Multi-Homed Inter-Autonomous System Provider using Mpls Vpn Technology

M.Naga Kumari, T.S.Padmaja, M.Devi Prasad

Abstract: To implement a Multi-Homed Inter-AS Provider network using MPLS VPN technology where Service Provider 1 and Service Provider 2 are providing services to geographically dispersed Customer A and B sites. This research work is great method of communication among partner branches of an organization each of them situated at distinct geographical areas with absence of the same ISP in every area. We came up with an idea of designing Multi-Homed Inter-AS provider network i.e., connecting multiple ISPs with MPLS VPN which provides global reachability. This design provides security confidently in Private/Public organizations through Internet replacement. In reliability, it becomes more important to use MPLS technology which is being widely adopted by worldwide service providers to connect geographically separated customer sites. In this research work, Customer Sites are connected with VPNs for secure private. Here, we provide a great survey about MPLS, BGP, and VPN Networks. We address the issues of traditional Inter-As Provider. This existing system connects the geographically separated customer sites with single link. Such, there is more traffic burden on that single link. Thus, the quality parameters of network such are speed and QoS (Quality of Service) are changing with traffic rate. To overcome these issues, we propose the Provision of Multi-Homed Inter-As Provider using MPLS VPN Technology. Our proposed design Inter-AS Multi-Homed Provider using MPLS VPN has explained in GNS3 Software for better understanding the system. This research work would be helpful for service providers to provide their services for long distance customers with more security and QoS parameters.

Keywords: Multi-Homed Links, MPLS-Multi Protocol Label Switching, VPN-Virtual Private Network, BGP-Border Gateway Protocol, and QoS-Quality of Service.

I. INTRODUCTION

An Organization which is dealing with 1 main site and more remote sites would lease different types of WAN services to connect these sites such as frame relay, leased lines or Multiprotocol Label switching (MPLS). In other hand, there is another option to establish a connection between these remote sites through the internet. This can be done by high-speed internet access technology like cable or digital subscriber line (DSL). Therefore, the remote sites can send IP packets to each other over the Internet, Using the Internet as a WAN. But, like other WAN options and leased lines internet is not nearly secure because, it a public IP based communication system. But our Multi-Homed Inter-AS Provider is a Private IP based communication system.

Thus this proposed system could provide seamless advantages to the customers along with connection such are QOS parameters.

II. METHODOLOGY

A. Existing System:

Until now, Internet Service Providers (ISPs) providing different type of connections such are VPN only connections, Internet based MPLS connections based on layers i.e., L2 VPNs & L3 VPNs, MPLS VPN network connections.

Along with all these, the Internet based MPLS VPNs Inter provider connection (Multiple ISPs) which are in exercise currently. The main theme of this research work is that to implement Multi-Link (Multi-Homed) connection between the different ISPs over customer sites with Private IP address scheme by the agreement of each provider. Multi-Homed connection is a very good way for sharing the load. Basically, the traditional Inter-AS Providers are designed with single link connections. May delay of data transmission will occurs if there is a high traffic. Also, the data couldn't be transmit of the link has damaged. In our Multi-Homed Inter-As Provider MPLS VPN network, the load will be transmitted by any link which is free on the time of transmission. If traffic is too high, then both links will share the total data which would helpful for speed of transmission. Also, if any one of the links has damaged, then the information can send through the remaining link without disturbing the transmission. The brief description about methodology of our network is as follows.

B. Proposed System:

The main of our design system Multi-Homed Inter-AS (Autonomous System) based on MPLS VPN Technology is to overcome the problems such are Scalability, Quality of Service, Security which are occur in conventional communication system. Along with all these, this is MPLS VPN Based Multi-Homed Inter-AS system involves the load sharing possibility through multi links which is not available in Inter-Provider network. Thus, through this design the transmission rate (TR) can increase easily. Also, two VPN site customers belong to two different service providers can communicate with their remote branches at a time. Whole this communication can be done without compromising any Quality of Service (QOS) parameters, Security issues, and Scalability.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

M.Naga Kumari*, PG Student, Dept. of ECE, Sri Padmavathi Mahila University, Tirupati, nagakumari048@gmail.com.

