Study and Analysis of a Dynamic Routing Protocols' Scalability over a Dynamic Multi-point Virtual Private Network

Ayoub Bahnasse
STIC Laboratory
Department of physics, Faculty of Sciences
Chouaïb Doukali University
El Jadida Morocco

Najib El Kamoun
STIC Laboratory
Department of physics, Faculty of Sciences
Chouaïb Doukali University
El Jadida Morocco

ABSTRACT
Dynamic Multipoint Virtual Private Network "DMVPN" is a solution for the dynamic creation of virtual Private IP tunnels between multiple sites automatically, quickly and with the least configuration. Routing protocols are component technologies' main parts of the DMVPN solution, they ensure the smooth establishment of tunnels and have a major impact on network's behavior and transported applications, many works have been conducted assessing the performances of DMVPN network with various routing protocols, this paper enhances and complements other studies, firstly by offering suitable configurations of routing protocols recommended for a scalable DMVPN network, secondly by studying scalability of DMVPN by varying number of sites and dynamic routing protocols. Used evaluation criteria are: Initial convergence delay, Sent traffic, Throughput, Queuing delay.

Keywords
DMVPN; Performances; Routing protocol; Convergence delay; scalability; EIGRP; BGP; OSPF.

1. INTRODUCTION
Taking into account the fast moving of digital communications, companies are tending increasingly to use these new technologies for the storage of their data and archiving their activities with a quick, secure and distributed manner over several sites, with the use of VPN technologies, companies can communicate with each other securely through a public shared infrastructure "Internet" with a low cost compared to traditional solutions such as Frame Relay, ATM … [1] [2].

Most of enterprises extend their branches, which constitutes a scalability problem, a reconfiguration of all equipment and a reservation of new static public IP address must be done. Dynamic Multipoint Virtual Private Network solution "DMVPN" [3] proposed by Cisco corporation guarantee a full meshed connection between multiple sites with a dynamic, quick and automatic manner, DMVPN offers scalability, i.e. involves no extra configuration on already configured equipment. DMVPN architecture consists mainly of a Hub and a Spoke routers, Hub router called head office router, play a main role on dynamic creation of tunnels between multiple spokes, the latters are called Branch office routers, from the deployment perspective spokes builds a dynamic permanent tunnel to the HUB but not to other spokes, tunnels between spokes are temporary created on demand and deleted when exchanges are finished. DMVPN solution is based on the standard protocols; Multipoint Generic Routing Encapsulation « mGRE », Next-Hop Resolution Protocol « NHRP », Internet Protocol Security « IPsec » and routing protocols, the settings of these protocols vary from one architecture to another, the method "Policy-Based Management of a Secure Dynamic and Multipoint Virtual Private Network" enables centralized management of multiple DMVPN equipment, through a single graphical interface [4].

- mGRE: Generic routing protocol [5] is a tunneling protocol that can encapsulate a variety of network layer protocols inside IP protocol [6], GRE tunnels forwards Unicast, Multicast and broadcast traffic but they are static it means that a specification of combination of source and destination of each tunnel is required, mGRE allows to establish multiple tunnel across a single physical interface with multiple dynamic destinations.
- NHRP: Next Hop Resolution Protocol [7] is a resolution protocol like ARP and RARP on frame relay network, NHRP is used by a Spoke connected to Non Broadcast Multi-Access "NBMA" to determine the IP address of the NBMA Next-Hop physical address (Public address), that could be of the HUB or another Spoke on the same cloud. All Spokes called Next-Hop Clients (NHC) register their physical addresses mapped to logical addresses (Tunnel address) with the HUB called Next-Hop Server (NHS), to ensure success of these registrations, NHS and NHC must be connected to the same Cloud and uses identical network ID and Network Password, the addresses of NHS must be pre-configured on each branch router. NHS Stores all registered mappings and replies to NHRP request from Clients. NHRP allows mGRE tunnel endpoint to discover each other's physical IP address.
- IPsec: defined on RFC 2401 is a network layer protocol, IPsec is a protocol suite to ensure Internet Protocol "IP" security, existing IPsec implementations usually include, Encapsulation Security Payload "ESP" [8] and Authentication Header protocol "AH" [9], ESP protocol ensure confidentiality (Encryption), Source authentication (Authentication) and data integrity checking (Integrity), AH protocol ensures integrity and authentication of data, IPsec operates in two majors modes, Tunnel mode and Transport mode; Transport mode is used for end to end communications, this mode does not change the original header it remains intact expected that IP protocol field is changed to ESP or AH, Network Address Translation can cause some integrity

