IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 9, September 2021

DOI: 10.17148/IARJSET.2021.8966

ANALYSIS OF BORDER GATEWAY PROTOCOL WITH VIRTUAL ROUTING AND FORWARDING INSTANCES USING GRAPHICAL NETWORK SIMULATOR

T.L.Kayathri[1], Dr.N.Kumaresan[2]

[1]Ph.D. Scholar – Electronics and Communication Engineering, Anna University Regional Campus, Coimbatore, Tamilnadu

[2]Assistant Professor, Electronics and Communication Engineering, Anna University Regional Campus, Coimbatore, Tamilnadu

Abstract: In general routing protocols are classified as Interior gateway routing protocols and Exterior gateway routing protocols. IGP mainly suffers from link failure, inefficient bandwidth, slow convergence rate for larger networks, and requirement of larger memory. To overcome the drawbacks of IGP we are moving for EGP which consists of e-BGP. BGP is mainly used for supporting edge customer services such as exterior routing. For transporting VPNv4 services across the customer sites BGP is mostly preferred in MPLS VPN networks. By using MPLS VPN services in BGP, it provides consistent end-to-end connectivity for the customers. Since the same routing protocol is used between the customer and the service provider networks there is no need to use the concept of redistribution. Thus in this paper BGP peering with MPLS VPN environment is preferred in two different networks. The first method is BGP PE-CE VPN sites implementing unique AS numbers and the second method is BGP PE-CE VPN sites implementing same AS numbers. These methods can be implemented using Graphical Network Simulator3 software tool.

Keywords: IGP, EGP, BGP, MPLS, VPN, GNS3

1. INTRODUCTION

In the past few years the growth of e-business has improved the company's growth and efficiency with lower operating cost and increased customer satisfaction. Since most of the company's depends on e-business the network has become more vulnerable to security threats.

The main scope of this paper is to provide more secure transmission in very large scale networks. Different security technologies has been used to overcome the different security issues. The more secure transmission can be established by implementing BGP routing protocols using MPLS Layer 3 VPN PE-CE routing sites.

In Interior Gateway Routing Protocol one can select the best route among the competing routes by using metrics for each subnet. But in case of BGP, it exchanges the routing information by using the same general process used by IGPs, but with some differences of course. In order to start the BGP process, one router must have the knowledge about IPv4 prefix. It then makes use of BGP protocol message (a BGP update message) to exchange the routing information with another router. With BGP, the another router is referred to as BGP neighbor or BGP peer. A major difference with BGP compared to IGPs is that BGP advertises the routes to other routers in other companies , whereas IGPs advertise routes to other routers inside the same enterprise. The main aim for BGP is to support the case in which a customer obtains IP backbone services from a service provider or service provider with which it maintains contractual relationships. The customer may be a group of enterprises that need an extranet, an ISP, an ASP and another VPN service provider that uses an identical method to offer VPN'S to customer of its own. This method makes it very simple for the customer to use the backbone services with high scalable and flexible features for the service provider and it further allows the SP to add more values.

2. HUB AND SPOKE TOPOLOGY

The main aim of using the hub-and-spoke system topology is to prevent the local connectivity between subscribers at the spoke provider edge (PE) routers and to ensure that a hub site provides subscriber connectivity. Any sites which have the connection with same PE router must forward these information about intercede traffic using the hub site. This topology ensures that the routing at the spoke sites move from the access-side interface to the network-side interface or vice versa but never from the access-side interface to the access-side interface. A hub-and-spoke system topology allows us to maintain access restrictions between sites and prevents situations where the provider edge router locally switches the spokes without passing the traffic through the hub site. Thereby preventing the subscribers from directly connecting to each other. It does not require one virtual routing and forwarding instances for each spoke.

Interior Gateway Protocol (IGP) or external BGP (eBGP) sessions commonly made their installation via hub PE-CE links. All the exported route targets from all the spoke PE's were imported by VRF 2hub. The customer edge of hub learns all routes from the spoke sites and resends them back to the VRF 2spoke of the provider edge hub sites and finally the VRF 2spoke exports all the targeted routes to the spoke PEs. If we use eBGP between the hub PE and CE, we must have to reproduce the autonomous system (AS) numbers in the path which is typically prohibited.

