International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Implementation of IPv6 Internet Service with MPLS Networks and MPLSL3VPN Service in IPv6 Networks

R.Vinodkumar, S.Vijayalakshmi, K.R.Kavitha, K.Karthick

Abstract— Exchanging the data packets seems as very challenging task due to exponential growth in network interface. Meanwhile, this increased interface makes use of next generation of internet protocol (IPv6) which will eventually replace the IPv4. Major issues in this replacement is the compatibility, both requires different set of routing protocols. Multi-Protocol Label Switching, a rapidly growing tele-communication infrastructure technology which works on special protocol suitable for both versions of Internet Protocol. MPLS uses the third OSI layer addressing coupled to second layer speed in switching and this paves the way for greater transfer of information, voice and video traffic. Virtual Private Network is the fastest growing technology for connecting the dispersed sites of same customer using the public network without any interference with other networks. This is an attractive technology to service providers because it enhances the flexibility for using variety of classes of services. This paper deals with the implementation of IPv6 networks for internet services using MPLS background which offers increased transfer in data, voice and video traffic. It also deals with, implementing MPLS based Virtual Private Network in IPv6 infrastructure using GNS3 simulator. This is done on behalf of the Border Gateway Protocol (BGP) which isolates the dispersed site in an Autonomous System (AS), connected to a public network.

Keywords—IPv6, Multi-Protocol Label Switching (MPLS), Virtual Private Network (VPN), Autonomous System (AS), Border Gateway Protocol (BGP).

I. INTRODUCTION

The age of automation begins with a great development in alleviating the work of humans. Such automation works under the greater information exchange between the needy and information may be any instructions, documents, files, etc. This information formulated is exchanged by a certain mechanism from one end to another end either in protected or unprotected manner. The exchanging mechanism needs some special devices/elements to connect each other. IoT uses the data for controlling and monitoring the physical world through collecting, processing and analyzing the data generated by IoT sensors and it finds exponential growth [2].

Manuscript published on 30 September 2019
* Correspondence Author
Dr.R.Vinod kumar*, Department of ECE, Sona College of technology, Salem, Tamilnadu, India, vinodkumarr@sonatech.ac.in
Dr.S.VijayaLakshmi, Department of ECE, Sona College of technology,Salem,Tamilnadu,India,vijisaumiya@gmail.com
Dr.K.R.Kavitha, Department of ECE, Sona College of technology, Salem, Tamilnadu, India, kavithakrece@gmail.com
K.Karthick, Department of ECE, Sona College of technology,Salem,Tamilnadu,India,karhickvicky1103@gmail.com

Message formulated from the different devices are transformed to any other devices is governed by routers. A router is third layer device of the OSI model because its forwarding decision is based on the data/content present in the network layer.

Router performance varies for different routing protocol and it is based on throughput, delay, jitter and packet delivery ratio. Among various routing protocols RIPng is best [3]. These protocols not care about the about the host and it only concentrate about the best path establishments.

Routers makes use of the logical network address for the identification of service provider and receiver. Because of the exhaustion in IPv4 addressing, IPv6 is deployed. For some interfaces, there is a need in the address transformation. This transformation impacts on network performance (feature implementation and cooperation method for IP's), data security and economy [4].

For various Autonomous System, BGP distributes the VPN routing table information. The slow route convergence and slow route table is overcome by increasing the table sending rate and decreasing the table rate[7]. In case of Large scale BGP, matrix approach is used to record the IP prefix and to monitor each update[1]. MPLS is the rapidly growing technology for its multiple service and its flexibility in traffic management. MPLS network provides layer 2 switching speed and layer 3 addressing. MPLS network shows increased throughput and increased utilization in TCP network, when compared to non-MPLS networks[5]. For MPLS-VPN networks, security threats is due to route modification, traffic injection, denial of service[9].

II. MPLS-VPN

MPLS makes use of the labels and provides the high switching speed of data. Label switching occurs at the MPLS core network, apart from this IP packet switching is deployed. In FEC (Forward Equivalence Class), a group of packets share the same requirements for their transport. Two planes involved in the MPLS operations:1. Control plane exchanges the routing information with the other routers with the help of routing protocols,2. Data plane involves in forwarding the data packets as labelled IP packets.

