

Virtual Private Network Load Balancing Using EIGRP Routing

Authors: Inderjeet Singh; Damandeep Kaur

Department of Electronics & Communication,
GCET Gurdaspur, India

Abstract— This Research paper presents the performance of Enhanced Interior Gateway Routing Protocol (EIGRP) with Virtual Private Network (VPN) Load Balancing with and without load balancing as well as without VPN techniques. The topology was first simulated using OPNET simulator. Load Balancing is a networking method for distributing workload across multiple systems which it can be sent equally among the route exist. EIGRP topologies were analyzed using three different scenarios including VPN network. Differences of tests on the network performance are analyzed such as such Voice End to End Delay, jitter, Voice Delay, Video End to End Delay, Video Delay, E-mail Upload as well as Download Response Time, Http Object Response Time. Results obtained from OPNET indicates that EIGRP with load balancing has a better performance which divides routes equally among Three route path and Provide optimum performance in network.

Keywords— Virtual Private Network, EIGRP, Load Balancing, OPNET, HTTP.

1 Introduction

Enhanced Interior Gateway Routing Protocol or EIGRP automates the routing decisions and configurations in computer networking. Cisco designed the protocol and is available only on Cisco routers. Minimum bandwidth is used from the source to destination, and the delay is measured using metrics of the network. This is an advanced protocol to measure the distance and uses both link servicing and distance routing. Hence it is called a hybrid protocol. It transitions well with IPv6 and has the support of IPv4 as well. This is a classless routing technique. Two routers are connected, and the network is shared in EIGRP.

Fundamentals of EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing protocol used for routers' decisions and configuration. EIGRP only sends incremental

Updates, which in short reduces the workload of the routers and the amount of information transmitted.

EIGRP is a classic hybrid protocol that supports classless routing, it supports automatic & manual summarization on an EIGRP enabled interface. It MD5 authentication on routers running EIGRP and also has a maximum hop count close to 255. EIGRP performs load balancing over the equal-cost path and un-equal cost path.



Figure : 1.1 EIGRP Network

To perform the functions of EIGRP, it creates three tables which are:

1. Neighbor Table
2. Topology Table
3. Routing Table

Following represents the ideology and concepts behind the three major tables:

1. Neighbor Table

The neighbor table contains information about routers and neighborhood relationships with those whom have been established.

- The Neighbor Table has Fields like H: Handle, Address, Interface, Hold Time, Uptime, Smooth Round Trip Time, Retransmission Timeout, Queue Count, Sequence Number.

2. Topology Table

- The topology table holds information about all the paths to networks understood by EIGRP routers.
- Command to list router information- 'show ip eigrp' topology.
- The topology table holds the following fields Passive, Feasible Distance, Advertised distance, Feasible distance
-

3. Routing Table

- The routing table stores the routes which are currently active in sending packets to the network. It stores the optimal route for the destination from the sender.
- Hello: It determines the neighbors' router and also serves as a keep-alive mechanism between the routers. If Router X is connected with Router Y and the Router X is not receiving the hello packets from Router Y, then it assumes that Router Y is not reachable and the network is down.
- Update: Updates are to send the information about the route to its neighbors. When a new router is found, the update packets sent to the neighbor to build up the topology table.
- Query: Queries are used specifically for requesting route info. They act as multi-part until they send received queries as the response. It will send the queries only when the destination state is active.
- Reply: Reply packets respond to a query that indicates the originator router that it does not need to go into an Active state as reliable successors for the destination network. Replies are sent when destinations go into an Active state. For

the reply packet, an acknowledgment is sent.

- ACK: Acknowledgment packet will be sent to Enhanced Interior Gateway Routing Protocol Query, Update and Reply packets. It is shared with unicast address and, also, acknowledgment not sent to Hello packets.
-

2. Load Balancing Load balancing refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a server farm or server pool. Modern high-traffic websites must serve hundreds of thousands, if not millions, of concurrent requests from users or clients and return the correct text, images, video, or application data, all in a fast and reliable manner. To cost-effectively scale to meet these high volumes, modern computing best practice generally requires adding more servers.

A load balancer acts as the "traffic cop" sitting in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it.