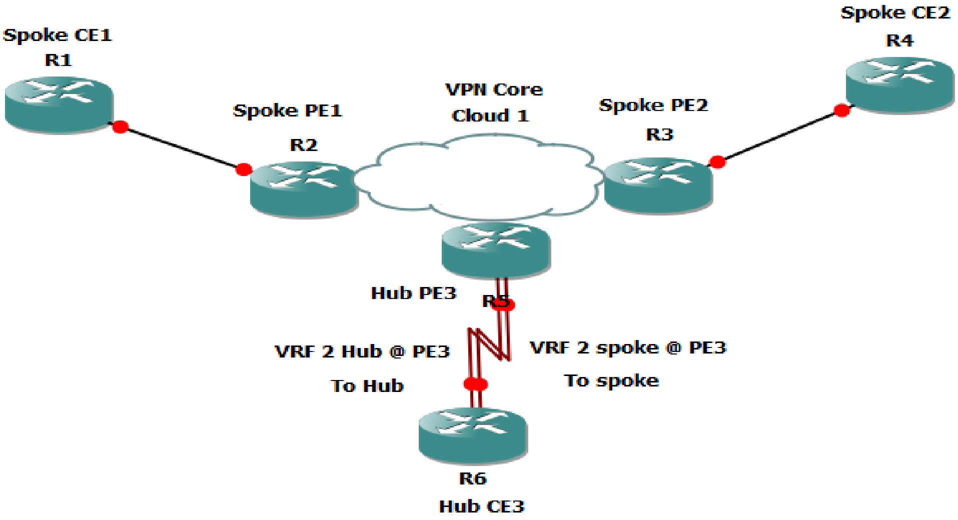


Fig. 1. Sample hub and spoke topology

From figure1, a hub-and-spoke topology is typically set up with a hub PE that is configured with two VRFs:
Connection -1 : VRF 2hub with a dedicated link connected to the hub customer edge (CE).
Connection -2 : VRF 2spoke with another dedicated link connected to the hub customer edge (CE).
Hence we will configure the router to allow this reproduced AS number at the neighbor of VRF 2spokes of the hub PE and also provide permission for VPN address family neighbors at all the spoke PEs. Further, we ought to disable the peer AS number check at the hub CE while distributing the routes to the neighbor at VRF 2spokes of the hub PE.

3. VIRTUAL PRIVATE NETWORK

A virtual private network is mainly considered as private data and voice network that uses the general public communication infrastructure. In VPN privacy is maintained by using security procedure and tunneling protocols. It is the cheaper alternative of, leased lines and the expensive owned networks, by using the shared public networks. In today's world companies are using VPNs for intranet and extranet for both voice and digital communication. The major classifications of VPN's are as follows:

3.1 Trusted VPN's

In Trusted VPN's the privacy can be maintained by legacy VPNs which was achieved by the service provider. It assures that the given circuit to the customer not be used by any other customer. It also permit customer to implement their own IP addressing scheme and security policies. In this case anyone who have physical access to the network can see the customer's traffic in service provider networks. Hence by using Trusted VPN's, the VPN customer must have the trust on the service provider that he will maintain the integrity of the communication link and uses best business practices to avoid security risks. Trusted VPNs are generally categorized into two types, they are layer 2 VPN and layer 3 VPNs.

3.2 Secure VPN's

By increasing the usage of Internet, companies started relying on Internet as a communication medium where customers and service providers were concerned with secure communication. Security is the major drawback in trusted VPNs, so the vendors started to create some protocols. These protocols contain some encrypting and decrypting technologies that

DOI: 10.17148/IARJSET.2021.8966

encrypt traffic at the edge of one network or at the originating device and transfer over the Internet like some other data and decrypt the data at receiving end of corporate network or at receiving end user device. The encrypted data transfer, ensures that the data is transferred in a secure tunnel between two networks. Even if unauthorized person sees the traffic, he cannot read it, and any change in data is not possible without the notice of legitimate person receiving the data, and will be rejected, if it is changed during transmission. “Secure VPNs” are the networks that are mainly constructed by using ‘encryption technologies’. They are generally classified into IPsec with Encryption in either tunnel or transport modes and IPsec Inside L2TP.

3.3 Hybrid VPN’s

In recent days service providers have begun to offer a trusted VPN by using Internet instead of the public switched telephone networks for communication. Even these type of trusted VPNs also had a drawback of real security, but it provide network segmentations for WAN. These VPNs can be controlled by single site and it also provide Quality of service guarantee. With these trusted VPNs, secure VPN can also be combined to provide security also and called hybrid VPNs. In Hybrid VPN’s security management can be achieved by customers himself or it can also be done by service providers. In general the part of hybrid VPNs are secure but it’s up to the customer security needs and full hybrid VPNs can be more secure. Hybrid VPNs are generally classified as any supported Trusted VPN combined with any secure VPN technology.

