International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

UPGRADING INTERNET SERVICE PROVIDER USING MULTI-PROTOCOL LABEL SWITCHING AND VIRTUAL PRIVATE NETWORK

Swarnalatha M[1], Jaya Chandra Lekha T R[2] , Sree Vidya T R[3]

[1, 3] *Student, ECE, Valliammai engineering college, Chennai, India*
[2]*Assistant Professor, ECE, Saveetha engineering college, Chennai, India*

ABSTRACT: *This paper describes on a developing technique MultiProtocol Label Switching (MPLS) and virtual private network (VPN) to internet service provider domain. It reduces IP routing path promoting traffic engineering and guaranteed quality of service to the customer. With the help of autonomous system boundary router (ASBR) the private customer are connected to the service network. In this method the ASBR use MP-eBGP (MultiProtocol –Exterior Border gateway protocol) to exchange the routing information between autonomous system. The Virtual Routing and Forwarding (VRF) maintains the routing information of the neighboring customer sites and delivers the IP packets with unique addressing format . We came up with an idea of designing an upgraded Inter-provider service network (ie) connecting multiple ISP with the private network mechanism which provide global reachability. The simulations that are done in Graphical Network Simulator software (GNS3) are well suited for emulation of the real network environment. The resultant networks are obtained by verification command for check of the end to end connectivity and monitor the traffic flows.*

Keywords: *MPLS, Inter provider service, autonomous system, VRF method, MP-eBGP method*

1. INTRODUCTION

As the Internet uses the pubilc ip based communication system, it is facing more security issues though an adequate amount of security services were deployed. Our proposed Inter-AS or Inter-Provider VPN feature involves private ip based communication system. It provides the customers seamless advantages with connection as well as the (QOS)quality of services with the MPLS technology incorporated. So far there are many ISPs providing MPLS VPN network connections, VPN only connections, Internet based MPLS connections based on layers ie.,L2 VPNs & L3 VPNs. Also the Interprovider connection (Multiple ISPs) through Internet based VPNs using MPLS in the background which are in exercise currently [7]. This project's main theme is that we can incorporate the different ISPs to implement connection over customer sites private ip address scheme by the agreement of each provider.

1.1. Routing protocol

The routing protocol used to maintain the routing information of the network sites. It is mainly classified as static and dynamic method. In this paper we have used BGP (Border Gateway Protocol) [2] inside the autonomous system and MPLS (Multi Protocol Label Switching) to enhance the inter provider service in networks. According to the need of the customer, the routing protocols [13] are used to forwarding the packets with reduced delays.

1.2 MPLS VPN

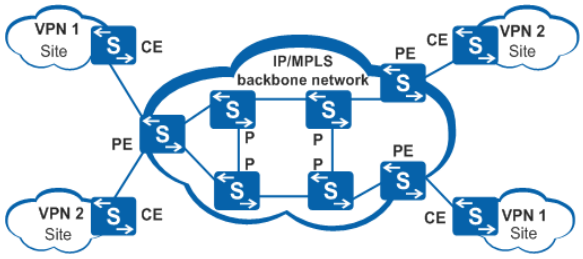

Figure 1 Flow chart of MPLS labeling

The figure 1 shows the devices on the MPLS VPN network such as customer edge (CE) and provider edge (PE). The provider (P) network forms the backbone of the IP/MPLS configuration where it provides the forwarding mechanism and does not maintain VPN information.

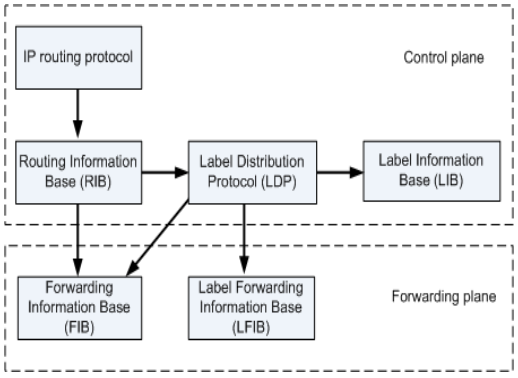

Figure 2 Flow chart of MPLS labeling

The above flow chart figure 2 explains the packet flow mechanism. In the control plane, the IP routing information flows to routing information base (RIB) for selecting the routing path. Allocation of the labels are done in [10] label distribution protocol (LDP).The upgraded information are processed in the forwarding information base (FIB) [15].

