IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Establishing VPN Connection Using IGP And BGP Routing Protocols.

[1]Mohammed Viquar Uddin, [2]Mirza Arbaz Ali Baig, [3]Mir Azher Ali Khan, [4]Mohammed Zaid

[1]B.E Student, [2] B.E Student, [3] B.E Student, [4] Assistant Professor

[1]Electronics and Communication,

[1]ISL Engineering College, Hyderabad, India.

***Abstract:*** This paper presents the performance of Virtual Private Network (VPN), Established through IGP- Interior gateway protocol and BGP- Border gateway protocol. The topology was simulated using GNS3 simulator. Which is a Graphical Network Simulator. Information is the true universal currency which we all carry with us every day. Thanks to how computer system connects us, we can share information globally, to share that information securely VPN connections are used widely. Which keeps your information secure and anonymous. Network testing such as ping command has been used to measure the connectivity as packet transfer. We have also analyzed a transmission of packet by using Wireshark tool. In this Paper we have established a VPN for a company whose head office is in Hyderabad and branch office is at Bangalore. A secure IPsec VPN tunnel has been created over a public network (Internet). This work is significant to forecast of network design and to analyze the performance of VPN.

***Index Terms*** **- Virtual private network-VPN, IGP, BGP Protocols, GNS3, ping command.**

## 1.INTRODUCTION

The Interior gateway protocol (IGP) is a dynamic route update protocol used between routers that run on TCP/IP hosts within a single autonomous system. The routers use this protocol to exchange information about IP routes. A network using IGP to route information within an autonomous system and EGP to route information between autonomous systems. Interior Gateway Protocols (IGPs) specify how routers within an autonomous system (AS) exchange routing information with other routers within the same autonomous system. This contrasts with Exterior Gateway Protocols (EGPs), which facilitate the exchange of routing information between different autonomous systems.

Routers use IGP when exchanging Internet Protocol data. A single adjustable formula combines for route comparison and creates IGP metrics.

The two IGP types are:

1. Distance-Vector Routing Protocol (DVRP): Uses the Bellman-Ford algorithm. Three core examples are RIP, Interior Gateway Routing Protocol and Enhanced Interior Gateway Routing Protocol.
2. Link State Routing Protocol (LSRP): Each router has access to all network topology data via the routing table. LSRP node transfers are used to construct connectivity maps. Examples include Open Shortest Path First and Intermediate System-to Intermediate System protocols.

**1.1 Routing Information Protocol (RIP)** is a dynamic protocol used to find the best route or path from end-to-end (source to destination) over a network by using a routing metric/hop count algorithm. This algorithm is used to determine the shortest path from the source to destination, which allows the data to be delivered at high speed in the shortest time. RIP plays an important role providing the shortest and best path for data to take from node to node. The hop is the step towards the next existing device, which could be a router, computer or other device. Once the length of the hop is determined, the information is stored in a routing table for future use. RIP is being used in both local and wide area networks and is generally considered to be easily configured and implemented.

**1.2 Enhanced Interior Gateway Routing Protocol (EIGRP)** Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance vector routing protocol based on the principles of the Interior Gateway Routing Protocol (IGRP). EIGRP is a successor to the Interior Gateway Routing Protocol (IGRP). Both are owned by Cisco and operate only on their devices. Cisco introduced EIGRP because it needed a protocol with faster converging abilities, route selection and calculation and the ability to record information from neighboring devices.

EIGRP has the following characteristics:

1. Advanced operational efficiency.
2. Capabilities of both link state and distance vector.
3. A classless routing protocols.

4. Unique features including use of Reliable Transport Protocol (RTP), a diffusing update algorithm (DUAL), updates and updated information about neighbors.
5. Faster converging because it precalculated routes and does not broadcast hold-down timer packets before converging.

**1.4 EIGRP** uses bandwidth, delay, load, and reliability to calculate the metric for its routing table (not hop count used by legacy protocols). For this reason, EIGRP always selects and calculates the most optimal route for efficiency. EIGRP uses a DUAL algorithm to avoid loops and send occasional hello packets to check the status of neighbor routers. Feasible and reported distance Two terms that you will often encounter when working with EIGRP are feasible and reported distance. Let's clarify these terms.