issues [10], Tunnel mode is the default mode, this mode protect the entire IP packet and wraps the original packets, encrypts it then adds a new IP header before sending it to other site.

- Dynamic routing protocols (detailed on the next section) are responsible for the creation, maintenance and updating dynamically routing tables, in order to ensure optimal exchange of data between various sites.

Many research studies have been conducted assessing the performances of DMVPN network [11][12][13], the first article evaluate the performances of DMVPN network varying both, dynamic routing protocols and the size of intermediaries routers, as DMVPN is a client solution, this was a good motivation to complete and to enhance the work by assessing DMVPN performances by varying the number of client side routers, others works deal with the best practices for deploying dynamic routing protocols on DMVPN networks but without showing the improvement to the network.

This paper firstly presents the suitable configurations of routing protocols recommended for a scalable DMVPN network, secondly studies the DMVPN network scalability by varying a number of sites and dynamic routing protocols. Used evaluation criteria are: Initial convergence delay, Sent traffic, Throughput, Queuing delay, this study was done using OPNET Modeler 14.5 simulator.

The rest of the paper is organized as follows, in section 2 we will be presenting dynamic routing protocols and their best practices recommended for DMVPN network, in section 3 we will present scenarios of scalability evaluation, section 4 will be reserved for interpretation of results obtained, and we will conclude on section 5.

2. DYNAMIC ROUTING PROTOCOLS ON DMVPN NETWORK

Dynamic routing is a network technique that ensures optimal data routing between different sites, dynamic routing uses multiple protocols and algorithms in order to enable routers to select best paths according to real-time network states, dynamic routing protocols detects also failures and rebuilds other paths [25]; there are two main types of dynamic routing protocols; Interior Gateway Protocol "IGP" and Exterior Gateway Protocol "EGP", IGP is used for exchanging routing information between routers within an autonomous system , EGP allows the interconnection between multiple autonomous systems, dynamic routing protocols can be divided into three categories : Distance Vector routing protocols (DV), Link State routing protocols (LS) and Path Vector routing protocol (PV) [Table. 1]

Table 1.Classificationof dynamic routing protocols

Name	Type	Update	Metric	VLSM	Summary
RIPv1	DV	30 sec	Hops	No	Automatic
RIPv2	DV	30 sec	Hops	Yes	Automatic
IGRP	DV	90 sec	Composite	No	Automatic
EIGRP	Advanced. DV	triggered	Composite	Yes	Automatic + Manual
OSPF	LS	triggered	Cost	Yes	Manual
IS-IS	LS	triggered	Cost	Yes	Automatic
BGP	DV	triggered	N/A	N/A	Manual

2.1 Enhanced Interior Gateway Protocol « EIGRP »

EIGRP is an advanced distance vector protocol developed by Cisco standardized IETF [14], EIGRP uses bandwidth, delay, load and reliability to calculate the metric for its routing table (1)

256*[(K1.Bandwidth) + (K2.Bandwidth) / (256-Load) + K3.Delay). (K5/ (Reliability + K4))) (1)

Among the advantages of the EIGRP routing protocol is ; its ability to operate in multiple architectures, it can be used in conjunction with IPv4, IPX and AppleTalk, more importantly, its modular architecture will readily enable to support for other routed protocols that may be developed in the future, EIGRP use Diffusing Update algorithm "DUAL" to provide fast convergence [15] and to determine whether a path advertised by a neighbor is looped or loop-free, and allows a router running EIGRP to find alternate paths without waiting on updates from other routers.