Functions: of load Balancing

- Distributes client requests or network load efficiently across multiple servers
- Ensures high availability and reliability by sending requests only to servers that are online
- Provides the flexibility to add or subtract servers as demand dictates

Benefits of Load Balancing

- Reduced downtime
- Scalable
- Redundancy
- Flexibility

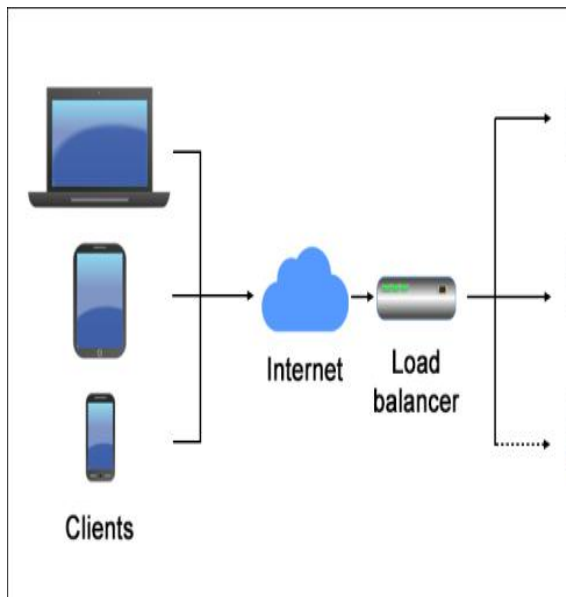


Figure 2.2 Load Balancing

3 Virtual Private Networks:

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

virtual private network, that is known as a VPN, protects your online activity and privacy by hiding your true IP address and creating a secure, encrypted tunnel to access the internet. No snoopers, trackers, or other interested third parties will be able to trace your online activity back to you. Moreover, you can reach a new level of internet freedom by using servers across different countries to unblock restricted content. While you could use this ability to open unlimited libraries of Netflix content, it also allows you to access international news or media that might be censored under oppressive regimes. Once you've downloaded the VPN software, you can secure a device and access global content safely and freely with a simple click. But what is a VPN, and how exactly does it protect you and keep your activity anonymous? While they're extremely easy to use, the tech behind

VPNs can be a little tricky to grasp. We've broken it down in simple terms below and have some VPN recommendations for you to try out.

Key Process of VPN

- **Proxying.** Like a proxy, a VPN hides your IP address and location to increase your online anonymity. The websites you visit only see the IP address and location of the VPN server instead.
- **Authentication.** The authentication process ensures that your VPN client only interacts with the VPN server you want to connect to. This prevents other third parties from intercepting your data.
- **Tunneling.** A VPN connection activates an encrypted tunnel for the internet traffic. This process encapsulates each data packet inside another data packet, making it difficult for malicious parties to read it.
- **Encryption.** Many websites that use an SSL/TLS, or an HTTPS certificate, will encrypt the data exchanged between your device and the target

server. However, this encryption is limited to the websites you visit. Meanwhile, a VPN tunnel encrypts all traffic. Many VPN providers use military-grade encryption, which is nearly impossible to be read by third parties.

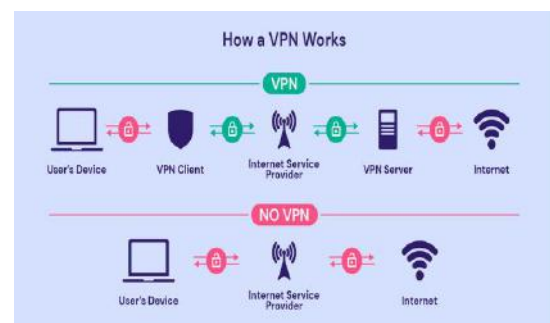


Figure 3.1 Working Mechanism of VPN

4 Literature Survey: we have got through different papers thoroughly which we thought can help us to reach up to specific conclusion. All the

papers were having great research. In these papers we have concluded that dynamic Routing protocol is responsible for path determination, Routing updates and choosing the best path in network (host node to destination node). Performance analysis of different Routing protocols has been done based on different performance metrics.

[1] This paper titled “Virtual Private Network Load Balancing Using OSPF Routing” presents the performance analysis of OSPF network. Multimedia Applications has been tested and analyzed when transferring the files by using both FileZilla Server and Client and video streaming were used VLC Media Player to transmit and received data. To provide the optimum performance in network, Open Shortest First Path (OSPF) has been implemented based on Internet Protocol. For analysis in transmission files concluded that when load balancing applied, transmission time is faster than VPN GRE tunnel since the topology in VPN is more secure and takes a longer time to transmit and received the data. Results obtained from network simulator and a test bed show that OSPF with load balancing is better compared other method such no-load balancing that proved a better result in term of speed, latency, and throughput and packet loss during video streaming. Other parameter showing that load balancing has optimum performance than other method used.

