INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue6)
Available online at www.ijariit.com

MPLS VPN using VRF (Virtual Routing and Forwarding)

Samiullah Mehraban
Student
VVP Engineering College, Rajkot
mehraban748@gmail.com

Prof. Komil B. Vora
Assistant Professor
VVP Engineering College, Rajkot
komil.vora.it@vvpedulink.ac.in

Prof. Darshan Upadhyay
Assistant Professor
VVP Engineering College, Rajkot
darshan.upadhyay.it@vvpedulink.ac.in

Abstract: Multi-Protocol Label Switching (MPLS) which was introduced by Internet Engineering Task Force (IETF) is usually used in communication networks which started attracting all the internet service provider(ISP) networks with its brilliant and excellent features that provide quality of services (QOS)and guarantees to traffic which carries data from one network to another network directly through labels.

Virtual Private Network (VPN) is one of the highly useful MPLS applications which allow a service provider or a large enterprise network to offer network Layer VPN services that guarantee and carries traffic securely and privately from customer's one to another through the service provider's network. To support multiple customers that Customers Request for secure, reliable, private and ultrafast connections over the internet MPLS VPN standards include the concept of a virtual router. This feature called a VRF table. VRF or Virtual Routing and Forwarding technology that permit a router to have various routing table or multiple VPN at the same time that they are located in the same router but they are independent and also the VRF feature in VPN now allows different customers to use same IP addresses connected to the same ISP. A VRF exists inside a single MPLS router and typically routers need at least one VRF for each customer attached to that particular router.

Keywords: MPLS, VPN, VRF, QOS, TE, IETF, PE, P, CE.

INTRODUCTION

There has been an unbelievable growth in the telecommunication area through the world in the past few years, which has led to an incredibly huge amount of traffic being sent and receive from one location to another location with different requirements and choices of services[8] such as online business transaction, video streaming and many more Internet Service Providers (ISPs) should to guarantee a high Quality of Service (QOS) with minimum packet loose and end-to-end delays with less complexity[1]. To ensure such reliability and high Quality of Service Multiprotocol Label Switching (MPLS) was introduced by IETF [5].It is a tunneling technology which gives the platform to create and implement MPLS based Virtual Private Networks (VPNs). It is developed to enhance packet forwarding over the high-performance backbone networks. MPLS forwards the IP packets to the destination routers instead of the end devices on the basis of small labels [5]. The label in MPLs mechanism is a short fixed-length identifier which is assigned by the entry router to the MPLS network and used by the interior routers to make a forwarding decision [1] The label in MPLS allows improving routing performance which in turn enhances QOS to data traffic [1] In SP's core network labels are shared between routers using LDP Label is associated with next-hop IP address. The first router will tell the path to follow. All packets that enter the MPLS network get a label depending on it is used for incoming unlabeled packets where the router matches the packet's destination IP address to the best prefix in the FIB and forwards the packet base on that entry[2].

There are many reasons why deployment of MPLS has become so popular. The most significant of them is the concept of VPN technology [8] that network connection between devices that do not exactly share a physical cable is called VPN [2]. VPN (Virtual Private Network) is simply a way of using a public network for private communications, among a set of users or sites [2] VPN which separates the traffic according to the standards set by the customers, making the connection secure and private. It can be used to establish private connections between different sites of the same customers that might be present at different locations. MPLS has the ability to capable of securing and protecting its path in the case of any failover.This helps the service provider to provide a guaranteed service to its customers. MPLS thus can provide multiple services at the same instant in the same network. A transparent tunnel can be created between the endpoints of the network depending on the class of traffic. All these configurations are done on the service provider's end and thus the customer does not have to worry about the routing required or deployment of extra resources [8] One of the other important and exceptional features of MPLS is Traffic Engineering (TE) that allows a service provider to

improve the traffic flow and links application as it would be demanded of a service provider's network. It gives an important amount of control in the hands of the service provider regarding the optimal utilization of the available resources [8]
There are different layer VPN that the first one is Layer 2 VPNs, where layer 2 frames are directly forwarded from source to destination sites using MPLS and another one is Layer 3 VPNs, where IP is the common layer between sites and MPLS [7] MPLS Layer 3 Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network.[3]
At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers. MPLS 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 [3] To support multiple customers MPLS VPN standards include the concept of a virtual router. This feature, called a VRF table, can be used to store routes separately for different customer VPNs. A VRF exists inside a single MPLS-aware router. Typically routers need at least one VRF for each customer attached to that particular router Also the VRF (Virtual Routing and Forwarding) feature in VPN now allows the customers to even use the same IP addresses.