VPNs were introduced to use common physical infrastructure to implement emulated point to point link between customer sites. VPNs are implemented in Overlay model and peer-to-peer model. Separation of customers routing information is done by using a dedicated PE router and this sometimes referred as dedicated PE peer-to-peer model.

It is not feasible to setup a dedicated PE router for every customer site.

MPLS based VPN architecture isolates the customer traffic on the same PE router and it accommodates customer by overlapping address spaces. MPLS VPN model consists of the Customer Edge (CE) router, Provider Edge (PE) router, Provider (P) router. CE router only forwards the IP addresses and data to the PE routers and no modification is done at the CE router for MPLS VPN. PE routers performs the main function of isolating the customer traffic by assigning an independent routing table to each customer. P routers responsible for the label switching of packets and do not carry any VPN routes. For the large number of customer VPNs in various sites is configured with multiprotocol BGP.

Customer isolation is achieved by using Virtual Routing and Forwarding (VRF) tables. VRF is similar to global routing table, but it contains routing table for the specific VPN. VRF contains IP routing table, CEF table, list of interfaces, rules for routing protocol exchange and VPN identifiers Route Distinguishers (RD) and Route Targets (RT). An exact copy of routing protocol is required for each VPNs, this is achieved with the help of routing contexts. RD is the 64-bit unique identifier prepended by 32-bit customer route which makes it unique 96-bit address. RT helps in identifying VPN membership of the route learned from the particular site.

III. IMPLEMENTATION

A. IPv6 INTERNET SERVICE IN MPLS NETWORKS:

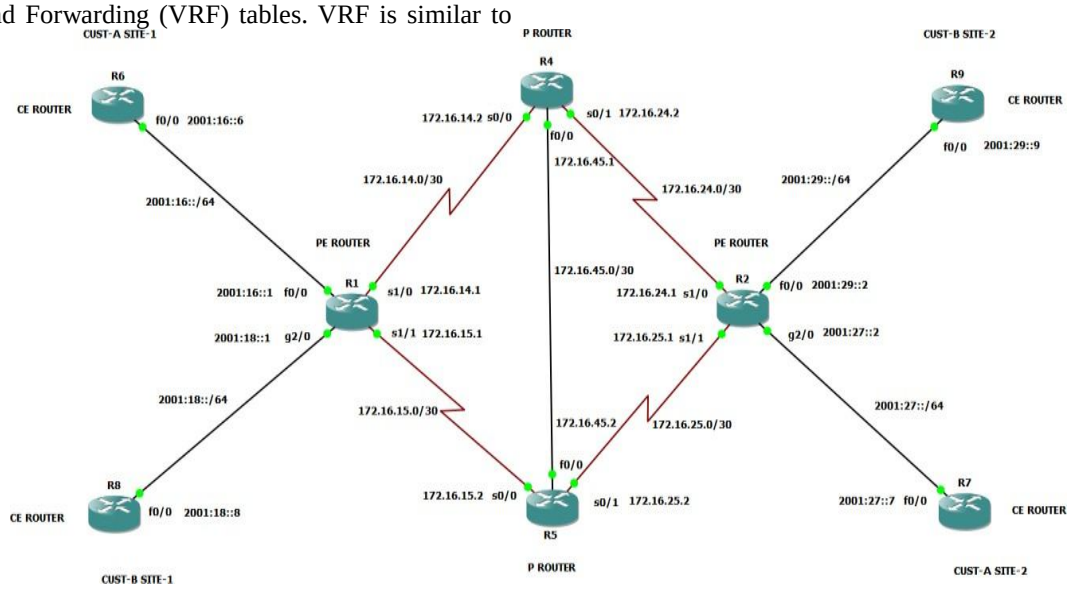

Figure 1. Implementation of MPLS6PE networks

The network consists of the various routers namely R1, R2, R4, R5, R6, R7, R8 and R9. Router R1, R2, R4 and R5 represents the MPLS service provider network. Other routers R6, R7, R8 and R9 acts as the customer network. Router R6 acts as the CE router to the site-1 of customer-A which away from the other sites of customer-A. Router R7 represents the CE router in site-2 of customer-A. Similarly, Routers R8 and R9 are the customer edge routers of the Customer-B in site-1 and site-2respectively. CE router is a dedicated router given to the customer site and is linked with the PE router of the Internet Service Provider (ISP). CE contains all the information about the IP interfaces in the site.