• Feasible distance (FD) – the metric of the best route to reach a network. That route will be listed in the routing table.
• Reported distance (RD) – the metric advertised by a neighboring router for a specific route. It other words, it is the metric of the route used by the neighboring router to reach the network.

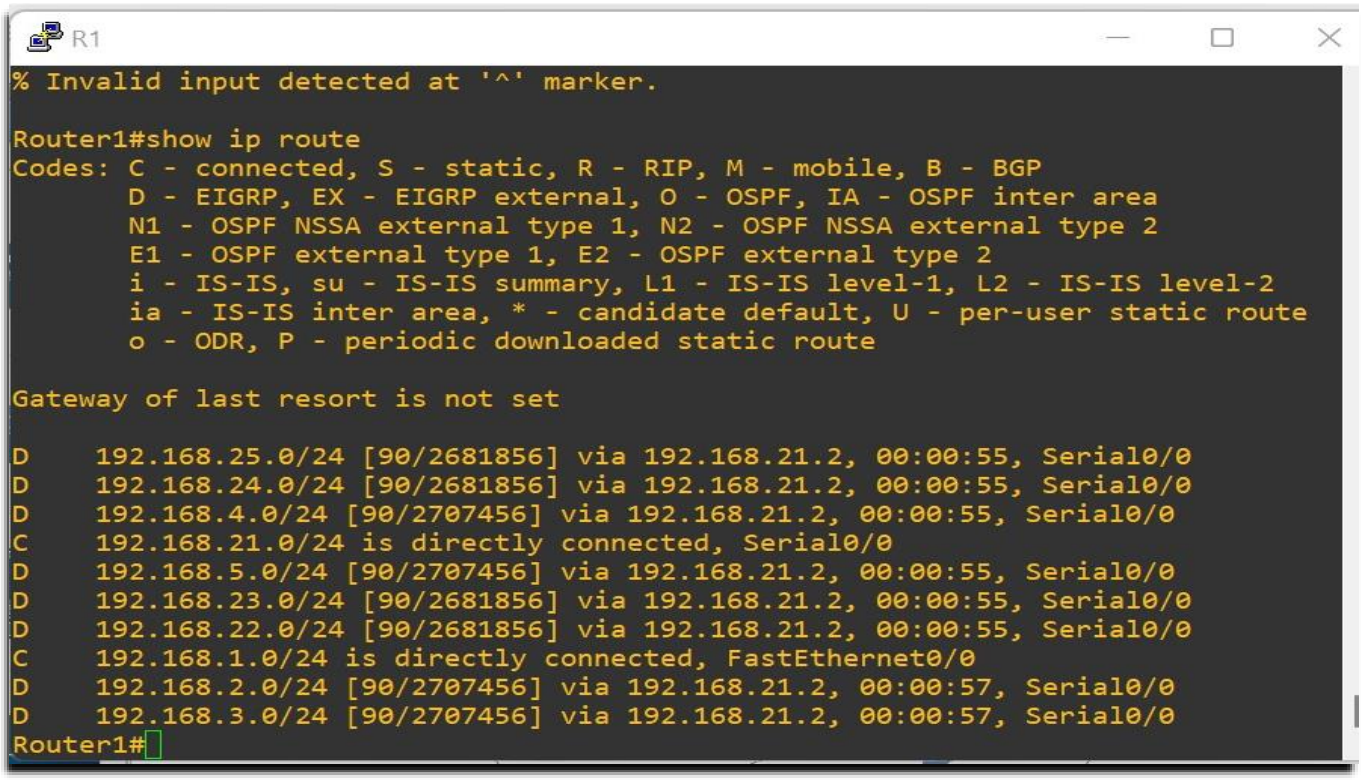



Figure 1: Router 1 EIGRP Routing Table

**Benefits of EIGRP**
• Enhanced Interior Gateway Routing Protocol converges at fast rapid times for the changes in the network topology.
• It makes use of link more effectively through (ECMP) Equal-Cost Multi-Path and unequal cost load sharing.
• It performs a much easier transition with a multi-address family.
• It supports both IPV4 and IPV6 networks.
• It provides encryption for security and can be used with iBGP for WAN routing.
• It reduces network traffic by making use of 'need-based' updates.
• Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance-vector routing protocol that is used on a computer network to help automate routing decisions and configuration.

