IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 4, April 2018

Implementing Hub and Spoke topologies in Virtual Private Network using Enhanced Interior Gateway Routing Protocol

Sree Vidya T R[1], Vasanthadev Suryakala S[2], Swarnalatha M[3]

ECE Department, Valliammai Engineering College, Kattankulathur[1]

ECE Department, SRMIST, Kattankulathur[2]

ECE Department, Valliammai Engineering College, Kattankulathur[3]

Abstract: This paper analysis the configuration of Enhanced Interior Gateway Routing Protocol (EIGRP) using the Virtual Private Network (VPN). The VPN enables service provider to implement point-to-point link connectivity between the customer locations. In this paper, the Hub and the Spoke topology are used to send traffic thus it provides safe and encrypted connection. They optimize their performance by taking automatic routing decisions for data transmission between the sites and enhance end to end connectivity. The proposed EIGRP uses the Diffusing Update Algorithm thus it takes place 90 milliseconds to achieve the convergence time. The proposed method ensures packet delay and does not have boundary decisions between routers. The main advantage of the proposed method is that the efficiency of the EIGRP is too better than the OSPF proposed. The GNS3 software result shows that EIGRP provides better performance than the OSPF protocol by their administrative distance, convergence time and metric calculations.

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

I INTRODUCTION

The Virtual Private Network is a private network which enables a secure way of connectivity through a public network. VPN creates tunnel through the network traffic is encrypted inorder to ensure network security and privacy as shown in Fig no.1. VPN technology is a way to allow remote users to securely access co-operate application and other resources inorder to ensure safety in VPN. The data travels through tunnels as discussed in [3] and the users must use authentication method to gain access to the VPN. The open VPN is a popular VPN protocol that is based on SSN, TLS encryption which is rapidly gaining its popularity due to the high level of security customizability and compatibility with most network environments.

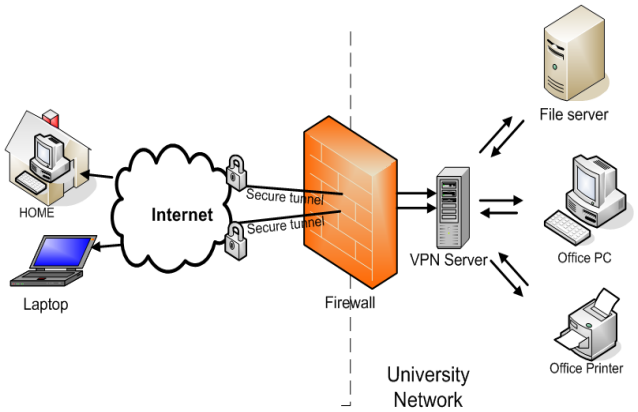

Fig No.1 Virtual Private Networks

VPN also creates a safe & encrypted connection over a less secure network similar as internet. VPN offers protection as it prevents anyone on the same network from intercepting the web traffic. Many VPN service also provide its own DNS resolution system. So VPN DNS system is considered as another layer of protection. VPN also mitigate some of the effects of net neutrality that treats ISP web services equally. There are different protocols used to secure & encrypt users like IP security, secure socket layer, transport layer security, point-to-point tunneling protocol.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 4, April 2018

1.1 ROUTING PROTOCOL

Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Most routing techniques enable the use of multiple alternate paths. Although many types of routing protocol three major classes are in wide spread use on IP network.

The routing protocols are of two types as shown in Fig no.2.

1. Routed protocol
2. Dynamic routing protocol

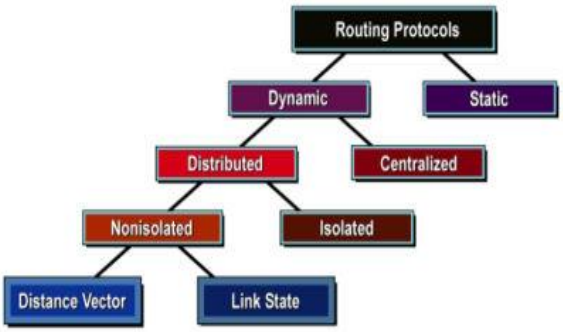

Fig No.2 Types of Routing Protocol

1.2 ROUTED PROTOCOL

These protocols forward the data's through routers as the routers are able to interpret the logical network specified by the routed protocol to operate properly. Routed protocol mostly relay on protocol for transport over LAN or WAN and the most commonly known routed protocol is Internet Protocol.

