# Review Paper on Virtual Private Network Load Balancing With EIGRP Routing Protocol

**Inderjeet Singh[1]; Damandeep Kaur[2]**

Department of electronics and communication,
GCET GURDASPUR, INDIA[1,2]
Indeerjeetsingh86@gmail.com[1]; damanaujla29@gmail.com[2]

**Abstract**

This paper presents the proposed of Virtual Private Network (VPN) Load Balancing on (Eigrp) Enhanced interior gateway routing protocol with and without load balancing techniques. In this paper all the aspects has been analysis related with VpnEigrp& load balancing. It is proposed investigation in which Eigrp Protocol will be analyses using three different scenarios such as Vpn, load balancing & without load balancing .Network testing such as ping command will analysis the network behavior that is used to measure Performance. Different of tests on the network performance will be analysis such as throughput, jitter performance, packet loss, delay, speed. This research is significant to forecast of network design and management to find best performance of virtual private network with & without load balancing.

**Keywords .Vpn, Eigrp, Jitter, Packet loss, Throughput, Delay**

## Introduction

A VPN (virtual private network) is a service that creates a safe, encrypted online connection. Internet users may use a VPN to give themselves more privacy and anonymity online or circumvent geographic-based blocking and censorship. VPNs essentially extend a private network across a public network, which should allow a user to securely send and receive data across the internet. Typically, a VPN is used over a less secure network, such as the public internet. Internet service providers (ISPs) normally have a rather large amount of insight into a customer's activities. In addition, some unsecured Wi-Fi access points (APs) may be a convenient avenue for attackers to gain access to a user's personal data. An internet user could use a VPN to avoid these encroachments on privacy.VPNs can be used to hide a user's browser history, Internet Protocol (IP) address and geographical location, web activity or devices being used. Anyone on the same network will not be able to see what a VPN user is doing. This makes VPNs a go-to tool for online privacy. A VPN uses tunneling protocols to encrypt data at the sending end and decrypts it at the receiving end. The originating and receiving network addresses are also encrypted to provide better security for online activities. VPN apps are often used to protect data transmissions on mobile devices. They can also be used to visit websites that are restricted by location. Private browsing does not involve encryption; it is simply an optional browser setting that prevents identifiable user data from being collected.

## 2 Working Mechanism of VPN

At its most basic level, VPN tunneling creates a point-to-point connection that cannot be accessed by unauthorized users. To actually create the tunnel, a tunneling protocol is used over existing networks. Different VPNs will use different tunneling protocols, such as Open VPN or Secure Socket Tunneling Protocol (SSTP). The protocol used may depend on the platform the VPN is being used on, such as SSTP being used on Windows OS, and will provide data encryption at varying strengths. The endpoint device needs to be running a VPN client (software application) locally or in the cloud. The client will run in the background. It is not noticeable to the end user unless there are performance issues.By using a VPN tunnel, a user's device will connect to another network while data is encrypted and IP address is hidden. This is what will hide private information from attackers or others hoping to get access to an individual's activities. The tunnel will connect a user's device to an exit node in another distant location, which makes it seem like the user is in another location.