**1.5 OSPF-Open Shortest Path First:**
The purpose of OSPF is to find the shortest way in a path network to the destination using minimum metric such as cost. If there are multiple routes to a network with the same route type, OSPF metric calculated as bandwidth based on cost used for selecting the best path with the lowest value of cost, the traffic will do a load balancing since it can support equal cost between the paths [2, 3]. OSPF has least cost of transmission with the maximum throughput by having equal cost to make the routing process faster and balancing the load equally on various paths [4]. To provide encrypt data in the private network, author mention in in his work that Virtual Protocol Network (VPN) tunnelling can secure the network topology and protect data in the network from fraud and misused data [5]. By implement GRE tunnel in the simulation environment from HQ to Branch office virtually involves creating tunnel interface from source to destination. Hence, many researchers come out with various types of solution to improve load balancing and encrypt data to overcome limitation and issues during transferring process to get better result. With load balancing techniques, a router can forward traffic across multiple path from source to a destination [6]. The cost of interface is inversely proportional to its bandwidth and the higher bandwidth indicates the lower cost in the path [7, 8]. It is based on an open standard. It can run on most routers. It uses the SPF algorithm to provide a loop-free topology. It uses both trigger updates and incremental updates to provide fast convergence. It supports VLSM and route summarization for a hierarchical design. It supports both versions of IP protocol. OSPFv2 supports IPv4 and OSPFv3 supports IPv6. It supports load balancing with equal-cost routes for the same destination. It supports networks of all sizes.

R11 - PuTTY

```
       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 3.0.0.1 to network 0.0.0.0

     3.0.0.0/24 is subnetted, 1 subnets
C       3.0.0.0 is directly connected, Serial0/0
     172.168.0.0/24 is subnetted, 11 subnets
O       172.168.4.0 [110/74] via 172.168.12.1, 00:00:14, Serial0/3
O       172.168.5.0 [110/74] via 172.168.14.1, 00:00:14, Serial0/5
O       172.168.6.0 [110/74] via 172.168.13.1, 00:00:14, Serial0/4
O       172.168.1.0 [110/74] via 172.168.10.1, 00:00:14, Serial0/1
O       172.168.2.0 [110/74] via 172.168.11.1, 00:00:14, Serial0/2
C       172.168.3.0 is directly connected, FastEthernet0/0
C       172.168.12.0 is directly connected, Serial0/3
C       172.168.13.0 is directly connected, Serial0/4
C       172.168.14.0 is directly connected, Serial0/5
C       172.168.10.0 is directly connected, Serial0/1
C       172.168.11.0 is directly connected, Serial0/2
S*   0.0.0.0/0 [1/0] via 3.0.0.1
R11#
R11#
```

Figure 2: Router 11 OSPF Routing Table

**Drawback of OSPF**

• It needs lots of information to calculate the best route for each destination. To store this information, OSPF consumes more memory than other routing protocols.

• To calculate the best route, it runs the SPF algorithm that requires extra CPU processing.

• It is complex to configure and difficult to troubleshoot. In a large network, only experienced network administrators can configure it. Since OSPFv1 has been updated and replaced by OSPFv2, network administrators commonly use the term OSPF to refer to OSPFv2. Because of this, unless the version of OSPF is explicitly mentioned, you can consider all references to OSPF to be OSPFv2.

