Implementation of Multiprotocol Label Switching VPN over IPv6

Kamlesh Kumar Soothar[†], Rabnawaz Sarmad Uqaili[*†], Saleemullah Memon[††], Arif Hussain Magsi[†††], Junaid Ahmed Uqaili[††], Muhammad Rashid[†]

[†]School of Information & Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China.
[††]School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China.
[†††]Computerization and Network Section, Sindh Agriculture University, Tandojam, Pakistan.

Abstract
Multiprotocol label switching (MPLS)-VPN is widely deployed between enterprises and service providers to offer a variety of advanced services to maintain their security over a single infrastructure. Many service providers are replacing frame relay and ATM services with MPLS VPNv4. In order to deal with shortcomings of IPv4, IPv6 is a tremendous approach to build up a broader global Internet. As MPLS does not support IPv6, thus by taking benefit from the MPLS features, we transport IPv6 VPN traffic on MPLS IPv4 core network to refer it as MPLS VPNv6 in this paper. It is a prominent solution for enterprises as it has enhanced security with optimized network performance. It deals with issues of scalability, easy management, redistribution policies, overlapping, and shortcoming of IP addresses. In this paper, we have created a single network infrastructure of MPLS VPN over which IPv4 and IPv6 traffic can be routed without applying any additional stress on the network. MPLS VPNv6 enables multiple service providers to connect corporate clients and offices at a distinct location into one network.

Key words:
MPLS, VPN, IPv6, VRF, MP-BGP.

1. Introduction

Multiprotocol label switching (MPLS) is an innovative creativity by the internet engineering task force (IETF) in order to deal with the flaws in the conventional IP networks [1]. MPLS is a standard-based technology that speeds up the network by forwarding the labels attached to the IP packets to overcome the IP lookups. MPLS technology has become well liked as a core technology with the advantage of fast-forwarding and efficient utilization of network. Before the MPLS, mainly prominent WAN technologies were ATM and frame relay [2]. MPLS and VPN are two different types of technologies. VPN provides secure and cheaper access to remote clients and offices instead of utilizing shared public internet. Due to security issues, VPN playing an essential role in mltinational companies around the world. Traditional VPN includes a peer-to-peer VPN and overlay VPN. In contrast, MPLS VPN is a new technology of VPN with its functions and technology features such as virtual routing and forwarding (VRF) and multi-protocol border gateway protocol (MP-BGP) [3].

MPLS VPNv6 is an expanded version of Layer 3 VPN technology. Additionally, VPNv6 separates routing table entries for VPN clients logically, as MPLS VPNv4 does [4]. The significant difference between MPLS VPNv4 and MPLS VPNv6 is that the transported protocol is IPv6, but the core remains on IPv4 as MPLS core does not support IPv6 [5]. Many service providers have deployed MPLS VPN in their IPv4 networks. As we are already facing the shortcomings of IPv4 addresses. Therefore, IETF has proposed IPv6 to fulfill the growing requirement for the future internet. Now eventually, ISP has to introduce IPv6 services to their clients but it can be expensive to make changes in their existing IPv4 infrastructure plus IPv6 does not eradicate the need to create VPNs and other applications. Therefore, the implementation of VPNv6 over MPLS would be the best solution as there is no need to make any changes in existing IPv4 MPLS VPN infrastructure. Several issues arise while migrating from IPv4 to IPv6 networks but VPNv6 can carry either IPv6 or IPv4 VPN services over a single network. To connect separated IPv6 networks over IPv4 networks, tunneling technologies are used but in VPNv6, there is no need for explicit tunneling. With VPNv6, user activities will be anonymous to protect their privacy. Without VPNv6, user's data is not secure and can be attacked by hackers, ISP, and at public access points.

The main contributions of this paper are as follows:

- We implement MPLS VPNv6 to communicate IPv4 and IPv6 over single network infrastructure without any explicit tunneling.
- Our proposed MPLS VPN over IPv6 overcomes shortcomings of IPv4 with enhanced network security.
- We optimize the network performance by MPLS

Manuscript received December 5, 2019
Manuscript revised December 20, 2019

features.

The rest of this paper is ordered as follows section 2 presents related work. Section 3 presents the detail description of the working mechanism of MPLS VPNv6 and the design scenario of the proposed network. Section 4 presents the simulation and results. Finally, section 5 concludes all work.

