IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 3, Ver. I (May - Jun.2015), PP 48-53
www.iosrjournals.org

Implementing VPN over MPLS

Engr. Awais Khan[1], Prof. Dr. Inayatullah Khan Babar[2]
[1](Department of Electrical Engineering, University of Engineering & Technology, Peshawar, Pakistan)
[2](Department of Electrical Engineering, University of Engineering & Technology, Peshawar, Pakistan)

Abstract: *Now a day's communication network and its services are migrating slowly towards new and upgraded versions. Multi-Protocol label Switching (MPLS) is a key feature in new technology and it delivers new services from old network to a new network during migration and it has totally focused on new network topology. MPLS is capable of providing secure and reliable connection for costumers through Multi-Protocol Label Switching Virtual Private Network (MPLS VPN). This thesis describes the requirements and motivation for using MPLS VPN as a data center inter-connects technology. A comparison of Traditional VPN has been made with that of MPLS VPN and also VPN has been implemented over MPLS using Graphical Network Simulator GNS3. MPLS technology is being used widespread in the Service Provider (SP) networks for the deployment of residential, business, and mobile services.*

Keywords: *Multi-protocol Label Switching (MPLS), Virtual Private Network (VPN), Virtual Routing and Forwarding (VRF), Label Switched Path (LSP)*

I. Introduction

In the last 15 years there are many different technologies used in transmission of network traffic from source to destination. Asynchronous Transfer Mode (ATM), Frame Relay, and PPP were included in these technologies. They are all useful and having their own benefits but there are some difficulties when these are being internetworked. In parallel to using these technologies research was made by many companies to find the alternate of these technologies because current technologies are so expensive. Out of these technologies some new ideas were developed by Cisco System regarding Tag switching, which was later became a standard known as Multi-Protocol Label Switching (MPLS).[1]

MPLS works on the basis of label switching. We assign a unique and independent label to every data packet and then these packets are routed and switched through the network on the basis of these labels. These labels are contained in the header of each packet and are overlooked by networking devices when processing and forwarding packets. This idea of label switching is being used for long in data communication industry. Frame Relay, X.25 and ATM are some example of label switching technologies which are in use since long. So the journey towards MPLS is really now in fast pace. As we know that ATM, Frame Relay and IP etc. can be easily and transparently carried through MPLS networks for the end user. Apart from large networks, MPLS is also now in use in large enterprise networks of organization such as Business companies, government organizations, hospitals, call centers and many more.

II. Multiprotocol Label Switching

MPLS (Multiprotocol Label Switching) is a standard networking technology in which packets are forwarded through the network based on label attached to these packets. Adjacent routers in MPLS network advertise labels among themselves and hence make peer to peer mapping. IP packets are forwarded by looking at the labels attached to these packets and not by looking into the destination IP addresses, so we can say that packet forwarding is by label switching instead of IP switching [4].

III. Packet Flow in an MPLS Network

Figure 1 shows a common MPLS network and its components. The devices inside the boundary of provider network are the components of MPLS network. All the data packets passing through this cloudily MPLS network are label based. The customer traffic outside this cloud are not label based, it may be IP based etc. The customer owned Customer Edge (CE) routers (as shown in figure Site 1, Site 2 and Site 3) whose interface is connected to label edge router (LER) or Provider Edge (PE) routers which are in domain of the Service Provider. Why PE routers known as LER? Because it add label to the incoming (ingress) traffic when enter into the MPLS network, and then remove the label on outgoing (egress) traffic when packets move out of the MPLS networks. Within the MPLS cloud, the behavior of PE router is like LSRs (label switches routers) because it switches packets from one node to the next looking into its labels.