4. VIRTUAL ROUTING AND FORWARDING INSTANCES

An Internet Service Provider uses Virtual Routing and Forwarding (VRF) to separate one client’s routes from another’s and also use Multiprotocol Label Switching (MPLS) to ensure that the routes reach only the authorized remote sites. Without the knowledge provided by VRF, customers could not transmit private network routes between remote sites i.e., the ISP routers would have no way of knowing which route belongs to which customer. With the support from ISP edge routers, routes are first separated by the physical or logical interface on which they arrive after that the router then stores routes from each customer in a separate VFR routing table. Therefore different customers routing tables cannot mix with each other. On a very important note, the ISP edge router connecting to the local site forms an MPLS Label Switch Path (LSP) with ISP edge router connecting to the authorized remote site. An LSP looks like a dynamic PVC which makes the edge routers to mark packets with an MPLS label that directs them toward the other router through the LSP so that only Customer A sites receive Customer A routes.

5. MPLS LAYER3 VPN

Multiprotocol Label Switching can be enabled by IP networks in order to provide some additional services. The services may include virtual private networks (VPNs), by using OSI Layer 3 VPN packets or OSI Layer 2 VPN frames using MPLS labels. It also provides traffic engineering and some other services which are not available in traditional IP networks. All devices in the forwarding paths must support MPLS functionality in order to use MPLS technique. This condition is suitable for both the provider (P) core devices and for provider-edge (PE) devices. While using these conditions if MPLS supported features like MPLS VPNs or MPLS Traffic Engineering (MPLS TE) were utilized than all the participating devices must support these features. In general customer-edge (CE) devices do not support MPLS functionality, because MPLS switching is performed in the provider core network but some advanced solutions like Carrier Supporting Carrier [CSC] do require CE devices to support MPLS functionality.

By using Layer 3, MPLS VPNs provide VPN IP peering between VPN devices and provider devices. Privacy is the major concern that can be implemented using per-VPN routing tables (VRFs) which prevent different VPNs from being able to communicate. The basic characteristics of a Layer 3 MPLS VPN illustrates any-to-any connectivity can be provided to sites belonging to the same VPN. It also ensure optimal forwarding inside the MPLS backbone. However in traditional VPNs similar services can be implemented only by a full mesh of connections and the MPLS VPN backbone uses MP BGP to propagate VPN routing information across the backbone.

6. BORDER GATEWAY PROTOCOL

BGP is an external routing protocol as it allows different autonomous systems to exchange routes. It is the major protocol that most ISPs use, and it was designed to allow diverse, sometimes competitive organizations to communicate: In order to minimize the number of routes exchanged it encounter the filtering process for both the routes it receives and those that it sends according to bit length. It also uses policies to determine best routes rather than per-hop counts, like RIP does, or link states, like OSPF does. In BGP, autonomous systems can set their own policy and it’s routers can communicate only with manually configured neighbors. BGP can also configure different policies for route exchange with different neighbors. It runs in External BGP (eBGP), which is the protocol used to communicate between two autonomous systems, and Internal BGP (iBGP), which is the protocol that the AS uses to synchronize its own routing tables. On the Procure Secure Router, eBGP is intended to allow a private network to send and receive routes from remote sites through the Internet. The private network itself will run an IGP like RIP or OSPF. In Wide Area Network router runs BGP to communicate with the connecting ISP router, also called the ISP edge router. This ISP edge router tunnels the routes advertised by the local router through the Internet to the remote sites. Therefore the routers internal to the ISP run an internal routing protocol and do not receive the private routes and only the ISP routers that connect to routers at the private organization's remote sites can receive these routes, which they then pass to the private routers.

7. SIMULATION AND RESULT DISCUSSION

Here the network designed for BGP consists of six routers along with their routing updates. Each router in the network is connected by using serial ports. The simulation has been done using GNS3 simulator. The results of these simulation is shown as follows:

7.1 Simulation model for BGP using unique AS number

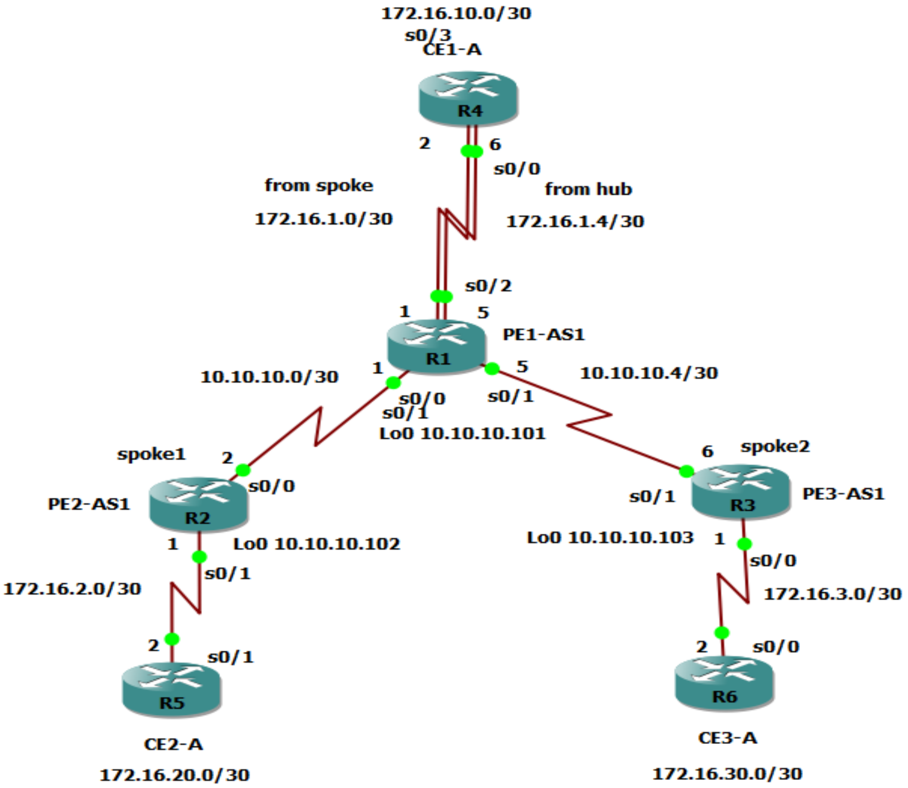
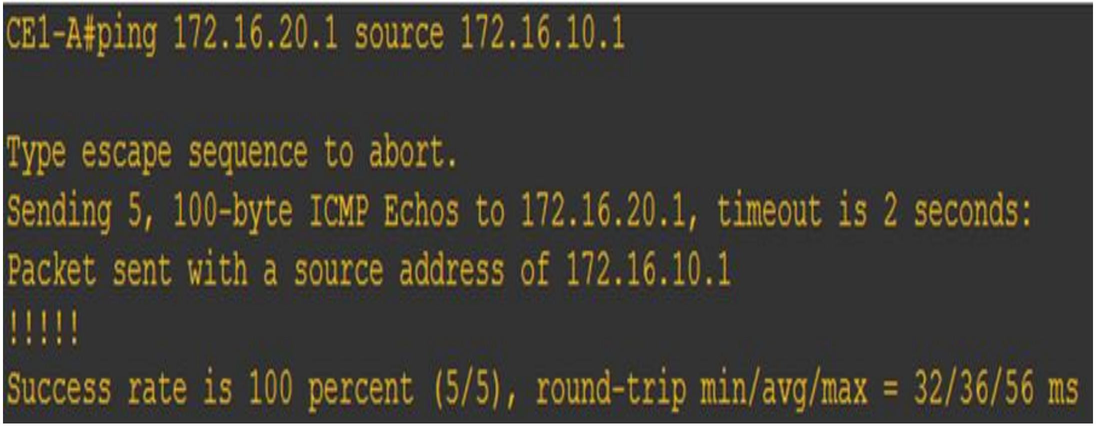