T.S.Padmaja, Senior Assistant Professor, Dept. of ECE, Sri Padmavathi Mahila University, Tirupati, padmajats@gmail.com.

M.Devi Prasad, Sub Divisional Engineer, Admin in Networking, Regional Telecom Training Centre, Hyderabad, deviprasadmadiraju@gmail.com

Retrieval Number: K22130981119/2019©BEIESP
DOI: 10.35940/ijitee.K2213.1081219
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The stepwise technics or methods which are applied for proposed Multi-Homed MPLS VPN Based Inter-ISP Provider Network systems are as follows. The overall research work has done using the GNS3 Software. Over view of our Multi-Homed Inter-AS Provider using MPLS VPN Technology has shown in the fig 1.

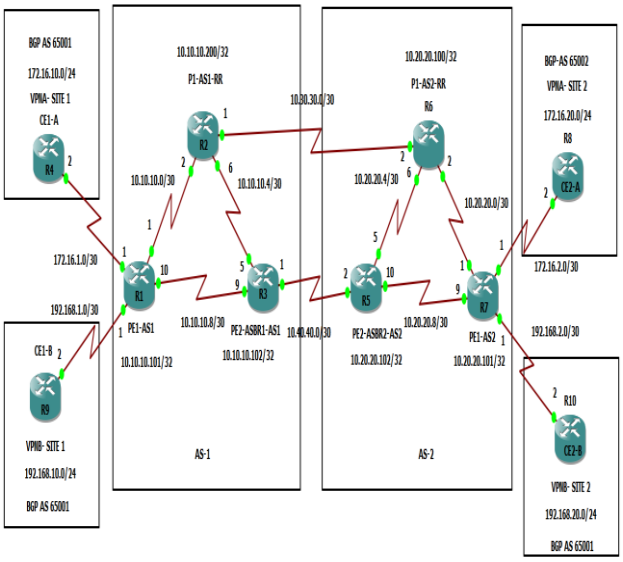


Fig.1. Multi-Homed Inter-AS Provider Using MPLS VPN Technology.

III. CONFIGUARATIONS OF INTERNAL SYSTEM

- **Network Topology:**

The proposed system Multi-Link Inter-AS Provider through MPLS VPN in network core is implemented using GNS3 Software. This network has implemented using 10 routers.

- **Routers**

Router is an electronic device which connects two networks. There are different types of routers are available for different applications in the market. Here, Both Service Provider networks are designed with Core, Distributive, and Access routers. VPN customer sites are connected to the edge routers. The functionality of each router of our Multi-Homed Inter-AS Provider is as follows.

- **P1-AS1-RR and P1-AS2-RR**

Here, both P1-AS1-RR and P1-AS2-RR are core routers. To reduce iBGP (Internal Border Gate Way Protocol) mesh, the provider network uses the Route-Reflector (RR) method. Also, in the provider network, these core routers P1-AS1-RR and P1-AS2-RR serve as both Autonomous System Boundary Routers (ASBR) and Route-Reflectors (RR). They are connected with the networks as 10.10.10.200 and 10.20.20.200. Inter-As link network (MP eBGP) between these two core routers is 10.30.30.0. Here, we have selected the Cicso C3700 version router as core router in order to support MPLS BGP forwarding. In provider network 1 (AS1), the method we are using to distribute the next hop information in the provider network 2 (AS2) is “Inter-AS next-hop-self”.

- **ASBR1-AS1 and ASBR2-AS2:**

These two routers in the provider network also serve as Autonomous System Boundary Routers (ASBR). Like in core routers, here also we are using one option that is Inter-AS redistribute connected option in order to distribute the next hop to devices in provider network.

- **PE1-AS1 and PE2-AS2:**

These two are the Peer Routers in Autonomous System 1(AS1) and Autonomous System 2 (AS2). They are directly connected with the VPN Customer Sites. The information can be transmitted using VRF (VPN Routing and Forwarding) method.

- **CE1 and CE2:**

These are the VPN Customer Site routers. Here CE1 Customer Site 1 has connected to LAN (Local Area Network) network 172.16.10.0 and Site 2 has connected to LAN 172.16.20.0. Like that, CE2 customer 1 LAN network is 192.168.10.0 and customer 2 LAN network us 192.162.20.0.

