International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 7; Issue 5(C); May 2018; Page No. 12409-12413
DOI: http://dx.doi.org/10.24327/ijcar.2018.12413.2181

Review Article

INVESTIGATION OF ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL FOR IMPLEMENTING HUB AND SPOKE TOPOLOGIES IN VIRTUAL PRIVATE NETWORK

Sree Vidya T R* and Usha Bhanu.N

ECE Department, Valliammai Engineering College, Kattankulathur-603203

A R T I C L E I N F O

Article History:

Received 6th February, 2018
Received in revised form 20th March, 2018 Accepted 8th April, 2018
Published online 28th May, 2018

Key words:

Routing Information Protocol (RIP), Routing Protocol, GNS 3 software tool, Open Short Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP).

A B S T R A C T

This paper investigates the performance & configuration of Enhanced Interior Gateway Routing Protocol (EIGRP) using the Virtual Private Network (VPN). The VPN is used to implement peer-to-peer link connectivity between the customer locations. In this paper, the Hub and the Spoke topology are ensured to send traffic thus it ensures safe and encrypted connection. Performance optimizationis done by automatic routing decisions for data transmission between the sites and it enhances end to end connectivity. The proposed method of EIGRP uses Diffusing Update Algorithm where it takes only 90 milliseconds to achieve the convergence time. The proposed method ensures packet delay and does not have any boundary decisions between routers. The main advantage of the proposed method is the efficiency of EIGRP which is more advanced than Open Short Path First (OSPF). The GNS3 software shows that EIGRP provides better performance than OSPF protocol by their administrative distance, convergence time and metric calculations.

INTRODUCTION

The Virtual Private Network is a private network which has a secure way of connectivity through a public network. VPN creates tunnel through the network traffic is encrypted to ensure network security and privacy as discussed in [1]. VPN technology is a way to allow remote users to securely access co-operate application and many resources for ensuring safety in VPN as shown in Fig no.1. The data travels through tunnels and the users must use authentication to gain access to the VPN. The open VPN is an important VPN protocol that is based on SSN. TLS is another protocols encryption which is rapidly gaining its popularity due to the high level of security customizability and compatibility with most network environments.

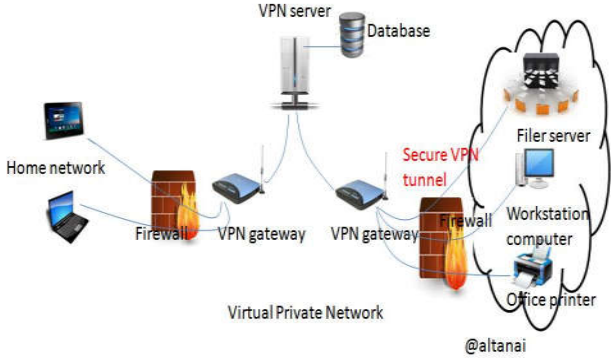

Fig No 1 Virtual Private Network

Corresponding author:* **Sree Vidya T R
ECE Department, Valliammai Engineering College, Kattankulathur-603203

VPN creates encrypted connection over a less secure network similar as internet. VPN creates protection as it prevents anyone on the same network from intercepting the web traffic as discussed in [5]. Many VPN service provide itsown DNS resolution system. So VPN DNS system is considered as other layer of protection. VPN also mitigate some of the effects of net neutrality that treats ISP web services equally.

Routing Protocol

Routing is the process of deciding a path for traffic in a network or between or across multiple networks. Most routing techniques enable the users to use multiple alternate paths as discussed in [9]. The routing protocols are to be classified as static, default and dynamic whereas the dynamic routing protocol is used in the proposed methodas shown in Fig no.2. Although different types of routing protocol are present two major classes are in wide spread use of IP network as discussed in [3].

1. Interior Gateway Protocol Type 1
2. Interior Gateway Protocol Type 2

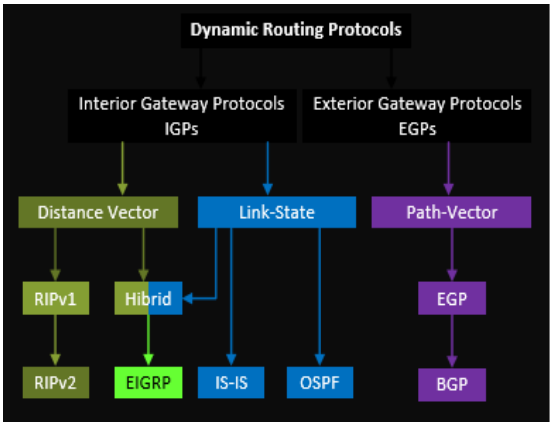

Fig No 2 Types of Routing Protocols

A routing protocol can be analyzed and formalized through the RFC (request for comments process). In this proposed technology the open written commentary is used to bring about standardization of EIGRP as discussed in [2]. The best example for routing protocol is OSPF which comprises of 2 steps they are forwarding and routing.

