Multi-Protocol Label Switching based Virtual Private Network

[1]Saurabh S. Dandekar, [2]Shriya P. Gokhale, [3]Ifrah A. G. Bhatkar, [4]Abhishek S. Bhatkar

[1,2,3,4]UG Student, FAMT Ratnagiri, Maharashtra, India.

[1]ssdandekar37@gmail.com, [2]shriya.gokhale2000@gmail.com, [3]ifrahbhatkar2311@gmail.com,

[4]bhatkar.abhishek81@gmail.com

Abstract: Over the past few years the internet has brought the world closer. Complexity of the network, the need of security and large number of users result in many problems in the networking technology. This paper emphasizes on MPLS VPN Technology. Today there is a need of faster and safer network which can be built over existing infrastructure. MPLS can be configured over a network and using this cloud VPN can be created. Today Internet Service Providers specifically use MPLS based VPN for communication as well as providing security. This paper provides basics of MPLS, VPN and together when implemented, what terminologies are used and how it actually works. MPLS VPN is an emerging technology which is serving as an outstanding solution over various existing mechanisms. MPLS takes lesser time than traditional IP routing and also provides facilities like MPLS TE, MPLS VPN, ATOM, QoS

Keywords: Any Transport Over MPLS (ATOM), Internet Protocol (IP), Multi-Protocol Label Switching (MPLS), Traffic Engineering (TE), Virtual Private Network (VPN), Quality of Service (QoS).

I. INTRODUCTION

A Multiprotocol Label Switching (MPLS) Layer 3 Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each customer site, one or more routers attach to one or more routers at the provider's site.

MPLS L3VPNs are based on the peer model. The peer model enables the service provider and the customer to exchange Layer 3 routing information. The service provider relays the data between the customer sites without customer involvement.

MPLS VPNs (L3VPNs) are easier to manage and expand than conventional VPNs. When a new site is added to an MPLS L3VPN, only the edge router of the service provider that provides services to the customer site needs to be updated.

II. MULTI-PROTOCOL LABEL SWITCHING

In recent couple of decades there is huge increase in the number of internet users and amount of traffic over internet. [1]. MPLS overcomes the major disadvantages of Traditional IP Routing. MPLS means Multi-Protocol Label Switching [4]. This technology is said to be Layer 2.5 technology as it operates in between Layer 2 and 3 of OSI Model. MPLS provides many facilities like VPN, QoS, Network Convergence, Security, Traffic Engineering which are hardly provided by traditional IP routing [4]. MPLS uses LDP (Label Distribution Protocol) to distribute labels or also known as "shims". MPLS plays major role in today's internet traffic.

A. Why MPLS?

i. MPLS saves look ups of routing table and in turn it saves machine cycles of routers preventing them from overheating.

ii. Lesser time requirement than traditional IP routing.

iii. MPLS offers Traffic Engineering (MPLS TE).

iv. MPLS offers ATOM(Any Transport Over MPLS).

v. MPLS facilitates QoS (Quality of Service).

B. Differences between MPLS and Traditional Routing:

Traditional IP Routing	MPLS network
In traditional IP networks, each router must process every packet to determine the next hop that the packet must take to reach its final destination.	In an MPLS network, only edge routers fully process each packet. Label switches within the network simply forward packets based on the label. This decreases latency experienced by traditional routed networks performing standard IP routing.
There is no such provision in traditional IP network.	In MPLS, routing table for every customer is separate

	from other routing table for another customer.
IP based networks lack the quality-of service features available in circuit based networks, such as ATM and Frame Relay	MPLS support QoS. MPLS replaces the virtual circuits (VC) which reduces the hardware components for connection between routers in the ATM network. MPLS provides an increase in the performance enhancements and service creation capabilities to the network.
There is no such provision in traditional IP network.	In MPLS, routing table for every customer is separate from other routing table for another customer.
Traditional IP routing/networks has poor support for traffic engineering.	MPLS has good support for traffic engineering.
Traditional IP routing/networks has poor integration support with Layer 2 backbones already existing in large service provider networks.	MPLS has good integration support with Layer 2 backbones.
Traditional IP routing/networks is not scalable as compared to MPLS.	MPLS does not have any scalability issue.
Traditional IP routing/networks clearly fits in OSI Model.	MPLS does not fit in OSI Model.
Poor IP over ATM integration	Better IP over ATM integration
There is no provision of Overlapping Address Pools in case of traditional IP routing/networks.	Overlapping Address Pools can exists in MPLS networks