**2. VPN-Virtual Private Network.**

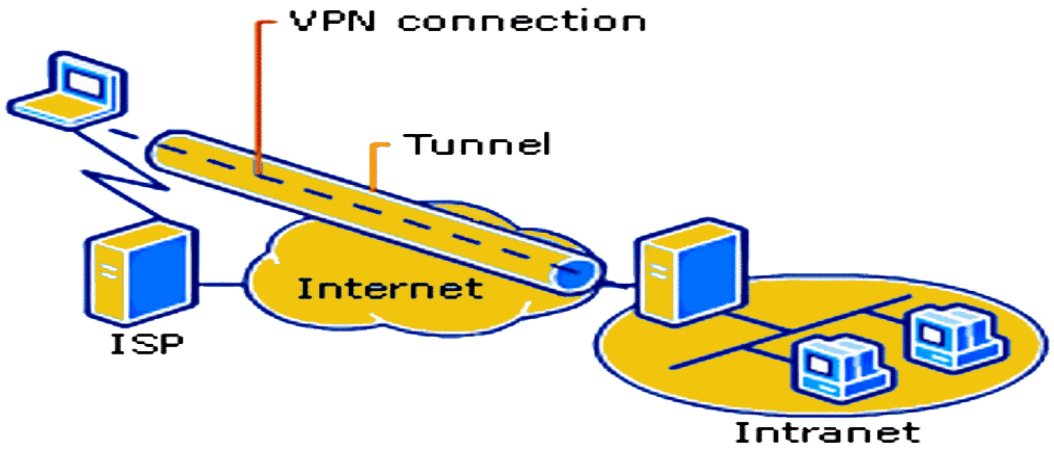



Figure 3: VPN Tunnel.

A Virtual Private Network (VPN) is used for creating a private scope of computer communications or providing a secure extension of a private network through an insecure network such as the Internet. VPN is a widely used in network security. VPN can be built upon IPsec or Secure Socket Layer (SSL). These are two fundamentally different approaches for building VPNs. In our work, we focused on the SSLbased VPNs which is often referred to as SSL VPNs. Designing and implementing the SSL VPNs exemplify a few security principles and technologies, including crypto, integrity, authentication, key management, key exchange, and Public-Key Infrastructure (PKI). To achieve this goal, we implemented a simple SSL VPN for Linux Ubuntu operating system.

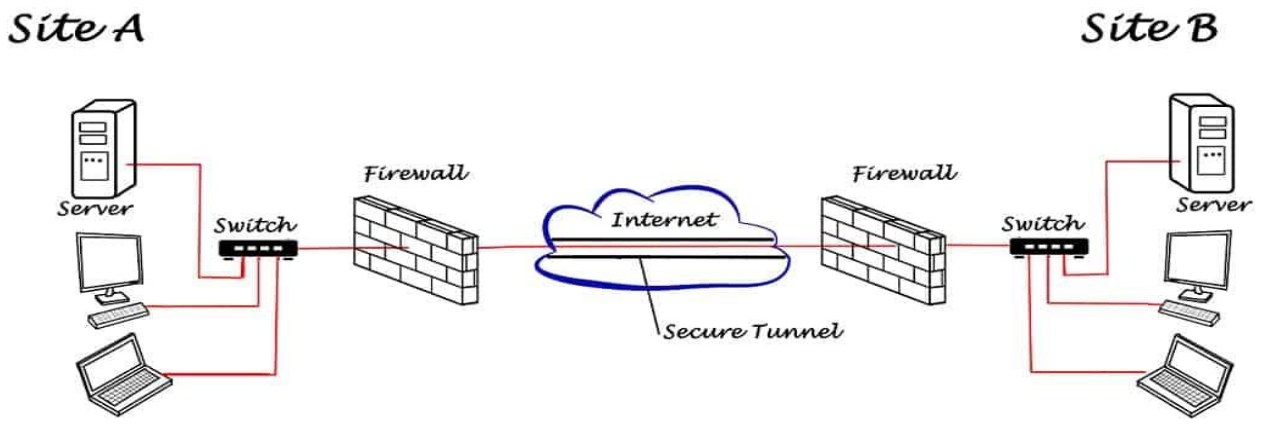



Figure 4: Site-to-site VPN Connection.