- **Multi-Homed Links (Link A and Link B):**

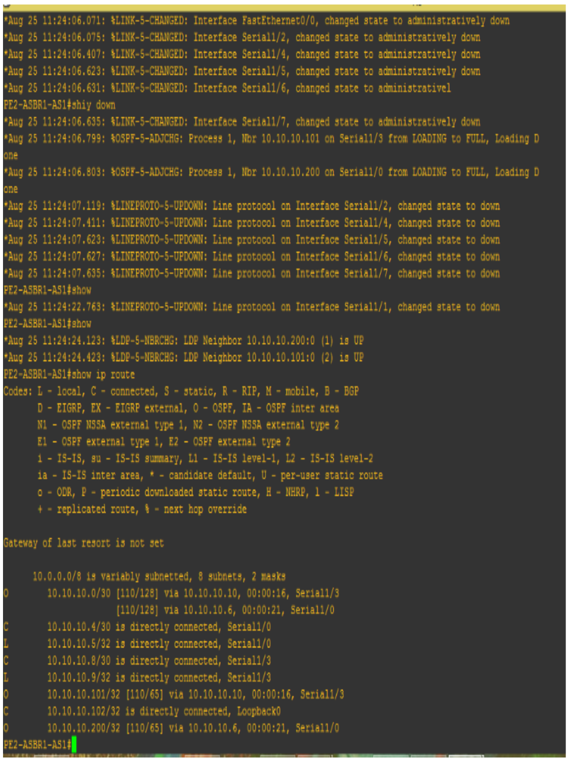
Inter-AS Link A is set up for Customer A to send their traffic. As well, Customer B can send their traffic using Inter-AS Link B. If anyone these links has goes down, then whole traffic can go through the operational link itself without disturbing the QOS parameters and security.

- **Open Shortest Path First (OSPF)**

In our Multi-Homed Inter-AS Provider Network, we are using the Open Shortest Path First (OSPF) Protocol. OSPF is an Interior Gateway Protocol. In the IP Datagram, the OSPF protocol number is 89 and its administrative distance is 110. In our design, OSPF has configured to every router in both Autonomous Systems expect VRF Customer sites. Through this, routers can send packets inside the Autonomous System. Routers can send the packets inside the Autonomous system using IGP of that AS. OSPF is a Link State Routing Protocol which is based on Shortest Path First Algorithm. In OSPF configuration, each router has the list of neighbors. This data base will be helpful to find the least cost path to reach the destination. How it is possible means, each router in network will sends the list of his neighbors to all the other routers. Therefore, when a router has received that information from all other routers, then it is ready to deduce the topology of the network, which will enable it. through the use of the Dijkstra algorithm, to find the least-cost path to any IP address on the entire network. If the AS is large, then, OSPF patrician the entire network into small area. Therefore, it is very useful establish the shortest path based on destination routers IP address. The OSPF Connections of each router in both Inter-AS provider networks are shown in the following figures.