Forwarding

It refers to routing process of receiving a packet on an interface and an knowing which interface to retransmit so that the packet can continue to reach its destination. Moreover forwarding is entirely dependent on the router as where to send this packet or to discard it.

Routing

It involves the router to know the direction inorder to forward packets and itrequire a route or road map which illustrates a path from source and destination. This route can be generated either by static or dynamically develop routes to all destination within a network.

The main objective of the project is to configure & design the routers with the help of GNS3 software tool and could be used in the real time process.

The organization of the paper is as follows- The existing RIP & OSPF protocol for VPN is discussed in section-2, the proposed EIGRP protocol and neighbor, topology & routing tables and Diffusing Update Algorithm for implementing Hub & Spoke topology in VPN networks are discussed in section-3. In section-4, implementation results are presented. Finally in section-5, concluding remarks are given.

Existing Method

Routing Information Protocol (RIP)

RIP is one of the oldest distance vector routing protocol which consider a hop count as a routing metric and also RIP prevents routing loops by implementing limited number of hops which is allowed in a path to deliver their destination as shown in Fig no.3. RIP uses a modified hop count to determine the network distance whereas other routing protocol provides less information on their own to other network. RIP uses Bellman Ford Algorithm to estimate its route. To sharing information RIP uses local broadcast routing protocol as discussed in [4]. PIP broadcast routing is updated for every 30 seconds and the routing information to any device is connected with their routing interfaces.

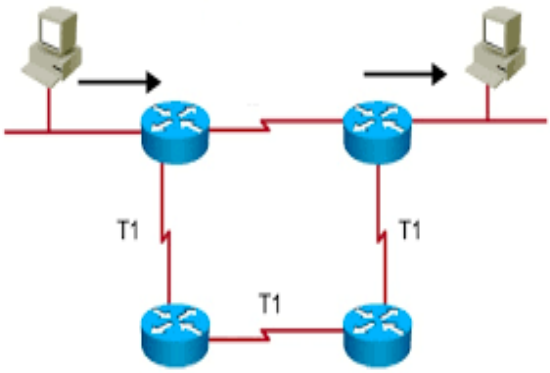

Fig No 3 Routing Information Protocol

Open Shortest Path First (OSPF)

OSPF is another routing protocol for internet protocol networks. It uses a link state routing algorithm and drops into the group of interior gateway routing protocol within a single autonomous system as shown in Fig no.4. It can load balance network traffic between multiple paths of the same metric value as discussed in [10]. It supports authentication using passwords and other valuable methods. It is effectively loop free for having a maximum hop metric of 65,535. OSPF is a link state protocol in which all routers in the routing domain interchange information and thus know about the complete topology of the network. Since each router performs the complete topology. OSPF is considered as more economical routing protocol than RIP as it involves less network traffic as discussed in [8][7]. OSPF is usually more efficient than RIP in exchanging routing information in a stable network.

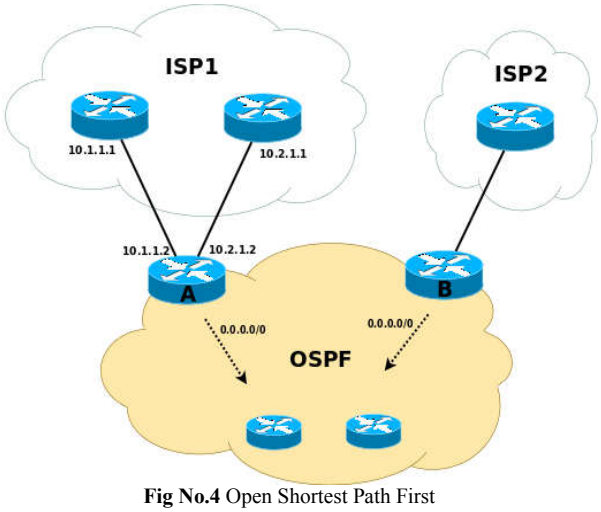

Fig No.4 Open Shortest Path First

Proposed Routing Protocol for VPN

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced vector routing protocol which is used in VPN technology for automating routing decisions and configuration. Thus it enables network routers to exchange information more efficiently compared with the other earlier protocols as discussed in [3]. EIGRP has gained importance recently due to ease of deployment and fast convergence. So it is widely used in complex and enterprise network.