2. PROPOSED SYSTEM

The proposed system MPLS labels describes the packet switching technique while the previous work discussed about the circuit switching technique. They have Multi Protocol Label Switching (MPLS) and virtual routing forwarding (VRF) method to enhance the speed and connectivity with secure manner [7]. The forwarding packets between the autonomous system and inter provider service are enhanced. The router configuration are done with unique addressing format for transfer of packets

The above figure 3 shows the proposed enhance network with the router. The work of router are mentioned as R4,R8,R9,R10 – Private customer(VPN) ; R1, R2, R3 – Autonomous system 1 labeling protocol ; R5, R6, R7 – Autonomous system 2 labeling protocol; R3, R5 – virtual routing forwarding (VRF) method

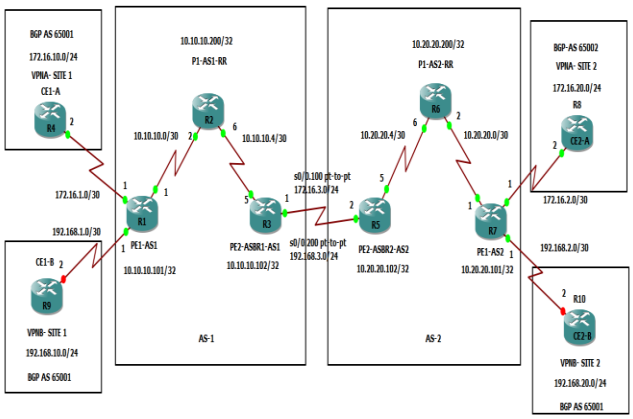

Figure 3 Proposed network

The development process contain autonomous system ,tunnel configuration, private customer configuration, routing protocol to check the connectivity the verifying commands are done in GNS 3 (graphical network system) software tool. The following development process are done to configure router in software tool for end to end connectivity of service provider

- IP addressing
- Routing protocol(BGP and OSPF)
- VPN customer connectivity
- Multi protocol label switching (MPLS) technique
- Tunnel by virtual routing forwarding (VRF)
- Autonomous system border router (ASBR)

IP addressing [R4] is done in all router with unique addressing and connectivity check by commands. Inside the autonomous system (open short path first) OSPF protocol is done in router (R1 , R2, R3, R5, R6, R7) used to update the routing table. Between the autonomous system (border gateway protocol) BGP protocol is done in router(R4 ,R8, R9, R10) are used to enhance the speed as discussed in the introduction section of this paper.

In MPLS labeling [14] are used and configured inside the autonomous system hence the configuration are in router(R1, R2, R3, R5, R6, R7) to enhance the proposed system. In order to maintain the security, virtual private customer are used to develop the forwarding packets. The configuration are done in customer router(R4, R8, R9, R10)To provide the inter domain service network, the virtual routing forwarding (VRF) [13] method is used with serial link of connectivity division in virtual manner to enhance the speed. The configuration is done in R3 and R5.

3. RESULTS AND DISCUSSION

Graphical network simulator (GNS 3) has the goal of helping our customers succeed in the networking domain. The simulations are undertaken for the complex networks, hence it is applied in the real time scenario.

3.1Border gateway protocol (BGP)

BGP is a standardized exterior gateway protocol (EGP), as opposed to RIP, OSPF and EIGRP which are interior gateway protocols (IGPs). BGP Version4 (BGPv4) is the current standard deployment. BGP is considered as a "Path Vector" routing protocol. The below figure 4 and 5 shows the BGP route of private customer B and A.

```
CE2-B_SITE2#
CE2-B_SITE2#sh ip bgp
BGP table version is 3, local router ID is 192.168.20.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.10.0     192.168.2.1                            0 2 1 2 i
*> 192.168.20.0     0.0.0.0                  0         32768 i
CE2-B_SITE2#
```

Figure 4 Customer B BGP route

```
CE1-A_SITE1#sh ip bgp
BGP table version is 3, local router ID is 172.16.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.10.0/24   0.0.0.0                  0         32768 i
*> 172.16.20.0/24   172.16.1.1                             0 1 2 65002 i
CE1-A_SITE1#
```

Figure 5 Customer A BGP route

BGP was not built to route within an Autonomous System (AS), but rather to route between AS's. BGP maintains a separate routing table based on shortest AS path and various other attributes, as opposed to IGP metrics like distance or cost. BGP is the routing protocol of choice on the Internet. Essentially, the Internet is a collection of interconnected Autonomous Systems.