A performance Study Framework for (MPLS) Networks
They work to build a new framework for modeling recovery mechanisms which have been suggested to improve the flexibility of MPLS networks against failures that when failures will happen in the MPLS network how to recover that to guarantee and to bring high QOS and improve network Performance and redundancy during failures they did a complete study on MPLS recovery mechanisms for protecting and brings back traffic after failure happening that there are different MPLS recovery mechanisms to set on variable parameters and scenarios for high-performance analysis purpose. That there are four recovery mechanisms were modeled namely Best Effort, Makam, Local Rerouting and Fast Reroute [1].

Best Effort Model
This model is working global recovery with rerouting mechanism that the source of traffic is responsible to reroute traffic to the recovery path [1].
When failure Indication signal (FIS) is received by the source, the recovery path is calculated and established [1]

B- Makam's Model
This model provides end-to-end protection between the ingress (head-end node) and egress (tail-end node) routers. When failure occurs in the original Label Switched Path (LSP) the node that identifies the (FIS) it notify the ingress router [1].

Local Rerouting Model
This model consists of both rerouting and local repair mechanisms.in this model the recovery path will be calculated dynamically by a local node when frailer occurs on LSP. This model will reduce the recovery time [1].

Fast Reroute Model
It is a local repair model with one to one back up that path affected by a failure is locally rerouted by the nearest node to the failure [1]. The nearest node to failure that is called Point of Local Repair (PLR) identifies the failure and redirects traffic immediately to a pre-established recovery path.

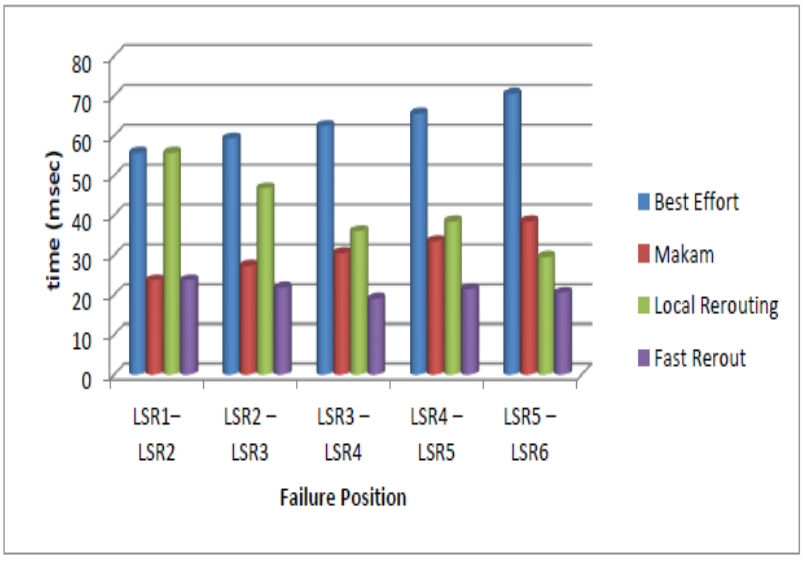

Fig. 1: Service Disruption Time [1]