The provider network works with the MPLS network where the data packets are label switched with high speed. Routers R1 and R2 acts as the Label Edge Router (LER) where the ingress and egress of labels to the IP packets actually occurs. It is the edge router of the internet service provider network (PE router). Router R4 and R5 acts as the Label Switching Router (LSR), responsible for mapping of labels.

Provider network works on the basis of IPv4 only because capital investment for their network is high.

In this inter-network, all the customer edge router is able to communicate with each other. Also, the provider edge router contains all routing information about all the customer network linked with it. Router R1, R2, R6, R7, R8 and R9 will establish the connection with each other at any time. But the CE routers were unable to communicate with the LSRs, because they exist in the label switching and vice- versa. PE router is the only router able to communicate with the CE router and the provider (P) router. PE router works on the basis of the IP packets as well as the label packets.

When customer- A site-1 wants to communicate with the customer-A site-2, initially the data is converted in to data packets and each packet is encapsulated with the various layer headers and is forwarded to the CE router. This CE router forwards the IP packets to PE router, this router reads the IP address of the destination. Based on this IP address, the IP packet is encapsulated with a new label (ingress), further routing depends on the labels in the label switched paths. On reaching the provider core router (P router), swapping of label takes place to reach another core router and this continues until it finds the destination edge router (PE). At the PE router the removal of label (egress) results in IP packet delivery at that router. Finally, the IP packet is transmitted to the CE router of the Customer-A site-2 where the actual packet forward to destination interface.

The same process is undertaken, when any customer site (A/B) tries to communicate with all other customers in the Autonomous System (AS). But the routing information about the all customer site is with the PE router.

This sometime may cause insecure data transformation when route is exposed. To secure the routing information of the customers, a dedicated path is required. Installing a dedicated path over a long distance requires larger investments. To avoid this, a private path is constructed over the public network by Virtual Private Networks (VPNs) with the help of VRF, RD and RT.

B. MPLS VPN IN IPv6 NETWORKS:

MPLS VPN based IPv6 network consists of the CE, PE and P routers. Each router performs its own function as in MPLS internet services. Router R1 and R2 resembles the PE router where the IP packet is converted into labeled packet with specific VPN routing table.