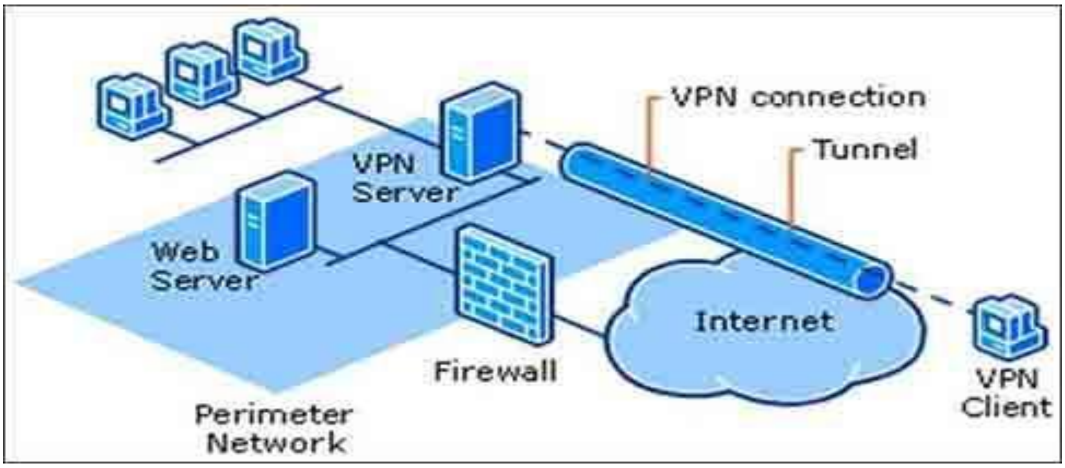

Figure 1.1 Virtual Private Networks

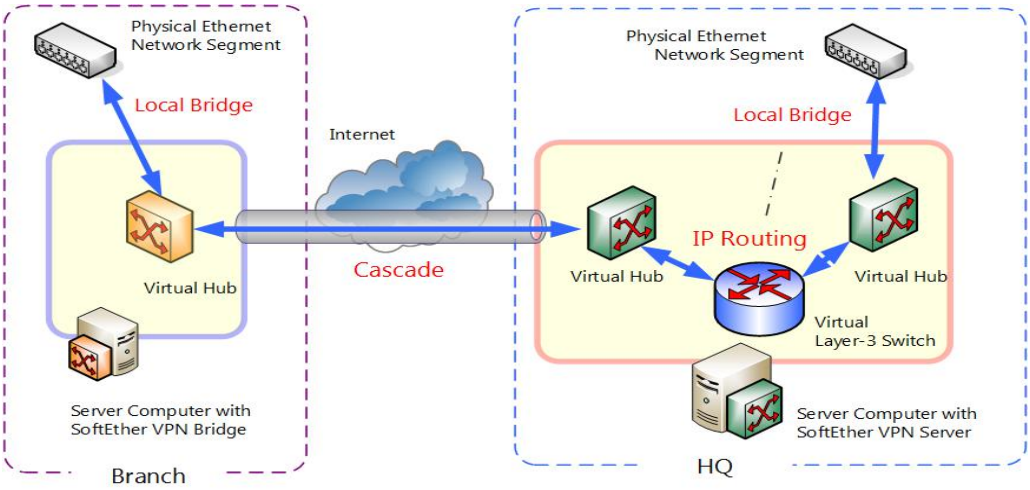
Physical Ethernet Network Segment
Local Bridge
Internet
Virtual Hub
Cascade
Server Computer with SoftEther VPN Bridge
Branch
Physical Ethernet Network Segment
Local Bridge
IP Routing
Virtual Hub
Virtual Hub
Virtual Layer-3 Switch
Server Computer with SoftEther VPN Server
HQ

Figure 1.2 working mechanism of VPN

### 3 Load balancer

**A network load balancer** is a load balancer that distributes traffic across multiple local and wide area networks so that large volumes of user requests are handled in a manner that maximizes performance and reliability. To review general information about load balancers, see Save 80% Compared to Hardware Load Balancers. A large network is typically built by connecting multiple smaller networks together. A network can be as small as two computers in a home or as big as the Internet. When the computers, servers, or devices in a network are in close proximity to each other, such as inside a single office or home, the network is referred to as a local area network *(LAN*). Connecting multiple LANs, usually across a larger geographical area, yields *a* wide area network (WAN). The Internet itself can be thought of as a WAN that aggregates many smaller WANs.