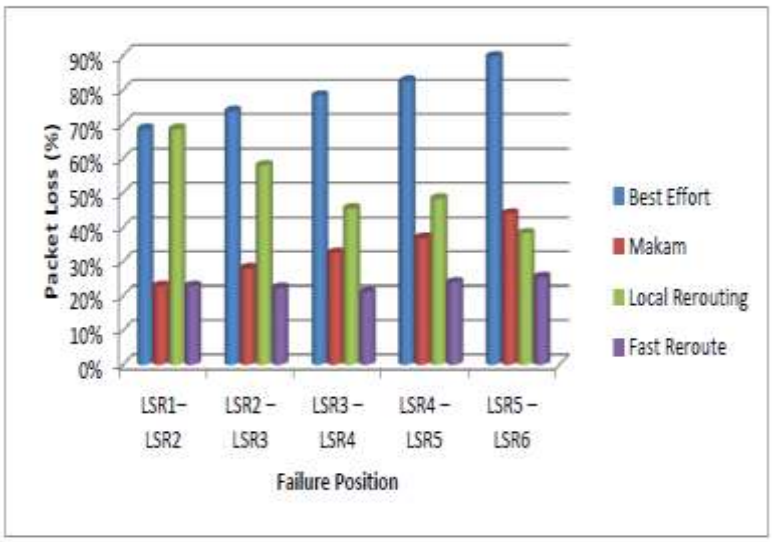

Fig. 2: The Dropped Packets [1]

From the four recovery model, newly introduced framework is able to model the MPLS recovery mechanisms and a performance study survey has been done from selected MPLS recovery mechanisms result achieved that best performance was achieved by Fast Reroute mechanism [1]

Architecture for MPLS L3 VPN Deployment in Service Provider Network

They represent and did testing and implementing scalability of MPLS L3 VPN technology that MPLS L3 VPN to provides the secure channel between two customer sites in a service provider and through this implementation we can save the routing table space on provider routers. By using the concept of Route Reflector (RR) to avoid more BGP (Border Gateway Protocol) periods and to make it more scalable [2].

And through VPN that Network connection between different devices that do not exactly use a physical cable is called VPN. VPN (Virtual Private Network) is simply a way of using internet for private communications, among a set of different users and sites. And we are using MPLS L3 VPN when we want to scale a small size service provider to a bigger size network [2]

Implementation of MPLS L3VPN using GNS3

They describe the view and perception to implement MPLS L3VPN using GNS3 that there are two types of VPN devices customer and provider network devices and they describe then advantage and disadvantage of MPLS L3 VPN that Advantage is [3]

(1) MPLS L3VPNs offers an extremely scalable VPN architecture
(2) MPLS L3VPN is can be offered as a managed service by SP
(3) MPLS L3VPNs allow an enterprise network to simplify their WAN routing.
(4) MPLS L3VPNs allow any-to-any connectivity for enterprise customer sites
(5) MPLS traffic engineering allows service providers to optimally use network bandwidth and support service-level agreements (SLA) with fast failover and bandwidth guarantee

Disadvantages of MPLS L3VPNs

1- MPLS L3VPNs mainly support IP traffic transport only
2- Some service providers do not support native IP multicast traffic transport between sites in MPLS L3VPNs.
3- MPLS L3VPN, the customer does not have complete control of their WAN IP routing

Implementation of Multi-Protocol Label Switching –Virtual Private Network for Corporate Networks

They focus and discuss the benefits available in IP VPNs and how the MPLS+BGP model is selected in the network. And how a branch office connects itself to other offices using MPLS VPN services delivered by a service provider and providing QOS to achieve security equivalent to that**.** Security is an important issue for corporate users To achieve that security Virtual Private Networks (VPNs) can be used to guarantee that traffic is securely tunneled over the Internet[4].VPN enables us to send data between two computers across a shared or public internetwork in a manner that follows the properties of a point-to-point private link. And allows a corporate network to connect to branch offices or to other companies over a public internetwork while maintaining secure communications. That there are two different methods to build VPNs across IP backbone. Customer Premises Equipment (CPE) and network-based**.** That most of them are using CPE method to build VPN across IP backbone. To build MPLS VPN across IP backbone there is some concept [4].

Routing Separation
To bring routing separation between different VPNs MPLS VPNs apply the following principles:
Each VPN should to allocate to a Virtual Routing and Forwarding (VRF) that every provider-edge router should maintain a separate VRF for every connected VPN. Unique VPN identifiers-for having routing separation across core network the provider-edge router needs unique VPN identifiers such as the route distinguisher [4].