1.3 DYNAMIC ROUTING PROTOCOL

These protocols accomplish dynamic routing with routing algorithm. It supports routed protocol and maintains routing table as discussed in [7]. It also dynamically exchanges information about topology network by distributing routing information throughout the network. Dynamic routing protocol has a set of standardization rules that allows routers to determine the rule whereas the routing protocol tells the router about the optimal path to destination.

The routing protocols uses numerical values known as metric to determine the optimal route. The numerical value can be explained as cost of the transiting link. And this information is stored in the routing table by the router in determining the best route to reach the destination 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.

II. EXISTING METHODOLOGY OF PROPOSED METHOD

2.1 ROUTING INFORMATION PROTOCOL (RIP)

RIP is one of the oldest distance vector routing protocol which has 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 reach its destination. RIP uses a modified hop count inorder to determine network distance whereas other routing protocol provides less information on their own to other network.

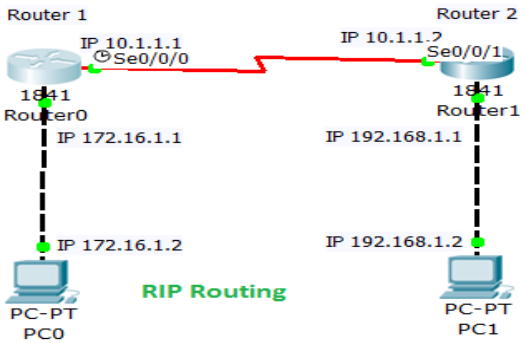

Fig No.3 Routing Information Protocol

RIP uses Bellman Ford Algorithm to calculate its route. To sharing information RIP uses local broadcast routing protocol. PIP broadcast routing is updated for every 30 seconds as shown in Fig no.3 and routing information to any device is connected with their interfaces.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 4, April 2018

2.2 OPEN SHORT PATH FIRST (OSPF)

OSPF is a routing protocol for internet protocol networks. It uses a link state routing algorithm and falls into the group of interior gateway routing protocol within a single autonomous system. It can load balance network traffic between multiple paths of the same metric value. It supports authentication using passwords and other methods. It is effectively loop free having a maximum hop metric of 65,535 as discussed in [4]. OSPF is a link state protocol in which all routers in the routing domain exchange information and thus know about the complete topology of the network as shown in Fig no.4. Since each router knows the complete topology. The use of SPF algorithm creates an extremely fast convergence. Moreover it provides routing information to the IP section of the TCP/IP protocol suite. This is the most commonly used alternative to RIP and it also send updates to table instead of entire tables to router. So OSPF is considered as more economical routing protocol than RIP as it involves less network traffic as discussed in [2] [8]. OSPF is usually more efficient than RIP in exchanging routing information in a stable network.

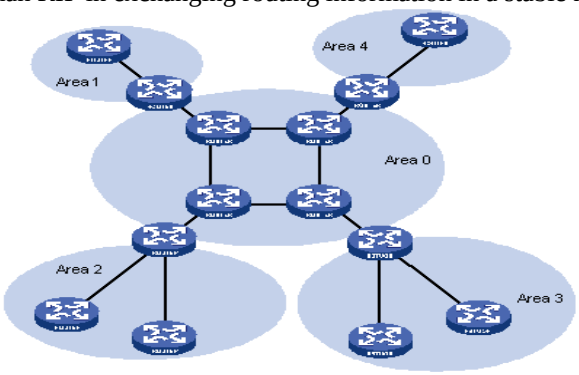

Fig No.4 OSPF Routing Protocol

It converges quickly than RIP because routing updates are sending immediately instead of periodically. It also uses less bandwidth since transmission takes place only when routing changes occur. OSPF also supports the logical grouping of network segments into areas. It announces routers outside the autonomous system so that it can calculate cost to reach outside network. OSPF uses subnet mask and also supports CIDR and variable lengths sub-netting, super-netting and non-contiguous network segments.

RIP use 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. In this proposed method the existing two 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 acts as dual way in evaluating the error as well as selecting the most appropriate shortest path available.

III PROPOSED METHODOLOGY

3.1 Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration as discussed in [1] [5].

