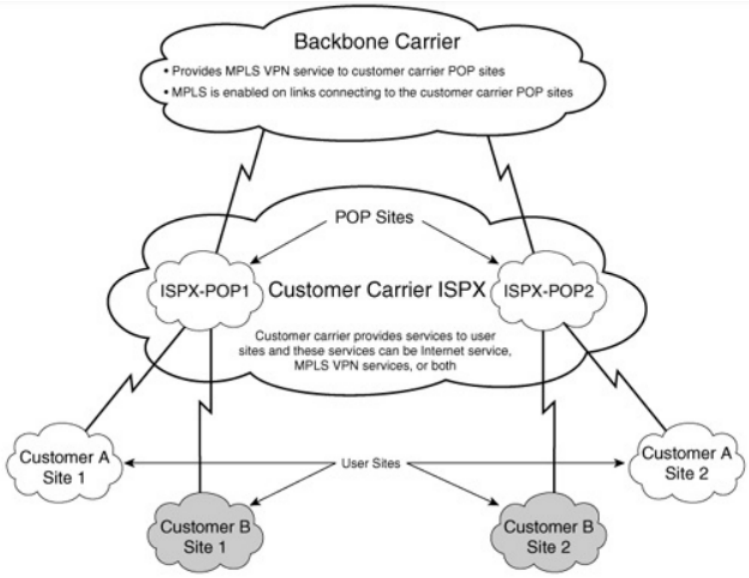

Fig 1. CsC network architecture

2.2 Advantages of Carrier supporting Carrier[5,7]

- The Customer Carrier can use the CsC Backbone Carrier to connect several point-to-point PoP locations.
- MPLS-VPN can be used to isolate traffic from various carriers' Points of Presence (PoP).
- A single Backbone Carrier can provide multiple services, such as MPLS-VPN or Internet service, to the Customer Carrier.

- The Customer Carrier can use any addressing scheme because MPLS-VPN is used to separate Customer Carriers.
- The MPLS-VPN Carrier supporting Carrier feature is scalable.
- VPNs in CsC can be configured for any bandwidth change and growth, if needed.
- The Backbone Carrier offers the Customer Carriers, network security and various bandwidths as per their requirements.

2.3 CsC topology of the study

Three deployment scenarios are possible in CsC architecture [4]

1. Customer Carrier is not running MPLS inside its PoP sites.
2. Customer Carrier is running MPLS inside its PoP sites.
3. Customer Carrier is providing MPLS-VPN services to user sites. [8]

In this study, the deployment of "Customer Carrier, providing MPLS-VPN services to user sites" is done. The deployment is executed using GNS3 simulator [9]. Graphical Network Simulator-3 (GNS3) is an open source network simulator. Research on CsC is performed by simulating the topology and configuring the routers.

The CsC architecture has the following components.

1. Customer Carrier network.
2. Backbone Carrier network.
3. Customer network.
4. IGP protocol viz. Open Shortest Path Finder (OSPF) run inside carrier networks to ensure reachability.
5. MPLS-VPN in Backbone Carrier (Customer Carrier VRF) [5].
6. MPLS-VPN in Customer Carrier (customer VRF) [5].
7. MP-iBGP for advertising VPN routes with labels.
8. Inter AS routing between Customer Carrier -Backbone Carrier.
9. Inter AS routing between customer – Customer Carrier.