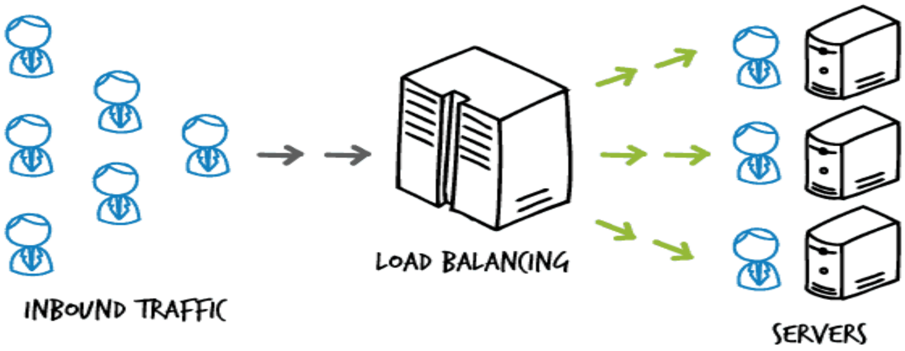

Figure 1.3 Load Balancing

To handle large traffic volumes at their websites, companies often place a load balancer in front of a group of servers connected to the same LAN and running the same applications (sometimes referred to as a *server farm*). For even greater redundancy, a company might distribute requests across the servers on multiple LANs aggregated into a WAN. One of the goals of load balancing is to maximize application reliability by eliminating single points of failure. Deploying network load balancers to load balance across servers on multiple LANs or even multiple WANs ensures that even if all servers in a LAN fail (or a network partition isolates the LAN), users don't experience failure, because traffic is redirected to accessible LANs where servers are still online.
A common type of network load balancer is a global server load balancer (GSLB), which distributes user requests across multiple geographically distributed groups of servers. Users experience fast responses to their requests because servers are nearby (either geographically or in terms of network hops), and companies can be confident in the high availability of their websites in all but the most extreme cases of network and server failure.

### 4 EIGRP

EIGRP is an enhanced version of IGRP. The same distance vector technology found in IGRP is also used in EIGRP, and the underlying distance information remains unchanged. The convergence properties and the operating efficiency of this protocol have improved significantly. This allows for an improved architecture while retaining existing investment in IGRP.

The convergence technology is based on research conducted at SRI International. The Diffusing Update Algorithm (DUAL) is the algorithm used to obtain loop-freedom at every instant throughout a route computation. This allows all routers involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in the recompilation. The convergence time with DUAL rivals that of any other existing Routing protocol.

EIGRP has been extended to be network-layer-protocol independent, thereby allowing DUAL to support other protocol suites.

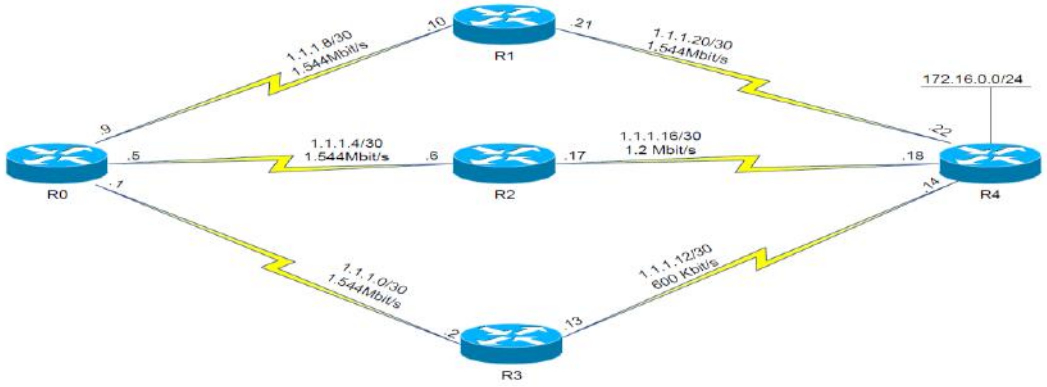

Figure 1.4 Example of EIGRP

### 4.1 How Does EIGRP Work?

EIGRP has four basic components:

**Hello:** used to identify neighbors. They are sent as periodic multicasts
**Update:** used to advertise routes, only sent as multicasts when something is changed
**Acknowledgement:** Acknowledgement receipt of an update. In fact, acknowledgement is Hello packet without data. It is always unicast and uses UDP.