Eigrp Tables

EIGRP consists of the tables where the first table is named as EIGRP Neighbor table. The neighbor tables will tries to gather all the information present in the neighbor router. Whereas the second table is called EIGRP Topology table, in this the data

of all the neighboring router information are collected and stored in this table. The third table is called as Global Routing table, this table tends to collect all the router information between the source and the destination as shown in Fig no.5. This table will try to find out the least metric path of the routers and implement the same of selecting the best shortest path.

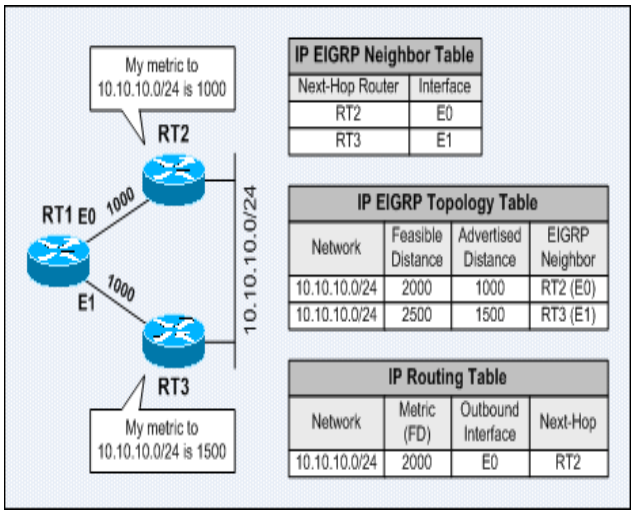

Fig No 5 EIGRP Tables

It is more of link state protocol due to its operations in tracking the routing tables. The most important aspect and advantage of EIGRP is load balancing feature where multiple route to a specific network through multiple routing process is enabled as discussed in [3][6]. And it also installs the route with lowest administrative distance in the routing table.The key aspect of EIGRP is that it improves network stability and reduces resource utilization and also it simplifies stub router configuration. Stub routing is nothing but which is been commonly used in hub and spoke topology.

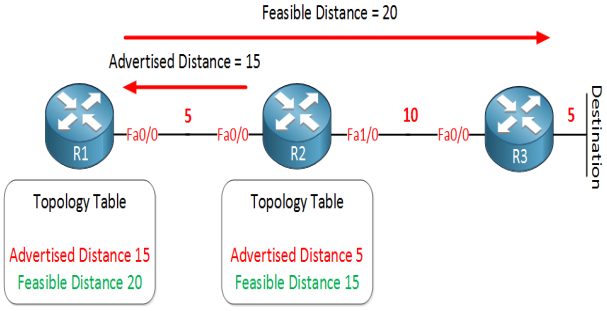

Fig No.6 Feasibility Condition

Feasibility condition is another criteria which is implied in EIGRP where it focus in calculating the advertised distance must be less than the feasible distance of the successor as shown in fig no.6 and thus it acts as a loop prevention mechanism of EIGRP and makes the best route to a network. Whereas the feasible distance is called the best metric path to a destination network including the metric neighbor advertising path and reported distance is called the total metric path to a destination network as advertised by upstream neighbor as shown in Fig no.6. EIGRP also enables few other features like stuck in active message (SIA) which means that no reply for a query because EIGRP sends a query when a route is lost and also another feasible route doesn't in the topology table. In such case the SIA causes two sequential events like auto summarization and route summarization.

Diffusing Update Algorithm

DUAL is enabling to ensure that the given route is recalculated globally whenever it causes a routing loop. DUAL is a key tool implemented in EIGRP as this enable to find the best shortest path available automatically and also it helps in saving the errors which happen while choosing the shortest path as discussed in [9]. It is a convergence algorithm that enables the routing protocol to prevent routing loops through continuous route computation. The DUAL protocol scans all routes to track the optimal path in terms of efficiency and path. DUAL FSM manages backup route in case of primary as well as the most efficient route is lost.