- **OSPF Configuration results:**

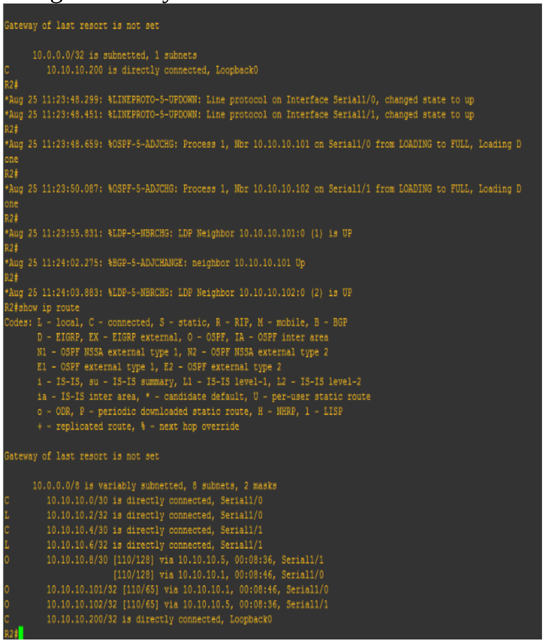
From the following figures, we can observe the OSPF connections with the neighbor routers of provider networks.



```
*Aug 25 11:24:06.071: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*Aug 25 11:24:06.075: %LINK-5-CHANGED: Interface Serial1/2, changed state to administratively down
*Aug 25 11:24:06.407: %LINK-5-CHANGED: Interface Serial1/4, changed state to administratively down
*Aug 25 11:24:06.623: %LINK-5-CHANGED: Interface Serial1/5, changed state to administratively down
*Aug 25 11:24:06.631: %LINK-5-CHANGED: Interface Serial1/6, changed state to administrativel
PE2-ASBR1-AS1#shiy down
*Aug 25 11:24:06.635: %LINK-5-CHANGED: Interface Serial1/7, changed state to administratively down
*Aug 25 11:24:06.799: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.101 on Serial1/3 from LOADING to FULL, Loading D
one
*Aug 25 11:24:06.803: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.200 on Serial1/0 from LOADING to FULL, Loading D
one
*Aug 25 11:24:07.119: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/2, changed state to down
*Aug 25 11:24:07.411: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/4, changed state to down
*Aug 25 11:24:07.623: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/5, changed state to down
*Aug 25 11:24:07.627: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/6, changed state to down
*Aug 25 11:24:07.635: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/7, changed state to down
PE2-ASBR1-AS1#show
*Aug 25 11:24:22.763: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed state to down
PE2-ASBR1-AS1#show
*Aug 25 11:24:24.123: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.200:0 (1) is UP
*Aug 25 11:24:24.423: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.101:0 (2) is UP
PE2-ASBR1-AS1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O        10.10.10.0/30 [110/128] via 10.10.10.10, 00:00:16, Serial1/3
                       [110/128] via 10.10.10.6, 00:00:21, Serial1/0
C        10.10.10.4/30 is directly connected, Serial1/0
L        10.10.10.5/32 is directly connected, Serial1/0
C        10.10.10.8/30 is directly connected, Serial1/3
L        10.10.10.9/32 is directly connected, Serial1/3
O        10.10.10.101/32 [110/65] via 10.10.10.10, 00:00:16, Serial1/3
C        10.10.10.102/32 is directly connected, Loopback0
O        10.10.10.200/32 [110/65] via 10.10.10.6, 00:00:21, Serial1/0
PE2-ASBR1-AS1#
```