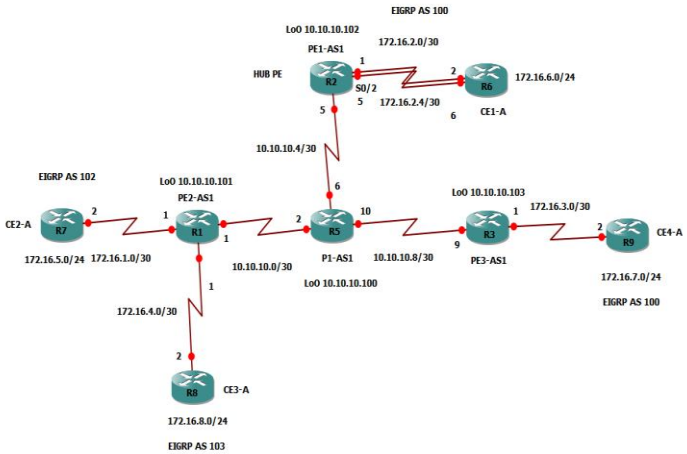

Fig No.5 Proposed EIGRP Routing Protocol

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 4, April 2018

The protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers. It is a network protocol that lets routers exchange information more efficiently than with earlier network protocols as shown in Fig no.5.

3.2 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.6. This table will try to find out the least metric path of the routers and implement the same of selecting the best shortest path.

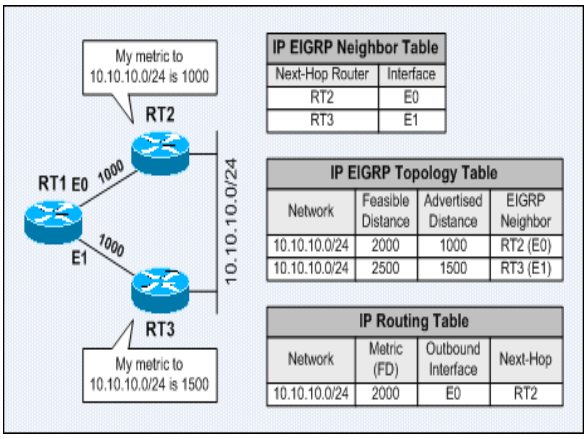

Fig No.6 EIGRP Neighbor table

3.3 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 [6]. It is an convergence algorithm that enable the routing protocol to prevent routing loops through continuous route computation as shown in Fig no.7. 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.

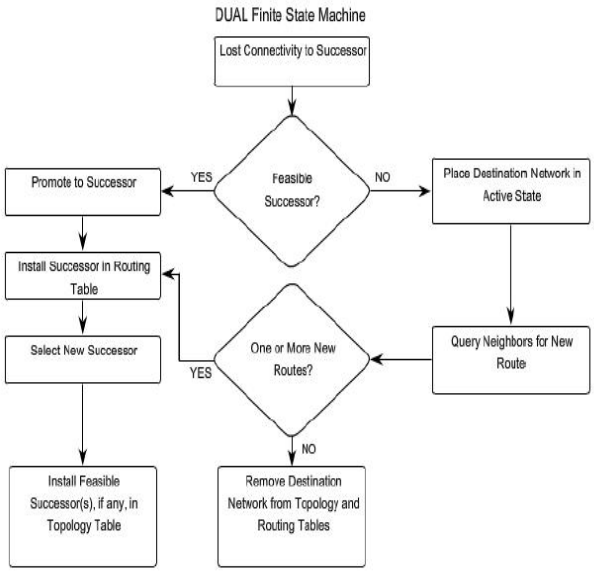

Fig No.7 DUAL Algorithm

3.4 HUB AND SPOKE TOPOLOGY

The hub and spoke topology network is a traditional proven and widely used topology for all types of network then it is called as star topology. Access point is physically connected to the internet with a wire like spokes on a wheel. All the user devices are connected to the wireless router in the center as shown in Fig no.8