3.2 Route Distinguisher (RD)

A route distinguisher is an address qualifier [14] used only within a single internet service provider's Multiprotocol Label Switching (MPLS) network. It is used to distinguish the distinct virtual private network (VPN) routes of separate customers who connect to the provider. The figure 6 shows the route distinguisher of Autonomous system to check the connectivity.

```
PE1-AS1#sh ip bgp vpnv4 all
BGP table version is 7, local router ID is 10.10.10.101
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:100 (default for vrf cust_A)
*> 172.16.10.0/24   172.16.1.2               0             0 65001 i
*>i172.16.20.0/24   10.20.20.102             0    100      0 2 65002 i
Route Distinguisher: 1:101 (default for vrf cust_B)
*> 192.168.10.0     192.168.1.2              0             0 65001 i
*>i192.168.20.0     10.20.20.102             0    100      0 2 65001 i
Route Distinguisher: 2:100
*>i172.16.20.0/24   10.20.20.102             0    100      0 2 65002 i
Route Distinguisher: 2:101
*>i192.168.20.0     10.20.20.102             0    100      0 2 65001 i
PE1-AS1#
```

Figure 6 RD of Autonomous area

3.3 Autonomous System Border Router(ASBR)

```
PE2-AS2-ASBR2#sh 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

     172.16.0.0/30 is subnetted, 1 subnets
C       172.16.3.0 is directly connected, Serial0/0
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O       10.20.20.0/30 [110/128] via 10.20.20.6, 00:33:48, Serial0/1
C       10.20.20.4/30 is directly connected, Serial0/1
C       10.20.20.102/32 is directly connected, Loopback0
S       10.10.10.102/32 [1/0] via 172.16.3.1
O       10.20.20.101/32 [110/129] via 10.20.20.6, 00:33:48, Serial0/1
O       10.20.20.200/32 [110/65] via 10.20.20.6, 00:33:50, Serial0/1
PE2-AS2-ASBR2#
```

Figure 7 ASBR route

Autonomous system boundary router shown in figure 7 is a router that is connected by using more than one routing protocol and that exchanges routing [11] information with routers autonomous systems. It typically also run an exterior routing protocol (e.g., BGP), or use static routes, or both.

3.4 MPLS labeling

Multi Protocol Label Switching (MPLS) [1] is a data-carrying mechanism in packet-switched networks. It operates at a layer that is generally considered to lie between traditional definitions of Layer 2 (data link layer) and Layer 3 (network layer or IP Layer), and thus MPLS is often referred to as a "Layer 2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients, which provide a datagram service model.[12]

The IP network has emerged as the network for providing converged, differentiated classed of services to user with optimal use of resources and also to address the issues related to Class of service (CoS) [9] and Quality of Service (QoS). MPLS is the technology that addresses all the issues in the most efficient manner. MPLS is a packet-forwarding technology that uses labels to make data forwarding decisions.[10]

```
P1-AS1-RR#
P1-AS1-RR#sh mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
200    Pop tag     10.10.10.101/32  0          Se0/0       point2point
201    Pop tag     10.10.10.102/32  0          Se0/1       point2point
202    300         10.20.20.102/32  0          Se0/1       point2point
P1-AS1-RR#
```

Figure 8 Mpls Forwarding Table

A label is an identifier which indicates the path a packet should traverse. Label is carried along with the packet. The receiving router examines the packet for its label [3] content to determine the next hop. Once a packet has been labeled, the rest of the journey of the packet through the backbone is based on label switching.

```
P1-AS1-RR#sh mpls ldp neighbor
    Peer LDP Ident: 10.10.10.101:0; Local LDP Ident 10.10.10.200:0
        TCP connection: 10.10.10.101.646 - 10.10.10.200.58016
        State: Oper; Msgs sent/rcvd: 29/31; Downstream
        Up time: 00:17:56
        LDP discovery sources:
          Serial0/0, Src IP addr: 10.10.10.1
        Addresses bound to peer LDP Ident:
          10.10.10.1      10.10.10.101
    Peer LDP Ident: 10.10.10.102:0; Local LDP Ident 10.10.10.200:0
        TCP connection: 10.10.10.102.646 - 10.10.10.200.36336
        State: Oper; Msgs sent/rcvd: 29/29; Downstream
        Up time: 00:17:55
        LDP discovery sources:
          Serial0/1, Src IP addr: 10.10.10.5
        Addresses bound to peer LDP Ident:
          172.16.3.1      10.10.10.102    10.10.10.5
P1-AS1-RR#
```

Figure 9 LDP Neighbor

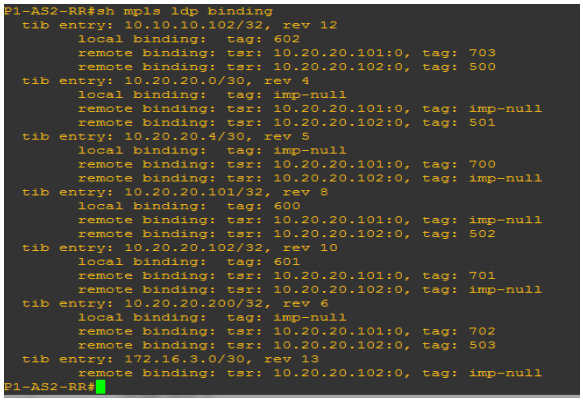

Figure 10 LDP Binding

3.5 VPN customer

The figure 11 and 12 shows VPN customer connectivity has been associated in the past with such remote connectivity services as the (PSTN), Public Switched Telephone Network but VPN networks have finally started to be linked with IP-based data networking [6]. Before IP based networking, corporations had expended considerable amounts of time and resources to set up complex private networks, now commonly called Intranets..

