International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 7, Issue 8 (June 2013), PP. 26-32

Approach to build MPLS VPN using QoS capabilities

Madhulika Bhandure[1], Gaurang Deshmukh[2] ,Saili Waichal[3], Varshpriya JN[4]
[1,2,3]MTech-NIMS(COMP) VJTI Mumbai
[4]Prof(COMP) VJTI Mumbai

Abstract:- A new standard for a new world of networking, MPLS is a forwarding mechanism based on Tag Switching. MPLS is an innovative approach in which forwarding decision is taken based on labels. It also provides a flexible and graceful VPN solution based on the use of LSP tunnels to encapsulate VPN data. VPNs give significant added value to the customer over and above a basic best effort IP service, so this represents a major revenue-generating opportunity for SPs. Multi-protocol Layer Switching (MPLS) VPNs are best solution for medium and large enterprises that currently deploy site-to-site VPN services. MPLS provides sophisticated traffic engineering capabilities that, coupled with IP QoS, enable multiple classes of service so business critical applications are treated with higher priority than less important applications and "best effort" services. We first present background on MPLS VPNs as well as QoS routing. Also we suggest some enhancements that will help to design the ideal MPLS VPN.

Keywords:- DDoS, MPLS, QoS, VPN, VRF.

I. INTRODUCTION

A virtual private network (VPN) is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible. A VPN provides varying levels of security so that traffic sent through the VPN connection stays isolated from other computers on the intermediate network, either through the use of a dedicated connection from one "end" of the VPN to the other, or through encryption. VPNs can connect individual users to a remote network or connect multiple networks together[1].

There are two types of VPN

1. Remote access VPN
2. Site-to-site VPN

This project aims at developing site-to-site VPN. Site-to-site VPNs connect entire networks to each other ,for example, connecting a branch office network to a company headquarters network. In a site-to-site VPN, hosts do not have VPN client software; they send and receive normal TCP/IP traffic through a VPN gateway. The VPN gateway is responsible for encapsulating and encrypting outbound traffic, sending it through a VPN tunnel over the Internet, to a peer VPN gateway at the target site. Upon receipt, the peer VPN gateway strips the headers, decrypts the content, and relays the packet towards the target host inside its private network.

Nowadays, the network traffic growth rapidly, so the traditional networks like ATM, frame relay, Ethernet are not able to support this situation. So service provider discovers a new technology that solves this problem. The new IP forwarding that can handle this situation is Multi Protocol Label switching (MPLS). This technology can give higher ability such as scale, traffic engineering capability and provides Quality of Services (QOS). MPLS is regarded as an enhancement to the traditional IP routing. This new technology is suitable for large network that requires optimal performance. Another reason why MPLS technology is important it that, it enables IP packet forwarding that support sophisticated packet classification and high rate data forwarding. For the next generation network, it is become the central element of network to be design with the high performance network with low cost. MPLS is the architecture for fast packet switching and routing by providing the designation, routing, forwarding and switching of traffic flow through the network.

This paper is organized as follows: Section 2 gives details about MPLS VPN. Section 3 gives the configuration details and introduce proposed topology for simulation. Section 4 shows the experimental results. Section 5 gives the idea of proposed system. Section 6 summarizes our work and concludes this paper.

II. MPLS VPN

MPLS popularity has increased exponentially in the last few years. One of the most compelling drivers for MPLS in service provider networks is its support for Virtual Private Networks (VPNs), in which the provider's customers can connect geographically diverse sites across the provider's network .First thing people confuse is the usage of the words MPLS and VPN. Both are separate terminologies. MPLS is the protocol that runs on top of your routing protocols. And VPN is all about creating a virtual network end to end across the

internet. Traditionally VPN were based on IPsec (layer 3) or TLS (layer 2) which were slow and sluggish and merely less on features. MPLS had all these points into consideration as it evolved right inside Cisco labs, where it took birth. Later on, it was adopted as an industry standard in late1990s[2].The MPLS VPN backbone and the customer sites exchange layer-3 customer routing information and packets are forwarded between multiple customer sites through the MPLS enabled backbone using the MPLS VPN services.