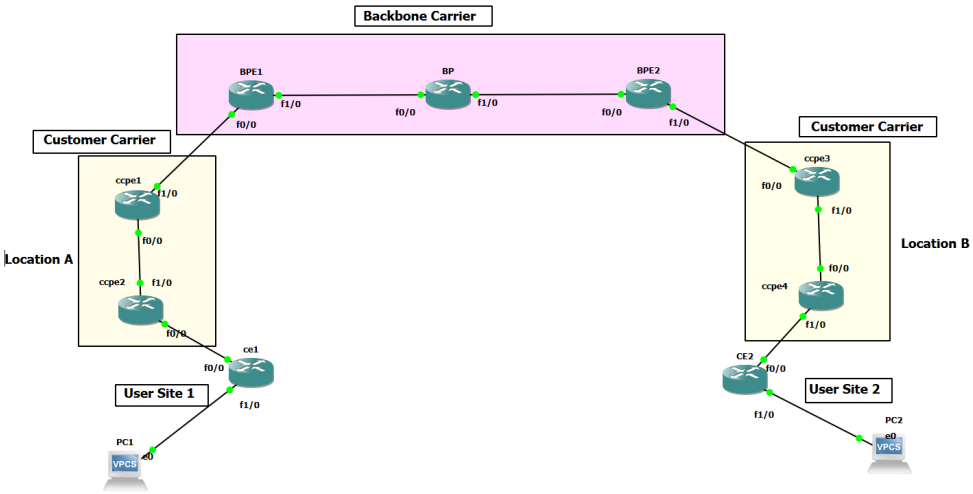

Fig 2. CsC Network topology of the study

- **Backbone Carrier network components:**
  - BPE1 and BPE2 are two MPLS provider edge routers.
  - BP is MPLS provider router.
- **Customer Carrier network components:**

  - CPE1, CPE2 are MPLS routers used in Location A.
  - CPE3, CPE4 are MPLS routers used in Location B.

- **Customer's network components:**
  - CE1, CE2 are customer routers at different locations connected to customer Carrier network.
  - PC1 and PC2 are user terminals.

2.4 Routing protocols used in the study

Step 1. Configuration of the Backbone Carrier routers [5]

- OSPF 1 – OSPF an IGP protocol is configured in the BPE1, BP and BPE2 routers for internal reachability.
- IP MPLS and LDP are configured in all three routers.
- A VRF named "AAA" with RD 1:100 is configured in BPE1 and BPE2 provider edge routers for the connecting the Customer Carrier network.
- OSPF 2 is run in VRF "AAA".
- MP-iBGP "router BGP 1" is configured between BPE1 and BPE2 to carry the VPNv4 address family routes. [5]

Step 2. Configuration of the Customer Carrier routers [5]

- CCPE 1 – Configured OSPF 2 IGP for internal routes and towards the VRF "AAA".
- Configured MPLS and LDP.
- Configured Router BGP 2 (iBGP peering with CCPE3 as next hop).
- CCPE 2 – configured OSPF 2 IGP for internal routes.
- Configured MPLS and LDP.
- Configured VRF named 'Customer 'with RD 2:100.
- Configured Router BGP 2 (MP- iBGP peering with CCPE4 as next hop) for carrying the labelled VPNv4 traffic.
- CCPE 3 - Configured OSPF 2 IGP for internal routes and towards the VRF "AAA".
- Configured MPLS and LDP.
- Configured Router BGP 2 (iBGP peering with CCPE1 as next hop).
- CCPE 4 - Configured OSPF 2 IGP for internal routes and towards the VRF "AAA".
- Configured MPLS and LDP.
- Configured Router BGP 2 (MP - iBGP peering with CCPE2 as next hop) for carrying the labelled VPNv4 traffic.
- Configured VRF named 'Customer 'with RD 2:100.

Step 3: Configuring Customer Routers

- CE1 – Router BGP 65001 peering with CCPE2.
- CE2 – Router BGP 65002 peering with CCPE4.

Step 4: Configuring VPCS

- PC1, PC2 – IP address and Gateway.

2.5 Router configurations of the study

Backbone Carrier PE router and Customer Carrier PE router configurations are given in Table 1.

Table 1. Backbone Carrier PE router and Customer Carrier PE router configurations