Traffic Separation
MPLS VPN is using the "true peer VPN" model they perform traffic separation at Layer 3 through the use of separate IP VPN forwarding tables. MPLS VPN is applying traffic separation between customers by assigning a unique VRF to each customer's VPN [4]

QOS Routing in MPLS VPNs
QOS routing may be used in such cases for finding routes for connecting a number of sites into a VPN or setting up paths for sessions within VPNs. QOS routing is also believed to be one of the key components for supporting QOS in MPLS VPNs [4].
MPLS VPN networks provide full address and traffic separation and hide addressing structure of the core network and the VPNs. And we can offer Internet connectivity to MPLS-based VPNs in a secure manner [4].

MPLS Multi-VRF Design and Implementation using GNS simulator
They present and describes the designing of such a Multi-VRF MPLS network on the service provider network which can separate a customer's large network into smaller sites and keep them separated to each other in a cost-effective way.
Before MPLS VPN if the customers were willing to set up a private link between their various sites they would request the service provider for a separate link which the customers should to be extra for that link that was a costly investment. Also, the customers could not use the same private IP addresses while connecting to the service provider network as the service provider could not distinguish between the various customers or its various departments. When MPLS VPN started getting implemented, it enabled the service provider to let private links to the customer on the same network without any additional links to be installed. Different departments can be separated by implementing VLANs on switches in the main site and mapping each VLAN to a VRF (sub) interface on the PE router. Even now they can use the same Private ip address with the help of VRF. That two main concepts is using mainly in MPLS VPN that is Route- Distinguisher (RD) and Route-Target (RT) that The RD is used to keep all prefixes in the BGP table unique and RT is used to send and receive routes between VRF's/VPNS. And MPLS Multi-VRF feature proves to be the best solution to many problems that are faced by the customer and the service provider [6].

MPLS-VRF integration: forwarding capabilities of BGP/MPLS IP VPN in GNU/Linux
They present and describe an implementation of the BGP/MPLS IP VPN functionalities for GNU/Linux that this implementation included the integration of the MPLS- and VRF for- Linux projects. That there are two different approaches for deploying MPLS-based VPNs that the first one is Layer 2 VPNs, where layer 2 frames are directly forwarded from a source to destination sites using MPL and another one is Layer 3 VPNs, where IP is the common layer between the site and MPLS [7].
This implementation supports the data forwarding functionalities that include following - Support IP addresses covering at PE routers and P routers are not be aware of VPN routes also it support one-to-one association in VPN route table ad also it Support one-to-many association in route table and in this way, we can deploy different QOS strategies between VPNs and even for different services within the same VPN [7].

Design of Traffic Engineered MPLS VPN for Protected Traffic using GNS Simulator
They present and describes designing of MPLS VPN(Virtual Private Network) along with dedicated traffic tunneling for each VPN with the help of OSPF(Open Shortest Path First) and MP-BGP(Multi-Protocol-Border Gateway Protocol) which help customer happy and the will have a scalable and manageable and reliable network.it will also include path protection and It also includes path protection in MPLS network and failover functionality and with the help of router reflector for having better efficiency in the network[8].
The most important thing in deployment MPLS is the concept of VPN which separates the traffic according to the conditions and standard set by the customers that making the connection secure and private. It also provides private connections between different sites of the same company that located at different locations. They focus to connect customers from its headquarters to its various sites through the internet using a private connection that enabled with traffic tunneling. And for recovery purpose during frailer, they use Fast Reroute (FRR) and also they use VRF (Virtual Routing and Forwarding) feature in VPN that now allows the customers to even use the same IP addresses. They use these steps for designing of that network Layer 3 MPLS VPNs, Multi-protocol BGP, and Route Reflector (RR), MPLS Traffic Engineering (TE), and Failover functionality in MPLS [8].
The use of this design will limit the wastage of unused links and also provide secure channel route for every customer at the same instant and in the same network infrastructure. This also the design will be cost effective for both the customers and service provider. The implementation of the proposed design will definitely reduce parameters like packet loss and delay in the network and another important thing that Failover functionality is provided for guaranteed service to customers by giving path protection to the important traffic engineered tunnels [8].