Fig. 2. Simulation model for BGP using unique AS number

DOI: 10.17148/IARJSET.2021.8966

7.2 Simulation result for BGP using unique AS number

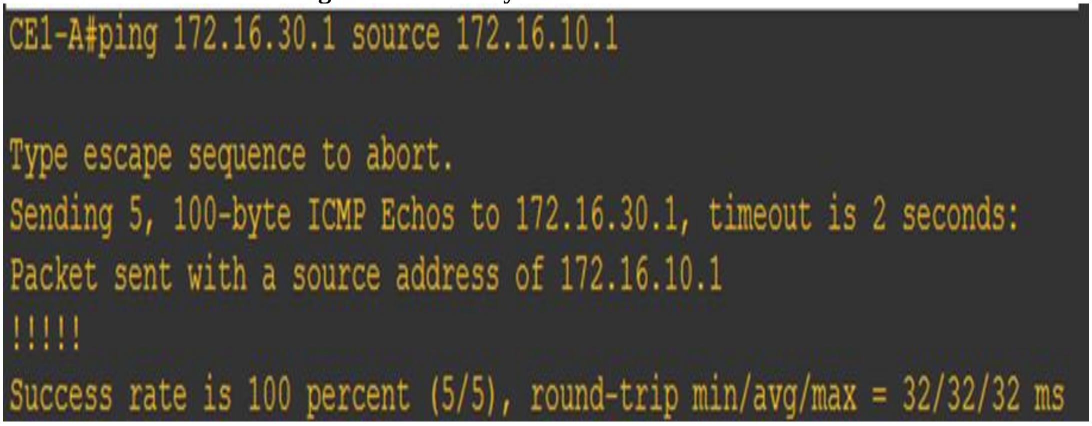
The simulation result for BGP using unique AS number is shown as follows:



```
CE1-A#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 = 32/36/56 ms
```

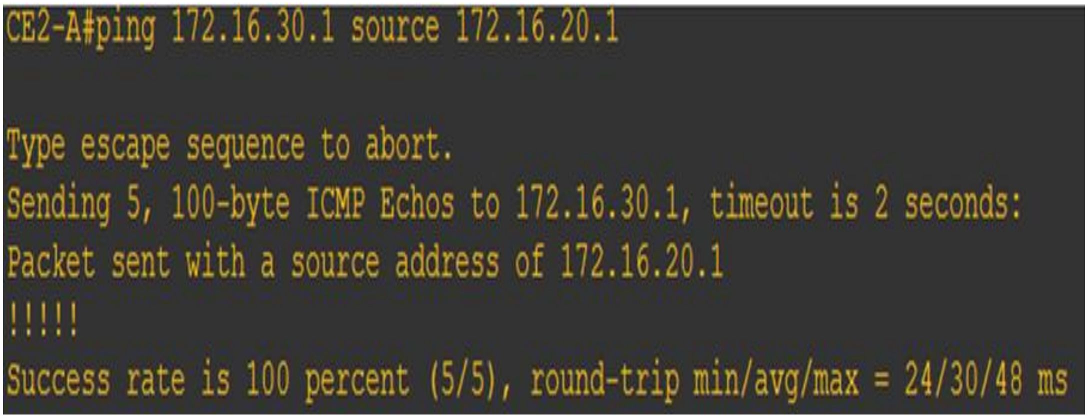
Fig. 3. Connectivity between customer 1 to 2



```
CE1-A#ping 172.16.30.1 source 172.16.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.1, 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 = 32/32/32 ms
```

Fig. 4. Connectivity between customer 1 to 3



```
CE2-A#ping 172.16.30.1 source 172.16.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/30/48 ms
```

Fig. 5. Connectivity between customer 2 to 3

Thus the simulation results shows the pinging configuration between the edge customers using BGP routing protocols for unique AS number.