A. Components of MPLS VPN

1. Customer networks: It is under customer's administrative domain.
2. Provider network: It is under Provider's admin control and responsible for providing routing between various customer's sites
3. CE Routers: Customer edge routers connecting the Provider MPLS network.
4. PE Routers: Provider MPLS edge router connecting to single or multiple customer CE routers.
5. P Routers: Provider MPLS backbone routers that interface with either other Provider backbone or PE routers.

MPLS based VPN accommodates for the overlapping IP address space between multiple customers by isolating each customer's traffic. The CE routers only get the traditional IP traffic and no labeled packets are forwarded to the CE routers. CE routers do not need any MPLS configuration for connecting to the Provider MPLS VPN network. PE Router is the first place where the MPLS VPN implementation starts, the PE router is responsible for isolating customer traffic if multiple customers are connected to the PE router. This is done in PE router by assigning an independent routing table to each customer, which is as good as assigning a dedicated router to each customer. The rest of the Provider network (P routers), the routing is done using the global routing table where P routers provide label switching between provider edge router and they are unaware of the VPN routes. The entire process is transparent to the customer as the CE routers are not aware of the presence of the P routers and Provider network's internal topology. In the Provider network the P routers are only responsible for the label switching and they do not carry VPN routes and do not participate in the MPLS VPN routing.

B. Architectural Ingredients Of Mpls Vpn

Virtual routing and forwarding table (VRF): Customer traffic isolation is achieved in MPLS with the use the VRFs. Each VRF can be thought of as a dedicated router being assigned to each customer CE router.VRF is similar to the global routing table except that it contains only all the routes for a specific VPN. It also contains VRF-specific CEF forwarding table. Any interface that is a part of VRF must support CEF. An interface (logical or physical) can be assigned to only one VRF. In these way in MPLS the actual physical router is divided into multiple virtual routers[3].

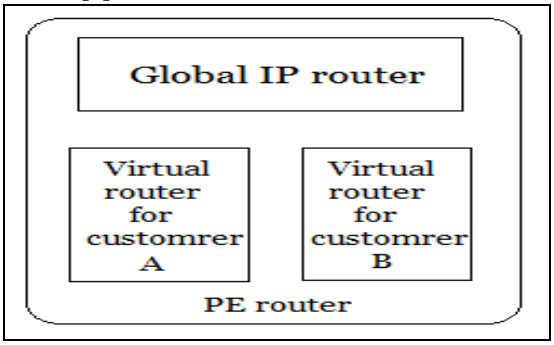

Fig. 1. VRF Instances

Route Distinguisher (RD): Ipv4 address space is limited. The problem is when customer had overlapping IP addressing , the routing would be wrong. For example most companies use private addressing for their internal network to prevent use of public addresses. It can be quite possible that two companies may have same internal address space 192.168.10.0/24. To prevent the customer routes from getting routed wrongly MPLS consists of 64-bit field called as Route Distinguisher. RD= 16 bit type + 48 bit value . The RD is only used to make Ipv4 address unique. Generally (ASN: IP Address) Autonomous system number is included in the RD value field to make an unique 96-bit address for each VPN. 64 bit –RD + 32 bit IP address =Unique VPN route The PE router implements this feature using the RD per VRF.

Route Target (RT): Route Targets are generally used to control the policy of who sees what routes. Typically carried as an extended BGP community. It is a 64 –bit quantity. For example, there are two companies A and B and both have sites X and Y. Sites X and Y of A can talk to each other and similarly for company B but Site X and Y of company A cannot talk to X and Y of B. If in case you need site X of A to talk to site X of B, route target comes into picture. In that case routes will be exported to remote PE and also imported from remote PE in order to make it work.