VPN- It replaces dedicated point to point links with emulated point to point links share common infrastructure. Customers Use VPN's primarily to reduce their operational cost.
**Examples: X.25, Frame-relay, ATM, GRE, DMVPN, IPSEC, MPLS, L2TPV3.**

**2.1 IPSEC VPN:**
Internet Protocol Security Virtual Private Network is a set of protocols developed by the internet engineering task force [IETF]. Which allows two or more hosts to communicate in a secure manner by authenticating and encrypting each IP packet of a communication session. IPsec is a framework of open standards for ensuring private communications over public networks. It has become the most common network layer security control, typically used to create a virtual private network (VPN). A VPN is a virtual network, built on top of existing physical networks, that can provide a secure communications mechanism for data and control information transmitted between networks. VPNs are used most often to protect communications carried over public networks such as the Internet.

- It supports Scales from small to very large networks.
- IPsec are available in Cisco IOS software version 11.3T and later.
- It also includes in PIX firewall version 5.0, ASA firewall.

A VPN can provide several types of data protection, including confidentiality, integrity, data origin authentication, replay protection and access control. Although VPNs can reduce the risks of networking, they cannot eliminate them.

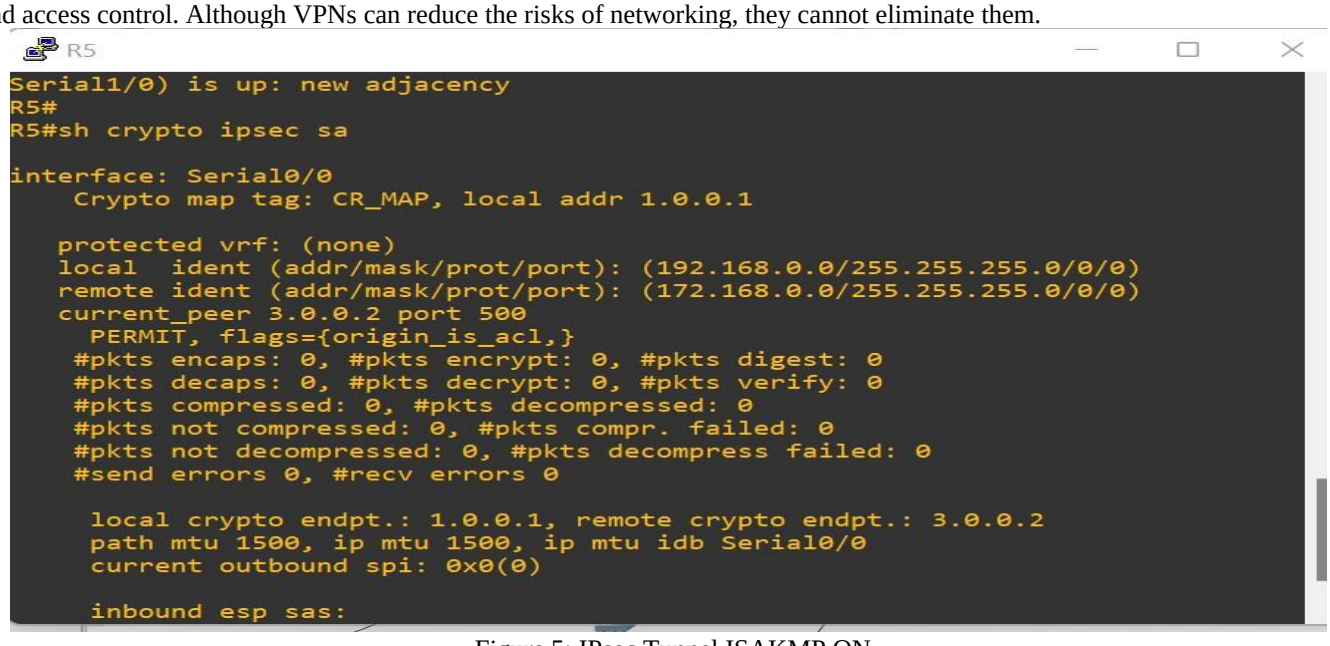
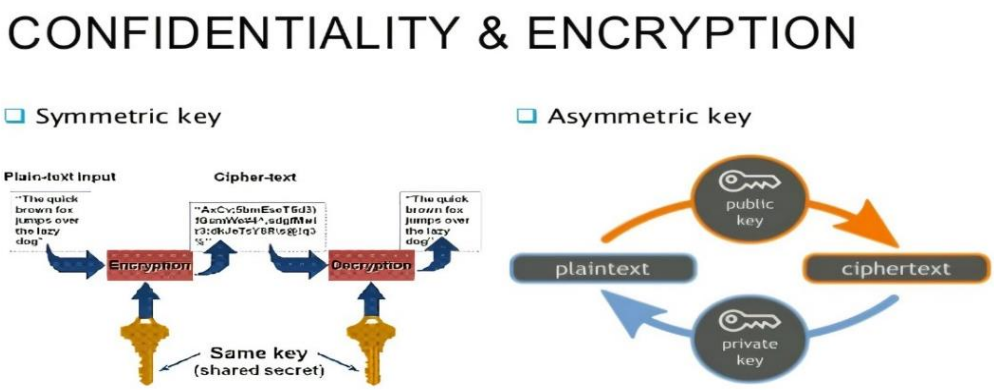