To ensure that DMVPN network works perfectly and guarantees an optimum dynamic routing exchanges some settings must be made; At the HUB side, IP SPLIT HORIZON option should be disabled to ensure that the HUB will advertise routes out the interface tunnel on which they was received , also to disable the IP NEXT-HOP-SELF option, by default, the HUB sets the IP next-hop value to be itself for routes that it is advertising, with this option Spokes will always pass through HUB to communicate each other [16]. At the spokes, STUB connected option [17] must be enabled in order to permit spoke to re-advertise only directly connected routes to reduce resource utilization by optimizing the size of routing updates and ensure stability.

Table 2 shows the recommended configuration of EIGRP on DMVPN network.

Table 2. EIGRP Cisco command line configuration of HUB and SPOKE routers

HUB	SPOKE
router eigrp 1 network 10.0.0.0 network 192.168.0.0 no auto-summary interface tunnel0 no ip split-horizon eigrp 1 no ip next-hop-self eigrp 1	router eigrp 1 network 10.0.0.0 network 192.168.1.0 no auto-summary eigrp stub connected

2.2 Open Shortest Path First "OSPF"

OSPF is a link-state routing protocol for both IPv4 and IPv6 networks, it is designed to be run internal to a single Area. Each OSPF router maintains an identical database describing the Area topology. From this database, a routing table is calculated by constructing a shortest-path tree. OSPF by convention area 0 represents backbone or core area, standard area's must have a direct or virtual connection to the OSPF backbone area in order to exchange routing tables between them, in order to reduce traffic amount between routers on the same area, an election of designated router "DR" and backup designated router "BDR" can be made,

OSPF in a DMVPN network that represents the same OSPF limits in other networks; we should not put more than three zones in the same router with a maximum of fifty per area. Router in a DMVPN network CPO resources are not consumed only OSPF but also by the IPsec encryption and NHRP trade [18] over the designated router must be connected with all the other spokes of its architecture.

For better scalability and stability, an OSPF router should not

be configured by more than three areas [19], in addition to a high CPU usage due to complex algorithm used by OSPF, the additional overhead of encryption and NHRP negotiations must be taken into consideration during the conception of the network topology.

DMVPN network stability and scalability using OSPF is limited by two factors, mainly the addressing plan and the design of the architecture topology, To create a scalable DMVPN network using OSPF it's required to implement an effective hierarchical addressing scheme. The addressing structure implemented can have a profound impact on the performance and scalability of the DMVPN network.

To ensure that DMVPN network works perfectly and guarantee an optimum dynamic routing exchanges some settings must be made; At the HUB side, The mGRE tunnel on the hub router must be configured as an OSPF broadcast network to allow the selection of a DR, the point to multipoint network type can also be used but the election is not guaranteed, contrariwise, tables topologies exchange will be made as in point-to-point network, this is a disadvantage, as the number of adjacencies will be too much high than broadcast network, [Fig. 1] shows the convergence duration in a DMVPN network consisting of five sites configured with OSPF point to multipoint and broadcast network, on the point to multipoint network ten adjacencies are created , while on the Broadcast mode just four adjacencies are established, offering a 150% rate of improvement of convergence duration.