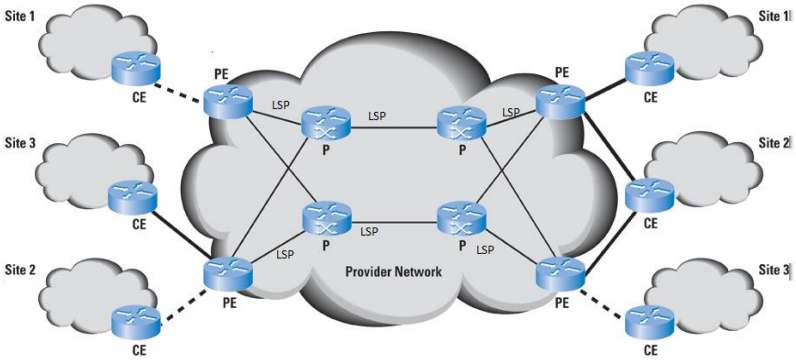

Figure: 1 Service Provider MPLS Network [20]

IV. Virtual Private Network

A VPN is a private network over a public or shared network in such a way as they are directly connected. In VPN, different features like management, security etc of a private network can be attained over a public network. In VPN different sites of costumers are connected but they are inaccessible from others costumer's sites. The VPN normally is used for one company and then several sites of that company to be connected through the common/ public service provider network. The advantage of VPNs is to allow remote locations of different costumers to be securely connected over a public networks, and hence the costumer do not need to buy dedicated network lines [5].

V. MPLS VPN Routing

The correct routing information should be updated for the VPNs in routing and forwarding (VRF) table of PE. The routing topology information for different VPNs needs to be populated in separate VRFs. This split-up is obtained by addition of an identifier called route distinguisher to general IP route advertisements.

RDs are eight byte chunks that is present ahead of IPV4 address route advertisements. RD for every VRF should be distinct. A route distinguisher may be representing as 100:25. Where 100 denote ASN of that particular service provider while 25 represents any specific VRF. Now this RD is distinct for all the customer's VRF and when there are many VRFs and they may have gone through different service provider's network, they are still recognizable through the help of these RDs. [6].

Routing updates accomplished with BGP. iBGP or interior BGP with MPLS extension is used for communication among PE routers. BGP updates among routers are based on incoming and outgoing routing plans which is configured on these nodes. [7].

Route Distinguisher = (type + ASN + Assigned number)

VPN IP Address = Route Distinguisher + IPv4 Address

VI. Implementation

Now a basic MPLS VPN will be configured as shown in the below Figure 5.1 in which a simple MPLS VPN model with serving two sites of a customer. For this purpose The Graphical Network Simulator (GNS3) software has been used, it is an open source software and is very powerful tool for networks. It runs virtual routers with real IOS.

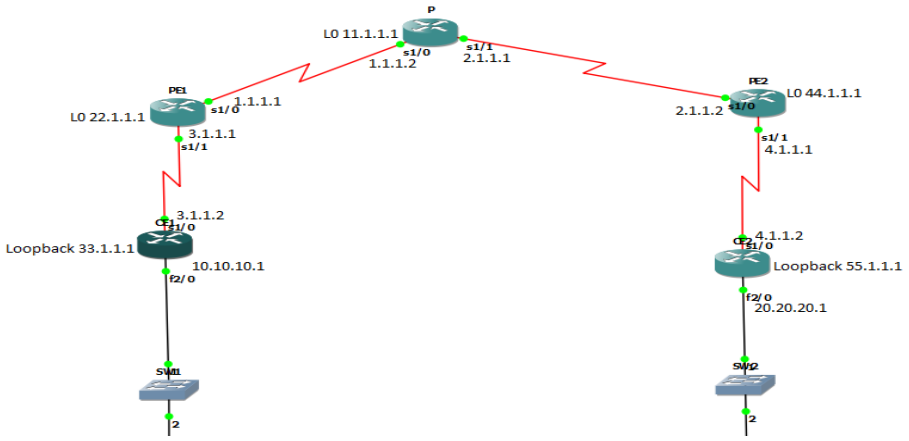

Figure 2 Lab Topology of VPN MPLS

As a review,

- P or Provider routers are present at the core of MPLS network; they run MPLS protocols and have no direct connection with the customer NEs.
- PE or Provider Edge routers are at the boundary of MPLS cloud and are links with P router at one end and with customer node at other end and all VPN services are configured at PEs.
- CE or Customer Edge router is placed at the boundary of customer network and is not running MPLS.
- An Interior gateway protocol (i.e. OSPF) is running between P and PE which also helps in LDP and BGP adjacencies inside the network.
- MP-BGP is running between PEs only.
- An Interior gateway protocol like OSPF is also running b/w CE & and its corresponding PE.