Backbone Carrier Provider Edge (PE) Router	Customer Carrier Provider Edge (PE) Router
router ospf 1	router ospf 2
net 10.10.10.0 0.0.0.3 area 0	net 10.20.20.0 0.0.0.255 area 0
net 10.10.10.101 0.0.0.0 area 0	exit
passive-interface loopback 0	int f0/0
exit	mplsip
ipcef	exit
mplsip mpls label protocol	router bgp 2
ldp	no synchronization
mpls label range 100 199	neighbor 10.20.20.102 remote-as 2
int f1/0	neighbor 10.20.20.102
mplsip	update-source loopback 0
mpls label protocol ldp	neighbor 10.20.20.102 next-hop-self
exit	no auto-summary
int f0/0	exit
mplsip	ipcef
exit	ipvrf customer
end	rd 2:100
conf t	route-target both 2:100
mplsldp router-id f0/0	exit
ipvrf AAA	int f1/0
rd 1:100	ipvrf forwarding customer
route-target both 1:100	ip add 172.16.2.1 255.255.255.252
exit int	exit
f0/0 ipvrf forwarding AAA	router bgp 2
ip add 10.12.12.1 255.255.255.252	address-family vpnv4
no shut	neighbor 10.20.20.102 activate
mplsip	neighbor 10.20.20.102 send-community extended
exit	exit
router ospf 2 vrf AAA	address-family ipv4 vrf customer
redistribute bgp 1 subnets	neighbor 172.16.2.2 remote-as 65002
net 10.12.12.0 0.0.0.255 area 0	neighbor 172.16.2.2 activate
end	no auto-summary
conf t	no synchronization
router ospf 1	
passive-interface loopback 0	
exit	
router bgp 1	
no synchronization	
no auto-summary	
neighbor 10.10.10.102 remote-as 1	
neighbor 10.10.10.102 update-source loopback 0	
exit	
router bgp 1	
address-family vpnv4	
neighbor 10.10.10.102 activate	
neighbor 10.10.10.102 send-community extended	
exit	
address-family ipv4 vrf AAA	
redistribute ospf 2 vrf AAA match	
internal external 1 external 2	
no synchronization	

2.6 Features of CsC

Carrier supporting Carrier (CsC) is a versatile concept that can be tailored to many contexts and goals, allowing carriers to improve their services [10], coverage, and efficiency in the telecommunication business. The main features are as follows.

- Resource Sharing is the basic feature of CsC, i.e., resource sharing between the supported and supporting carriers. Infrastructure, backhaul connectivity and even technical competence are examples of these resources.
- Resources can be allotted dynamically according to the changing network requirement, traffic pattern. This will help in optimising the usage.
- CsC networks are interoperable, allowing different carriers to seamlessly collaborate and exchange traffic or services. IETF standard RFC 4364 [11] defines the interoperable standards.
- Security and Privacy measures are available in CsC network models which are very critical to protect sensitive information and maintain the integrity of the network.
- Quality of Services (QoS) for end-users can be provided ensuring seamless connectivity with high-quality experiences [12].

3 Results and discussion

3.1 End to End reachability test

After configuring all the protocols above, end to end reachability test is performed using ICMP ping command, given from PC1 to PC2 and vice-versa (Figure 3). This is successful.

```
PC1> ping 172.16.10.1
84 bytes from 172.16.10.1 icmp_seq=1 ttl=255 time=15.513 ms
84 bytes from 172.16.10.1 icmp_seq=2 ttl=255 time=15.999 ms
84 bytes from 172.16.10.1 icmp_seq=3 ttl=255 time=15.266 ms
84 bytes from 172.16.10.1 icmp_seq=4 ttl=255 time=15.822 ms
84 bytes from 172.16.10.1 icmp_seq=5 ttl=255 time=16.100 ms

PC1> ping 172.16.20.1
84 bytes from 172.16.20.1 icmp_seq=1 ttl=247 time=260.150 ms
84 bytes from 172.16.20.1 icmp_seq=2 ttl=247 time=260.362 ms
84 bytes from 172.16.20.1 icmp_seq=3 ttl=247 time=261.135 ms
84 bytes from 172.16.20.1 icmp_seq=4 ttl=247 time=259.460 ms
84 bytes from 172.16.20.1 icmp_seq=5 ttl=247 time=259.831 ms

PC1> ping 172.16.20.2
84 bytes from 172.16.20.2 icmp_seq=1 ttl=55 time=257.266 ms
84 bytes from 172.16.20.2 icmp_seq=2 ttl=55 time=259.833 ms
84 bytes from 172.16.20.2 icmp_seq=3 ttl=55 time=276.672 ms
84 bytes from 172.16.20.2 icmp_seq=4 ttl=55 time=272.892 ms
84 bytes from 172.16.20.2 icmp_seq=5 ttl=55 time=274.985 ms
```

Fig 3. ICMP ping command results from PC1 in usersite-1 to PC2 in usersite-2

Process of Control plane forwarding: CE1– CCPE2 (VRF customer) CCPE4 (VRF customer) – CE2. [4]

Process of data forwarding: CE1-CCPE2 (VPN labelled VRF “customer”)-CCPE1-BPE1 (VPN labelled VRF “AAA”)-BP-BPE2-CCPE3 -CCPE4-CE2. [4]