**5 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 a dynamic Routing protocol is responsible for path determination, Routing updates and choosing the best path in a network (host node to destination node). Performance analysis of different Routing protocols has been done based on different performance metrics.

**[1]** 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.

**[2]** 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.

**[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 performance analyses on RIPv2,EIGRP, and OSPF using Cisco Packet Tracer" RIPv2 , EIGRP, and OSPF Routing protocols have been taken . and performance of protocols is checked by performance metric like convergence time, scalability, end-to-end delay, and throughput the evaluation results show that show that RIPv2 has better performance than others in small and condensed networks. OSPF & EIGRP have better performance for medium-sized and scattered networks. Overall EIGRP is more stable and consistent in both small and relatively large networks.

**[5]** In the paper titled "final project OSPF, EIGRP and RIP performance analysis based on Cisco Packet Tracer" EIGRP , OSPF and RIP protocols have been taken and performance of protocols is checked by performance metric like network convergence, Ethernet delay, email upload response time, http page response time, video conferencing packet end-to-end delay, voice packet delay the evaluation results show . That EIGRP compared to RIP and OSPF performs better in terms of network convergence activity and Routing protocol traffic and Ethernet delay. OSPF performs better in terms of http page response time and video conferencing packet end-to-end delay. RIP performs better in terms of voice packet delay.

**[6]** in the paper titled "performance comparison of EIGRP/ is-is and OSPF/ is-is" EIGRP , OSPF and ISIS protocols have been taken and performance of protocols is checked by performance metrics like throughput, http object response time, database response time and e-mail download response time. The evaluation results show that is-is convergence time in EIGRP/is-is network is much faster than OSPF/ISIS . In the comparison of these protocols in database query response time, EIGRP/is-is shows a better database query response time than of the other protocols at the whole time. EIGRP/is-is protocol performs very well in email download performance metric for the whole simulation time. In the http page response time is-is become well than other protocols.

## 6 Conclusions

It can be concluded from the different research based on VPN EIGRP as well as Load balancing that these three terms have very significant role in era of packets networks related with security and performance regarding . VPN has been used to secure the particular network working mechanism of vpn is that data is traveled between the sender and receiver through via tunnel. Eigrp has higher convergence rate rather than other protocols. Load balancing is used to balance the load of network so that performance ofparticular network can be enhanced .although it is proposed research which will be used with packet tracer simulator

## 6. References

[1] Rick Graziani and Allan Jonson, “Routing protocols and concepts: CCNA exploration companion guide,” Pearson Education. London, 2008.
[2] 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.
[3] Renata Teixeira, Jennifer Rexford, “Managing Routing Disruptions in Internet Service Provider Networks,” IEEE Communications Magazine, March 2006.
[4] Douglas E. Comer, “Internetworking with TCP/IP, Principles, Protocols and Architecture,” 5th ed. Vol.1, Pearson Prentice Hall, 2006.
[5] Tony Larsson and NicklasHedman, “Routing Protocols in Wireless Ad-hoc Networks-A simulation Study (Master’s thesis),” Dept. Com. & Eng., Luleå Univ., Stockholm, 1998.
[6] Talal Mohamed Jaffar, “Simulation-Based Routing Protocols Analysis (Thesis),” Ph.D., Dept. Elect. Eng., Georgia Institute of Technology, 2007.
[7] Jeff Doyle. (2001, Nov 16). “Dynamic Routing Protocols,” http://www.informit.com/articles/
[8] Online source. (2004, Aug 27), “Advanced IP Addressing Management,”CiscoSystems, http://www.informit.com/articles/
[9] Radia Perlman, “A Comparison between Two Routing Protocols: OSPF and IS-IS,”IEEE Network Magazine, September, 1991.
[10] Cisco, “Internet Technology Handbook.”
[11] https://searchnetworking.techtarget.com/definition/virtual-private-network
[12] https://www.nginx.com/resources/glossary/network-load-balancer