C. How does MPLS work?

Unlike traditional routing which uses complex and long IP addresses to route the traffic, MPLS uses simple and smaller labels or shims to take forwarding decisions. These labels reside in between Layer 2 and Layer 3 of OSI Model and hence MPLS is said to be a Layer 2.5 technology. In MPLS VPN it uses completely Layer 3 and makes labels based on IP addresses.

D. MPLS Header

MPLS header is 32 bit long which is divided into 4 fields, viz. Label value, Experimental field (Exp), Set field (S) and Time to Live (TTL).

Label: 20 bits Exp: 03 bits

S: 01 bit TTL: 8 bit

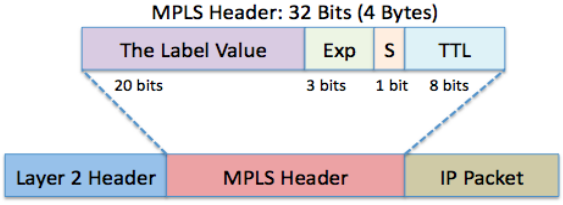

Fig. 1 MPLS Header

III. VPN

The problem arises that all the offices are far away from each other. The organizations have to install a physical medium to establish this connectivity. As a result, they have to install their own lines or use leased lines. But this results in very high costs, technical and legal headache. Is there any way to solve this issue? The optimum solution is Virtual Private Network (VPN). A VPN is defined as a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. Thus, VPN is used to counter this narrative. It makes a tunnel securely transmit private data over a public network. It hides the customer's network from public access as well, despite using the public network infrastructure. It is a very important element when considering security aspects of a network[3].

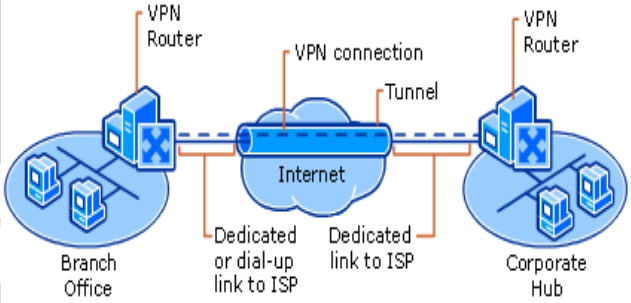

Fig. 2 Virtual Private Network

IV. MPLS VPN

A. What is MPLS VPN?

MPLS based VPN is a term that has been greatly discussed in the networking world since a few years. The question that arises is what is an MPLS based VPN in a real network implementation scenario. As we know, MPLS is a technology used in WAN. It is deployed by ISPs in their cloud. It has no direct linkage with the customer's network. MPLS VPN is a VPN network construction based on the MPLS-based core network. A MPLS based VPN is the implementation of VPN using the MPLS cloud. All the customer sites communicate with each other using the MPLS enabled provider network. MPLS labels make a tunnel in this scenario [3].

MPLS technology is used in WANs (Wide Area Networks). VPN is built over MPLS Core and it is advantageous over traditional VPN as it can provide Layer 3 facilities. MPLS Labels make tunnel through the network to create private networks virtually. MPLS VPN is implemented by Service Provider and users are totally unaware of it.

B. Terminologies related to MPLS VPN:

1) Devices into customer network:

i) Customer Devices (C):

These are simple devices like switches and routers at customer end and are unaware of VPN and MPLS [2].

ii) Customer Edge Devices (CE):

These devices are located at the edge of customer network and provider network (via Provider Edge devices.) [2]

2) Devices in Provider Network:

i) Service Provider Devices (P):

These are routers and switches at provider side. They are not directly connected to customer network and have no knowledge about customer's VPN. Routers in the best path chosen are known as Label Switching Routers (LSR) [2].

ii) Service Provider Edge devices (PE):

PE devices are connected directly to customer -via CE devices. PE devices are aware of VPN. They are also known as Label Edge Routers (LER) as they take part in label switching [2].