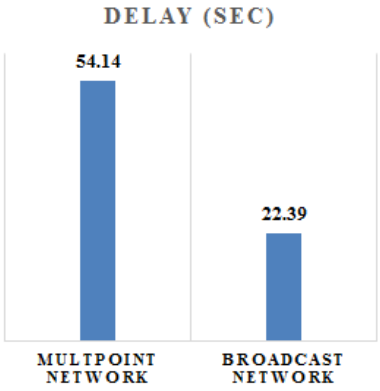

Fig 1: OSPF Broadcast network Versus OSPF point to Multipoint network

HUB router must have the higher priority to become designated router of the area, and each spoke router is configured with an OSPF priority of 0, to prevent a spoke from becoming the DR. In addition, the hello timer on the spoke should be changed from the default of 10 seconds to 30 seconds if the spoke is configured with p2p GRE and the hub is mGRE. The tunnel IP MTU must match on all GRE interfaces, OSPF areas running over DMVPN should be stubby or totally stubby areas to minimize Link State Advertisements flooding over the WAN [20]

Table 3 shows the recommended configuration of OSPF on DMVPN network.

Table 3.OSPF Cisco command line configuration of HUB and SPOKE routers

HUB	SPOKE
router ospf 10 net 10.0.0.0 0.0.0.255 area 0 net 192.168.0.0 0.0.0.255 area 0 area 10 stub no-summary interface tunnel0 ip ospf network broadcast ip ospf priority 200	router ospf 10 net 10.0.0.0 0.0.0.255 area 0 net 192.168.1.0 0.0.0.255 area 0 area 10 stub no-summary interface tunnel0 ip ospf network broadcast ip ospf priority 0

2.3 Border Gateway Protocol "BGP"

BGP, defined on RFC 1771, is an External Routing Protocol "EGP", generally used to interconnect different autonomous systems, it aims to exchange prefixes (IP addresses + Mask) between neighbors using TCP port 179 connections.

BGP can be used to exchange routing information: in the same autonomous system (Interior BGP- iBGP), or between different autonomous systems (Exterior BGP- eBGP). Generally eBGP sessions are established over the point-to-point links, in contrast iBGP sessions are usually established between remote logical addresses.

BGP is not a transitive protocol, i.e. it sends routing updates to manually specified neighbors. In the case of a network that consists of 40 sites, 780 adjacencies must be configured in order to achieve convergence state. A route reflector (RR) option [26], offers an alternative to the logical iBGP full-mesh requirement, A RR acts as a meeting point for IBGP sessions. Multiple BGP routers can peer with a common meeting point, Route reflectors can then advertise updates received from an iBGP peer to another iBGP peer.

Table 3 shows the recommended configuration of BGP on DMVPN network.

Table 4 BGP Cisco command line configuration of HUB and SPOKE routers

HUB	SPOKE
router bgp 1 no synchronization neighbor UCD peer-group neighbor UCD remote-as 1 neighbor UCD route-reflector-client bgp listen range 10.0.1.0/24 peer-group UCD network 192.168.0.0 no auto-summary	router bgp 1 no synchronization neighbor 10.0.1.1 remote-as 1 neighbor 10.0.1.1 send-community no auto-summary network 192.168.1.0

3. SCENARIOS OF SCALABILITY EVALUATION

This section describes the proposed scenario used to evaluate scalability of DMVPN network using OSPF, EIGRP and BGP routing protocols, the scenarios was created using DMVPN Automatic Simulation Tool [21].

Opnet modeler is a communication system discrete event simulator "DES" developed by OPNET Technologies, which enables the design and study of all communication networks and distributed systems. Opnet Modeler compared to other simulators offers a fast simulation capabilities and the ease of use [22] [23] [24].

Figure 2 illustrates a DMVPN scenario, consisting of six

routers: one HUB and five SPOKEs.

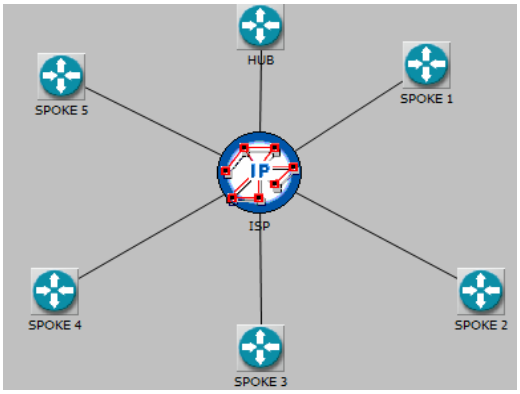

Fig.2. 6 SITES

In order to study the scalability of the DMVPN network, an increase in the number of sites is required; two additional scenarios was proposed: [Fig.3] illustrates a scenario consisting of 11 routers (10 Spokes and 1 HUB) and [Fig.4] illustrates a scenario consisting of 20 Spokes and 1 HUB.