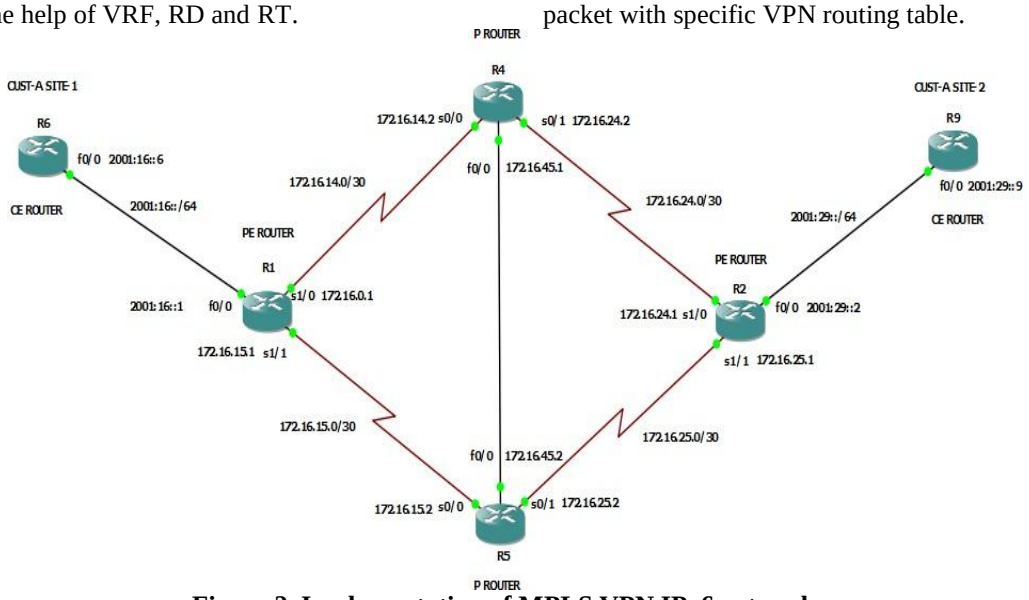

Figure 2. Implementation of MPLS VPN IPv6 networks

This VPN routing table isolates the customer traffic in the PE router. PE router is capable of working in the IP-based and label-based packets because of the routing protocol used in it. Router R4 and R5 is the core router of the service provider which works on the basis of the label switching by using the label switched paths. R6 and R9 is the CE router of the customer-A site-1 and customer-B site-2 respectively. R6 and R9 interfaces the end users in the customer sites and is able to collect the routing information of that interface. When a data is formulated from the end user, it directly reaches the PE router through the CE router. At R1, the IP s is converted into 24-byte unique address (RD) consists of 8- byte unique identifier pretended by 16-byte customer identifier (VPNv6).

The VPNv6 helps in identifying the customer in the customer network and by using the IP of the customer, the service provider is not able to reach the customer. For the identification of VPN membership, higher order 16 bits of BGP extended

PN membership of the specific site

(RT). The RT is appended to the customer prefix when it is converted to VPNv6 prefix by R1 router. MP-BGP is configured between the R1and R2 (PE) routers for exchanging the VPNv6 routes.

A VPN label is assumed for each VPN and is assigned for each prefix learned from CE router at the R1 (ingress PE) router. This label is propagated over the core network of MPLS service provider and the VPN label is only understood by the R2 (egress PE) router. In between the edge routers there is swapping of labels in the packets at the core router and proceeds to reach the destination path. At R2 the label is completely removed, the packet is forwarded to the desired destination. For each and every customer VPN network, there is separate VRF table, RT and RD, that is very useful to identify the customer in scalable network. In the same way, a customer in site-2 tries to communicate with site-1, it utilizes the VRF and RD taken from both sites through BGP.

IV.RESULT AND ANALYSIS

A. IPv6 INTERNET SERVICE IN MPLS NETWORKS:

The below results denote how the internet connection is established with each site.

```
R1#ping 2001:29::9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:29::9, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 240/311/420 ms
```

Figure 3. Connection between R1 and R9

Fig 3 shows that the connection is established between the R1and the R9.

```
R1#ping 2001:27::7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:27::7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 232/436/944 ms
```

Figure4. Connection between R1and R7

Fig 4. Shows the connection establishment between R1 (site-1) and R7 (site-2).

```
R2#ping 2001:16::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:16::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 152/220/320 ms
```

Figure 5. Connection between R2 and R6

Fig 5. Shows the connection is established from R2 (site-2) to R6 (site-1)

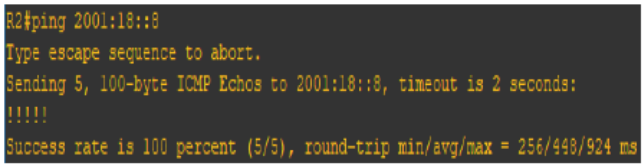

Figure 6. Connection between R2 and R8

Fig 6. Denotes the connection between the R2 and R8 routers.

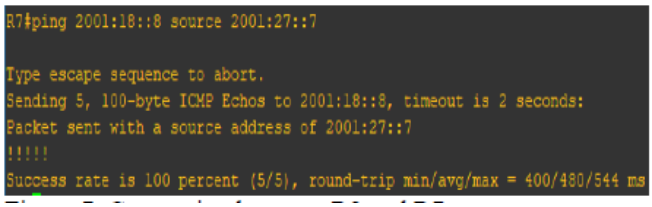

Figure 7. Connection between R8 and R7

Fig 7. Shows the connection between customer site (R8 and R7) with the different PE router.

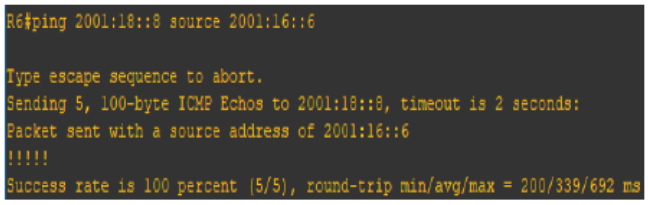

Figure 8. Connection between R8 and R6

Fig 8. Shows the connection between the customer site (R8 and R6) with the same PE router.