Hub and Spoke Topology

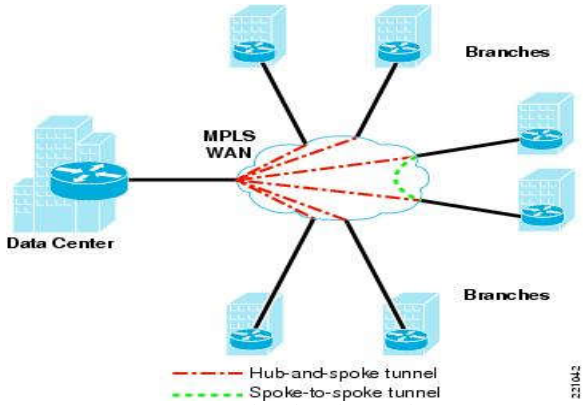

Fig No 7 Hub and Spoke Topology

The hub and spoke topology network is a widely used topology for all types of network then it is called as star topology. Access point is physically attached to the internet with a wire like spokes on a wheel as shown in Fig no.7. All the user devices are linkedto the wireless router in the center.

In hub and spoke topology multiple VPN routers communicates strongly & securely with a central VPN routers and a separate secured tunnel extends between each individual spoke and the hub as shown in fig no.7. So this topology allows customers at remote sites to access the hub network.

RESULT AND DISCUSSION

In this paper GNS-3 software is implementing by applying EIGRP protocol. GNS-3 is a network simulator which allows a combination of virtual and real device which is used to simulate complex network. The main aim of this proposed method is to connect the source and destination through the intermediate routers. In this paper 8 intermediate routers are used as shown in Fig no.9. In GNS-3 software a VPN is applied inorder to configure each router for providing a secured connection. Moreover EIGRP protocol is imposed inorder to promote automatic routing between the source and destination. DUAL algorithm as discussed in section 3.2 scan the routing path and it managed the backup route when the most efficient route is lost.

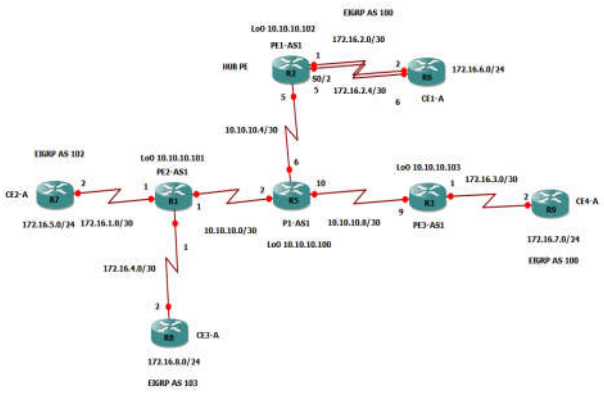

Fig No.8 EIGRP Configuration

In this paper ping performance is another important feature that could be seen in passing the information through various routers where all the information is stored in the hub which acts as a central point in data transmission and data is delivered to all the customer sites through spoke. Thus the end to end connectivity is achieved which is shown in Fig no.10 by providing information to all the customer sites.

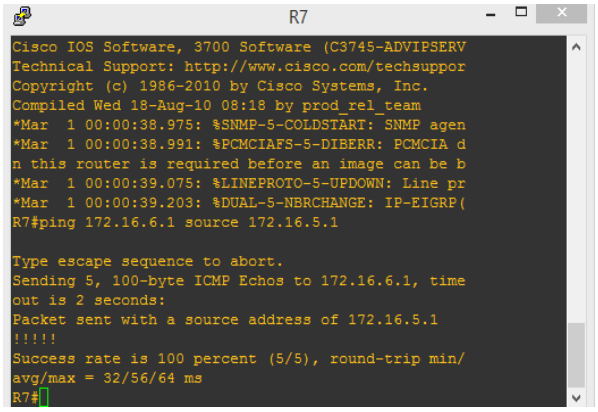

Fig No.10 End-to-End Connectivity

RIP as discussed in section 2.1 is used to send the information through routers by using the shortest path which is available but the only destination is that if there is any error in the chosen shortest path. RIP ultimately stops transmitting the data with the best shortest path available if so any error occurs in the chosen shortest path it tends to select the next best shortest path. But the only drawback in OSPF is that it will not save the data of routing information where the error has occurred.