The important aspect of this configuration is that MP-iBGP session is formed between CCPE2 and CCPE4 in VPNv4 address family. VPNv4 label exchange is transparent to the Backbone Carrier. The Backbone Carrier holds only the internal routes of the Customer Carrier and not that of the Customer Carrier’s customers. The Customer Carriers’ routers CCPE2 and CCPE4 hold the VRF routing information for its clients and use MP-iBGP sessions between CCPE2 and CCPE4 to transport VPNv4 information between the two client sites. Because the Backbone Carrier is providing MPLS-VPN to the Customer Carrier, which in turn is also providing MPLS-VPN service to Customer. This type of deployment scenario is known as hierarchical VPN.

3.2 Performance Analysis

3.2.1 Consistency performance of CsC deployment using Extended ICMP ping command

To analyse the consistency performance [12] of the CsC deployment, extended ICMP ping commands are run from customer router in usersite-1 to customer router in usersite-2 and vice-versa (Figure 4). In this study, a range of packet sizes is used from minimum packet size of 1000 bytes to maximum 18024 bytes in order to analyse round trip time (It is double the latency time).

The round trip time (RTT), taken for various packet sizes from usersite-1 (R8) to usersite-2 (R9) and vice-versa is given in Table 2.

Table 2. RTT for Extended ICMP ping command from Customer router usersite–1 to usersite–2 and vice-versa

Packet size (in Bytes)	Extended Ping command from R8 to R9			Extended Ping command from R9 to R8		
	Minimum time (inms)	Average time (inms)	Maximum time (inms)	Minimum time (inms)	Average time (inms)	Maximum time (inms)
1000	248	239	244	248	239	244
2000	232	240	248	232	240	248
5000	240	240	244	240	240	244
10000	228	240	244	228	240	244
18024	256	256	260	256	256	260

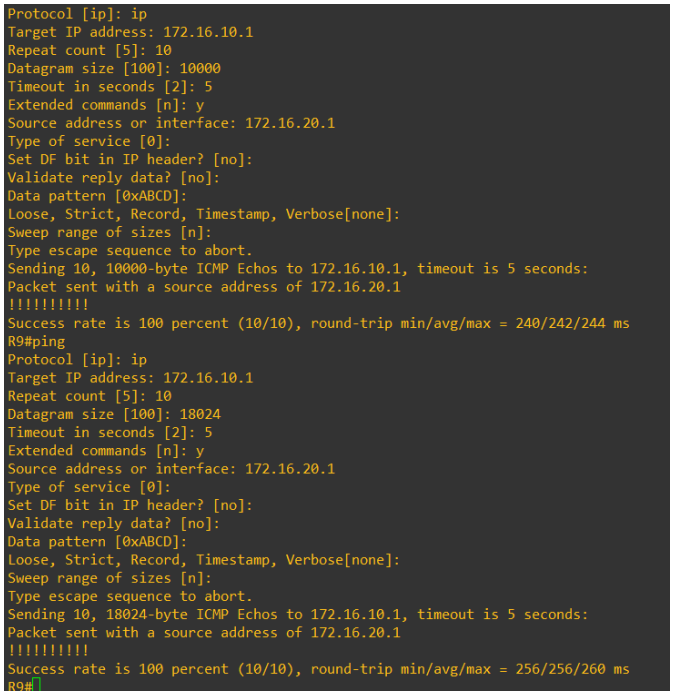

Fig 4. Display of results of Extended ICMP ping command from R9 to R8

From the above Table 2 and the above display of results, it is seen that the average round trip time is around 240 ms, which shows that Carrier supporting Carrier is working fine and consistent.

3.2.2 UDP and TCP Traffic Generation using Ostinato and Monitor using Wireshark

Additionally, to analyse the performance of the deployed CsC network, Ostinato, a traffic generator tool, is connected to the CsC network and different types of traffic like TCP and UDP segments are generated as shown Figure 5. Wireshark, a network monitor/analyser tool, is used to analyse the performance of the traffic generated also as shown in Figure 5.

UDP packets with frame length 64 bits are generated using Ostinato. While the packets are transmitted, Wireshark capture is initiated. The Wireshark input/output graph of the traffic generated is given in Figure 6. Here in UDP transmission, it is observed that on an average 1250 packets per second are transmitted and received. It is also observed that the average transmitted bit rate and received bit rate are 380 bits/sec.