BGP: BGP version 4 is the protocol for the internet. It is well suited to carry thousands of routes and that is why it is a good candidate to carry MPLS VPN routes. As the packet traverses along the MPLS network it has two labels associated with it.

a) IGP Label: It is the top label in the stack. It is a label that is bound to Ipv4 prefix in the routing table. It gives the information about next hop to packet.

b) VPN Label: The bottom label is VPN or BGP label. This label usually indicates the next hop a packet should take after reaching egress PE router. To sum it up IGP label is used to forward the packet to the correct egress PE router while the egress PE router uses VPN label to forward the IP packet to correct CE router.

III. MPLS CONFIGURATION AND SIMULATION

The simulation environment employed in this paper is based on GNS 3.0 simulator.

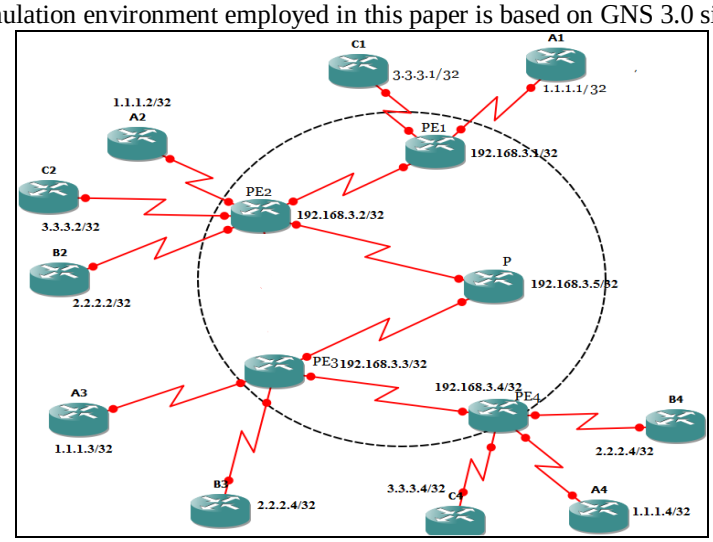

Fig. 2. Network Topology

The network consists of 15 nodes. Out of which, 5 nodes are service provider nodes and remaining are customer nodes. All links were setup as duplex. The work is simulated using a network with following characteristics.

- Service provider network with 4 provider edge router(PE1-PE4) and one core router(P)
- All type of traffic
- With QoS
- Traffic routed by LSP
- OSPF as IGP

A. Configuring the CE Router

Configuration of the CE router is very simple. The only restriction is that the routing protocol used between the CE and PE routers must currently be RIP version 2, EIGRP, OSPF, or EBGP. Static routes can also be used. The CE router is not necessary to be mpls enabled. We have OSPF between CE and PE in our simulation[4].

B. Configuring the PE Router

Configuration of the PE router is much more complicated than that of the CE router. There are 12 basic steps involved and they are as follows.

1.Configure the loopback interface to be used as the BGP update source and LDP router ID.

2. Enable CEF

(config)#ip cef

3. Configure the label distribution protocol.

(config)#mpls label protocol ldp

4. Configure the TDP/LDP router-id (optional).

(config)# mpls ldp router-id loopback0

5. Configure MPLS on core interfaces.

(config)# mpls ip

6. Configure the MPLS VPN backbone IGP.

We have used OSPF as backbone IGP. We can use any IGP.

7. Configure global BGP parameters.

```
PE1(config)# router bgp 3
                no synchronization
                no auto-summary
                redist static
                redist connected
                neighbor 192.168.3.2 remote-as 3
               neighbor 192.168.3.2 update-source
                  lo0
               network 192.168.3.1 mask
                   255.255.255.255
```

This is configuration of PE1 router.