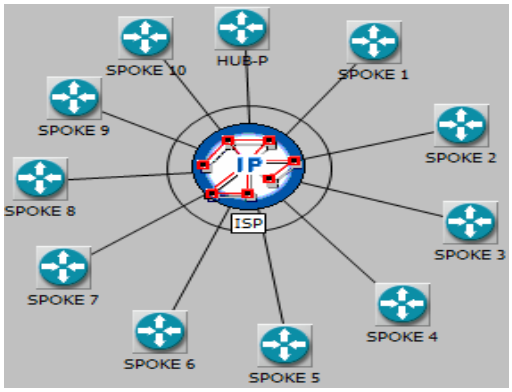

Fig.3. 11 SITES

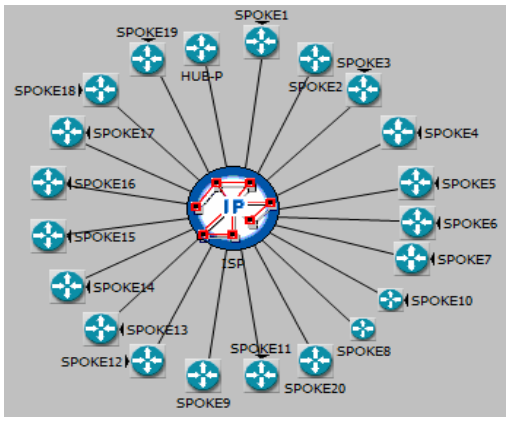

Fig.4. 21 SITES

A brief description of the IPsec attributes used in different scenarios is shown in table 5.

Table 5.IPsec attributes used in simulations

IKE 1 and 2 encryption	IKE 1 and 2 hash	authentication	DH	Tunnel mode
DES	MD5	Pre-share	5	Transport

4. INTERPRETATION OF OBTAINED RESULTS

4.1 Convergence Duration

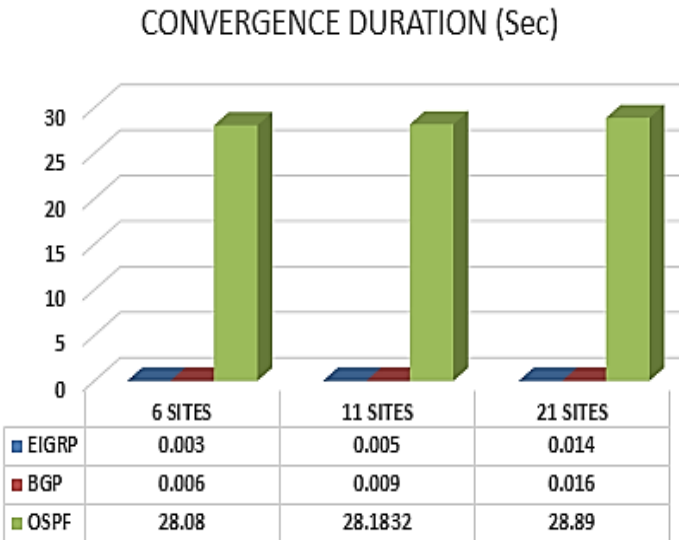

Fig.5.Convergence Duration

Figure 5 represents the convergence duration of three scenarios with different routing protocols, as shown above, EIGRP offers the most optimal convergence delay because of DUAL algorithm used, EIGRP uses two techniques to converge quickly, firstly, EIGRP send partial updates only when a change occurs, secondly, EIGRP takes into consideration the available bandwidth during the transmission of routing updates, By default, EIGRP uses 50 percent of an interface's bandwidth for routing exchanges, this prevents the EIGRP process from over-utilizing a link.