2. Related Work

Researchers have proposed different models and approaches to improve the efficiency of MPLS VPN technology. The authors in [6] analysis that MPLS VPN is considered as most prominent and widely deployed implementation of MPLS, most of the internet service providers have replaced ATM and FR services that were well known before it. The authors in [7] described that MPLS provides QoS with the guarantee to carry data from the sender to the receiver directly by using labels, the most useful application of MPLS is a VPN which is an L3 VPN for internet service providers for ensuring privacy and security of data over a single network infrastructure. The authors in [2] implemented MPLS VPNv4 instead of traditional VPNs over the backbone core network is an effective solution for service providers to overcome the security threads and cost-effective solution to fulfills the requirement of customers within limited available resources. In [8], The feature of VRF is to allows a router to have several routing tables located in the same router, which enables the customer to use the same subnet of the IP address connected to the same network of the MPLS service provider. [9] elaborates that VRF on service providers can isolate network cost-effectively by separating the customer's large network in small sites, customers, and service providers network with the least number of links and routes without compromising security by implementing MPLS VPN infrastructure. [10]-[11]discussed the applications and security of VRF, that it distinct the routes between ISP and customer. Customer's data can be privatized and secured through VRF and route distinguisher (RD) in the MPLS environment. Routing protocol and static routing in the VPN environment identified by the VRF table result in an enhanced security, reliability and faster routing. In [4], an expandable solution in the context of networking is mentioned that provider routers should be unconscious of the VPNs, and expandability can be achieved through MPLS VPN. However, after all, prior work mentioned above, most of the enterprises still facing a series of problems, including shortcomings of IPv4 and address overlapping. In order to meet next-generation network design, implementing MPLS VPNv6 resolves series of problems, including the coexistence of IPv4 and IPv6, explicit tunneling, and transparency. MPLS VPNv6 has several benefits, including network performance, flexibility, scalability and easy traffic management.

3. Implementation of the Proposed Network

- **Working mechanism MPLS VPNv6**

MP-BGP is the center of MPLS VPN architecture for both IPv4 and IPv6, which is used to distribute IPv6 to the service provider's backbone network [12]. A VRF is created by the addition of the VRF CISCO Express Forwarding (CEF) table, related routing protocol and VPN routing table. A VRF is simply a virtual routing and forwarding. Each VPN has its own VRF instance for that Provider Edge (PE) router. PE router has the ability to store two routing tables; one is the global routing table and the other one is the VRF routing table. We can configure only one VRF at PE router pointing towards the customer edge (CE) router. For every VPN, there is a specific routing table and CEF table per VPN to transmit packets from PE router. MP-BGP is responsible for propagating VPN prefixes over the MPLS VPN core network. IPv4 prefixes are unique when BGP conveys them over the provider network. RD can be considered to tackle the issue by making unique IPv4 prefixes. VPNv4 prefixes propagate between the PE routers through MP-BGP. It is the responsibility of RD to make unique VRF prefixes while MP-BGP conveys them. Although RD does not show that prefix belongs to which VRF. One RD is assigned on the PE router to each VRF instance. One of the main feature of MPLS VPN is it establishes communication between two sites known as route targets (RT). To find out which route should be imported into VRF from MP-BGP is demonstrated by the BGP extended community. Additional BGP extended community received an exported VPNv4 route. Importing an RT for matching extended community means that the VPNv4 route received from MP-BGP would be checked. There are two possibilities for the prefix; if its outcome is matched, then it would be added in the VRF routing table as an IPv4 route; otherwise, the prefix would be rejected. As each site does contain the information of VRF therefore, provider routers cannot forward them. The provider edge router exchanges routing updates with the CE device translates the CE routing data into VPNv4 routes, and exchanges VPNv4 routes with other PE devices via the MP-BGP. Therefore, user IP packets are transformed into labels in the network to accomplish a VPN for every user.

Moreover, provider routers do not require routing table of users by utilizing two MPLS labels. In this manner, there

is no need to have BGP in the provider routers but the VPN routes should be known to the PE routers. Thus, only the edge routers keep the knowledge of VPN in the MPLS-VPN network that is the scalable solution for the MPLS VPN [8].