TCP packets with frame length 67 bits are generated using Ostinato. While the packets are transmitted, Wireshark capture is initiated. The Wireshark input/output graph of the traffic generated is shown in Figure 7. It is observed that on an average of 1000 packets per second are transmitted and received per second. It is also observed that the average throughput is 35 Mbps.

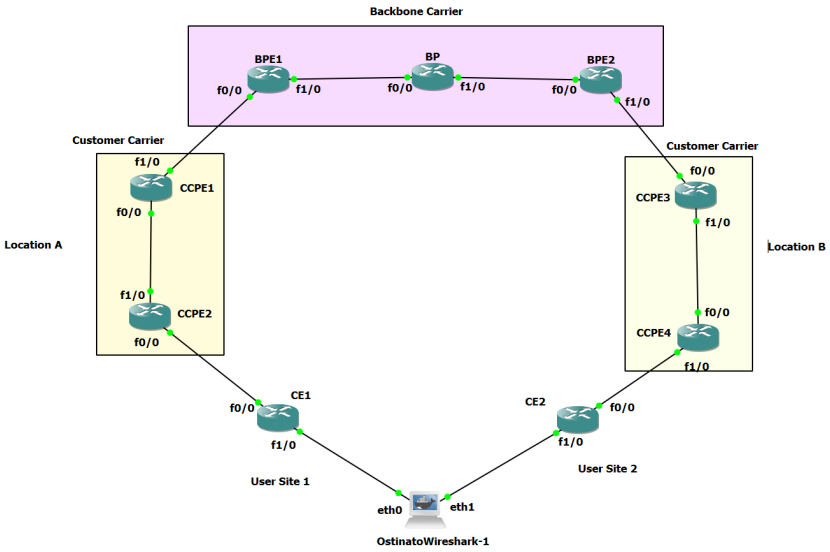

Fig 5. Ostinato Traffic Generator/Wireshark, connected to the CsC network

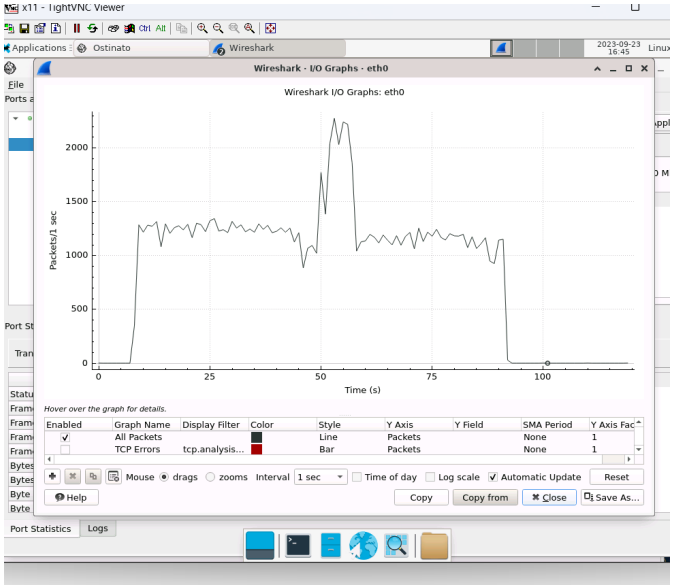

Fig 6. Wireshark Input/Output graph for the generated UDP packets

Fig 7. Wireshark Input/Output graph for the generated TCP packets

3.3 Findings

From the deployed topology and its implementation, it is found that MPLS-VPN services provided by the Customer Carrier to its customers, is working good. In the performance analysis of the CsC network using ICMP Extended ping command, it is seen that the average round trip time is around 240 ms which shows that Carrier supporting Carrier is working fine and consistent. Additionally, in UDP transmission, it is observed that on an average 1250 packets per second are transmitted and received and the average transmitted bit rate and received bit rate are 380 bits/second. In TCP transmission, it is observed that on an average of 1000 packets per second are transmitted and received per second and the average throughput is 35 Mbps. Hence, UDP and TCP traffic transmissions confirm the consistency and performance accuracy of the proposed model.