Fig.2: PE2-ASBR1-AS1 OSPF Configurations

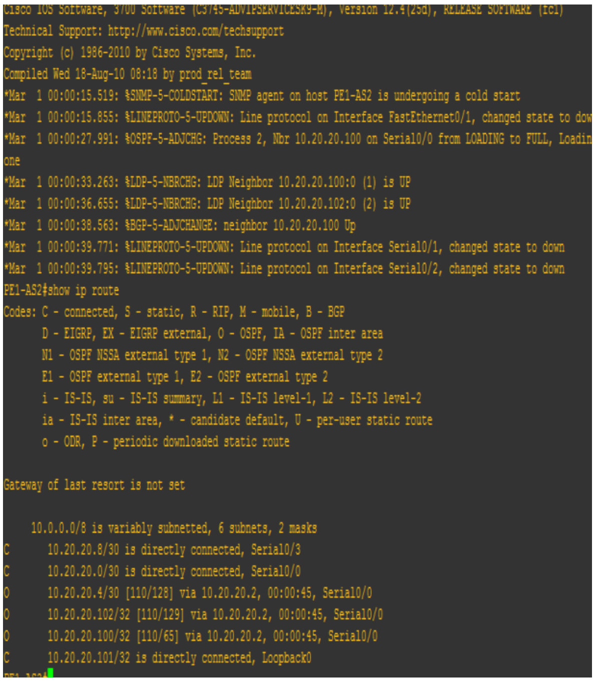
Fig.2. shows the Open Shortest Path First Configurations at PE2-ASBR1-AS1. As the PE2-ASBR2-AS2 router have same OSPF configurations with their neighbor routers in the provider network 2. From the above figure, we can observe that the PE2-ASBR1-AS1 is OSPF connection through 'O' symbol. PE2-ASBR1-AS1 has configured through OSPF protocol with the 10.10.10.100 & 10.10.10.200 routers. Remaining is directly connected.



```
Gateway of last resort is not set

      10.0.0.0/32 is subnetted, 1 subnets
C        10.10.10.200 is directly connected, Loopback0
R2#
*Aug 25 11:23:48.299: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
*Aug 25 11:23:48.451: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed state to up
R2#
*Aug 25 11:23:48.659: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.101 on Serial1/0 from LOADING to FULL, Loading D
one
R2#
*Aug 25 11:23:50.087: %OSPF-5-ADJCHG: Process 1, Nbr 10.10.10.102 on Serial1/1 from LOADING to FULL, Loading D
one
R2#
*Aug 25 11:23:55.831: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.101:0 (1) is UP
R2#
*Aug 25 11:24:02.275: %BGP-5-ADJCHANGE: neighbor 10.10.10.101 Up
R2#
*Aug 25 11:24:03.883: %LDP-5-NBRCHG: LDP Neighbor 10.10.10.102:0 (2) is UP
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C        10.10.10.0/30 is directly connected, Serial1/0
L        10.10.10.2/32 is directly connected, Serial1/0
C        10.10.10.4/30 is directly connected, Serial1/1
L        10.10.10.6/32 is directly connected, Serial1/1
O        10.10.10.8/30 [110/128] via 10.10.10.5, 00:08:36, Serial1/1
                       [110/128] via 10.10.10.1, 00:08:46, Serial1/0
O        10.10.10.101/32 [110/65] via 10.10.10.1, 00:08:46, Serial1/0
O        10.10.10.102/32 [110/65] via 10.10.10.5, 00:08:36, Serial1/1
C        10.10.10.200/32 is directly connected, Loopback0
R2#
```

Fig.3. OSPF Connections at P1-AS1

From the above Fig.3. We can observe how the Core Router in AS1 has configured with their neighbors through OSPF.



```
Cisco IOS Software, 3700 Software (C3745-ADVIPSERVICESK9-M), Version 12.4(25d), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 18-Aug-10 08:18 by prod_rel_team
*Mar  1 00:00:15.519: %SNMP-5-COLDSTART: SNMP agent on host PE1-AS2 is undergoing a cold start
*Mar  1 00:00:15.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to dow
*Mar  1 00:00:27.991: %OSPF-5-ADJCHG: Process 2, Nbr 10.20.20.100 on Serial0/0 from LOADING to FULL, Loadin
one
*Mar  1 00:00:33.263: %LDP-5-NBRCHG: LDP Neighbor 10.20.20.100:0 (1) is UP
*Mar  1 00:00:36.655: %LDP-5-NBRCHG: LDP Neighbor 10.20.20.102:0 (2) is UP
*Mar  1 00:00:38.563: %BGP-5-ADJCHANGE: neighbor 10.20.20.100 Up
*Mar  1 00:00:39.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to down
*Mar  1 00:00:39.795: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/2, changed state to down
PE1-AS2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.20.20.8/30 is directly connected, Serial0/3
C       10.20.20.0/30 is directly connected, Serial0/0
O       10.20.20.4/30 [110/128] via 10.20.20.2, 00:00:45, Serial0/0
O       10.20.20.102/32 [110/129] via 10.20.20.2, 00:00:45, Serial0/0
O       10.20.20.100/32 [110/65] via 10.20.20.2, 00:00:45, Serial0/0
C       10.20.20.101/32 is directly connected, Loopback0
```

Fig.4: OSPF Connections in PE2-AS2

- **Boarder Gateway Protocol (BGP):**

Here, in order to build a route within an Autonomous System (AS), also to route between AS's we configure the BGP protocol in the system. The current standard deployment is BGP Version4 (BGPv4). Every BGP Autonomous Systems are assigned with a particular Autonomous System Number (ASN), which is a 16-bit number ranging from 1-65535. Among that, there is a specific subset of this range that is 64512 - 65535 has been reserved for private (or internal) use.