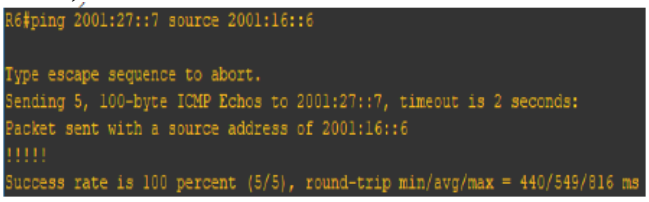

Figure 9. Connection between R7 and R6

Fig 9 shows the connection establishments between R7 and R6 through a PE router.

Figure 10. Connection between R8 and R4

Fig 10. Shows that the denial of connection between CE router (R8) and the MPLS core router (R4).

From the above results, the connection between customer sites are established irrespective of their sites. They can communicate with each other without any restrictions. But customer site is not able to connect with the MPLS core network.

B. MPLS VPN IN IPv6 NETWORKS:

The below results give the connection between the routers in the MPLS VPN IPv6 networks.

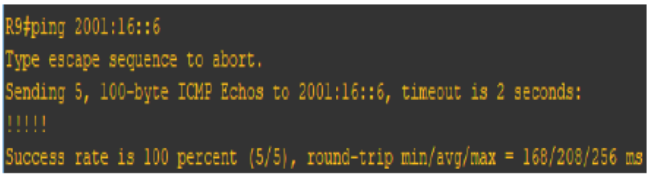

Figure 11. Connection between R9 and R6

Fig 11. depicts the connection between the customer site from R9 to R6 belong to a same customer.

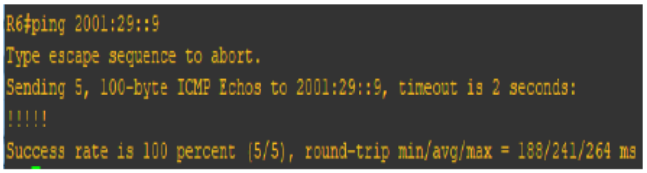

Figure 12. Connection between R6 and R9

Fig 12 shows the connection between the customer site from R6 to R9 which belongs to same customer..

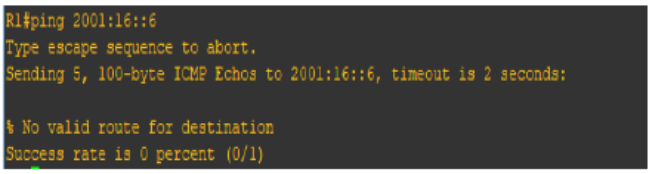

Figure 13. connection between R1 and R6

Fig 13 shows that there is no connection between the provider edge (R1)router and the customer edge (R6)router. Because the customer IP is converted to VPNv6 address, there is no way for R1 to communicate with R6 with the help of IP address of customer.

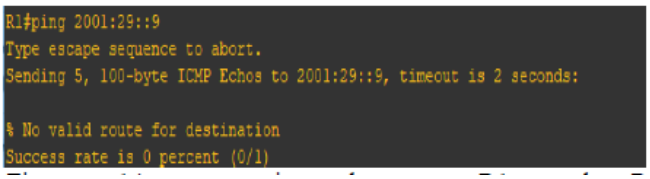

Figure 14. connection between R1 and R9

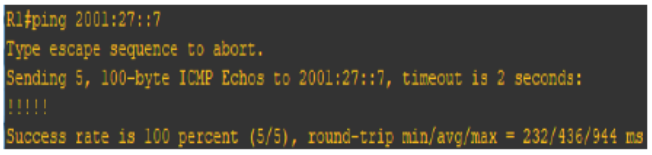

Figure4. Connection between R1and R7

Fig 4. Shows the connection establishment between R1 (site-1) and R7 (site-2).