8. Configure MP-BGP neighbor relationships.

```
PE1(config)# router bgp 3
                address-family vpnv4
                neighbor 192.168.3.2 activate
                 no auto-summary
```

9.Configure the VRF instances.

```
ip vrf vpna
 rd 3:10
 route-target both 3:10
!
interface e0/0
 ip vrf forwarding vpna
 ip address 150.1.31.1 255.255.255.252
```

Similarly we have to create VRF for B and C customers on required PE route

10. Configure PE-CE routing protocols / static routes.

```
router ospf 3
 network 0.0.0.0 255.255.255.255 area 0
```

11.Redistribute customer routes into MP-BGP.

```
router ospf 3 vrf vpna
 redistribute bgp 3 subnets
 network 150.1.0.0 0.0.255.255 area 0
!
router bgp 3
 address-family ipv4 vrf vpna
 redistribute ospf 3
```

Here we redistributed routes of customer A. Similarly we have to redistribute routes of B and C customer.

PE routers are all located in a single autonomous system, configured as fully meshed and are running internal BGP. The generally run the upper version of BGP which is MP-BGP. They have MP-iBGP session between them. The P routers just perform the work of label swapping and switching. They do not have any information of customer routes.

IV. EXPERIMENTAL RESULTS

Now we have 3 customers A, B,C which are connected at multiple sites. As we said above that VRF in MPLS VPN create multiple virtual routers instances, following is the output that we observed on PE2 router. Here all 3 customers are connected so there are 3 vrf instances , one for each customer.

PE2# show ip route

It will show global routing table

```
     192.168.3.0/24 is variably subnetted, 9 subnets, 2 masks
O       192.168.3.8/30 [110/192] via 192.168.3.17, 00:00:46, Serial1/1
O       192.168.3.12/30 [110/128] via 192.168.3.17, 00:00:46, Serial1/1
O       192.168.3.3/32 [110/129] via 192.168.3.17, 00:00:46, Serial1/1
C       192.168.3.2/32 is directly connected, Loopback0
O       192.168.3.1/32 [110/65] via 192.168.3.22, 00:00:46, Serial1/0
O       192.168.3.5/32 [110/65] via 192.168.3.17, 00:00:46, Serial1/1
O       192.168.3.4/32 [110/193] via 192.168.3.17, 00:00:47, Serial1/1
C       192.168.3.16/30 is directly connected, Serial1/1
C       192.168.3.20/30 is directly connected, Serial1/0
```

Fig 3. Global routing table

PE2# show ip vrf vpnb

It will show routing table for customer B (vrf vpnb)

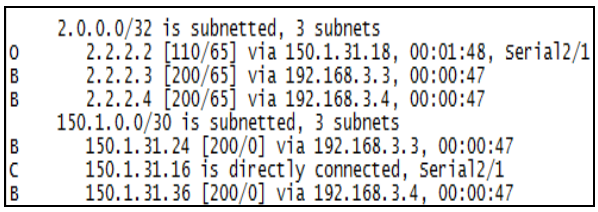

Fig 4. VRF VPNC

PE2# show ip vrf vpnb
It will show routing table for customer C (vrf vpnc)

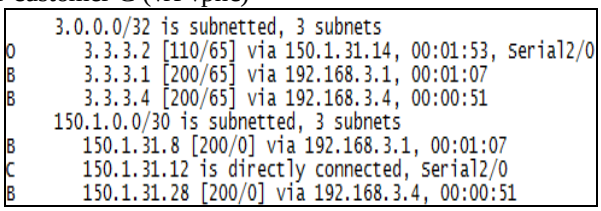

Fig 5. VRF VPNB

PE2# show ip vrf
It shows that there are 3 vpn instances are created vpna, vpnb, vpnc with RDs 3:10, 3:20,3:30 respectively.