[2] This paper titled “Load Balancing using Load Sharing Technique in Distribution System” described that three phase distribution system always faces unbalancing in the load because of overloading of one phase compared to the other phases. To solve this problem equal sharing of load on each phase of the distribution system is followed. Current flow in the neutral wire, energy losses can be reduced by equal sharing of load. The proposed technique which consists of microcontroller and relay based hardware is used for balancing the loads in the three phase distribution network. The proposed hardware results show that it is a effective method for providing stability in all the three phases and maintain perfect voltage regulation and reduce three phase unbalancing.

[3] in the paper titled “a comparative study of is-is and IGRP protocols for real- time application based on Cisco Packet Tracer “ ISIS and IGRP Routing protocols have been taken and performance of protocols is checked by performance metric like convergence duration time, throughput, packet delay variation, packet end-to-end delay and traffic sent the evaluation results show that show that the best results in the combination of two protocols of IGRP and is-is, achieved in traffic sent and received for videoconferencing, throughput, jitter, packet delay variation for voice and convergence activity time parameters. whereas, packet end-to-end delay and packet delay variation for videoconferencing of is-is protocol is better than is-is/IGRP protocol.

[4] in the paper titled “simulation based EIGRP over OSPF performance analysis” EIGRP and OSPF Routing protocols have been taken and performance of protocols is checked by performance metric like convergence time, jitter, end to end delay, throughput, packet loss. The evaluation results show that EIGRP Routing protocols provide a better performance than OSPF Routing protocol for real time video application and voice application.

[5] in the paper titled “ performance comparison of EIGRP and ISIS/RIP protocols” EIGRP and combination of ISIS/RIP protocols have been taken and performance of protocol is checked by performance metric like terms of convergence time, throughput and end-to-end delay. the evaluation results show that the combination of is-is/RIP protocol shows better performance compared to EIGRP protocol in terms of throughput and end-to-end delay. Whereas, the network convergence of EIGRP protocol is better than is-is/RIP protocol.

[5] Results: To Find the output OPNET Simulator has been used. Three different Scenario’s has been created with EIGRP protocol as Eigrp with VPN , without VPN & with Load Balancing . Results have been described in brief.

5.1 Voice End to End Delay: The time taken for a packet to be transmitted across a network from source to destination

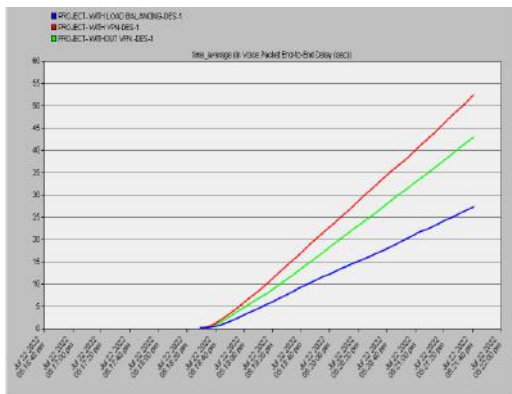


Figure 5.1 Voice End to End Delay

As per Above Figure in which Voice Delay from One End to other End is described. It is shown that Network with load Balancing is so far better than VPN as well as without VPN.

5.2 Voice Delay: Over all delay in Voice Performance Metric

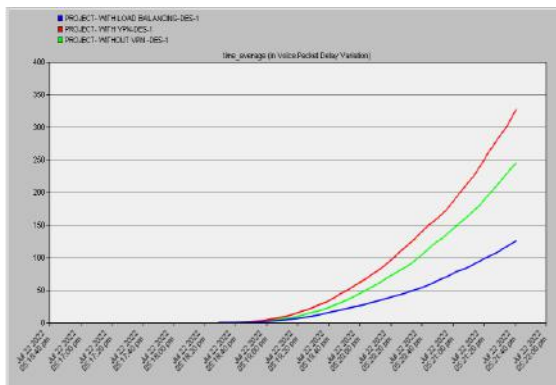


Figure 5.2 Voice Delay

As End to End Delay Network with Load balancing is also provide best Performance in Voice Delay Also. It is shown that Network with load balancing is so far better than VPN as well as without VPN.

5.3 Voice Jitter

In Voice over Internet Protocol (VoIP) technologies, jitter refers to a delay in receiving a voice data packet.