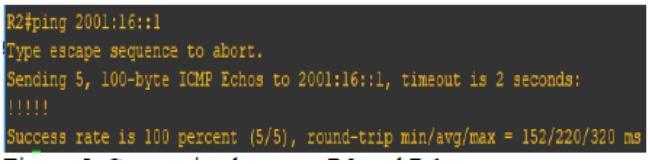

Figure 5. Connection between R2 and R6

Fig 5. Shows the connection is established from R2 (site-2) to R6 (site-1)

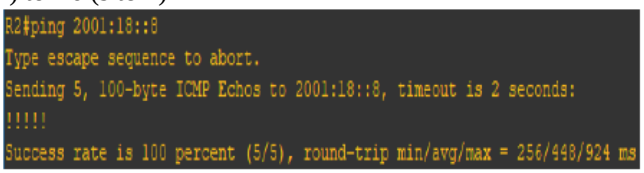

Figure 6. Connection between R2 and R8

Fig 6. Denotes the connection between the R2 and R8 routers.

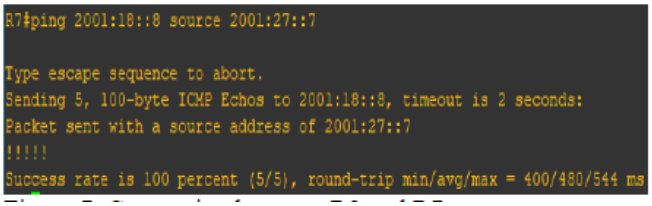

Figure 7. Connection between R8 and R7

Fig 7. Shows the connection between customer site (R8 and R7) with the different PE router.

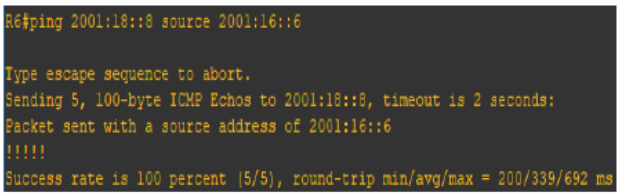

Figure 8. Connection between R8 and R6

Fig 8. Shows the connection between the customer site (R8 and R6) with the same PE router.

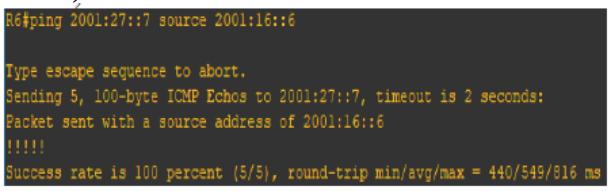

Figure 9. Connection between R7 and R6

Fig 9 shows the connection establishments between R7 and R6 through a PE router.

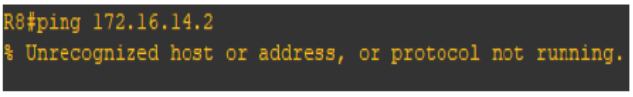

Figure 10. Connection between R8 and R4

Fig 10. Shows that the denial of connection between CE router (R8) and the MPLS core router (R4).

From the above results, the connection between customer sites are established irrespective of their sites. They can communicate with each other without any restrictions. But customer site is not able to connect with the MPLS core network.

C. MPLS VPN IN IPv6 NETWORKS:

The below results give the connection between the routers in the MPLS VPN IPv6 networks.

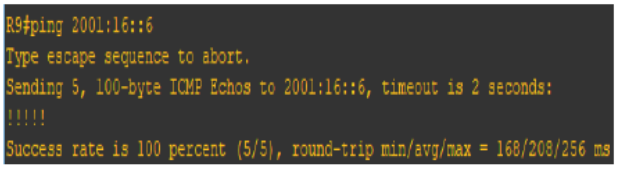

Figure 11. Connection between R9 and R6

Fig 11. depicts the connection between the customer site from R9 to R6 belong to a same customer.

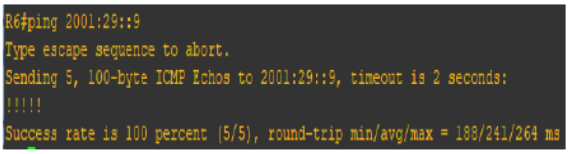

Figure 12. Connection between R6 and R9

Fig 12 shows the connection between the customer site from R6 to R9 which belongs to same customer..