Table No.1 Comparison of the proposed EIGRP protocol with existing protocols

	RIP[4]	OSPF[10]	EIGRP
Hop count	15	65,556	256
Administrative distance	140ms	110ms	90ms
Transmission mode	broadcast	multicast	multicast
Convergence	fast	fast	Very fast
Update timers	Every 30 seconds	Every 30 minutes	When changes occurs only
Security	Less secured	secured	More secured.

The performance of OSPF & EIGRP protocol is compared with the RIP protocol for VPN network architecture in terms of hop count, administrative distance, transmission mode, convergence time, update timers, and security. It is observed that the maximum allowable hop count limit is greater for OSPF compared to RIP & EIGRP which eliminates the problem being discarded without reaching the destination. As the administrative distance for EIGRP is 90ms compared to the existing protocol, the convergence time is also fast. The router overhead is also greatly reduced in the EIGRP as the routing table gets updated only when it is required. The security in data transmission is also improved as we are using a private key.

In this proposed method the existing drawbacks are overcome by implementing both selecting the shortest path as well as if so any error happens in the shortest path the data information of such path will be saved for further error checking process in EIGRP. Thus EIGRP as discussed in section 3.1 act as dual way in evaluating the error as well as selecting the most appropriate shortest path available. The data transmission is highly secured compared to the existing method as shown in Table no.1. The administrative distance of the EIGRP method is 90 milliseconds with hop count of 256.

CONCLUSION

In this paper EIGRP is used in computer network for automating routing decisions and configuration. Moreover this network protocol also let the router to exchange information more efficiently compared with the earlier network protocols. In the proposed method EIGRP DUAL algorithm is configured whenever there is a bug or error occurs in a router. The software automatically scan all the routers most appropriate and the shortest path available. In this paper the convergence times are only 90 milliseconds and have high accuracy in travel speed comparing the OSPF which is 110 milliseconds. Thus EIGRP protocol is found to be the best protocol that suits the VPN network architecture. In future, the EIGRP can be replaced by the Border Gateway Protocol (BGP) to minimize the convergence time and improve the security of data.

Reference

1. R.S.Naoum and M.Maswady, “Performance Evaluation for VOIP over IP and MPLS”, *World of Computer Science and Information Technology Journal* (WCSIT), Vol.2 (3), pp. 110- 114, 2015
2. “Quagga routing suite,” web site, http://www.nongnu.org/quagga/ accessed to February 2015.
3. A.Chadha and A.K.Gupta, “Review on Enhanced Interior Gateway Routing Protocol”, *Global Journal of Computer Science and Technology Network, Web & Secuirty,* Vol. 13(6), 2013.
4. K.Mirzahosein, A.Nguyen and S.Elmasry, “Analysis of RIP, OSPF and EIGRP Routing Protocols using OPNET”, Simon Fraser University, School of Engineering Final Year Project, ENCS 427: Communication Networks, 2013.
5. I.S.I Alsukayti and T.J.Dennis, “Performance Analysis of VoIP over BMG/MPLS VPN Technology”, PGNET Conference, 2013.
6. I.Kaur, “Performance Evaluation of Hybrid Network using EIGRP & OSPF for different Applications”, *International Journal of Engineering Science and Technology (IJEST),* Vol.3(5), pp.3950-3960, 2011.
7. D. Frost, S. Bryant,” Packet Loss and Delay Measurement for MPLS Networks”, Internet Engineering Task Force (IETF),2011

8. S.G.Thorenoor, "Dynamic Routing Protocol Implementation Decision between EIGRP, OSPF and RIP based on Technical Background Using OPNET Modeler", Second International Conference on Computer and Network Technology, pp.191-195, 2010.
9. Deepankar Medhi, Karthikeyan Ramasamy, Network Routing Algorithms, Protocols, and Architectures, Elsevier, 2007.
10. David Bauery, Murat Yukselz, Christopher Carothersyand, ShivkumarKalyanaramanz" A Case Study in Understanding OSPF and BGP Interactions Using Efficient Experiment Design", IEEE computer society, 2006

How to cite this article:

Sree Vidya T R and Usha Bhanu.N (2018) 'Investigation of Enhanced Interior Gateway Routing Protocol for Implementing Hub and Spoke Topologies in Virtual Private Network', *International Journal of Current Advanced Research,* 07(5), pp. 12409-12413. DOI: http://dx.doi.org/10.24327/ijcar.2018.12413.2181

****