- **BGP Implementation over MPLS VPN**

In MPLS VPN networks, BGP is largely used for PE-CE routing. As we said before, the current de facto Internet standard for Inter-domain (AS) exterior routing is BGP version 4(BGP4). MP-BGP is used and plays a vital role in the transportation of VPNv4 prefixes across the service provider network in MPLS VPN networks.

- **Multiprotocol Label Switching (MPLS) & Virtual Private Network (VPN)**

MPLS: The main concept behind our research work is Multiprotocol Label Switching. As, we all know MPLS is one of the data carrying method which lies between data link layer (Layer 2) and Network Layer (Layer 3). Thus it is referred as Layer 2.5 protocol. MPLS data carrying mechanism is such an efficient method in order to achieve security as well QOS. This packet forwarding MPLS Technic assigns labels at each router. Therefore, routers forward data to next router based on label address. Therefore, all packet forwarding decisions are based on Labels only.

MPLS supports any type of traffic in both circuit switched and packet switched networks. Labels send along with the packets. Such, each label has next hop address at which has to data transmit. Whenever, a router get label with packet, then, based on next hop address, it swap and push the label to next router. In this way labels are swapped, pushed, Pop to until reach the destination.

VPN: Virtual Private Network is a private communication between the two devices or remote in the public network virtually. Means, it is very secure way for remote sites to transmit their information. Simply, VPN is a IP based network which uses the public network paths and provides the protection and security to the private networks. It is the best technic for remote site communication for secure transmission.

- **MPLS VPN Architecture**

Simply the MPLS VPN network is a advancement of peer to peer (PE-PE) model. In the MPLS VPN backbone, the Customer Sites exchange Layer 3 customer routing information. In customer sites data is forwarded using the MPLS enabled SP IP backbone. In MPLS based VPN networks, provider assigns the IP to each of its customers in order to avoid the overlapping address spaces like in traditional Peer-Peer model. It supports the multiple customer connectivity in service provider's network.

- **Multi-Homed Inter-AS Provider using VRF Method**

Our main agenda of our Multi-Homed Inter-AS MPLS VPN provider is to establish a communication between two different ISP's and between remote sites. Therefore, these two different ISPs are located as one at metropolitan area and another one at remote area.

Therefore, the VRF (Virtual Route Forwarding) is one of the uncomplicated methods which allow MPLS VPN providers to exchange their Virtual Route Forwarding information between different Multi-Protocol Label Switching (MPLS) customer branches. In our design, the distributive routers i.e., PE1-AS1 and PE2-AS2 are located in AS1 and AS2. Here, these routers are interconnected with end sites of customer A and B. Then, VRFs are configured on PE1-AS1 and PE2-AS2 in order to connect with VPN client routes.

Each interface which is connected between the ASBRs is belongs to a single client VRF. In our design, this single client VRF can run RIPv2, EIGRP, eBGP, static routing or OSPF to distribute the VPN routes to its adjacent peer.

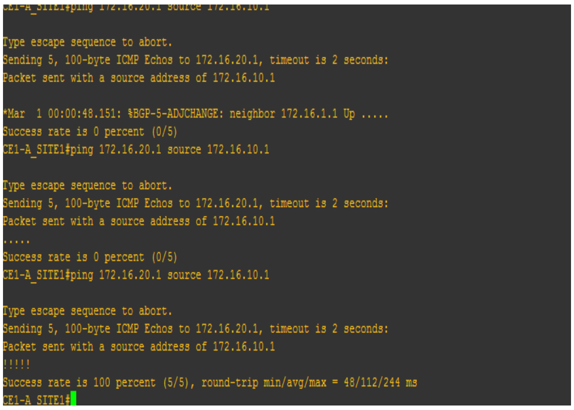
VRF is the best method to this type of application, retaining the type of the route and offering better security policy and scalability mechanisms. Between the two ASBR routers, the VPN routing information passed in IPv4 (version4) format. VRF configuration Routers in the network are configured with the following:

1) The autonomous systems provider edge routers numbered as AS 65001 and AS 65002 which are configured with MPLS using protocol(LDP) & also designed with BGP configuration.

2) Route reflectors which are used by each ISP are updated with IP ranges using BGP protocol. 3) Border routers (ASBRs) are configured with VRF thereby using BGP protocol.