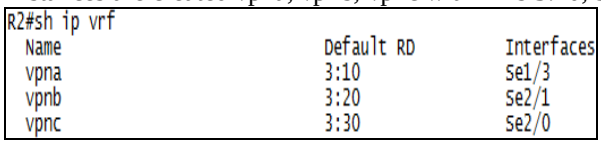

Fig 6. VRF instances

V. PROPOSED SYSTEM

MPLS vpn is the technology which is alternative to all other old-fashioned vpns like leased lines, IP tunnels. It is cost effective and provides better flexibility and scalability. Though it is best available solution, it has some drawbacks. Also if we use extra features like QoS, traffic engineering, the throughput of overall architecture will be more. The integration of MPLS vpn with QoS will provide both customer and service provider the new and better option to connect the remote sites. Here we are suggesting few enhancements which will improve overall performance and will provide secure connection.

A. Disabling TTL propagation

Service provider are mainly focusing on MPLS vpn these days because it is best available solution. But the internal structure of service provider network architecture should be protected from external network. The internal structure of SP consist of PE and P routers. These routers should be hidden from outside world. This information should also not be leaked to customer. Customer can issue traceroute command for its remote site and can get all addresses of PE and P routers in its LSP path and idea about their placement in network. SP never want that the outside world get idea about its internal architecture. Addresses in the core network can be hidden from view in a VPN by configuring the no mpls ip propogate-ttl forward command on SP routers. Now if traceroute is issued from any VRF or any customer router, no core addresses are returned; however; the address of egress PE router is visible. This enhancement can secure SP architecture.
(config)#no tag-switching ip propagate-ttl

B. Quality of Service

Nowadays QoS for web services is becoming more and more vital to service providers. But due to the dynamic and unpredictable characteristics of the web services, it is very difficult duty to offer the desired QoS for web service users.[5] Additionally, different web service applications with dissimilar QoS necessities will fight for network and system resources such as bandwidth and processing time. However, an enhanced QoS for MPLS vpn will bring competitive advantage for service provider. To provide such a better QoS, it is first necessary to identify all the possible QoS requirements for vpn, which is the objective of this document. This paper discusses possible approaches for supporting vpn with QoS. The QoS requirements for vpn here mainly refer to the quality that the customer will experience. These may include performance, reliability, scalability, capacity, robustness, exception handling, accuracy, integrity, accessibility, availability, interoperability, security, and network-related QoS requirements.

QoS allows to choose a profile that allows customer to choose bandwidth according to company needs. For example if company runs most on voice and video applications then customer can ask most of the bandwidth to these applications The typical profiles into which Class of Service is divided are Real Time (Voice

and Video),Business critical, Best effort. Following are the few enhancements can be added to network to fulfil customer requirements[6].

1) Filter web traffic from specific site. Customer can request to disallow web traffic for particular web site. e.g. to disallow web traffic from www.facebook.com

```
class-map match-all DISALLOWED_SITES
match protocol http url "WWW. FACEBOOK.COM"
!
policy-map WEB_FILTER
class DISALLOWED_SITES
drop
```

2) Reserve B/W during congestion. Now in case of congestion , customer may demand that particular traffic pattern should be given more importance. So we can prioritize customer traffic by writing policies. e.g. if customer demands that during congestion following should be the prioritization.

voice traffic 15% of bandwidth
http and https traffic 10%
SNMP AND SYSLOG traffic 10%

Policy for that is as below.

```
class-map match-any MONITORING
match protocol syslog
match protocol snmp
class-map match-any WEB
match protocol http
match protocol secure-http
class-map match-any VOICE
match protocol rtp
match protocol h323
match protocol mgcp
match protocol sip
match protocol skinny
policy-map qos
class MONITORING
bandwidth percent 10
class VOICE
bandwidth percent 15
class WEB
bandwidth percent 10
```

3) Use PBR to mark packets. Now there can be few customers who just want best effort service. At same site, there can be few customers who are running real time services. So according to services used, the packets can be marked using IP precedence field. e.g. to configure the router to mark all packets from network 192.168.5.x 255.255.255.0 to be marked with ip precedence 7 while leaving fastethernet 0/1 .

```
ip cef
!
route-map PBR
match ip add 1
set ip precedence 7
!
access-list 1 permit 192.168.5.0 0.0.0.255
!
int fa0/1
ip policy route-map PBR
!
```