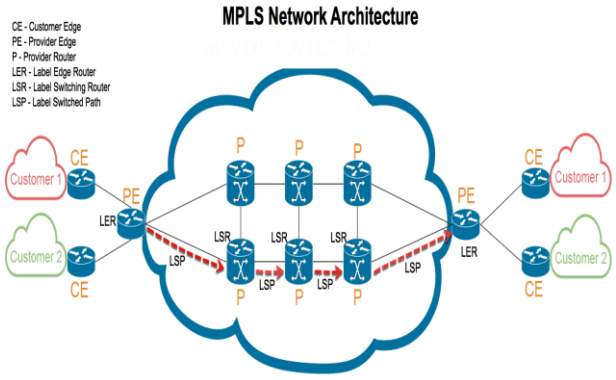

Fig. 3 MPLS Network Architecture

C. Working of MPLS VPN:

A large number of customers are connected to Provider Edge (PE) Router through their respective Customer Edge (CE) Router. When multiple customers having same private IP are connected to a single PE, it creates ambiguity in forwarding the packet to desired destination even though MPLS is used. In order to avoid this problem, Internet Service Providers create Virtual Router Forwarding Tables (VRFs) on their PE for each different CE. These VRFs create independent routing table for each customer and keep it updated. Creating VRFs is like virtually creating multiple routers in single router. Data sent by particular VRF on source PE router enters same VRF on destination PE router thus eliminating the ambiguity. Label switching is done using two labels viz. outer label and inner label. Outer label is the normal MPLS label which is swapped hop by hop and inner label is used for communication between two VRFs. When the packet reaches the desired VRF then the PE pops both the labels and forwards the packets to the desired customer through its CE. Thus this technique provides tunnels through network and avoids leakage of data to unintended customer.

D. Protocols used:

a) Border Gateway Protocol (BGP) as External Gateway Protocol (EGP)

b) Internal BGP (iBGP)/Enhanced Interior Gateway Routing Protocol (EIGRP)/Open Shortest Path First protocol (OSPF)/Routing Information Protocol (RIP) as Interior Gateway Protocol (IGP)

V. CONCLUSION

Please include a brief summary of the possible clinical implications of your work in the conclusion section. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. Consider elaborating on the translational importance of the work or suggest applications and extensions.

ACKNOWLEDGMENT

It gives us an immense pleasure to present the review paper of our project here. It has been quite experience, facing a number of problems at stages and coming up with appropriate solutions, at time the discussion amongst us or suggestions from our friends and teachers.

We thank our guide **Prof. G. S. Kulkarni,** Associate Professor**,** Electronics and Telecommunication Engineering, in the best possible way. Without his guidance it wouldn't have been possible to reach this stage. We are very grateful for his support and motivation.

We express our gratitude to **Dr. S. V. Chougule**, Associate Professor and Head of the Department, Electronics and Telecommunication Engineering for her invaluable suggestions and constant encouragement.

Lastly, we would like to put our thanks on record to the teaching and non-teaching staff for rendering their support directly or indirectly.

REFERENCES

[1] Samiullah Mehraban, Prof. Komil B. Vora, Prof. Darshan Upadhyay, "MPLS VPN using VRF (Virtual Routing and Forwarding," International Journal of Advance Research, Ideas And Innovations In Technology, ISSN: 2454-132X, Vol. 3 issue6, Year 2017.

[2] Akshay, Pooja Ahlawat, Maharshi Dayanand University, Haryana, "Implementation of MPLS L3VPN using GNS3", IJSER, vol 3 Issue 4, April 2015.

[3] Farooq Ahmed, Zain Ul Abedin Butt, 3rd ed., "MPLS based VPN Implementation in a Corporate Environment", Journal of Information Technology & Software Engineering, January 2016

[4] Jaykumar Kaimal, "MPLS based VPN",George Mason University Technocal Report Series.