4 Conclusions

The significance of this work is to give a solution to smaller service providers in order to deliver MPLS-VPN services to its customers with their sites across wider geographical area. It is not necessary for the smaller service providers to have infrastructure and connectivity in all such locations. Instead, they can use the transport services of another service provider who already have infrastructure and connectivity in wider areas. CsC helps data transport of labelled packets instead of IP packets across both the service providers. In this architecture, the users are getting all the benefits of MPLS-VPN like security, QoS and scalability. Normally in data networks, UDPs are used for voice/video calls in Real-Time Protocols (RTPs). TCPs are used for browsing and other applications in which three-way handshakes take place.

In our proposed study, it is seen that the average round trip time is around 240 ms, which shows that Carrier supporting Carrier is working fine and consistent. In UDP transmission, it is observed that on an average 1250 packets per second are transmitted and received and the average transmitted bit rate and received bit rate are 380 bits/second. In TCP transmission, it is observed that on an average of 1000 packets per second are transmitted and received per second and the average throughput is 35 Mbps.

Our proposed study is advantageous to both Backbone Carrier Service Providers and Customer Carrier service providers in terms of capital cost, operational cost, overlapping addresses, Border Gateway Protocol (BGP) free core and expertise. The Backbone service providers can use their infrastructure and give CsC services to any number of smaller service providers.

5 Acknowledgements

The authors thank Dr. K. S. Easwarakumar, Professor, Department of Computer Science, Anna University CEG campus, Chennai for useful discussions and encouragement. The first author (MJ) is very grateful to “Baby-Perumal Research Institute” at Chennai for research guidance and computing facilities.

References

1) De Ghein L. MPLS Fundamentals. 2nd ed. Fundamentals;Cisco Press. 2006.
2) Khandare S, Nandedkar SJ. Performance Analysis of MPLS-VPN and Traditional IP Network. *International Research Journal of Engineering and Technology (IRJET)*. 2019;06(04):4571–4576. Available from: https://www.irjet.net/archives/V6/i4/IRJET-V6I4996.pdf.
3) Mehraban S, Vora KB, Upadhyay D. Deploy Multi Protocol Label Switching (MPLS) Using Virtual Routing and Forwarding (VRF). In: 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE. 2018;p. 543–548. Available from: https://ieeexplore.ieee.org/document/8553949.
4) Lobo L, Lakshman U. MPLS Configuration On Cisco IOS Software. Networking Technology series;Cisco Press. 2005. Available from: https://www.ciscopress.com/store/mpls-configuration-on-cisco-ios-software-9781587051999.
5) Russo N. MPLS VPN Carrier supporting Carrier using LDP and IGP. . Available from: https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/mpls/b-mpls/m_mp-carrier-ldp-igp.pdf.
6) Russo N. Global MPLS Design Using Carrier Supporting Carrier (CSC). Technical Whitepaper, Version 1.2. 2021. Available from: http://njrusmc.net/pub/csc_optc.pdf.
7) MPLS VPN Carrier Supporting Carrier with BGP. . Available from: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ias_and_csc/configuration/xe-16/mp-ias-and-csc-xe-16-book/mpls-vpn-carrier-supporting-carrier-with-bgp.pdf.
8) Sijisivanandan S, Krishnan BS. Carrier Supporting Carrier (One ISP is supporting other ISP for sending Internet/VPN traffic): With Customer Carrier Providing MPLS VPN Services to User Sites. *International Research Journal of Engineering and Technology (IRJET)*. 2020;7(6):6899–6901. Available from: https://www.irjet.net/archives/V7/i6/IRJET-V7I61280.pdf.
9) GNS3 Network Simulation tool. . Available from: https://gns3.com.
10) Jitaru A, Rincu CI, Frunza AI. Evaluation of Carrier Supporting Carrier Networks for Various Types of Services. In: 2018 International Conference on Communications (COMM). IEEE. 2018;p. 297–300. Available from: https://ieeexplore.ieee.org/document/8484768.
11) Rekhter Y, Rosen EC. BGP/MPLS IP Virtual Private Networks (VPNs) RFC 4364. 2020. Available from: https://datatracker.ietf.org/doc/rfc4364/.
12) Prabavathi P, Ravindran M, Gokila C. Quality of Service Enhancement of a Carrier Supporting Carrier Network using MQC QOS. *Natural Volatiles & Essential Oils*. 2021;8(5):3174–3188. Available from: https://www.nveo.org/index.php/journal/article/view/897/823.