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 9, September 2021

DOI: 10.17148/IARJSET.2021.8966

7.3 Simulation model for BGP using same AS number

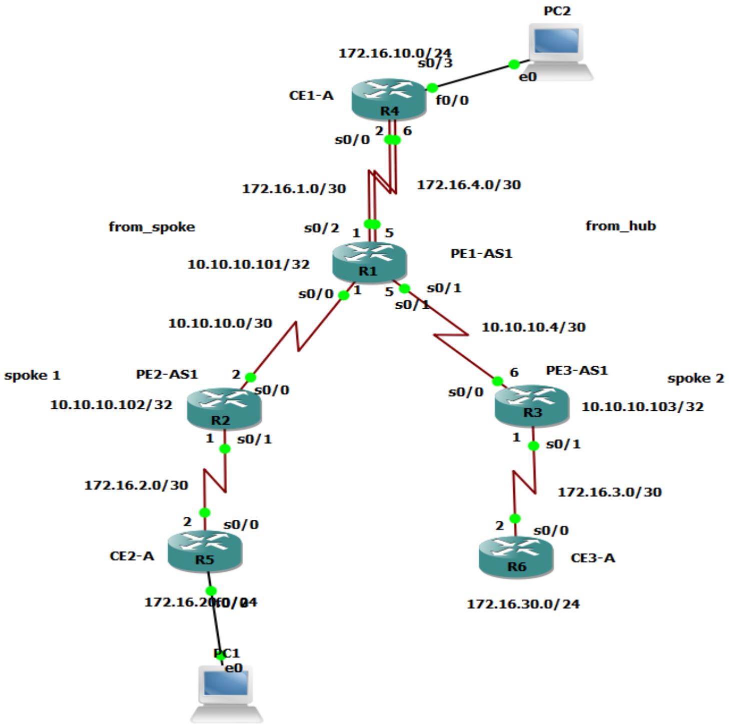
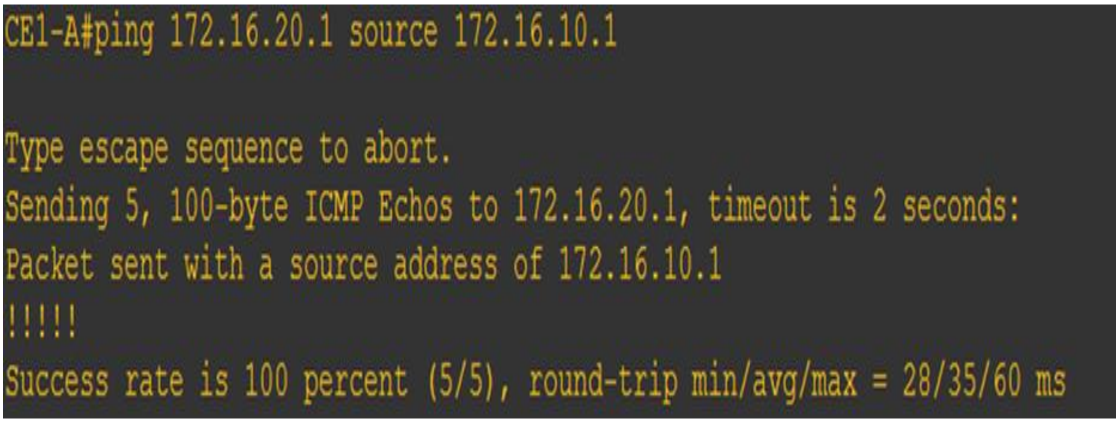


Fig. 6. Simulation model for BGP using same AS number

7.4 Simulation result for BGP using same AS number

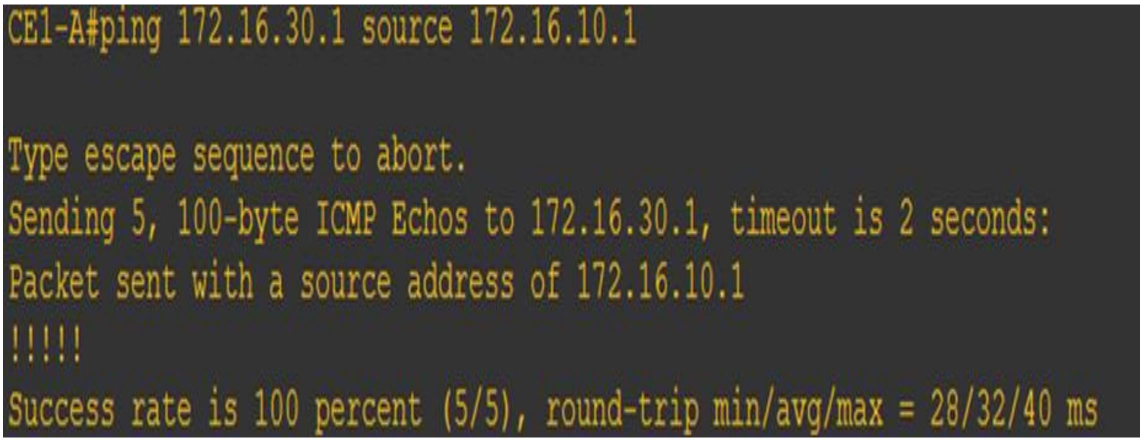
The simulation result for BGP using same AS number is shown as follows:



```
CE1-A#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 = 28/35/60 ms
```