- **Design scenario of the proposed network**

As shown in Fig. 1, when the request generated from the client reaches to PE1 router, it checks the address family table to see whether the request is coming from VRF member or not. If the requesting client is not in the member of VRF, then the PE router would discard the request of accessing the server. Meanwhile, if the requesting client is a member of the VRF, then the PE router forwards the request to the MPLS core network and then eventually to other PE router. Afterward, the PE router on the server-side verifies that request is generated from VRF member, then it allows the client to access the server; otherwise, the request declined. We have created a server on another PC and connected it to the physical interface of CE2. Then we have used two virtual clients, namely MUET and NED, using oracle VM virtual box. After the configuration of MPLS VPNv6, we successfully access the server from the virtual MUET client through our MPLS VPNv6 network.

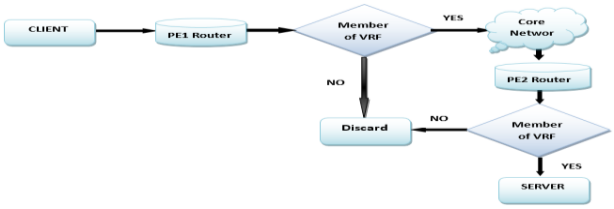


Fig. 1 Flow chart

4. Simulation and Results

In this paper, CISCO IOS image "c7200-advipservicesk9-mz.152-4.S5.bin"is used in GNS3. We have configured the MPLS VPNv6 network then fetched a virtual machine client to access the server. Two virtual systems are used; one is MUET client and the other is NED client through virtual box. After implementing the network, it showed that how the IPv6 host would get services in MPLS VPNv6 over IPv4 core infrastructure. Usually the internet cloud is running MPLS VPN over IPv4 and no ISP provides VPN services over IPv6. We made MPLS VPNv6, which can provide services to IPv4 and IPv6 hosts without any explicit tunneling. The server machine made through Xampp was successfully accessed from a virtual IPv6 client. Wireshark is used to show the packets of protocols running over the same network lines and the protocol of each packet.

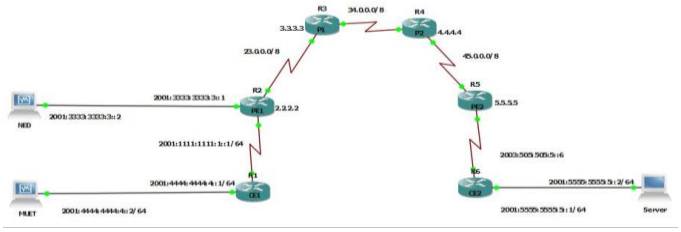


Fig. 2 Network topology

Fig. 2 shows the network topology. There are six routers used, containing two providers (P) routers, two PE routers and two CE routers. We have configured MPLS on core routers that are running on IPv4, used OSPF routing protocol. Two CE routers are running on IPv6, used EIGRP routing protocol. VPN is created by configuring VRF on the PE routers pointing towards the CE routers. Normally, tunneling techniques are used for routing IPv4 and IPv6 traffic, which produces stress for the routers. In MPLS VPNv6, the network can route IPv4 and IPv6 traffic without requiring any explicit tunneling. MPLS VPNv6 is the solution to connect IPv6 customers through an existing IPv4 infrastructure. The client edge routers have full reachability as shown in Fig. 3.

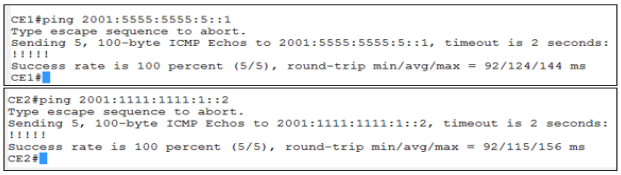


Fig. 3 Ping connectivity between CE1 & CE2

Ping from MUET client to server is shown in Fig. 4. It illustrates that MUET client has connectivity to the server because it is a member of the VPN. Whereas, unsuccessful ping from NED client to server is shown in Fig. 5. NED is not a member of the VPN, so it can't reach to server.

