IJARCCE

ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10752

Dynamic Multipoint Virtual Private Network using Routing Information Protocol in GNS-3

Poojitha Hegde[1], Prof. P. Jayarekha[2]

M.Tech., Computer Network and Engineering, BMS Institute of Technology, Bangalore, Karnataka, India[1]

BMS Institute of Technology, Bangalore, Karnataka, India[2]

Abstract: Computer networks has become the most substantial problem in our day-to-day life. The subsequent research paper presents an outline regarding the evolving technology of Dynamic Multipoint VPN. The main purpose of this research paper is to understanding the working principle of Dynamic Multipoint VPN in GNS3 tool using RIP protocol by building tunnel and providing security features(encryption) so that spokes can access hub resources.

Keywords: VPN, GNS3, RIP, tunnel, encryption

I. INTRODUCTION

Computer network has become the most substantial issue in our day-to-day life. Computer network is a collection of two or more interconnected computer systems that has latent to transmit, receive and exchange data, voice and video traffic. In modern time, computer networks are crucial as information technology is increasing quickly all over the world. Networks can be wired or wireless but most networks will use both. In this dissertation, DMVPN is designed using GNS3. GNS3 stands for Graphical Network Simulator-3 is a network software emulator which is used to simulate complex networks. It may be used on multiple OS such as Windows, Linux, MacOS and runs on traditional PC hardware. To simulate Cisco IOS, GNS3 uses Dynamips emulation software. VPN permit users to send and receive information athwart public network. VPN is formed by establishing a virtual point-to-point connection through dedicated circuits or with tunnelling protocols over the existing networks. The drawbacks comprises being blocked by certain services, decrease your speed ,isn't legal in all countries. DMVPN is a hub and spoke network used to build VPN with multiple site without statistically configuring all devises. In DMVPN ,one central router is located at the head office which accepts the role of the hub while all other branch routers are spokes that links to the hub router so the branch offices can access the company resources.

II. TECHNOLOGY TO BE USED

IP Address: IP Address stands for Internet Protocol address which is a numerical label assigned to every device connected to a computer network. It is used for identification of LAN and host which is also called hierarchical address. The versions of IP are IPv4 and IPv6.IPv4 is a 32-bit address with 2^{32} unique address. IANA globally manages IP address and five RIRs that manages with in a region of the world for allocation and registration of internet number resources. The IP Address of each device connected to a network will be assigned by network administrators.

RIP: RIP stands for Routing Information Protocol used to find best path from source to destination using hop count as a routing metrics. Hop count is defined as between source and destination number of routers occurs. Lowest hop count path is considered as the best path route to reach a destination.15 is the maximum hop count allowed and with hop count 16 is considered as network unreachable.

Tunnelling: Tunnelling is a technique in computer network allows the transfer of data from one network to another network through public network. The different tunnelling protocols are point-to-point tunnelling protocol (PPTP), GRE, SSH, IPsec.

NHRP: NHRP is an acronym for Next Hop Resolution Protocol which allows NHC (Next Hop Client) to dynamically register with NHS (Next Hop Server). In DMVPN, spoke routers are NHC whereas hub router is NHS. Once all clients are registered spoke routers can discover other spoke routers within same NBMA network.

mGRE: mGRE stands for multipoint GRE is a tunnelling protocol which enables node to communicate with many nodes i.e. It is one to many links.

3DES: DES or TDES stands for Data Encryption Algorithm because it uses Data Encryption Standard cipher three times

ISSN (O) 2278-1021, ISSN (P) 2319-5940

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10752

to encrypt its data.DES created on a Feistel network is a symmetric key algorithm. The same key is used for encryption and decryption process by the symmetric key cipher.

MD5:MD5 stands for Message Digest algorithm 5 most widely used hash algorithm which was created by Ronald Rivest. Based on any input length, MD5 creates 128-bit hash value.