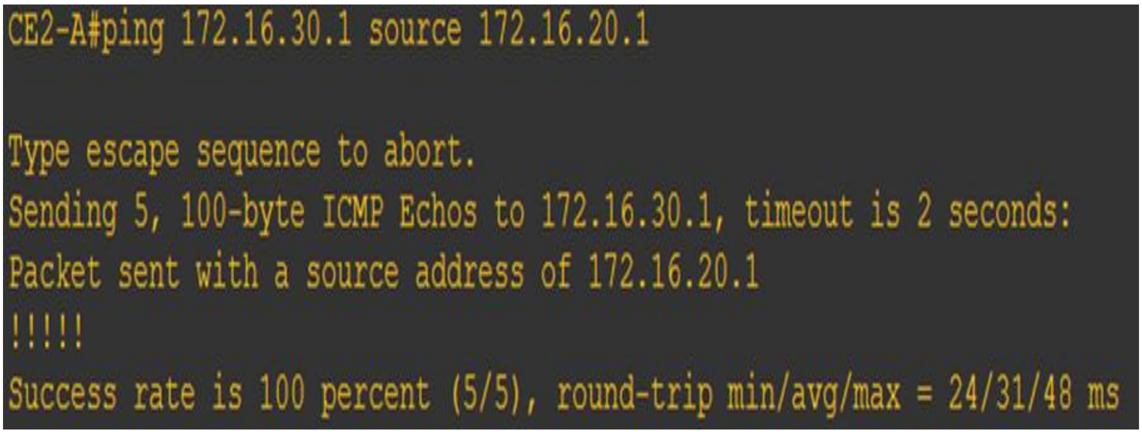
Fig. 7. Connectivity between customer 1 to 2



```
CE1-A#ping 172.16.30.1 source 172.16.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.1, 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 = 28/32/40 ms
```

Fig. 8. Connectivity between customer 1 to 3



```
CE2-A#ping 172.16.30.1 source 172.16.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/31/48 ms
```

Fig. 9. Connectivity between customer 2 to 3

Thus the simulation results shows the pinging configuration between the edge customers using BGP routing protocols for same AS number.

8. COMPARISON OF ROUTING PROTOCOLS

Table 1. RTT(ms) for BGP using Unique AS number

Round Trip Time(ms)	**Customer 1 to 2**	**Customer 1 to 3**	**Customer 2 to 3**
Min	28	28	24
Avg	35	32	31
Max	60	40	48

Table 2. Comparison of routing protocols

CHARACTERISTICS	RIP	OSPF	BGP
Type	Distance Vector	Link State	Path Vector
Default Metric	Hop Count	Cost	Multiple Attributes

Administrative Distance	120	110	20(External)
			200(Internal)

Hop count Limit	15	None	EBGP Neighbors: 1(default) IBGP Neighbors: None
Convergence	Slow	Fast	Average
Update Timers	30sec	Only when changes occurs (LSA table is refreshed every 30 mins)	Only when changes occurs
Updates	Full table	Only changes	Only changes
Classless	No	Yes	Yes
VLSM	No	Yes	Yes
Algorithm	Bellman ford	Dijkstra	Best path algorithm

Update Address	Broadcast	224.0.0.5(OSPF routers)
		224.0.0.6(DR'S & BDR'S)
			Unicast

Protocol & Port	UDP Port 520	IP Protocol 89	TCP Port 179
Proprietary	No	No	No
Interior/Exterior	Interior	Interior	Exterior
Summary	Auto	Manual	Auto

Table 3. RTT(ms) for BGP using Same AS number

Round Trip Time(ms)	Customer 1 to 2	Customer 1 to 3	Customer 2 to 3
Min	32	32	24
Avg	36	32	30
Max	56	32	48

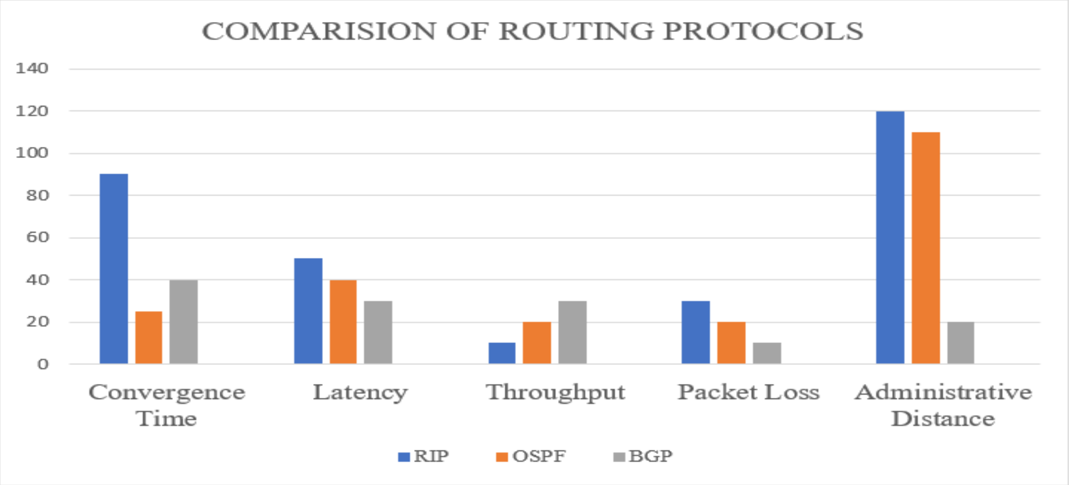


Fig. 10. Comparison of Routing Protocols (practically)