In the above topology, OSPF has been used separately in the provider network & on CE.
We will perform following steps in order to get the functionality of MPLS VPN.

1. To enable MPLS on all routers in provider backbone network.
2. To build VRFs & allocate them for the routing interfaces.
3. To construct MP-BGP among PEs.
4. To configure OSPF b/w every PE and it's connected CE router.
5. And finally to enable route redistribution b/w customer sites and the provider network

First we will do the basic configurations of all the routers and assigning addresses as per Figure 1
Then, an Interior gateway protocol like Open Shortest Path First (OSPF) has been run on the routers of provider network i.e. on PE1, P and PE2.

```
PE1#configure terminal
PE1(config)#router ospf 1
PE1(config-router)#network 1.0.0.0 0.255.255.255 area 0
PE1(config-router)#network 22.0.0.0 0.255.255.255 area 0
PE1(config-router)#exit
PE1(config)#exit
```

Figure 4 Running OSPF on PE1 Router

Now we will to run MPLS on Router PE1, P and PE2.

```
PE1#configure terminal
PE1(config)#ip cef
PE1(config)#mpls ip
PE1(config)#mpls label protocol ldp
PE1(config)#mpls ldp router-id loopback 0
PE1(config)#interface serial 1/0
PE1(config-if)#mpls ip
PE1(config-if)#end
```

Figure 5 Running MPLS on PE1 Router

Create Virtual routing and forwarding (VRF) between PE1 & CE1

```
PE1#configure terminal
PE1(config)#ip vrf customer
PE1(config-vrf)#rd 1:1
PE1(config-vrf)#route-target 1:1
PE1(config-vrf)#end
```

Figure 6 VRF Configuration (PE1 to CE1)

Similarly between PE2 and CE2

```
PE2#configure terminal
PE2(config)#ip vrf customer
PE2(config-vrf)#rd 1:1
PE2(config-vrf)#route-target 1:1
PE2(config-vrf)#exit
PE2(config)#interface serial 1/1
PE2(config-if)#ip vrf forwarding customer
% Interface Serial1/1 IP address 4.1.1.1 removed due to enabling VRF customer
PE2(config-if)#ip address 4.1.1.1 255.0.0.0
PE2(config-if)#end
PE2#ping 4.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.1.1.2, timeout is 2 seconds:
Success rate is 0 percent (0/5)
```

Figure 7 VRF Configuration (PE2 to CE2)

MP-BGP need to be configured for the VRF advertisement among PEs. It support multiple address family e.g. ipv6 or ipv4. Only PE routers run MP-BGP while the P routers only use MPLS and OSPF etc for packets forwarding with the SP network.

```
PE1#configure terminal
PE1(config)#router bgp 1
PE1(config-router)#no auto-summary
PE1(config-router)#no synchronization
PE1(config-router)#neighbor 44.1.1.1 remote-as 1
PE1(config-router)#neighbor 44.1.1.1 update-source loopback 0
PE1(config-router)#address-family vpnv4
PE1(config-router-af)#neighbor 44.1.1.1 activate
PE1(config-router-af)#exit
PE1(config-router)#exit
PE1(config)#exit
```

Figure 8 MP-BGP Configuration on PE1 towards PE2

```
PE2#configure terminal
PE2(config)#router bgp 1
PE2(config-router)#no auto-summary
PE2(config-router)#no synchronization
PE2(config-router)#neighbor 22.1.1.1 remote-as 1
*Dec  4 14:53:43.787: %BGP-5-ADJCHANGE: neighbor 22.1.1.1 Up
PE2(config-router)#neighbor 22.1.1.1 update-source loopback 0
PE2(config-router)#address-family vpnv4
PE2(config-router-af)#neighbor 22.1.1.1 activate
PE2(config-router-af)#
*Dec  4 14:54:23.151: %BGP-5-ADJCHANGE: neighbor 22.1.1.1 Down Address family
activated
PE2(config-router-af)#exit
PE2(config-router)#exit
PE2(config)#exit
```

Figure 9 MP-BGP Configuration on PE2 towards PE1

We can see the console message that MP-BGP neighbor ship is made b/w PE1 & PE2.