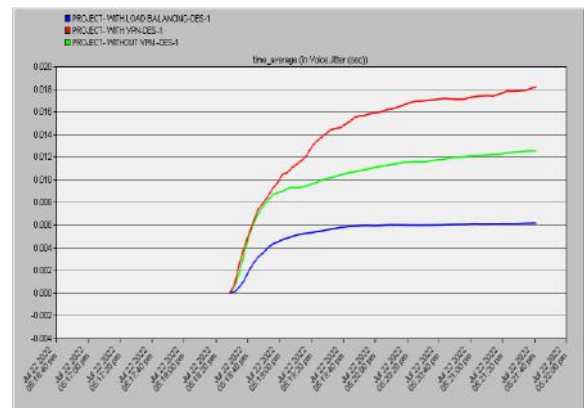


Figure :5.3 Voice Delay

In Voice Delay Network Performance, VPN network Delay time is worst . without VPN is providing better than VPN . Network with Load Balancing is providing minimum delay among of them .

5.4 Voice MOS Value : The Mean Opinion Score (MOS) has been a commonly-used metric to measure the overall voice call quality for decades.

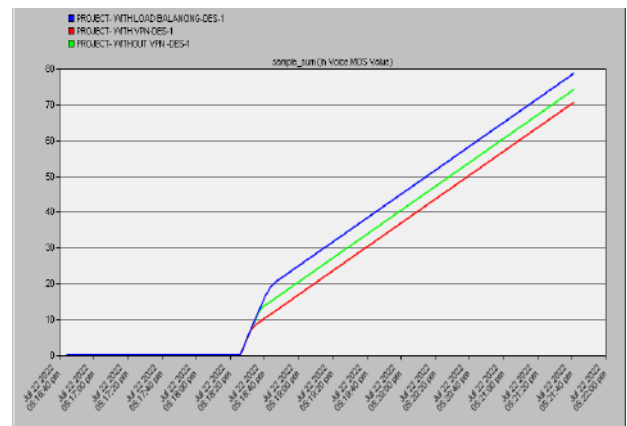


Figure :5.4 Voice MOS

AS in others Voice Results Network with Load Balancing is providing much better performance , in MOS also load Balancing is best rather than others Network.

5.5 Video End to End Delay : The time taken for a packet to be transmitted across a network from source to destination

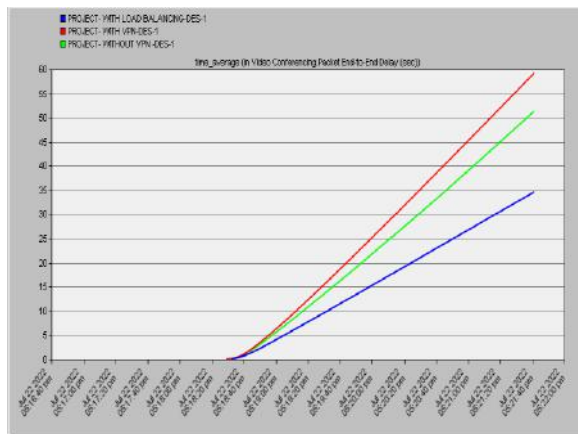


Figure :5.5 Video End to End Delay

As per Above Figure in which Video Delay from One End to other End is described. It is shown that Network with Load Balancing is so far better than VPN as well as without VPN.

5.6 Http Object Response Time :

The response time is calculated as the time it takes to perform a HTTP GET to the specified URL.

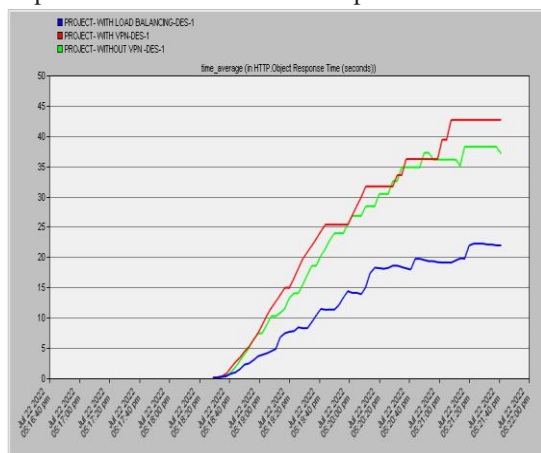


Figure :5.6 Http Object Response Time

As Like Voice and Video performance, Http Object Response time of Load Balancing Network is also Best .