Figure 5: IPsec Tunnel ISAKMP ON

**2.2 IPSEC IS ONLY STANDARD LAYER 3 TECHNOLOGY THAT PROVIDES.**

- ✓ **Confidentiality**
- ✓ **Data Integrity**
- ✓ **Authentication**
- ✓ **Replay Detection.**

**Confidentiality:** IPsec uses encryption algorithms to prevent cybercriminals from reading the packet contents. Generally, in networking terminology confidentiality mean's the content are not visible to third parties.




**Data Integrity:** No one can Modify the data. Because of Hashing Algorithm is used. A VPN is a virtual network, built on top of existing physical networks, that can provide a secure communications mechanism for data and control information transmitted between networks.

**Authentication:** It is a method of verifying the peer. IPsec provides authentication for each packet, like a stamp of authenticity on a collectible item. This ensures that packets are from a trusted source and not an attacker.

**Replay** Detection: It means Ensuring packet received only once.

**Protocols are used in IPsec:** IPsec is not one protocol, but a suite of protocols. The following protocols make up the IPsec suite.

**Authentication Header (AH):** The AH protocol ensures that data packets are from a trusted source and that the data has not been tampered with, like a tamper-proof seal on a consumer product. These headers do not provide any encryption; they do not help conceal the data from attackers.

**Encapsulating Security Protocol (ESP):** ESP encrypts the IP header and the payload for each packet — unless transport mode is used, in which case it only encrypts the payload. ESP adds its own header and a trailer to each data packet.

**Security Association (SA):** SA refers to several protocols used for negotiating encryption keys and algorithms. One of the most common SA protocols is Internet Key Exchange (IKE).

**Internet Protocol (IP)** is not part of the IPsec suite, IPsec runs directly on top of IP.

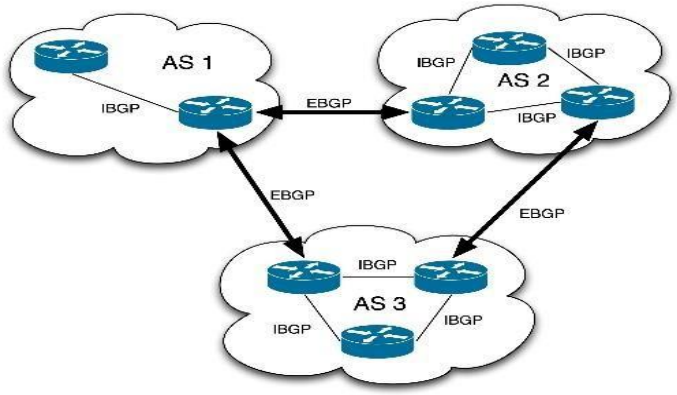
## 3. METHODOLOGY

Border Gateway Protocol (BGP) is used as an EGRP. Border Gateway Protocol (BGP) Means a gateway protocol that enables the internet to exchange routing information between autonomous systems (AS). As networks interact with each other, they need a way to communicate. This is accomplished through peering. BGP makes peering possible. Without it, networks would not be able to send and receive information with each other.
Inter-autonomous System Configuration BGP's *i*nter-autonomous system configuration allows it to make two autonomous systems communicate with each other. Otherwise, they would not be able to connect and share information.