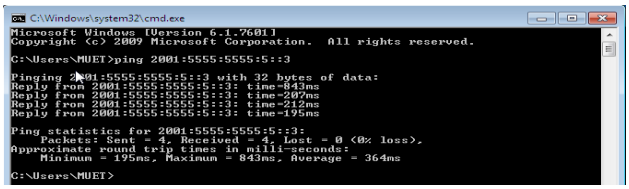


Fig. 4 Ping from MUET client to server

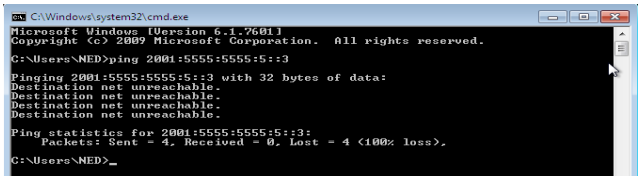


Fig. 5 Ping from NED client to server

Fig. 6 verifies that the server is accessed from MUET client through our MPLS VPNv6 network. By traceroute command, we observed the number of hops passed by the packet. MUET client is connected to CE1, and the server is connected to CE2 through the physical interface. Service is accessed by MUET clients using a browser. It can be observed that MUET client has accessed Xampp server through the MPLS VPNv6 network.

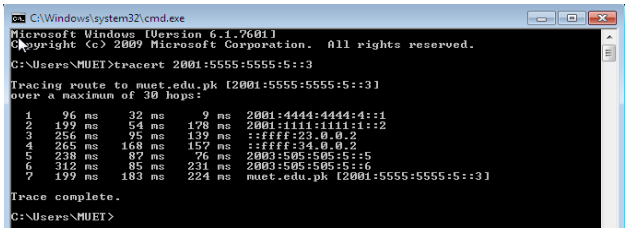


Fig. 6 Traceroute for accessing server from MUET client

Fig. 7 captured between PE1 and P1 router using Wireshark. As CE routers are running on IPv6, therefore IPv4 and IPv6 exist over the same link. The label distribution protocol (LDP) verifies that MPLS is running properly and OSPF is running on core routers. It was captured while pinging to show connectivity. Ping requests and replies can be verified.

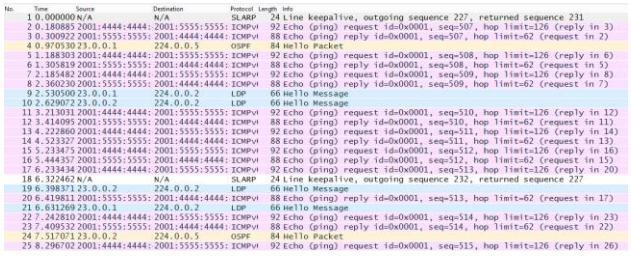


Fig. 7 Wireshark snap of PE1 to P1 link

5. Conclusion

With the rapid development of business and enterprises, most of the corporate clients need virtual technology with security and fast-forwarding on the same physical IPv4 based core infrastructure. This requirement is accomplished by implementing MPLS VPNv6. We have implemented MPLS VPN over IPv6 using VRF and MP-BGP, which satisfies the needs of the customer in limited resources cost-effectively. Communication is set up between the two IPv6 CE routers over existing IPv4 MPLS core infrastructure without applying additional pressure on the provider routers. Results show that MUET client has full reachability to server with 100% success. Whereas NED client is unreachable to server as it is not part of VRF. LDP packets verifies that MPLS is running properly to improve network performance.

Acknowledgments

The authors would like to thank Dr. Kamran Ali Memon and Mr. Junaid Ahmed Uqaili from Beijing University of Posts and Telecommunications for their excellent support and discussions.

References

[1] L. Andersson and S. Bryant, “The IETF Multiprotocol Label Switching Standard: The MPLS Transport Profile Case,” IEEE Internet Comput., vol. 12, no. 4, pp. 69–73, Jul. 2008.

[2] A. Shahzad and M. Hussain, “IP Backbone Security: MPLS VPN Technology,” Int. J. Futur. Gener. Commun. Netw., vol. 6, no. 5, pp. 81–96, Oct. 2013.

[3] D. Grayson, D. Guernsey, J. Butts, M. Spainhower, and S. Shenoi, “Analysis of security threats to MPLS virtual private networks,” Int. J. Crit. Infrastruct. Prot., vol. 2, no. 4, pp. 146–153, Dec. 2009.