4) NBAR. NBAR, by adding intelligent network classification to your infrastructure, helps in ensuring that the network bandwidth is used efficiently by working with QoS feature. With NBAR, network-traffic classification becomes possible and by this we can know how much of say , HTTP traffic is going on. By knowing this, QoS standards can be set.e.g. Configure NBAR on int fa0/0 interface of Router so that HTTP download for images are limited to 100kbps. Assume all images are jpeg, jpg & gif.

```
ip cef
class-map match-any image
match protocol http url *gif
match protocol http url *jpeg
```

```
match protocol http url *jpg
policy-map HTTP_NBAR
class image
police 100000 conform-action transmit exceed drop
int fa0/0
service-policy input HTTP_NBAR
```

C. Prevention against DDoS attack

Basic denial of service attack involves bombarding an IP address with large amounts of traffic. If the IP address points to a Web server, then it (or routers upstream of it) may be overwhelmed. Legitimate traffic heading for the Web server will be unable to contact it, and the site becomes unavailable. Service is denied.

A distributed denial of service attack is a special type of denial of service attack. The principle is the same, but the malicious traffic is generated from multiple sources although orchestrated from one central point. The fact that the traffic sources are distributed often throughout the world makes a DDoS attack much harder to block than one originating from a single IP address. There are a few technical measures that can be taken to partially mitigate the effect of an attack especially in the first minutes -- and some of these are quite simple. For example, we can rate limit your router to prevent your Web server being overwhelmed. Also we can add filters to tell router to drop packets from obvious sources of attack. We can write commands timeout half-open connections more aggressively and drop spoofed or malformed packages. We can set lower SYN, ICMP, and UDP flood drop thresholds. e.g. there is a DDOS attack using icmp[7].

Commands to limit icmp packets to 1Mbps on Serial 1/0.

```
ip access-list extended 101
permit icmp any any
!
interface Serial1/0
rate-limit input access-group 101 100000 8000 8000 conform-action transmit exceed-action drop
```

VI. CONCLUSIONS

MPLS vpn simplifies the network infrastructure by allowing the consolidation of multiple technologies and applications such as voice, video and data. MPLS provides sophisticated traffic engineering capabilities that, coupled with IP QoS, enable multiple classes of service so business critical applications are treated with higher priority than less important applications Via the above-mentioned theories analysis and experiment simulation we can see, the MPLS VPN best among all other vpns and it works best even in case of overlapping address spaces. The proposed system will provides enhanced security, scalability and high availability and will satisfy customer needs in better way.

REFERENCES

[1]. https://en.wikipedia.org/wiki/Virtual_private_network

[2]. Cisco "MPLS VPN Technology"Chris Metz"The Latest in VPNs: Part II" Published by the IEEE Computer Society May 2004

[3]. Yoo-Hwa Kang, and Jong-Hyup " The Implementation of the Premium Services for MPLS IP VPNs"

[4]. LeeYanfei Zhao, Zhaohai Deng" A Design of WAN Architecture for Large Enterprise Group Based on MPLS VPN" 2012 International Conference on Computing, Measurement, Control and Sensor Network

[5]. M. El Hachimi, M.-A Breton, and M. Bennani, "Efficient QoS Implementation for MPLS VPN," International Conference on Advanced Information Networking and Applications, pp. 259-263,March 2008.

[6]. Muhammad Romdzi Ahamed Rahimi, Habibah Hashim, Ruhani Ab Rahman "Implementation of Quality of Service (QoS) in Multi Protocol Label Switching (MPLS) Networks" 2009 5th International Colloquium on Signal Processing & Its Applications (CSPA)

[7]. http://www.esecurityplanet.com/network-security/5-tips-for-fighting-ddos-attacks.html.