Unlike the EIGRP or BGP, OSPF performs a DR election during the first exchanges, the designated router forms full adjacencies to all neighbors and calculates topology map, in addition to time required by flooding LSA, the time of encryption and decryption of LSA is added. In order to calculate loop free path, DR router relies on all routers within the same area to have the same view of network's topology, that justifies the higher delay proposed by OSPF protocol.

BGP was designated to scale with the internet growth, taking into account that no policies was configured and the number of peers isn't enough to impact the BGP convergence such as Internet peers, also the neighbor's adjacencies was already specified, BGP offers a small convergence delay compared to OSPF.

During the increase of sizes of the networks, routing protocols have kept the same orders in terms of convergence duration, however, EIGRP convergence duration was influenced by a factor of 66.66 percent on 11 sites compared to 6 sites, and by a factor of 180% on 21 sites compared to 11 sites, these results are justified by the growth of formed adjacencies. BGP requires a higher delay on 11 sites scenario in comparison to 6 sites scenario by a factor of 50%, and 77.77% on 21 sites scenario compared with 11 sites. OSPF remains the most stable despite its high convergence delay, 0.36% and 2.50% are the additional convergence delays required respectively from the transition from 6 sites to 11 sites and from 11 sites to 21 sites.

4.2 Traffic sent

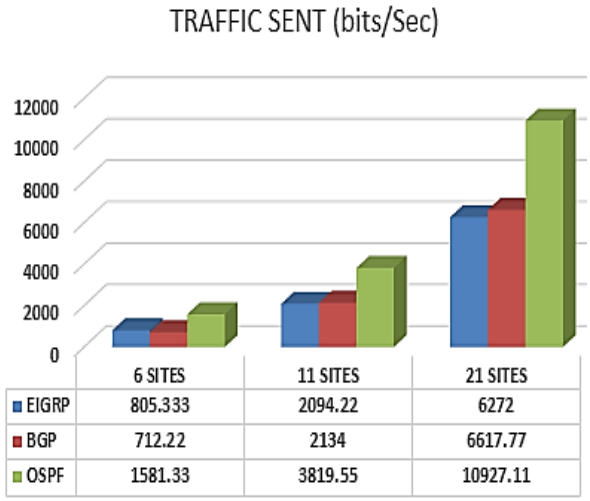

Fig. 6. Traffic sent

From the simulation results as shown on Figure 6, EIGRP generates less traffic in the network compared to OSPF and BGP, for several reasons among them we have noticed ; the simplicity and the reduced number of messages during the formation of adjacencies, also the calculation of topology is performed on each topology router. In opposition to EIGRP, OSPF performs an election of the designated router by flooding LSA type 1 and 2, and pass through many state to achieve the convergence state (Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading and Full). BGP doesn't dynamically establish adjacencies like EIGRP neither performs an election as OSPF, but it relies on TCP to open sessions, given that the Route Reflector option is enabled, this option as mentioned previously reduces the number of adjacencies but also overloads the HUB link, this later advertises updates received from an iBGP peer to another iBGP peer.

4.3 Throughput

Figure 7 illustrates required throughput on ISP-HUB link to achieve convergence state, as expected the throughput is consistent with sent traffic. OSPF requires the highest throughput followed by BGP and EIGRP, even if the sent traffic of BGP was nearly similar to that of EIGRP, BGP requires more throughputs than the EIGRP does. Protocols keep the same order on all ISP-SPOKE links.