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 4, April 2018

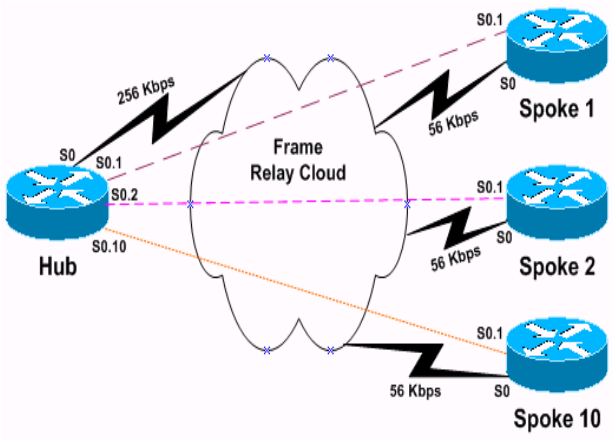

Fig No.8 Hub and Spoke Topology

.In hub and spoke topology multiple VPN routers communicate securely with a central VPN routers and a separate secured tunnel extends between each individual spoke and the hub as discussed in [4]. So this topology allows customers at remote sites to access the main network. It is also called as a mesh topology in which the devices are connected with many redundant interconnections between network nodes, whereas in true mesh topology every node is connected to other node in the network. A hub is a common connection point for devices in a network and it is used to connect segments of a LAN & contains multiple ports when a packet arrives at one port it is copied to other port so that all segments of the LAN could be viewed by all packets. It is a most basic networking device that connects multiple computer devices together.

IV. RESULTS AND DISCUSSIONS

This paper is done by applying GNS3 software, as this software does all the function in real time mode. It is uniform and effectively loop free, that can balance load network traffic between multiple paths of same metric which has been maintained throughout the entire section. Apart from that this method also supports logical grouping of network in to segments. In this paper 8 routers are designed of individual users with EIGRP configuration, each router is tested by using commands and end to end connectivity is verified as shown in Fig no.9. Since each router has unique IP address it creates a highly secured data transmission.

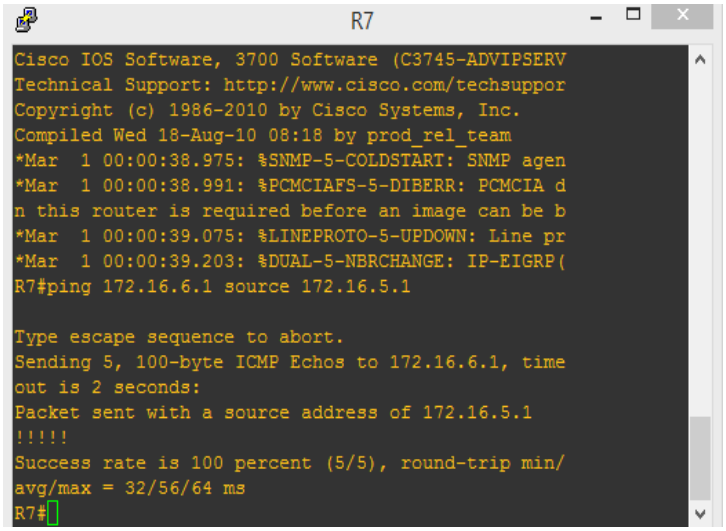

Fig No.9 Peer-to-peer connectivity

The existing method used in virtual private network is routing information protocol, which uses public key so it is less secured. It uses broadcast function, thus connectivity is done only to a single router at a time. . In this proposed the routers are implemented for 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 acts as dual way in evaluating the error as well as selecting the most appropriate shortest path available. And it uses unique IP address so the data transmission is highly secured compared to the existing method.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 4, April 2018

V. CONCLUSION

In this paper, the EIGRP for high secured data transmission using unique IP address is proposed. The simulation result shows that EIGRP provides end to end connectivity to all the users. The simulation result shows that EIGRP configuration provides end to end connectivity to all the routers. It uses Hub and spoke topology to control the traffic mechanism. Multicasting is done for the routers obtaining a reduced convergence time of 90milliseconds. This method also analyze the performance of MPLS routing protocol, which having the maximum hop count of about 256 and the data is highly secured by using the IP address & private key utilization and also it have both equal and unequal cost load balancing. In future, the EIGRP can be replaced by the Border Gateway Protocol (BGP) to minimize the convergence time and improve the security of data.

REFERENCES

[1] 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.
[2] 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.
[3] I.S.I Alsukayti and T.J.Dennis, "Performance Analysis of VoIP over BMG/MPLS VPN Technology", PGNET Conference, 2013.
[4] 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.
[5] D. Frost, S. Bryant," Packet Loss and Delay Measurement for MPLS Networks", Internet Engineering Task Force (IETF),2011
[6] 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.
[7] Deepankar Medhi, Karthikeyan Ramasamy, Network Routing Algorithms, Protocols, and Architectures, Elsevier,2007.
[8] David Bauery, Murat Yukselz, Christopher Carothersyand, Shivkumar Kalyanaramanz" A Case Study in Understanding OSPF and BGP Interactions Using Efficient Experiment Design", IEEE computer society,2006.