Features of BGP:

- It is an Open Standard which means it can be run on any device.
- BGP is an Exterior Gateway protocol. Which means it will be going to exchange the routers between two or more AS-Autonomous Number System.
- It is designed for inter-AS domain routing.
- Designed to scale huge inter-network like internet.
- It is an Classless means supports FLSM, VLSM, CIDR, Auto and Manual Summary BGP-4.

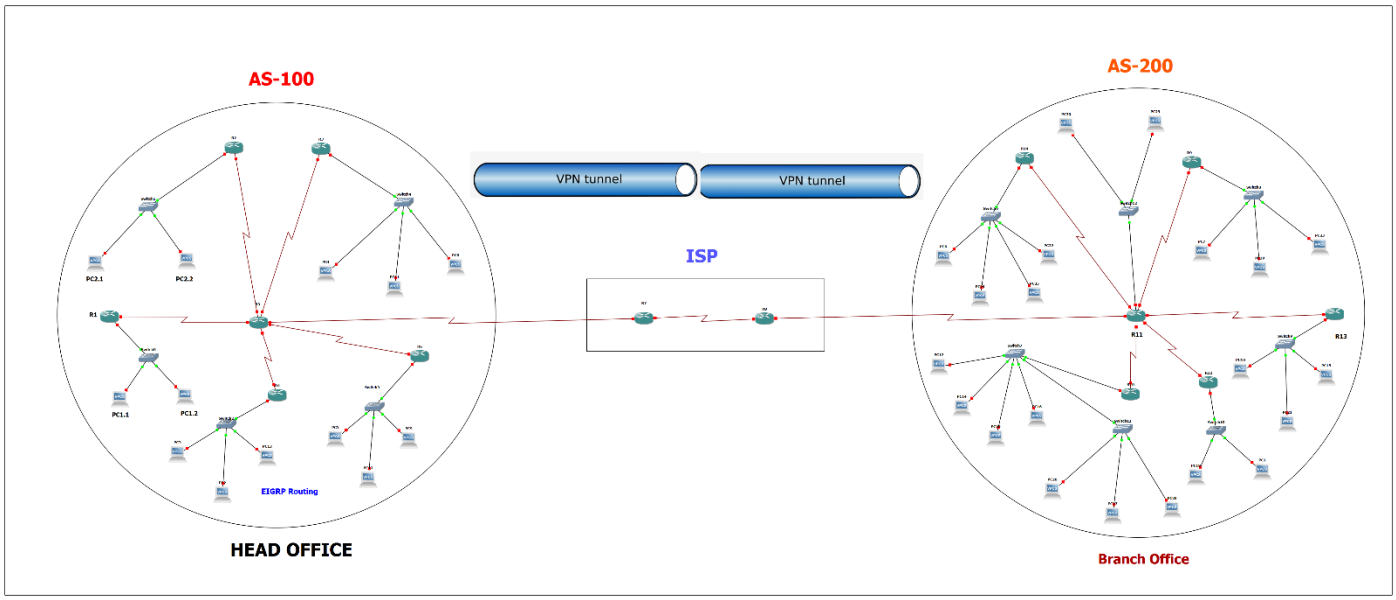
The next-hop paradigm dictates that a packet of data goes to the next or most optimal choice among all the potential routers it can be sent to. Because BGP supports next-hop, connections can be optimized for faster network performance, instead of having to navigate far, disparate routing BGP points, wasting valuable time. Also, because of this support, administrators do not have to configure BGP for next-hop connections.