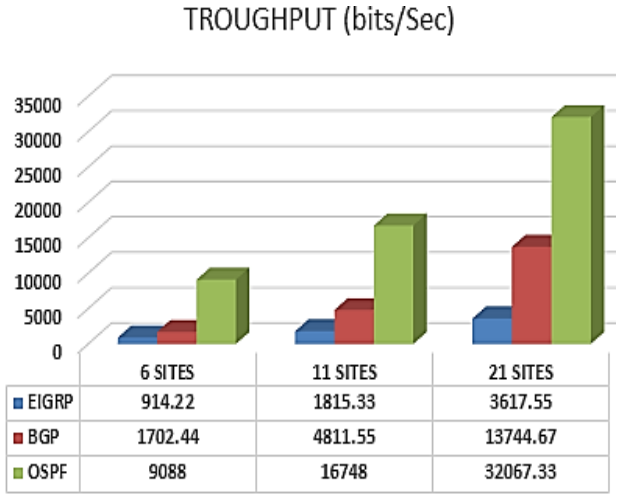

Fig. 7. Throughput

4.4 Queuing

This criterion represents instantaneous measurements of packets waiting times in the transmitter channel's queue. Measurements are taken from the time a packet enters the transmitter channel queue to the time the last bit of the packet is transmitted, it depends on both the router and the routing protocol.

Figure 8 represents the queuing delay on the HUB side, shown values are small because no user flow was simulated. Below graph indicates that EIGRP has Lowest queuing delay than OSPF and BGP.

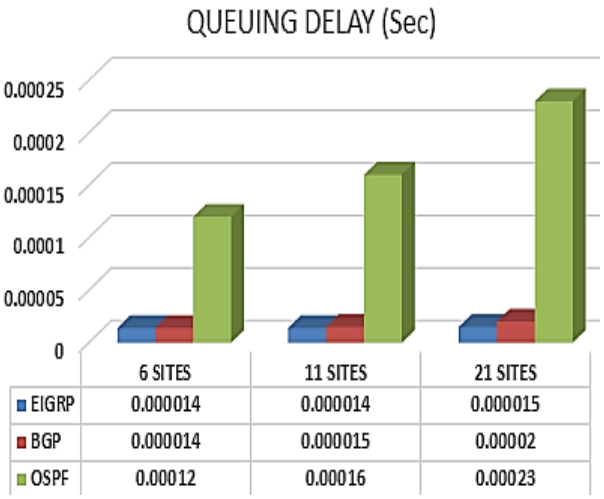

Figure 8. Queuing Delay

5. CONCLUSION

This paper discussed the Dynamic Multipoint Virtual Private Network Solution, suitable configurations of EIGRP, OSPF and BGP routing protocols for a scalable DMVPN network and studied the behavior of DMVPN network using previously mentioned protocols. Comparative analysis shows that EIGRP protocol is the best in terms of initial convergence delay, Throughput and queuing delay, BGP shows its efficiency compared to OSPF, this later is not recommended on DMVPN network as shown on obtained results.

6. REFERENCES

[1] Bhaskaran, S., Desai, S., Jou, L., & Matthews, A. R. (2007). U.S. Patent No. 7,263,106. Washington, DC: U.S. Patent and Trademark Office.

[2] Chase, C. J., Holmgren, S. L., Medamana, J. B., & Saksena, V. R. (2001). U.S. Patent No. 6,188,671. Washington, DC: U.S. Patent and Trademark Office.

[3] Dynamic Multipoint VPN (DMVPN) Design Guide, Corporate Headquarters Cisco Systems, Inc. 2006, 104 p

[4] Bahnasse, A., & El Kamoun, N. (2014). Policy-based Management of a Secure Dynamic and Multipoint Virtual Private Network. Global Journal of Computer Science and Technology, 14(8).

[5] Hanks, Stan, David Meyer, Dino Farinacci, and Paul Traina. RFC 2784-"Generic routing encapsulation (GRE)." (2000).

[6] P. Christian. RFC 3147 - Generic Routing Encapsulation over CLNS Networks. Nortel Networks, July 2001

[7] Luciani, J., D. Katz, D. Piscitello, B. Cole, and N. Doraswamy. "Next hop resolution protocol (NHRP)."