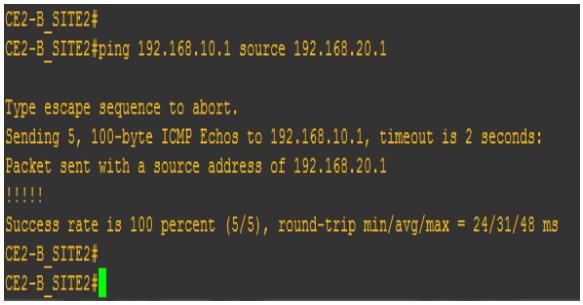

Figure 11 Connectivity of Customer A

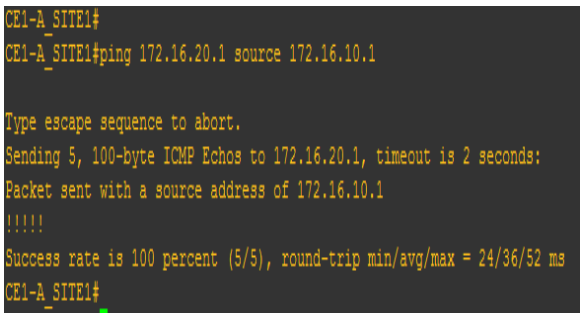

Figure 12 Connectivity of Customer B

4. CONCLUSION

This paper can be seen that privatization and security both are achieved in the network with minimum links and routers by implementing labeling technique and also measure of traffic [8] between inter- provider domain network . The packets in the autonomous systems can be transferred by multiprotocol label switching in high speed without delay to the service provider. The network is stimulated in GNS tool [5] and results are seen by verifying commands and also check the end to end connectivity of customers In future, designs of topologies are changed based on the customer capacity to enhance the networks. However, the upgraded protocols can also provide more advancement to the upgraded network. Later it becomes transparency, flexibility and high efficiency to the needs of the customer and the service provider.

REFERENCES:

1. Zhenxing song, P.W.C Prasad , “Upgrading Internet Service Provider(ISP) Network in Multiprotocol Label Switching (MPLS) and Border Gateway Protocol(BGP) environment, IEEE conference ,2016

2. L. Lang, "BGP routing design and optimization of large scale network." 2015.

3. Ming-Song-Sun , “ Engineering Analysis and Research of MPLS VPN ”IEEE, 2013

4. M. J. Wood, and S. Sibrina,"Static, dynamic and intelligent VRF routing for services traffic" U.S. Patent, US 7792097 B1, 2013.

5. R. Tomar, H. Kumar, A. Dumka, A. Anand,"Traffic management in MPLS network using GNS simulator using class for different services" 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 978-9-3805-4416-8, 2015.

6. Y. Lan, C. Zhengshi, "The research on the OSPF security optimizing of Campus Network" 2015 International Conference on Network and Information Systems for Computers (ICNISC), DOI: 10.1109/ICNISC.2015.121, 2015.

7. R. Emiliano, and A, Mário "Automatic network configuration in virtualized environment using gns3" 10th International Conference on Computer Science & Education (ICCSE), DOI: 10.1109/ICCSE.2015.7250212 , 2015.

8. E. Rosen, “L3VPN Working Group K. Patel Internet-Draft Cisco Systems Intended status: Standards Track Y. Rekhter Expires, Juniper Networks, October 2, 2014

9. D. Awduche, "MPLS and traffic engineering in IP networks." IEEE Communications magazine, pp. 42-47, 1999.

10. Y. Rekhter, and R. Eric, "Carrying label information in BGP-4", RFC 3107, (2001).

11. Ivan Pepelnjak and Jim Guichard, “MPLS and VPN Architectures,”Cisco Press, March 2001.

12. E. Rosen, A. Viswanathan and R. Callon, “Multiprotocol Label Switching Architecture,” Internet Engineering Task Force, ,2001.

13. E. Rosen and Y. Rekhter, “BGP/MPLS VPNs,” Internet Engineering Task Force, RFC 2547, 1999.

14. T. Bates, R. Chandra, D. Katz and Y. Rekhter, “Multiprotocol Extensions for BGP-4,” Internet Engineering Task Force, RFC 2283, 1998.

15. Lan jun and Lin bi ying, “Research for Service Deployment Based on MPLS L3 VPN Technology,” in 2011 International Conference on Mechatronic Science, Electric Engineering and Computer, Jilin, China, 2011.