A Model of Path Fault Recovery of MPLS VPN and Simulation
They present and describe to puts forward a model of path fault recovery of MPLS VPN, which is DR-PFR(Double Recovery-Path Fault Recovery), for the failure on the path of MPLS VPN when fail coming in the path. This method DR-PFR can solve the failures in both the working path and the backup path. When there be a fails to come in the network DR-PFR can enable the network and

recover timely and effectively reduce the impacts on users. As we see that MPLS VPN becomes attractive and daily use VPN with its low cost, high security and advanced quality of service that traffic between VPN sites are transmitted through the label switched path and the performance of VPNs are depends on the label switched path. That If main and Pre-established LSP fails, the traffic carrying on the LSP can't reach the destination hence to deliver reliable service, we must expect potential network problems and provide complete fault recovery mechanism through DR-PFR.as we can see that DR-PFR model makes MPLS VPN more strong and secure that If the working path fails, on account of local backup path, data loss rate is lower than global recovery and when both the working path and the local backup path fail, the DR-PFR model can still ensure that the network recovers quickly[9].

CONCLUSION

Recently it is compulsory for the service provider to satisfy all the needs of the customer in limited amount of resources and in a cost-effective way that different customer need to maintain the quality of services in terms of packet loss, jitter, delay, privacy , security, fast forwarding, and tunneling in an effectively and efficiently manner and as we saw and We have highlighted some of the papers pointing towards the flexibility, scalability, and easy traffic engineering benefits of MPLS VPNs compared to traditional VPNs and IP based networks that it will satisfy the needs of the customer in limited amount of resources and in a cost-effective way and also we are using of MPLS L3 VPN when we want to scale a small size service provider to a bigger size network. In this topology, we have shown how to deploy a service provider network that it is scalable and flexible network and in turn will prove to that MPLS VPN is cost effective for both the customers and service provider. And according to recovery mechanisms in MPLS, there were four different recovery mechanisms that during network failures they prove high delivery performance and among this four recovery mechanism, the best performance was achieved by Fast Reroute and DR-PFR (Double Recovery-Path Fault Recovery) mechanism that according to performance it is too high and fast.

REFERENCES

[1] Tariq M. Almandhari, Fahad A. Shiginah," A performance Study Framework for Multi-protocol Label Switching (MPLS) Networks", 8th IEEE GCC Conference and Exhibition, Muscat, Oman, 1-4 February 2015

[2] Ravi Kumar CV, Dhanumjayulu C, Bagubali A and Bagadi KP," Architecture for MPLS L3 VPN Deployment in Service Provider Network", Journal of Telecommunications System & Management 2017, 6:1

[3] Akshay1, Pooja Ahlawat," Implementation of MPLS L3VPN using GNS3", International Journal of Scientific Engineering and Research (IJSER) 2014

[4] M. Kanmani1, S. Beulah Hemalatha," Implementation of Multi-Protocol Label Switching – Virtual Private Network for Corporate Networks", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, February 2015

[5]Abid Shahzad and Mureed Hussain," IP Backbone Security: MPLS VPN Technology", International Journal of Future Generation Communication and Networking, Vol.6, No.5 (2013)

[6] Snehal Yadav and Amutha Jeyakumar,"MPLS Multi-VRF Design and Implementation using GNS simulator", 2nd IEEE International Conference on Engineering and Technology (ICETECH), 17th & 18th March 2016, Coimbatore, TN, India.

[7] Jon Ander Picó, Jose Oscar Fajardo, Alex Muñoz, Armando Ferro," MPLS-VRF integration: forwarding capabilities of BGP/MPLS IP VPN in GNU/Linux", Manuscript received October 31, 2007

[8] Snehal Yadav and Amutha Jeyakumar," Design of Traffic Engineered MPLS VPN for Protected Traffic using GNS Simulator", IEEE WiSPNET 2016.

[9] Shu-mei LI, Hai-Ying LIANG," A Model of Path Fault Recovery of MPLS VPN and Simulation", IEEE 2011