RFC2332 (2001).

[8] Huttunen, Ari, Brian Swander, Victor Volpe, Larry DiBurro, and Markus Stenberg. UDP encapsulation of IPsec ESP packets. RFC 3948, January, 2005.P.

[9] Kent, Stephen. IP authentication header. RFC 4302, December, 2005

[10] Adoba, B., & Dixon, W. (2004). RFC 3715–IPSec-network address translation (NAT) compatibility requirements.

[11] Jankuniene, R., & Jankunaite, I. (2009, June). Route creation influence on DMVPN QoS. In Information Technology Interfaces, 2009. ITI'09. Proceedings of the ITI 2009 31st International Conference on (pp. 609-614). IEEE.

[12] Asati, R., Khalid, M., Retana, A. E., Van Savage, D., & Sethi, P. P. (2013). U.S. Patent No. 8,346,961. Washington, DC: U.S. Patent and Trademark Office.

[13] Chen, H. (2011, May). Design and implementation of secure enterprise network based on DMVPN. In Business Management and Electronic Information (BMEI), 2011 International Conference on (Vol. 1, pp. 506-511(pp. 1842-1845). IET.

[14] Savage, D., Slice, D., Ng, J., Moore, S., & White, R. (2013). Enhanced Interior Gateway Routing Protocol. Internet Engineering Task Force.

[15] Yang, Q. F., Shi, H. H., & Zhu, S. (2013). Analysis the Advantages and Packet Format of EIGRP. Applied Mechanics and Materials, 336, 2464-2467.

[16] Sullenberger, M. L., & Vilhuber, J. (2008). U.S. Patent No. 7,447,901. Washington, DC: U.S. PatentC: U.S. Patent and Trademark Office.

[17] Nguyen, L. H., Van Savage, D., Slice Jr, D. E., Van Tran, T., & Yang, Y. (2011). U.S. Patent No. 7,898,981. Washington, DC: U.S. Patent and Trademark Office.

[18] Cisco Systems, Dynamic Multipoint VPN (DMVPN) Design Guide (Version 1.1), 2008

[19] Berkowitz, Howard (1999), "OSPF Goodies for ISPs", North American Network Operators Group NANOG 17, Montreal

[20] Aggarwal, A., & Khera, S. (2012). Combat Resources Shortages by making Stub Areas and Route Summarization in OSPF. International Journal of Scientific and Research Publications, 2(8).

[21] Ayoub BAHNASSE and Najib EL KAMOUN, "Policy-Based Automation of Dynamique and Multipoint Virtual Private Network Simulation on OPNET Modeler" International Journal of Advanced Computer Science and Applications(IJACSA), 5(12), 2014. http://dx.doi.org/10.14569/IJACSA.2014.051201.

[22] Mishra, Vinita, and Smita Jangale. "Analysis and comparison of different network simulators." International Journal of Application or Innovation in Engineering & Management (2014)

[23] Schilling, Bjorn. "Qualitative comparison of network simulation tools." Institute of Parallel and Distributed Systems (IPVS), University of Stuttgart (2005).

[24] Lucio, Gilberto Flores, Marcos Paredes-Farrera, Emmanuel Jammeh, Martin Fleury, and Martin J. Reed. "Opnet modeler and ns-2: Comparing the accuracy of network simulators for packet-level analysis using a network testbed."WSEAS Transactions on Computers 2, no. 3 (2003): 700-707.

[25] BAHNASSE, A., & ELKAMOUN, N. (2015). Study and evaluation of the high availability of a Dynamic Multipoint Virtual Private Network. Revue MéDiterranéEnne Des TéLéCommunications, 5(2).

[26] Park, J. H., Oliveira, R., Amante, S., McPherson, D., & Zhang, L. (2012). BGP route reflection revisited. Communications Magazine, IEEE, 50(7), 70-75.