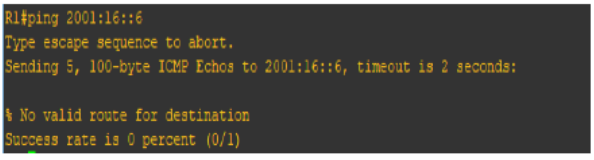

Figure 13. connection between R1 and R6

Fig 13 shows that there is no connection between the provider edge (R1)router and the customer edge (R6)router. Because the customer IP is converted to VPNv6 address, there is no way for R1 to communicate with R6 with the help of IP address of customer.

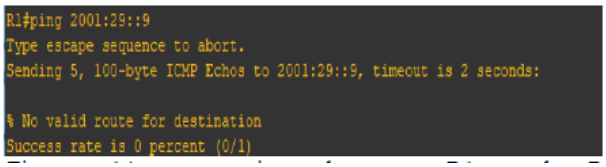

Figure 14. connection between R1 and R9

Fig 14 also shows denial of connection request from provider edge router R1 to Customer edge router R9 in site 2.

Based on the above results, it is clear from that the connection is established between same customer sites only. And there is no chance for the provider edge router to connect with the customer edge with IP address. This is because of each IP address is converted into VPNv6 identifiers by using the RD and RT.

V. CONCLUSION

The implementation of internet service in IPv6 network on the basis of MPLS path paves the way for the better speed in data transmission and helps in interconnecting the various sites belonging to different customers. Each and every router in the AS will able to communicate with each other except the core router of the MPLS networks. On the basis of the internet network, a new virtual private network is implemented in the IPv6 networks with the support of the MPLS networks. This network is able to accommodate a large number of interfacing nodes which will support the exponential growth in IoT.

REFERENCES

1. Meng Chen, Mingwei Xu, Qing Li, Yuan Yang, “Measurement of large-scale BGP events: Definition, detection, and analysis”, Computer Networks, Volume 110, 9 December 2016, Pages 31-45.
2. David Airehrour , Jairo Gutierrez ,Sayan Kumar Ray, “Secure routing for internet of things: A survey”, Journal of Network and Computer Applications, Volume 66, May 2016, Pages 198-213.
3. Dipti Chauhan, Sanjay Sharma, “Performance Evaluation of Different Routing Protocols in IPv4 and IPv6 Networks on the basis of Packet Sizes”, Procedia Computer Science, Volume 46, 2015, Pages 1072-1078.
4. StanfordL.Levin , StephenSchmidt,“ IPv4 to IPv6: Challenges, solutions and lessons”, Telecommunications Policy, Volume 38, Issue 11, December 2014, Pages 1059-1068.
5. Jasmina barakovic, Himzo brjric, Amir husic, “Multimedia Traffic Analysis of MPLS and non-MPLS Network”, 48th International Symposium ELMAR-2014
6. Vandana Kushwaha, Ratneshwer Gupta, “Congestion control for high- speed wired network: A systematic literature review”, Journal of Network and Computer Applications, Volume 45, October 2014, Pages 62-78.
7. Jian Mai and Jiang Du, “BGP Performance Analysis for Large Scale VPN”, Third international conference on information science and technology IEEE 2013.
8. Yimin Qiu, Hongbing Zhu, Yi Zhou Jinguang Gu, “A Research of MPLS-based Network Fault Recovery” ,Third International Conference on Intelligent Networks and Intelligent Systems IEEE 2010.
9. Denise Grayson, Daniel Guernsey, Jonathan Butts, Michael Spainhower, Sujeet Shenoi, “Analysis of security threats to MPLS virtual private networks”, International Journal of Critical Infrastructure Protection, Volume 2, Issue 4, December 2009, Pages 146-153.

AUTHORS PROFILE

Dr.R.Vinodkumar, Professor/ECE, SonaCollege of Technology, Salem. His area of interest is Wireless networks. He has published more than 25 international and National journals/Conferences.

Dr.S.Vijayalakshmi, AP/ECE, SonaCollege of Technology, Salem. Her area of interest is Digital Image Processing. She has published more than 20 international and National journals/Conferences.

Dr.K.R.Kavitha, Professor/ECE, Sona College of Technology, Salem. Her area of interest is Nano Electronics. She has published more than 25 international and National Journals/Conferences.

K.Karthick, PG Student, Sona College of Technology, Salem. His area of interest is wireless communication and networks.