9. CONCLUSION

From the above simulation results it shows that BGP works well when compared with other routing protocols. As it has higher efficiency and throughput rate it provides excellent connectivity to the edge customer services for large enterprise networks. When comparing the simulation results for unique and same customer sites it is better to use same AS number for each customers in order to reduce the memory size and also to reduce the cost of the network.

REFERENCES

1. Armitage, Grenville. "MPLS: the magic behind the myths [multiprotocol label switching]." IEEE Communications Magazine 38.1 (2000): 124-131.
2. W Quoitin, Bruno, Cristel Pelsser, Louis Swinnen, Ouvier Bonaventure, and Steve Uhlig. "Interdomain traffic engineering with BGP." IEEE Communications magazine 41, no. 5 (2003): 122-128.
3. Chiussi, Fabio M., Denis A. Khotimsky, and Santosh Krishnan. "Mobility management in third-generation all-IP networks." IEEE Communications magazine 40.9 (2002): 124-135.
4. Che, Xianhui, and Lee J. Cobley. "VoIP performance over different interior gateway protocols." International Journal of Communication Networks and Information Security 1.1 (2009): 34.
5. Cianfrani, Antonio, Vincenzo Eramo, Marco Listanti, Marco Marazza, and Enrico Vittorini. "An energy saving routing algorithm for a green OSPF protocol." In INFOCOM IEEE Conference on Computer Communications Workshops, 2010, pp. 1-5. IEEE, 2010.
6. Bahl, Vasudha. "Performance Issues and Evaluation considerations of web traffic for RIP & OSPF Dynamic Routing Protocols for Hybrid Networks Using OPNET TM." International Journal 2, no. 9 (2012).
7. Jayaprakash, Mr R., and Ms K. Saroja. "RIP, OSPF, eigrp routing protocols." International Journal of Research in Computer Application and Robotics 3.7 (2015): 72-79.
8. Patel, Haresh N., and Rashmi Pandey. "Extensive Reviews of OSPF and EIGRP Routing Protocols based on Route Summarization and Route Redistribution." Int. Journal of Engineering Research and Applications 4.9 (2014): 141-144.
9. Van den Schrieck, Virginie, Pierre Francois, and Olivier Bonaventure. "BGP add-paths: the scaling/performance tradeoffs." IEEE Journal on Selected Areas in Communications 28.8 (2010): 1299-1307.
10. Kempf, James, et al. "OpenFlow MPLS and the open source label switched router." Proceedings of the 23rd International Tele traffic Congress. International Tele traffic Congress, 2011.
11. Calle, Eusebi, José L. Marzo, and Anna Urra. "Protection performance components in MPLS networks." Computer Communications 27.12 (2004): 1220-1228.
12. Hunt, Ray. "A review of quality of service mechanisms in IP-based networks—integrated and differentiated services, multi-layer switching, MPLS and traffic engineering." Computer Communications 25.1 (2002): 100-108.
13. Zhen Xing Song, P.W.C.Prasad, Abeer Alsadoon, L.Pham, A.Elchouemi,"Upgrading ISP network in MPLS and BGP environment." International Conference on Advances in Electrical, Electronics and system engineering (2016): 237-241.
14. Samiullah Mehraban, Prof. Komil.B.Vora, Prof. Darshan Upadhyay,"Deploy Multi Protocol Label Switching(MPLS) using VRF. "International Conference on Trends in Electronics and Informatics (2018): 543-548.
15. Vidhu Baggan, Pradeepta Kumar Sarangi, Devendra Prasad, Jyoti Snehi,"Augmenting BGP with MPLS for enhancing network path restoration. "International Conference on System Modelling and Advancement in Research Trends (2020).
16. Sri Vigna Hema V; Devadharshini S; Gowsalya P. "Malicious Traffic Flow Detection in IOT Using Ml Based Algorithms". International Research Journal on Advanced Science Hub, 3, Special Issue ICITCA-2021 5S, 2021, 68-76. doi: 10.47392/irjash.2021.142