**BGP Routing as a role service of Remote Access**. You can now install the **Routing** role service of the Remote Access server role without installing the **Remote Access Service (RAS)** role service when you want to use Remote Access as a BGP LAN router. This reduces the BGP router memory footprint and only installs the components required for dynamic BGP routing. The Routing role service is useful when only a BGP Router VM is required, and you don't require use of DirectAccess or VPN. In addition, using Remote Access as a LAN router with BGP provides you with the dynamic routing advantages of BGP on your internal network.

**BGP Statistics (Message counters, Route counters)**:

The BGP Router supports displaying the message and route statistics, if required, by using the **Get-Baptistic** Windows PowerShell command. Equal Cost Multi Path Routing (ECMP) support. The BGP Router supports ECMP and can have more than one equal cost routes plumbed into the BGP routing table and stack. The BGP router selection of the route for transmitting data packets is random with ECMP enabled. Hold Time configuration. The BGP Router supports configuration of the Hold Timer value according to your network requirements. This timer can be dynamically changed to accommodate interoperability with third party devices or to maintain a specific maximum time for BGP peering session timeous.




In this paper we have created a VPN connection by using IGP and BGP routing Protocols for a company whose head office is in Hyderabad and Branch office is at Bangalore. A secure VPN Tunnel is Created over a public network internet. The topology was simulated in GNS3 simulator. VPN is tested through ping command from one network to another network.

## 4. CONCLUSION

This paper presents the performance analysis of IGP and BGP network. A Secure VPN is Created Through Public Network. Which can be used to Connect your company or university's network from anywhere in the world, Keep Your Messages Private and Secure, Improve the security of public Wi-Fi and Keep your devices safe.

## 5. ACKNOWLEDGMENT

The author would like to thank the Faculty ISL Engineering College, Bandlaguda, Hyderabad, for the support grant in publishing this paper.

## 6. REFERENCES


1) Nur Fatin Nadhirah Norazlan, Ruhani Ab. Rahman, Murizah Kassim, Abd Razak Mahmud Faculty of Electrical Engineering, University Technology MARA, 40450 UiTM Shah Alam, Selangor, MALAYSIA ruhani467@uitm.edu.my
2) [1] M. Kassim, M. Ismail, M. I. Yusof, and M. A. Abdullah, "Time based traffic policing and shaping algorithms on campus network internet traffic," Journal of Telecommunication, Electronic and Computer Engineering, vol. 9, pp. 135-140, 2017.
3) [2] A. Mishra, "Network Load Balancing and Its Performance Measures," International Journal of Computer Science Trends and Technology (IJCST), vol. 3, pp. 77-81, 2015.
4) [3] C. Wijaya, "Performance analysis of dynamic routing protocol EIGRP and OSPF in IPv4 and IPv6 network," in 2011 First International Conference on Informatics and Computational Intelligence, 2011, pp. 355-360.
5) [4] H. Hasan, J. Cosmas, Z. Zaharis, P. Lazaridis, and S. Khwandah, "Development of performance of OSPF network by using SDN concepts," in 2016 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2016, pp. 1-5.
6) [5] S. Jahan, M. S. Rahman, and S. Saha, "Application specific tunneling protocol selection for Virtual Private Networks," in 2017 International Conference on Networking, Systems and Security (NSysS), 2017, pp. 39-44.
7) [6] A. Al-Darrab, I. Al-Darrab, and A. Rushdi, "Software-Defined Networking load distribution technique for an internet service provider," Journal of Network and Computer Applications, vol. 155, p. 102547, 2020.
8) [7] S. McQuerry, Interconnecting Cisco Network Devices, Part 1 (ICND1): CCNA Exam 640-802 and ICND1 Exam 640-822: Pearson Education, 2007.
9) [8] M. Kassim, A. Azmi, R. AbRahman, M. I. Yusof, R. Mohamad, and A. Idris, "Bandwidth control algorithm on youtube video traffic in broadband network," Journal of Telecommunication.