III. BASIC ARCHITECTURE

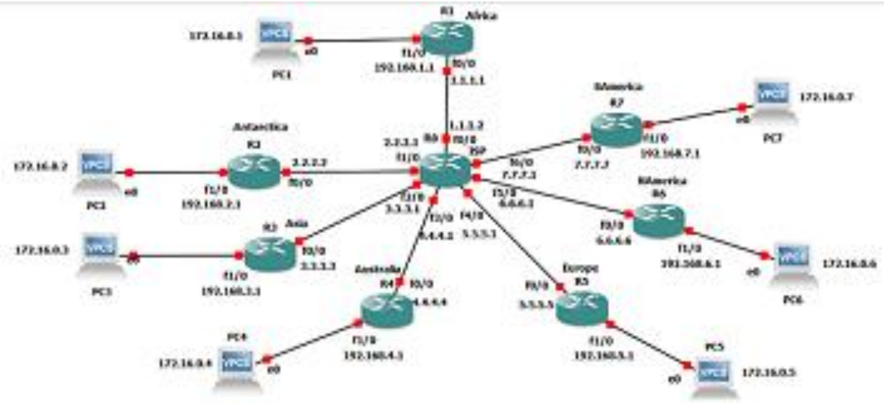


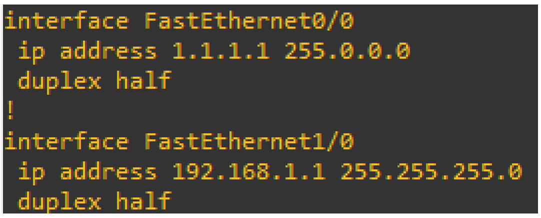
Fig.1. System Design

IV. WORKING OF DMVPN

The implementation part is divided into three phases both for hub and spoke they are

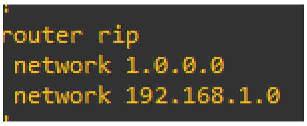
- Connectivity phase
- Confidentiality phase
- Encryption phase

In connectivity phase, it consists of commands for assigning IP address and routing protocols namely RIP for both Hub and spoke routers.



```
interface FastEthernet0/0
 ip address 1.1.1.1 255.0.0.0
 duplex half
!
interface FastEthernet1/0
 ip address 192.168.1.1 255.255.255.0
 duplex half
```

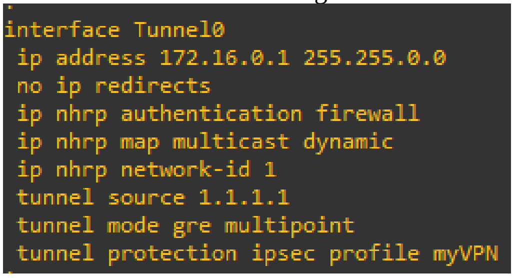
Fig.2. Assigning IP Address



```
router rip
 network 1.0.0.0
 network 192.168.1.0
```

Fig.3. Assigning RIP

In confidentiality phase, it consists of commands used for building a tunnel.



```
interface Tunnel0
 ip address 172.16.0.1 255.255.0.0
 no ip redirects
 ip nhrp authentication firewall
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 tunnel source 1.1.1.1
 tunnel mode gre multipoint
 tunnel protection ipsec profile myVPN
```

Fig.4. Building tunnel

IJARCCE

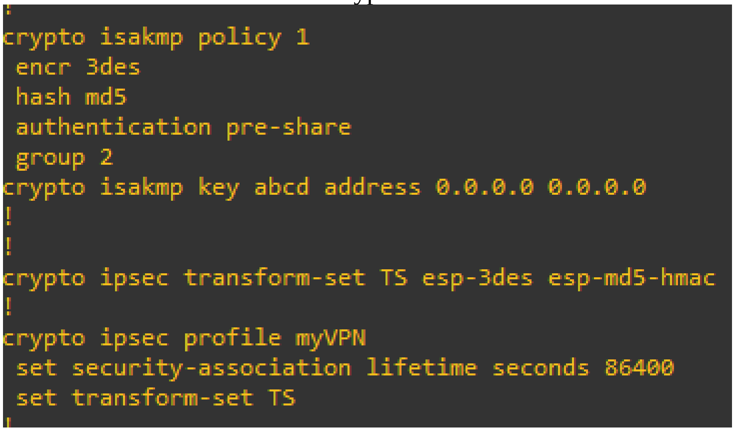
ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10752