Now OSPF will be configured between PE & connected CE

```
CE1#configure terminal
CE1(config)#router ospf 1
CE1(config-router)#network 10.10.10.1 0.0.0.0 area 0
CE1(config-router)#network 3.1.1.2 0.0.0.0 area 0
CE1(config-router)#network 33.1.1.1 0.0.0.0 area 0
CE1(config-router)#end
```

```
PE1#configure terminal
PE1(config)#router ospf 2 vrf customer
PE1(config-router)#router-id 22.1.1.1
OSPF: router-id 22.1.1.1 in use by ospf process 1
PE1(config-router)#network 3.1.1.1 0.0.0.0 area 0
PE1(config-router)#
*Dec  4 16:34:01.102: %OSPF-5-ADJCHG: Process 2, Nbr 33.1.1.1 on Serial1/1 from
LOADING to FULL, Loading Done
PE1(config-router)#end
```

Similarly OSPF will be configured between PE2 and CE2.

Now in the last step we will redistribute routes b/w customer sites and Service Provider network. So first we will redistribute OSPF 2 into BGP.

```
PE1#configure terminal
PE1(config)#router bgp 1
PE1(config-router)#address-family ipv4 vrf customer
PE1(config-router-af)#redistribute ospf 2 match internal external 1
PE1(config-router-af)#
PE1(config-router-af)#end
```

```
PE2#configure terminal
PE2(config)#router bgp 1
PE2(config-router)#address-family ipv4 vrf customer
PE2(config-router-af)#redistribute ospf 2 match internal external 1
PE2(config-router-af)#end
```

And then we will redistribute BGP into OSPF 2

```
PE1#configure terminal
PE1(config)#router ospf 2
PE1(config-router)#redistribute bgp 1 subnets
PE1(config-router)#end
```

```
PE2#configure terminal
PE2(config)#router ospf 2
PE2(config-router)#redistribute bgp 1 subnets
PE2(config-router)#end
```

VII. Results/ Analysis

Thus Routing Tables of Router CE1 and CE2 have been completely converged, as we can see all the routes of CE2 visible/accessible in CE1.

```
CE1#show ip route
C    33.0.0.0/8 is directly connected, Loopback0
C    3.0.0.0/8 is directly connected, Serial1/0
O IA 4.0.0.0/8 [110/65] via 3.1.1.1, 00:06:42, Serial1/0
     55.0.0.0/32 is subnetted, 1 subnets
O IA    55.1.1.1 [110/129] via 3.1.1.1, 00:06:42, Serial1/0
O IA 20.0.0.0/8 [110/129] via 3.1.1.1, 00:06:42, Serial1/0
C    10.0.0.0/8 is directly connected, FastEthernet2/0
```

Similarly all the routes of CE1 are visible/ accessible in CE2 as shown below.

```
CE2#show ip route
     33.0.0.0/32 is subnetted, 1 subnets
O IA    33.1.1.1 [110/129] via 4.1.1.1, 00:05:52, Serial1/0
O IA 3.0.0.0/8 [110/65] via 4.1.1.1, 00:05:52, Serial1/0
C    4.0.0.0/8 is directly connected, Serial1/0
C    55.0.0.0/8 is directly connected, Loopback0
C    20.0.0.0/8 is directly connected, FastEthernet2/0
O IA 10.0.0.0/8 [110/129] via 4.1.1.1, 00:05:52, Serial1/0
```

Hence the VPN has been successfully implemented over MPLS in the given scenario.