IV. SIMULATION AND RESULT

- **Customer A Site 1 Data Forwarding Result:**



```
CE1-A_SITE1#ping 172.16.20.1 source 172.16.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.20.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1

*Mar  1 00:00:48.151: %BGP-5-ADJCHANGE: neighbor 172.16.1.1 Up .....
Success rate is 0 percent (0/5)
CE1-A_SITE1#ping 172.16.20.1 source 172.16.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.20.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
.....
Success rate is 0 percent (0/5)
CE1-A_SITE1#ping 172.16.20.1 source 172.16.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.20.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/112/244 ms
CE1-A_SITE1#
```

Fig.5.Data Forwarding from Customer Site 1 to Site 2

V. CONCLUSION

Our proposed Multi-Homed Inter-AS Provider system bears the interrelationship of different ISPs which are giving MPLS VPN services to geographically separated customer site branches. This system has developed on the Private IP range implication. Here, all the hosts and routers are designated with the Private IP addresses. Here, we can also connect the internet as the media between routers and hosts which is based on Public IP address range. As well, Internet is one of the very popular media where the number of companies using it. But there is a heavy risk in this Public IP connection. Therefore, unauthorized persons can hack the information in Internet-based connections easily. So, there is no guarantee for the security of customer's data while transmitting. One of the main agenda of this system is to provide secure transmission of information between customers. Here, it has achieved through the Private IP range connections.

Another unanimous advantage of our system is the Multi-Link connection between ISPs. Here, we established a multi-link connection between these two ISPs. Each link is assigned for each customer. If anyone of that link has damaged, then both customers traffic will go through the alternate link. As well, if there is heavy traffic at one link then both links will share the overall traffic.

Hence, the Customers A and B which are giving MPLS VPN services to their geographically separated branches can transmit their information safely, securely, and along with satisfying QOS parameters through our proposed Multi-Homed Inter-AS Provider System.

REFERENCES

1. *Wendell* Odom, "Virtual Private Networks" in Cisco CCENT/CCNA ICND1 100-101, Cisco press, 2013, pp. 1130 - 1144.
2. Umesh Lakshman, Lancy Lobo - CCIE No. 4690, "Inter-provider VPNs" in MPLS Configuration on Cisco IOS Software, Cisco press, 2005, pp. 455 - 507.
3. Chris Hoffman. (2013,Jan 15). "What Is a VPN, Why would I need one?" [Online]. Available: https://www.howtogeek.com .
4. Luyuan Fang, Nabil Bita et.al, "Interprovider IP MPLS services: Requirements, Implementations and Challenges", IEEE Communications Magazine, June. 2005.
5. Madhulika Bhandure et al., "Approach to build MPLS VPN using QOS capabilities", www.ijerd.com e-ISSN: 2278-067X, June 2013, Volume 7, Issue 8, pp. 26 - 32.
6. Tejender Singh Rawat et al., "A Review paper on MPLS VPN Architecture", www.ijetmas.com May 2015, Volume 3, Issue 5, ISSN 2349-4476 .

7. Vassilis Foteinos et al., "Operator-Friendly Traffic Engineering in IP/MPLS Core networks", Vol.11 No.3, 1932-4537 © 2014 IEEE. Personal use is permitted, but republication / redistribution requires IEEE permission,http://www.ieee.org/publications_standards/publications/rights/index.html for more information .

AUTHORS PROFILE

M.Naga Kumari currently pursuing Master of Technology in the department of Digital Electronics and Communication Systems from School of Engineering and Technology, Sri Padmavathi Mahila Viswavidyalayam. Tirupathi and her main research work focuses on communication, VLSI, and IOT based education.

T.Srinivasa Padmaja is currently working as a Senior Assistant Professor in ECE department, School of Engineering and Technology, Sri Padamavathi Mahila University, Tirupati. She has received her M.Tech from SRM University.

Devi Prasad Madiraju Working as Sub Divisional Engineer (Admin & Networking) Regional Telecom Training Centre, Gachibowli, Hyderabad, Telangana Circle. Worked as SDE Broadband node incharge in Hyderabad National Internet Backbone , Telephone bhavan, Hyderabad.