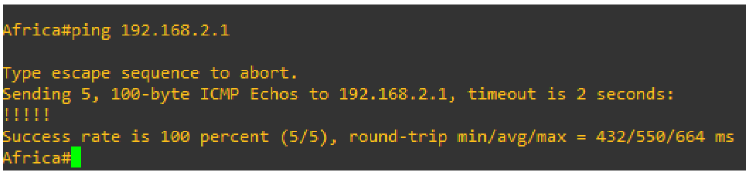
In encryption phase, it consists of commands used for encryption.



```
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key abcd address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto ipsec profile myVPN
 set security-association lifetime seconds 86400
 set transform-set TS
!
```

Fig.5. Providing Encryption

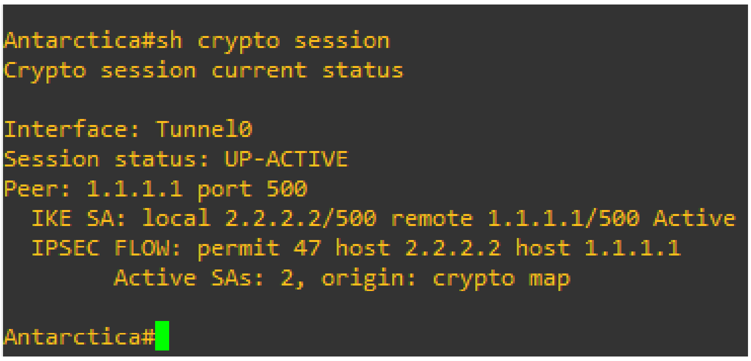
V. RESULTS



```
Africa#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 432/550/664 ms
Africa#
```

Fig.6. Ping command



```
Antarctica#sh crypto session
Crypto session current status

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 1.1.1.1 port 500
  IKE SA: local 2.2.2.2/500 remote 1.1.1.1/500 Active
  IPSEC FLOW: permit 47 host 2.2.2.2 host 1.1.1.1
        Active SAs: 2, origin: crypto map

Antarctica#
```

Fig.7. Verifying DMVPN crypto tunnel

VI. CONCLUSION

In this paper we initially discuss about VPN and its disadvantages. Then we explore various base papers and their implementation. Next, we analyse how DMVPN is more efficient than VPN and discuss about the methodology of DMVPN using GNS3 tool. Finally, we discuss about the result.

REFERENCES

[1] Billl Treneer (n.d.) Dynamic Multipoint Virtual Private Network

[2] Nemah Alsayed (12-May-15) Virtual Private Networks, Dar Al-Hekma University

[3] Ayoub Bahnasse (August 2015) Study and Analysis of a Dynamic Routing Protocols' Scalability over a Dynamic Multi-point Virtual Private Network, International Journal of Computer Applications.

[4] Roumaissa Khelf and Nacira Ghoualmi-Zine "A Survey on Dynamic Multipoint Virtual Private Networks ".Network and System Laboratory-LRS Computer Science department Badji Mokhtar-Annaba University : The 8th International Seminary on Computer Science Research at Feminine .

[5] Ritika kajal, Deepshikha Saini, Kusum Grewal (October 2012) Virtual Private Network, : International Journal of Advanced Research in Computer Science and Software Engineering

[6] Weili Huang and Fanzheng Kong. The research of VPN over WLAN.