IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 3, March 2019

Implementation of Hub & Spoke Topologies in VPN using EIGRP

Gayathri.G[1], Sindhuja.G[2]

Assistant Professor, Department of Computer Science, Ponnaiyah Ramajayam Institute of Science and Technology
Prist University, Thanjavur[1]

M.C.A., Scholar, Department of Computer Science, Ponnaiyah Ramajayam Institute of Science and Technology
Prist University, Thanjavur[2]

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).

1. 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 in order 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 in order 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. 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.

II. LITERATURE REVIEW

Dynamic Multipoint VPN (DMVPN) is a Cisco proprietary technology that allows secure exchange of data between remote sites (typically branches of an organization) without needing to route traffic through an organization head quarters, as in traditional point-to-point VPN. Traditional IPSec VPNs connect sites in a point-to-point topology; in typical networks, each branch is connected to the headquarters (called the hub). This makes branch-to-branch communication to operate lower than the optimum, as traffic from a branch to another must first be routed through the headquarters. This method also places a lot of pressure on the hub router's resources as the overhead increases. A DMVPN network, on the other hand, creates a mesh-like VPN topology by dynamically providing secure channels between each remote site on an on-demand basis. The security feature of DMVPNs is usually provided by the IP security (IPsec) technology, which handles the encryption, and other technologies such as Internet Security Management and Key Management Protocol (ISAKMP). IPSec is a framework of open standards that secures connection between pairs of routers, gateways, hosts, server and PCs, or PCs and gateways. As with every other protocol, IPSec defines rules for secure connections [4].

Benefits of DMVPN includes: reduced hub router configuration because several lines of configurations are written to define crypto map characteristics, access lists, and Generic Routing Encapsulation (GRE) tunnel interfaces for each spoke router that is added to the network for ordinary VPN. With DMVPN, only a single multipoint GRE (MGRE) interface and a single IPSec profile are configured. This greatly reduces the amount of configurations that must be entered no matter how

DOI 10.17148/IJARCCE.2019.8319

many more spokes are added to the network, as many spokes can be grouped into MGRE interface, eliminating the need for separate physical/logical interface for each spoke on the network as in ordinary multipoint VPN [4][5]. DMVPN allows spoke routers to have dynamically assigned physical interface IP addresses. Whenever a spoke router comes online, registration packets containing its new physical interface IP address are sent by it to the hub router. Registered spokes obtain IP addresses of other registered spokes from the hub router. DMVPNs can be used to extend the Multiprotocol Label Switching (MPLS) networks that are deployed by service providers to take advantage of the ease of configuration of hub and spokes, to provide support for dynamically addressed customer premises equipments (CPEs), and to provide zero-touch provisioning for adding new spokes into a DMVPN [6]. Every spoke registers as a client of the Next Hop Resolution Protocol (NHRP) server, which is also the hub.

III. EXISTING SYSTEM

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 in order to determine network distance whereas other routing protocol provides less information on their own to other network.

OPEN SHORT PATH FIRST (OSPF)
OSPF is a routing procedure for internet procedure networks. It uses a linkage state routing algorithm and reductions into the group of inner entry routing procedure within a single independent system. It can load stability network traffic flow 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 procedure in which all routers in the routing domain exchange info and thus know about the complete topology of the network

DISADVANTAGES:

- Routing procedures are used on all devices to distribute the routing info. Nevertheless of the routing procedure, routers always forward packets based on the destination address only.
- The only immunity is policy-based routing (PBR) that bypasses the purpose-based routing lookup. Routing lookups are accomplished on every router.
- Every router in the network makes an autonomous decision when forwarding packets.
- Traditional IP forwarding does not have a scalable machine to allow the application of the backup link (unequal load balancing).
- Policy-built routing could be used to select some packets and route those along the backup link.
- But this is not likely in high capacity traffic due to presentation limitations.

IV. PROPOSED SYSTEM

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].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. 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

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 The DUAL protocol scans all

DOI 10.17148/IJARCCE.2019.8319

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.

Advantages:

- Provide a diversified range of services (Layer 2, Layer 3 and Dial up VPNs) to meet the requirements of the entire spectrum of customers from Small and Medium to Large business enterprises and financial institutions.
- Make the service very simple for customers to use even if they lack experience in IP routing.
- Make the service very scalable and flexible to facilitate large-scale deployment.
- Provide a reliable and amenable service Offering SLA to customers.
- Capable of meeting a wide range of customer requirements, including security, quality of Service (QOS) and any-to-any connectivity and Capable of offering full managed services to customers.

V. HUB &SPOKE

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 . 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.

VI. 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 TechnologyNetwork, 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.

DOI 10.17148/IJARCCE.2019.8319