[4] A. Dumka, H. L. Mandoria, K. Dumka, and A. Anand, “MPLS VPN using IPv4 and IPv6 protocol,” 2015 Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2015, pp. 1051–1055, 2015.

[5] V. Joseph and S. Mulugu, “Understanding Advanced MPLS Layer 3 VPN Services,” in Network Convergence, Elsevier, 2014, pp. 73–323.

[6] M.-S. Sun and W.-H. Wu, “Engineering analysis and research of MPLS VPN,” in 2012 7th International Forum on Strategic Technology (IFOST), 2012, pp. 1–5.

[7] Z. Nahidha and S. Alagumani, “Implementation of Mpls Layer 3 Vpn Router on Isp,” vol. 119, no. 16, pp. 3075–3081, 2018.

[8] S. Mehraban, K. B. Vora, and D. Upadhyay, “Deploy Multi Protocol Label Switching (MPLS) Using Virtual Routing and Forwarding (VRF),” in 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018, no. Icoei, pp. 543–548.

[9] S. Yadav and A. Jeyakumar, “MPLS multi-VRF design and implementation using GNS simulator,” in 2016 IEEE International Conference on Engineering and Technology (ICETECH), 2016, no. March, pp. 962–966.

[10] S. H. Sridhar and J. Arunnehru, “Traffic Engineering: An Application of MPLS L3 VPN Technology,” in 2018 2nd

International Conference on Trends in Electronics and Informatics (ICOEI), 2018, no. Icoei, pp. 1147–1151.
[11] K. M. M. Fathima, "A Survey on Multiprotocol Label Switching in Virtual Private Networks," in 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, 2018, pp. 737–740.
[12] W. Goralski, "MPLS-Based Virtual Private Networks," in The Illustrated Network, Elsevier, 2017, pp. 513–533.

Kamlesh Kumar Soothar received his B.E. degree in Telecommunications Engineering from Mehran University of Engineering and Technology (MUET), Pakistan in 2016. He is currently pursuing his M.S. degree in Electronics and Communications Engineering from Beijing University of Posts and Telecommunications (BUPT), Beijing, China. His research interests include computer networks and wireless communications.

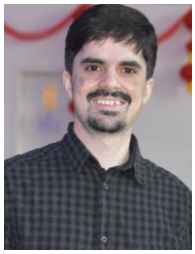
Rabnawaz Sarmad Uqaili received the B.E. degree in Telecommunication Engineering from Mehran University of Engineering and Technology (MUET), Jamshoro, Pakistan in 2016. He is currently pursuing M.S. degrees in Electronics & Communication Engineering from Beijing University of Posts and Telecommunications (BUPT), Beijing, China.

*Corresponding author: rabnawazuqaili@gmail.com

Saleemullah Memon received his B.E. degree in Electronic Engineering from Quaid-e-Awam University of Engineering, Science and Technology (QUEST), Pakistan in 2017 and M.S. degree in Electronics and Communication Engineering from Beijing University of Posts and Telecommunications (BUPT), Beijing, China in 2019, where he is currently pursuing his Ph.D. degree in Electronic Science and Technology. His research interests include millimeter-wave antenna, SWIPT and WSNs.

Arif Hussain Magsi received his B.S. and M.S. degrees in Computer Science from Shah Abdul Latif University Khairpur, Pakistan in 2009 and 2017 respectively. Currently, He is pursuing his Ph.D. degree from Beijing University of Posts and Telecommunications (BUPT), Beijing, China.

Junaid Ahmed Uqaili, received his B.E. degree in Electronic Engineering from Mehran University of Engineering & Technology (MUET), Pakistan, in 2016 and received the M.S. degree in Electronic Science & Technology from University of Electronic Science & Technology (UESTC), China in 2019. Currently he is working toward the Ph.D. degree at Beijing University of Posts and Telecommunications (BUPT), Beijing, China. His research interests include RF and mm-Wave integrated circuits design, modeling active and passive devices and power dividers.



Muhammad Rashid received his B.E. in Electrical Telecommunication Engineering from Government College University Faisalabad, Pakistan in 2015. Currently he is pursuing his M.S. degree in Electronics and Communications Engineering from Beijing University of Post and Telecommunication (BUPT), Beijing, China.