5.7 E-mail Download Response Time: Time Taken to Download Particular E-mail data Known as E-mail Download Response Time.

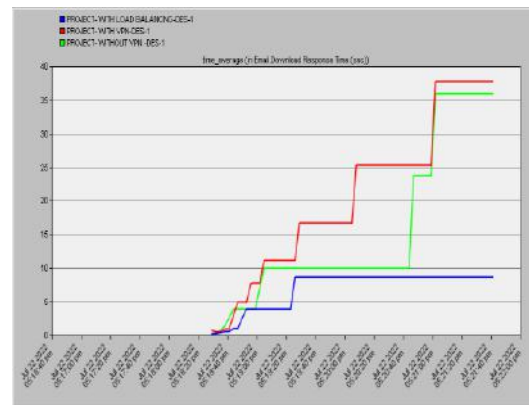


Figure 5.7 E-mail Download Response Time

Above Figure Results are Described Network performance with OPNET simulator, in which it is shown that Worst download Response time is Above 35 seconds which is provided by with VPN Network , Without VPN is little bit better than Vpn. Network with Load Balancing is fine best that is below 10 seconds .

5.8 E-mail Upload Response Time: Time Taken to uplad Particular E-mail data Known as E-mail upload Response Time.

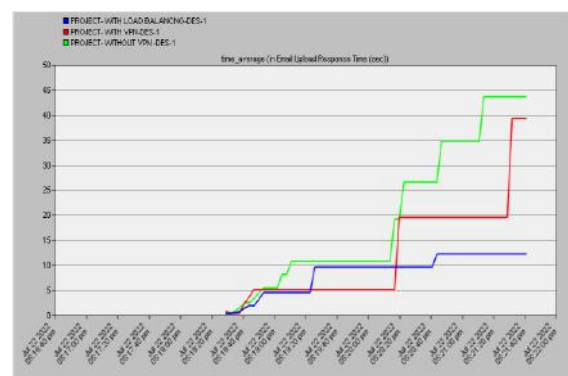


Figure 5.8 E-mail Upload Response Time

Above Figure Results are Described Network performance with OPNET simulator, in which it is shown that Worst download Response time is Above 40 seconds which is provided by with Without VPN Network , With VPN is little bit better than WithoutVpn. Network with Load Balancing is fine best that is Just above of 10 seconds .

6 Conclusions

It can be concluded from Results that Network with Load Balancing is providing best Results in Every Performance Metrics such as Voice End to

End Delay, jitter, Voice Delay, Video End to End Delay, E-mail Upload as well as Download Response Time, Http Object Response Time. Network with VPN Providing Worst Performance. Because VPN will slow your internet connection down, because your internet traffic is going through the VPN server: it's an extra step in the process. In Future Network Performance can be annealed with security term also.

7. References

- [1] Norazlan Nur Fatin Nadhirah et al (2020) Virtual Private Network Load Balancing Using OSPF Routing, 978-1-7281-5033-8/20/\$31.00 ©2020 IEEE
- [2] Nancy J Joys et al (2020) Load Balancing using Load Sharing Technique in Distribution System ,(ICACCS) , 978-1-7281-5197-7/20/\$31.00 ©2020 IEEE.
- [3]Rick Graziani and Allan Jonson, "Routing protocols and concepts: CCNA exploration companion guide," Pearson Education. London, 2008.
- [4] Catherine Boutremans, GianlucaIannaccone, Christophe Diot, "Impact of link failures on VoIP performance," In Proceedings of NOSSDAV Workshop, ACM press, pages 63-71, May 2002. Florida, USA. [5] Renata Teixeira, Jennifer Rexford, "Managing Routing Disruptions in Internet Service Provider Networks," IEEE Communications Magazine, March 2006.
- [6] Douglas E. Comer, "Internetworking with TCP/IP, Principles, Protocols and Architecture," 5th ed. Vol.1, Pearson Prentice Hall, 2006.
- [7] Tony Larsson and NicklasHedman, "Routing Protocols in Wireless Ad-hoc Networks-A simulation Study (Master's thesis)," Dept. Com. & Eng., Luleå Univ., Stockholm, 1998.
- [8] Talal Mohamed Jaffar, "Simulation-Based Routing Protocols Analysis (Thesis)," Ph.D., Dept. Elect. Eng., Georgia Institute of Technology, 2007.
- [9]Jeff Doyle. (2001, Nov 16). "Dynamic Routing Protocols," <http://www.informit.com/articles/>
- [10] Online source. (2004, Aug 27), "Advanced IP Addressing Management,"CiscoSystems, <http://www.informit.com/articles/>
- [11] Radia Perlman, "A Comparison between Two Routing Protocols: OSPF and IS-IS,"IEEE Network Magazine, September, 1991.

- [12] Cisco, "Internet Technology Handbook." <https://searchnetworking.techtarget.com/definition/virtual-private-network>.