VIII. Conclusion

The advantages of MPLS VPN are so diverse i.e. it is easily manageable (addition or deletion of a new sites just require the connectivity/ configuration of a customer site with the PE router), secure (since a separate VRF is maintained for each customer site, hence there no chance of security breach as all the customers are well segregated) and scalable (no complete mesh between customer sites is required), so it is now the need of service provider to implement. Its ability of combining the plus points of overlay & peer to peer VPN model makes it the priority solution by ISPs to offer their services to the customers. Traffic engineering, QoS are the additional features of using MPLS network, also management of network including addition or deletion of new sites is extremely easy.

In the near future all traditional VPN technologies will soon be replaced with MPLS VPN, due to its flexibility, fast routing & switching and more secure features.

References

[1]. J. t. Johnson, "Five reason to move to MPLS (Multi protocol Label Switching)," Network World, 29 March 2007.
[2]. L. Paulson., "Using MPLS to unify multiple network types," Computer ,sponsored by IEEE computer society , vol. 37, no. 5, pp. 15-17, 2004.
[3]. S. G. K. N. a. P. P. Veni, "Performance analysis of network traffic behavior in conventional network over MPLS," in Communication Control and Computing Technologies, 2010.
[4]. W. G. Hannes Gredler, "Traffic Engineering and MPLS", the Complete IS-IS Routing Protocol,," 2005.
[5]. F. Palmieri, "Evaluating MPLS VPN against traditional approaches," in Eighth IEEE Symposium on Computers and Communications (ISCC'03), June 30, 2003.
[6]. D. H. F. Badran, "Service Provider Networking Infrastructures with MPLS," in Sixth IEEE Symposium on Computers and Communications (ISCC'01), July 05, 2001.
[7]. R. Pulley, "Implementing VPNs Using MPLS," in Proceedings of MPLS Forum, 2000.
[8]. L. M. G. Heron, "An Architecture for L2VPNs," in IETF draft: draft-ietf-ppvpn-12vpn-00.txt, 2001.
[9]. S. Previdi, "Introduction to MPLS-BGP-VPN," in Proceedings of MPLS Forum , 2000.
[10]. R. Y. Rosen E, "RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)," in RFC 4364, IETF, 2006.
[11]. I. P. J. Guichard, "MPLS and VPN Architectures," Cisco Press, 2000.
[12]. R. Venkateswaran, "Virtual Private Networks," in IEEE Potentials, Mar. 2001.
[13]. V. Alwayn, "Advanced MPLS Design and Implementation," Cisco Systems, 2002.
[14]. A. Y. S. V. C. Mahesh Kr. Porwal., "Traffic Analysis of MPLS and Non MPLS Network including MPLS Signaling Protocols and Traffic distribution in OSPF and MPLS," in International Conference on Emerging Trends in Engineering and Technology, ICETET, July, 2008.
[15]. D. O. Awduche, "MPLS and Traffic Engineering in IP Networks," in IEEE Communications Magazine, December 1999.
[16]. P. B. Liwen He, "Liwen HPure MPLS TechnologyThe Third International Conference on Availability, Reliability and Security, IEEE," in The Third International Conference on Availability, Reliability and Security, IEEE, 2008.
[17]. A. H. a. B. B. Xipeng Xiao, "Traffic Engineering with MPLS in the Internet," in Global Center Inc. Lionel M, NI, Michigan State University., 2001.
[18]. D. Wright, "Voice over MPLS Compared to Voice over Other Packet Transport Technologies," in IEEE Communications Magazine, November 2002.
[19]. U. L. a. L. Lobo, "MPLS Configuration on Cisco IOS Software," in Cisco Press, Oct 17,2005, Copy right 2006.
[20]. L. D. Ghein, MPLS Fundamentals, Cisco Press , November 2006, Copy right 2007.
[21]. J. Reagan, Cisco CCIP MPLS Study Guide" Copy rights 2002 Sybex Inc, Sybex Inc, Copy rights 2002.